UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

The use of blockchain for collecting value-added tax on online cross-border trade in digital goods

by

RUDDY KAPASULA KABWE

Submitted in fulfilment of the requirements for the degree

DOCTOR OF LAWS

In the Faculty of Law,

University of Pretoria

30 June 2024

Supervisor: Professor SP van Zyl

UNIVERSITY OF PRETORIA

PLAGIARISM POLICY AGREEMENT

The University of Pretoria places great emphasis upon integrity and ethical conduct in the preparation of all written work submitted for academic evaluation.

While academic staff teaches you about referencing techniques and how to avoid plagiarism, you too have a responsibility in this regard. If you at any stage uncertain as to what is required, you should speak to your lecturer before any written work is submitted.

You are guilty of plagiarism if you copy something from another author's work (eg a book, an article or a website) without acknowledging the source and pass it off as your own. In effect you are stealing something that belongs to someone else. This is not only the case when you copy work word-for-word (verbatim), but also when you submit someone else's work in a slightly altered form (paraphrase) or use a line of argument without acknowledging it. You are not allowed to use work previously produced by another student. You are also not allowed to let anybody copy your work with the intention of passing it off as his/her work.

Students who commit plagiarism will not be given any credit for plagiarised work. The matter may also be referred to the Disciplinary Committee (Students) for a ruling. Plagiarism is regarded as a serious contravention of the University's rules and can lead to expulsion from the University.

The declaration which follows must accompany all written work submitted while you are a student at the University of Pretoria. No written work will be accepted unless the declaration has been completed and attached.

Full names of candidate: Ruddy Kapasula Kabwe

Student number: 18379045

Date: 30 June 2024

Declaration

I understand what plagiarism is and I am aware of the University's policy in this regard.

Signature of candidate: Ruddy Kapasula Kabwe

Signature of supervisor: ……………………………………….

UNIVERSITY OF PRETORIA

DECLARATION OF ORIGINALITY

Full names of student: **Ruddy Kapasula Kabwe**

Student number: **18379045**

Declaration

1. I understand what plagiarism is and I am aware of the University's policy in this regard.
2. I declare that this thesis is my own original work. Where other people's work has been used (either from a printed source, Internet, or any other source), this has been properly acknowledged and referenced in accordance with departmental requirements.
3. I have not used work previously produced by another student to any other person to hand in as my own.
4. I have not allowed and will not allow anyone to copy my work with the intention of passing it off as his or her own work.

Signature: Ruddy Kapasula Kabwe

ACKNOWLEDGEMENTS

I thank God for providing me with the patience and resolve to complete this study.

This journey would not be complete without the following people, and I extend my sincerest gratitude to:

- My parents, for always offering their unconditional support and encouragement throughout the duration of this thesis.
- My brothers and sister for always being available to assist me.
- My brother, Moses Kabwe for taking the time to proofread and edit this thesis. Thank you, brother.
- The University of Pretoria for giving me financial assistance to help me complete this thesis.
- My friend and colleague, Dr Princess Thembelihle Ncube for her advice and for her support during my studies.
- Prof Carika Keulder for her initial input and comments at the start of this thesis.
- My supervisor, Prof SP van Zyl. Thank you for always providing valuable input. Thank you for making time to read this thesis. Thank you for your patience. Thank you for the impact you have had on my career.
- Thank you to every person who contributed to this thesis in one way or the other.

ABSTRACT

The collection of value-added tax from the cross-border supply of digital goods remains a challenge for tax authorities around the world. South Africa is no different. The traditional methods of collecting VAT from the supply of digital goods relies on the honesty of the consumer and on the supplier to account for and remit VAT to the tax authorities in the jurisdiction where the goods are consumed. The traditional collection models are often unreliable, inefficient, burdensome, and expensive for the consumers and the suppliers. The adoption of blockchain technology as a model to collect VAT on the cross-border supply of digital goods has the potential to alleviate the compliance burden on consumers and suppliers of digital goods, improve the efficiency of tax administration, and reduce VAT fraud. Importantly, blockchain technology can create trust between tax authorities, suppliers of digital goods, and consumers.

This thesis critically discusses the advantages and disadvantages of implementing blockchain technology for the collection of VAT on the cross-border supply of digital goods in South Africa. This thesis unpacks the consideration factors for policymakers in the implementation of blockchain technology for the collection of VAT on cross-border trade in digital goods. The thesis makes recommendations for the South African VAT Act to be amended to make provision for the collection of VAT by utilising blockchain technology.

KEYWORDS

Architecture; anonymisation; bitcoin; blockchain technology; blockchain standards; consensus; cryptotaxcurrency; decentralisation; DICE; digital goods; digital invoice; e-commerce; electronic services; ENIGMA; Ethereum; foreign suppliers; hard fork; immutability; node; operator; oracle; participant; PbD; privacy; private blockchain; private key; processing; pseudonymisation; public blockchain; public key; public key infrastructure; registration mechanism; reverse-charge mechanism; SARS; scalability; sharing economy; smart contracts; soft fork; taxpayer; transparency; trust; TVACoin; VAT collection; VATCoin; VAT fraud; zero-knowledge proof.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

4IR	Fourth Industrial Revolution
AEOI	Automatic Exchange of Information
AI	Artificial intelligence
API	Application Programme Interface
Apps	Applications
AVCM	Automated VAT collection mechanism
B2B	Business to Business transaction
B2C	Business to Consumer transaction
C2A	Consumer to Administration transaction
C2B	Consumer to Business transaction
C2C	Consumer to Consumer transaction
CBDC	Central Bank Digital Currency
CCTV	Closed-circuit television
CNIL	*Commission Nationale de l'informatique et de Libértes*
CoE	Council of Europe
DAO	Decentralised Autonomous Organisation
dApps	Decentralised Applications
DLT	Distributed Ledger Technology
DTA	Double Tax Agreement
DPD	Data Protection Directive
ECHR	European Convention on Human Rights
EDP	Electronic Distribution Platform
EMV	Ethereum Virtual Machine
EOI	Exchange of Information
EP	European Parliament
EU	European Union
FATCA	Foreign Account Tax Compliant Act
FBI	Federal Bureau of Investigation

FLR	Full Liability Regime
GCC	Gulf Cooperation Council
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
HMRC	His Majesty's Revenue and Customs
ICT	Information communication technology
IEEE	Institute of Electrical and Electronics Engineers Standards
IEEE SA	Institute of Electrical and Electronics Engineers Standards Association
IP	Intellectual Property
IPR	Intellectual Property Rights
ISO	International Standards Organisation
IT	Information Technology
JSL	Joint and Several Liability
KYC	Know-your-customer
MITC	Missing Trading Intra-Community Fraud
MPC	Multi-Party Computation
MTF	Missing Trader Fraud
NSA	National Security Agency
OECD	Organisation for Economic Development and Co-operation
PAJA	Promotion of Administrative Justice Act
PAIA	Promotion of Access to Information Act
PbD	Privacy by Design
PC	Personal Computer
PET	Privacy enhancing technologies
PKI	Public Key Infrastructure
POPI	Protection of Personal Information Act
PwC	Price Waterhouse Coopers
SADC	Southern African Development Community
SARB	South African Reserve Bank
SARS	South African Revenue Service

SDOs	Standards Development Organisation
TAA	Tax Administration Act
UK	United Kingdom
USA	United States of America
USD	United States dollar
VAT	Value-Added Tax

LIST OF FIGURES

CHAPTER 1: INTRODUCTION

1.1 Background

The implementation of the Taxation Laws Amendment Act 43 of 2014[1] brought about significant changes to the Value Added Tax Act 89 of 1991 (the VAT Act) which, for the first time in South Africa, provided for the taxation of the online cross-border trade in digital goods.[2] Prior to this new dispensation, the VAT Act did not adequately cater for the taxation of cross-border supply of digital goods to South African consumers (private consumers). The gap in the VAT Act was perceived to be anti-competitive because local businesses supplying goods and services[3] to private consumers were susceptible to Value-Added Tax (VAT)[4] while foreign[5] supplies of intangible goods to private consumers were not subject to VAT. The contrast in the taxation of goods and services between local and foreign businesses resulted in a niche but polarised market. For example, a foreign supplier[6] like *Amazon* supplied digital goods to private consumers at a significantly lower price compared to similar digital or tangible goods sold by their brick-and-mortar counterparts in South Africa. It was difficult for local businesses to compete with their international counterparts partly because the local

[1] See *Government Gazette* No 38405 (20 January 2015).

[2] Section 1 of the VAT Act was amended to add paragraph (b)(vi) of the definition of 'enterprise'. Paragraph 1(b)(vi) reads: "the supply of electronic services by a person from a place in an export country, where at least two of the following circumstances are present: (aa) The recipient of those electronic services is a resident of the Republic; (bb) any payment to that person in respect of such electronic services originates from a bank registered or authorised in terms of the Banks Act, 1990 (Act No. 94 of 1990); (cc) the recipient of those electronic services has a business address, residential address or postal address in the Republic."

[3] The VAT Act currently does not specifically define the term 'digital goods.' Digitals goods are digital versions of tangible goods that can be delivered over the Internet. 'Digital goods' are defined as 'electronic services' for purposes of the VAT Act. Section 1 of the VAT Act defines 'electronic services' as those services prescribed by the Minister by regulation in terms of the VAT Act. The definition of 'electronic services' includes any services supplied by means of an electronic agent, electronic communication, or the Internet for any consideration. The definition specifically excludes educational services, telecommunications services and services supplied by an export country to a resident country.

[4] Ebrill *et al* explain VAT as follows: "Despite its name, VAT is not generally intended to be a tax on value added as such: rather it is usually intended as a tax on consumption. Its essence is that it is charged at all stages of production, but with the provision of some mechanism enabling firms to offset the tax they have paid on their own purchases of goods and services against the tax they charge on their sales of goods and services." See Ebrill, L. Keen, M. Bodin, J.P. Summers, V. (2001). *The Modern VAT* (International Monetary Fund, Washington DC) at 1.

[5] The businesses are 'foreign' because they originate from countries outside of South Africa.

[6] For purposes of this thesis, a 'foreign supplier' denotes a foreign online business capable of supplying digital goods or services to consumers on the Internet.

businesses' goods and services were perceived to be more expensive by private consumers. Interestingly, foreign suppliers also had an advantage because they used the Internet to conduct trade with private customers while their local counterparts did not have the same facilities. Private consumers realised that they could purchase the same goods sold by local businesses, but in digital format, on the Internet from foreign suppliers at a reduced price. The continuous trade of digital goods on the Internet led to the eventual growth of electronic commerce (e-commerce) in South Africa.

E-commerce[7] changed the traditional business model by making the Internet the forefront of business paradigm.[8] Previously, if a private consumer desired to buy a book or movie, they would have gone to a local store to purchase these goods. With e-commerce, it is possible to purchase the same movie or book in digital format at the comfort of one's home. To do this, the private consumer requires an Internet connection for download purposes and a personal computer (PC) or mobile phone. E-commerce has made it easier for private consumers to access an array of catalogue consisting of digital goods and services from around the world. At the focal point of e-commerce and e-commerce transactions[9] is the Internet.[10] The proliferation of Internet use, coupled with the growth of e-commerce, has led to globalisation. In this regard, Bardopoulos states:

> "The current escalation of globalisation which in turn has compounded taxation issues has been expedited by the development of the Internet. With the introduction of the Internet and the advent of eCommerce, the traditional concept of international trade and commerce can no longer be effectively applied to the new taxing complications

[7] The Organisation for Economic Development and Co-operation (OECD) defines 'e-commerce' as: "The sale or purchase of goods or services, whether between businesses, households, individuals, governments, and other public or private organisations, conducted over computer mediated networks." Available at https://www.oecd.org/sti/ieconomy/1835738.pdf. Accessed 10 December 2022.

[8] The ease at which digital goods and services are acquired on the Internet and the convenience of trading online has led to the exponential growth of e-commerce. When online companies report substantial record profits during fiscal year-end meetings or during investor conferences, the significance of e-commerce is made apparent especially when profits are a direct result of trading online. Thus, online companies understand the need for e-commerce and the importance it plays in attaining revenue.

[9] An e-commerce transaction involves at least two parties: the online business or retailer and a consumer.

[10] The *Oxford Advanced Learner's Dictionary* (2005) Oxford University Press at 781 defines the 'Internet' as: "an international computer network connecting other networks and computers from companies, universities."

> and issues manifested by technological amelioration. Unprecedented tax issues in respect of eCommerce transactions in the Internet may be classified as pertaining to the next generation taxing regime. The clumsy attempt to impose 'physical world' laws upon a 'virtual world' has generated multiple points at issue and has accentuated the impracticability of imposing 'physical world' laws on a 'virtual world'."[11]

Countries proceeded to tax e-commerce transactions to level the playing field between foreign suppliers and brick-and-mortar businesses. Each country implemented its own laws to tax e-commerce transactions. In doing so, various legal issues pertaining to the taxation of e-commerce became prevalent. Since the VAT laws and VAT design, as we know it, were implemented at a time when the concept of e-commerce was non-existent,[12] it became necessary for tax authorities to engage with policymakers and various stakeholders to determine if the VAT laws had sufficient provisions and mechanisms to adequately tax e-commerce transactions.

Once VAT has been imposed on a specific transaction, the next logical step is to administer the VAT. If a country decides to adopt a VAT system, a 'good' VAT administration does not necessarily come into existence automatically, for the simple reason that it takes time to develop a 'good' VAT administration system.[13] The salient aspects of a 'good' VAT administration include enforcement mechanisms, strict penalties for non-compliance, effective tax collection mechanism, well-defined tax laws, audits, facilities that encourage taxpayers to meet their tax obligations and a simple registration procedure that will enable filling, payment, and refund procedures.[14] No element is more important than the other, but altogether form the core of what makes VAT administration effective.

[11] Bardopoulos, M. A. (2012). *The impact of technology on taxation and is VAT the eTax solution?* PhD thesis University of Cape Town at 1 – 2.

[12] Gutuza, T. (2010). Tax and e-commerce: where is the source *South African Law Journal* 127(2): 329; See also Van Zyl, S. P. (2013). *The collection of Value Added Tax on online cross-border trade in Digital Goods*. Unpublished LLD thesis (UNISA) at 126.

[13] Bird, R. M. & Gendron, P. P. (2007). *The VAT in developing and transitional countries* (Cambridge University Press, New York) at 162.

[14] Ebrill, L. Keen, M. Bodin, J.P. Summers, V. (2001). *The Modern VAT* (International Monetary Fund, Washington DC) at 141; See also Bird, R. M. & Gendron, P. P. (2007). *The VAT in developing and transitional countries* (Cambridge University Press, New York) at 162.

E-commerce brings several complexities to VAT administration. First, the borderless nature of e-commerce makes it difficult for tax authorities to identify the foreign suppliers and the private consumer.[15] Identifying the parties to a transaction is fundamental for any tax system.[16] Without the identity of the parties to a transaction, administration of VAT is impossible. If the identities of the parties are not known to tax authorities, VAT liability cannot be established, rendering the application of VAT laws impracticable. Second, the location of foreign suppliers and private consumers can be difficult to establish.[17] The nexus between e-commerce transactions and the location of the supplier and consumer is important. If the foreign supplier cannot locate the jurisdiction of the private consumer, then that foreign supplier cannot remit the correct amount of tax to the relevant tax authority in the country of consumption. It is quite possible for private consumers to conceal their identity on the Internet.[18] Private consumers mask their identity to protect their privacy, but the concealment of one's

[15] Basu, S. (2007). *Global perspectives on e-commerce taxation law* (Routledge, UK) at 93; Kabwe, K., R. (2017). *Consumption tax collection models in online trade in digital goods* unpublished LLM mini-dissertation (UNISA) at 25; Basu, S. (2008). International taxation of e-commerce: persistent problems and possible developments *Journal of Information Law and Technology* at 7. Available at https://warwick.ac.uk/fac/soc/law/elj/jilt/2008_1/basu/basu.pdf. Accessed 17 March 2019; *Green paper on electronic commerce for South Africa* at 44. Available at https://www.gov.za/sites/default/files/gcis_document/201409/electroniccommerce1.pdf. Accessed 17 March 2019.

[16] *Green paper on electronic commerce for South Africa* at 44. Available at https://www.gov.za/sites/default/files/gcis_document/201409/electroniccommerce1.pdf. Accessed 17 March 2019.

[17] Basu, S. (2007). *Global perspectives on e-commerce taxation law* (Routledge, UK) at 93; Kabwe, K., R. (2017). *Consumption tax collection models in online trade in digital goods* unpublished LLM mini-dissertation (UNISA) at 25; Basu, S. (2008). International taxation of e-commerce: persistent problems and possible developments *Journal of Information Law and Technology* at 7. Available at https://warwick.ac.uk/fac/soc/law/elj/jilt/2008_1/basu/basu.pdf. Accessed 17 March 2019. *Green paper on electronic commerce for South Africa* at 40. Available at https://www.gov.za/sites/default/files/gcis_document/201409/electroniccommerce1.pdf. Accessed 17 March 2019.

[18] Ligthart, J. E. (2004). Consumption Taxation in a Digital World: A Primer Tilburg University & University of Groningen at 7. Kabwe, K. R. (2017). *Consumption tax collection models in online trade in digital goods* unpublished LLM mini-dissertation (UNISA) at 61. Van Zyl, S. P. (2013). *The collection of Value Added Tax on online cross-border trade in Digital Goods*. Unpublished LLD thesis (UNISA) at 196. Basu, S. (2008). International taxation of e-commerce: persistent problems and possible developments *Journal of Information Law and Technology* at 20. Basu, S. (2004). To tax or not to tax? That is the question? Overview of options in consumption taxation of e-commerce *The Journal of Information, Law and Technology* at 3. Available at https://www.researchgate.net/profile/Subhajit_Basu5/publication/313793368_To_Tax_or_Not_to_Tax_That_is_the_question_Overview_of_Options_in_Consumption_Taxation_of_E-_Commerce/links/58a5f11faca27206d995b90b/To-Tax-or-Not-to-Tax-That-is-the-question-Overview-of-Options-in-Consumption-Taxation-of-E-Commerce.pdf. Accessed 9 April 2019.

identity on the Internet could point towards one's reluctance to pay taxes.[19] The wilful masking of one's online identity is a cause for concern for tax authorities not only because it has far-reaching consequences for the administration of VAT but it can also be construed as tax evasion. This challenge is compounded where VAT laws are poorly drafted in so far as they purport to place an unnecessary compliance burden on foreign suppliers to identify the private consumer.[20]

E-commerce is intrinsically paperless. This is problematic for tax authorities because there is no paper trail that can link a foreign supplier to a private consumer. Online transactions occur in a virtual world where tax authorities have no access to the information that is exchanged between private consumers and foreign suppliers. Tax authorities cannot perform an audit function on these transactions. In South Africa, it is a requirement for a vendor or foreign supplier to keep the records of all transactions for a period of five years.[21] Tax authorities cannot enforce this requirement if the foreign suppliers cannot be located or identified in the tax jurisdiction; more pertinently, enforcement is not possible if the identity of the foreign supplier cannot be established.

One of the most fundamental challenges posed by the taxation of e-commerce transactions is the effective collection of VAT.[22] Although e-commerce has various components,[23] Business to Consumer (B2C) e-commerce transactions pose the

[19] Ligthart, J. E. (2004). Consumption Taxation in a Digital World: A Primer Tilburg University & University of Groningen at 7. Van Zyl, S. P. (2013). *The collection of Value Added Tax on online cross-border trade in Digital Goods*. Unpublished LLD thesis (UNISA) at 196. Basu, S. (2004). To tax or not to tax? That is the question? Overview of options in consumption taxation of e-commerce *The Journal of Information, Law and Technology* at 3. https://www.researchgate.net/profile/Subhajit_Basu5/publication/313793368_To_Tax_or_Not_to_Tax_That_is_the_question_Overview_of_Options_in_Consumption_Taxation_of_E-_Commerce/links/58a5f11faca27206d995b90b/To-Tax-or-Not-to-Tax-That-is-the-question-Overview-of-Options-in-Consumption-Taxation-of-E-Commerce.pdf. Accessed 9 April 2019. See Basu, S. (2008). International taxation of e-commerce: persistent problems and possible developments *Journal of Information Law and Technology* at 20.

[20] Kabwe, K. R. (2017). *Consumption tax collection models in online trade in digital goods* unpublished LLM mini-dissertation (UNISA) at 96; See also Part (vi) (aa) – (cc) of the definition of 'enterprise' in the VAT Act.

[21] Section 29 of the Tax Administration Act 28 of 2011.

[22] *Green paper on electronic commerce for South Africa* at 45. Available at https://www.gov.za/sites/default/files/gcis_document/201409/electroniccommerce1.pdf. Accessed 17 March 2019.

[23] E-commerce can be classified into various groups. Business to Consumer (B2C), Business to Business (B2B), Business to Administration (B2A), Consumer to Business (C2B), Consumer to Consumer (C2C) and Consumer to Administration (C2A).

greatest challenge to tax authorities.[24] Businesses, and business to business (B2B) e-commerce transactions in particular, are more likely to conform to a country's VAT laws since tax administrators have a stronger fiscal hold over businesses[25] as compared to private consumers.[26] It is also worth noting that it is much simpler for tax authorities to keep track of a business that is geographically located in its tax jurisdiction.[27] Moreover, it is a statutory requirement for businesses to be registered in their respective tax jurisdiction.[28] When a business supplies goods and services to another business, the recipient business has to account for VAT in the jurisdiction where the goods and services are consumed. This VAT collection mechanism, referred to as the reverse-charge or self-assessment mechanism,[29] is conducive for B2B transactions because the recipient business is registered in the country of consumption which enables the tax authorities in that country to verify and audit the recipient business.[30] B2B transactions encourage the registration of businesses in the country of consumption, which also promotes tax compliance. Administering VAT under B2B transactions also allows for greater compliance control due to the availability of identification information to tax authorities as prescribed by tax laws.[31]

The same cannot be said for B2C transactions. In B2C, the foreign supplier does not necessarily have a physical presence in the country of consumption. Consequently, it is difficult for tax authorities to enforce control and compliance measures on an entity that exists in the virtual world. The seemingly lack of enforcement measures raises

[24] Van der Merwe, B. A. (2003). VAT and e-commerce *South African Mercantile Law Journal* 15(3): 373.

[25] The reason for this is because it is much easier for countries to identify business entities and to enforce penalties on them in the event of non-compliance with VAT laws.

[26] Van der Merwe, B. A. (2003). VAT and e-commerce *South African Mercantile Law Journal* 15(3): 373; See also Steyn, T. (2010). VAT and e-commerce: still looking for answers? *South African Mercantile Law Journal* 22(2): 234.

[27] *Green paper on electronic commerce for South Africa* at 44. Available at https://www.gov.za/sites/default/files/gcis_document/201409/electroniccommerce1.pdf. Accessed 17 March 2019.

[28] For example, see section 14 of the Companies Act 71 of 2008 and section 22 of the Tax Administration Act; See also *Green paper on electronic commerce for South Africa* at 44. Available at https://www.gov.za/sites/default/files/gcis_document/201409/electroniccommerce1.pdf. Accessed 17 March 2019.

[29] See discussion at paragraph 3.4.9 below.

[30] Steyn, T. (2010). VAT and e-commerce: still looking for answers? *South African Mercantile Law Journal* 22(2): 234.

[31] Steyn, T. (2010). VAT and e-commerce: still looking for answers? *South African Mercantile Law Journal* 22(2): 234.

several interjurisdictional issues. For this reason, it becomes important for VAT laws to have specific rules that create a nexus for the country of consumption to apply and enforce its laws on the subject matter of tax.[32] These rules are known as *place of supply* rules. It follows that if a country's laws do not contain specific *place of supply* rules, it puts a further strain on the *fiscus* and VAT collection.

If a foreign supplier provides cross-border tangible goods to a private consumer, those goods should be relatively simple to track since the goods go through customs at the airport before delivery is effected by courier companies or by the national post office.[33] However, it becomes problematic when a foreign supplier provides digital goods to a private consumer. By their nature, digital goods are intangible and cannot be traced by customs or by tax authorities.[34] In South Africa, the onus rests on the private consumer to account for, collect, and remit the necessary VAT upon receipt of the digital goods, to the South African Revenue Service (SARS).[35] Compliance can only take place if the private consumer is aware of their liability to pay VAT to SARS. If the consumer is not aware of their tax liability, then the amount due to the *fiscus* goes uncollected.

Furthermore, it remains impractical for SARS to enforce the reverse-charge collection mechanism because the *fiscus* does not have appropriate infrastructure in place to identify the recipient of digital goods.[36] Enforcement can only take place if the identity of the consumer is known to SARS. Without the necessary infrastructure at its disposal, SARS cannot identify the private consumer which then leads to revenue loss. It appears that since e-commerce transactions yield trifling amounts of VAT, one would not expect SARS to allocate all its resources to collect these amounts simply because

[32] Millar, R. (2008) Jurisdictional Reach of VAT *University of Sydney Law School*: Legal research paper 8(64): 175. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1162510. Accessed on 2 April 2017.

[33] Van der Merwe, B. A. (2003). VAT and e-commerce *South African Mercantile Law Journal* 15(3): 373; Steyn, T. (2010). VAT and e-commerce: still looking for answers? *South African Mercantile Law Journal* 22(2): 233.

[34] This challenge is not limited to South Africa. The OECD has highlighted that it is a global issue. See OECD OECD/WBG/ATAF (2023). *VAT Digital Toolkit for Africa* OECD Paris. Available at https://www.oecd.org/tax/consumption/vat-digital-toolkit-for-africa.pdf Accessed 12 August 2023.

[35] Section 14(1)(a) and (b) of the VAT Act. This is another example of the reverse-charge mechanism.

[36] Kabwe, K. R. (2017). *Consumption tax collection models in online trade in digital goods* unpublished LLM mini-dissertation (UNISA) at 39 – 40.

it is not economically viable to do so. For these reasons, it has been submitted that the reverse-charge mechanism is not an appropriate mechanism for the collection of VAT on B2C e-commerce transactions.[37]

If a foreign supplier is a VAT vendor,[38] then the supplier is obligated to register and account for VAT in South Africa by means of the registration mechanism. Once the threshold has been met and the foreign supplier carries on an enterprise in South Africa,[39] the supplier is required to register as vendor on the SARS website and thereafter complete the necessary form together with accompanying documents before sending this information back to SARS via electronic mail (e-mail).[40] Essentially, the registration mechanism requires the foreign supplier to establish the identity or identities of consumers in order for the supplier to register in the country of consumption. Establishing the identity of the consumer is imperative for foreign suppliers because it determines the jurisdiction where the foreign supplier will register and account for VAT.[41] If the foreign supplier cannot identify the consumer, then it cannot register in the country of consumption leading to revenue loss for the *fiscus*. Due to the nature of e-commerce, foreign suppliers have multiple consumers in multiple jurisdictions. Utilising the registration mechanism would then necessitate registering in every jurisdiction where the supplier has consumers. The requirement to

[37] Kabwe, K. R. (2017). *Consumption tax collection models in online trade in digital goods* unpublished LLM mini-dissertation (UNISA) at 39 – 40; Lamensch, M. (2012). Are reverse charging and the one-stop-scheme efficient ways to collect VAT on digital supplies? *World Journal of VAT/GST Law* 1(1): 3; Coetzee, L. & Meiring, M. (2016). Value-Added Tax on imported electronic services: A critical evaluation of the newly enacted South African legislation *Journal of Economic and Financial Sciences* 9(1): 31; Van Zyl, S. P. (2013). *The collection of Value Added Tax on online cross-border trade in Digital Goods*. Unpublished LLD thesis (UNISA) at 356; Davis Tax Committee (2014). *Addressing Base Erosion and profit shifting in South Africa: Davis Tax Committee interim report* at 53. Available at http://www.taxcom.org.za/docs/New_Folder/2%20DTC%20BEPS%20Interim%20Report%20on%20Action%20Plan%201%20-%20Digital%20Economy,%202014%20deliverable.pdf. Accessed 18 March 2019.

[38] Section 1 of the VAT Act defines a 'vendor' as: "any person who is or is required to be registered under this Act." Section 23(1A) of the VAT Act states that a foreign supplier must register as a vendor if they carry on an enterprise in South Africa and the taxable supplies exceed R1 million in any consecutive 12-month period. A foreign supplier is deemed to have an enterprise in South Africa if the latter supplies electronic services (digital goods) to a private consumer who is a resident of South Africa; if the payment originates form a bank in South Africa or if the recipient of the digital goods has a business, residential or postal address in South Africa.

[39] Section 23(1A) read with the definition of 'enterprise' of the VAT Act.

[40] Kabwe, K., R. (2017). *Consumption tax collection models in online trade in digital goods* unpublished LLM mini-dissertation at UNISA at 35.

[41] Kabwe, K., R. (2017). *Consumption tax collection models in online trade in digital goods* unpublished LLM mini-dissertation at UNISA at 56.

register in every jurisdiction adds further strain on foreign suppliers because it requires them to expend resources and capital on the identification of consumers and on compliance with different VAT laws.

Although the Organisation for the Economic Development and Co-operation (OECD) prefers a simplified version of the registration mechanism for the collection of VAT on B2C transactions,[42] it is my view that the registration mechanism is not an effective mechanism for the collection of VAT on B2C transactions. It is also my view that the registration mechanism and the reverse-charge mechanism do not provide long term solutions for the collection of VAT on the cross-border supply of digital goods enabled by the exponential growth of e-commerce. In a world where freedom of trade is propagated, foreign suppliers struggle to trade in jurisdictions where there is a heavy burden on them to collect and remit taxes to tax authorities. This compliance burden emanates from strict tax laws, often in languages that foreign suppliers do not even understand. In such instances, foreign suppliers are compelled to cease trading in jurisdictions where the compliance costs outweigh the costs of doing business. In some instances, foreign suppliers may decide to make use of Electronic Distribution Platforms (EDPs),[43] to shift the liability to pay tax. The shift in tax liability could lead to further revenue losses for the country of consumption especially in instances where VAT legislation in that country does not specifically provide for the supply of digital goods by EDPs. This is emphasised by Basu who states that “businesses never really like to spend money on tax compliance.”[44]

[42] OECD (2017). *International VAT/GST Guidelines* at 71. Available at https://www.oecd-ilibrary.org/docserver/9789264271401-en.pdf?expires=1553858743&id=id&accname=guest&checksum=548681052C34CEC274E3A3887BFCB279. Accessed 29 March 2019. See also OECD (2017). *Mechanisms for the effective collection of VAT/GST* at 22. https://www.oecd.org/tax/tax-policy/mechanisms-for-the-effective-collection-of-VAT-GST.pdf. Accessed 29 March 2019.

[43] The Australian Tax and Superannuation Laws Amendment (2016 Measures No 1) Act 2016 (52 of 2016) inserted the following definition of an ‘EDP’ in section (subdivision) 84 – 70 of *A New Tax System (Goods and Services Tax)* Act 1999: “(1) A service (including a website, internet portal, gateway, store or marketplace) is an electronic distribution platform if: (a) the service allows entities to make supplies available to end-users; and (b) the service is delivered by means of electronic communication; and (c) the supplies are to be made by means of electronic communication. (2) However, a service is not an electronic distribution platform solely because it is: (a) a carriage service (within the meaning of the Telecommunications Act 1997); or (b) a service consisting of one or more of the following: (i) providing access to a payment system; (ii) processing payments; (iii) providing vouchers the supply which are not taxable supplies because of section 100-5.”

[44] Basu, S. (2007). *Global perspectives on e-commerce taxation law* (Routledge, UK) at 309.

It stands to reason that alternative mechanisms should be implemented for the collection of VAT on the cross-border online trade in digital goods. In the 2019 Budget Speech,[45] the then South African Minister of Finance[46] stated that SARS was in the process of strengthening its information technology (IT) and IT systems that would be crucial for tax collection.[47] This statement by the Minister of Finance highlights the call for tax authorities to explore and use IT systems and technological solutions for the collection and the administration of VAT, particularly on the cross-border online trade in digital goods.

In September 2023, SARS released a discussion paper on VAT modernisation.[48] The aim of the discussion paper is to modernise the VAT administrative framework and to implement real-time transmission of VAT data from vendors to tax authorities using secure channels.[49] To achieve this, SARS plans to modernise the digital transmission of VAT data in phases. VAT vendors, including large businesses and international vendors, will be required to digitally transmit VAT data to SARS.[50] SARS aims to run education awareness campaigns to provide information to vendors so that they can understand what is expected of them. This will also enable them to comply with the new VAT laws. To encourage compliance, vendors may deduct the initial costs of transitioning to the new system for income tax and VAT purposes.[51] To deter non-compliance, penalties will be imposed on vendors that do not comply with the new

[45] Available at http://www.treasury.gov.za/documents/national%20budget/2019/speech/speech.pdf. Accessed 2 March 2019.

[46] At the time, the Minister of Finance was Mr. Tito Titus Mboweni.

[47] Mboweni, T. T. (2019). 2019 *Budget Speech* at 7. Available at http://www.treasury.gov.za/documents/national%20budget/2019/speech/speech.pdf. Accessed 2 March 2019.

[48] SARS (2023). *Discussion Paper: Value-Added Tax Modernisation*. Available at https://www.sars.gov.za/wp-content/uploads/Docs/VAT/Discussion-Paper-on-Value-Added-Tax-Modernisation.pdf. Accessed 4 October 2023.

[49] SARS (2023). *Discussion Paper: Value-Added Tax Modernisation* at 1 – 3. Available at https://www.sars.gov.za/wp-content/uploads/Docs/VAT/Discussion-Paper-on-Value-Added-Tax-Modernisation.pdf. Accessed 4 October 2023.

[50] SARS (2023). *Discussion Paper: Value-Added Tax Modernisation* at 4. Available at https://www.sars.gov.za/wp-content/uploads/Docs/VAT/Discussion-Paper-on-Value-Added-Tax-Modernisation.pdf. Accessed 4 October 2023.

[51] SARS (2023). *Discussion Paper: Value-Added Tax Modernisation* 4 – 5. Available at https://www.sars.gov.za/wp-content/uploads/Docs/VAT/Discussion-Paper-on-Value-Added-Tax-Modernisation.pdf. Accessed 4 October 2023.

rules.[52] This is an important development in South Africa as it highlights the need to use modern technology such as blockchain to transmit tax data to authorities in real-time.

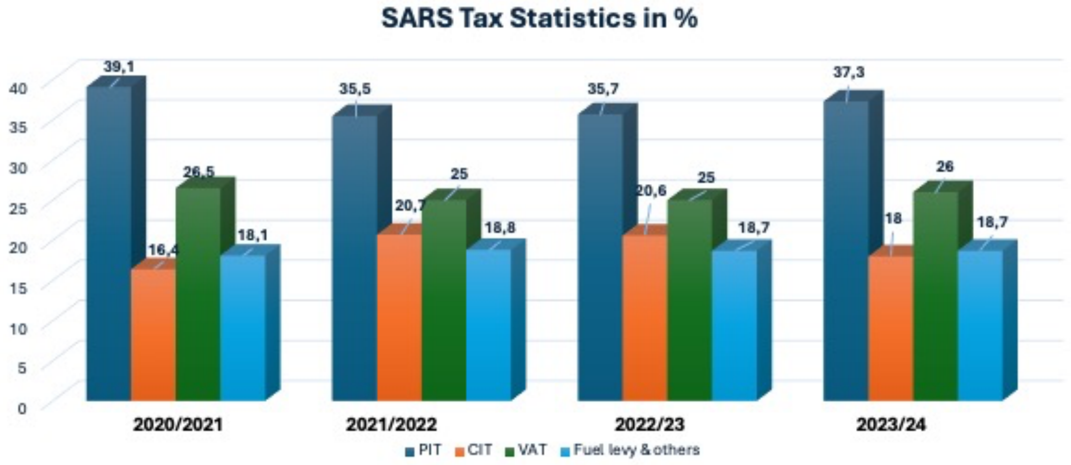


Figure 1[53]

Figure 1 above shows that VAT is a significant source of revenue for in South Africa. It is common cause that countries need revenue to fund public expenditure. If the tax base shrinks because of a failing VAT collection mechanism, countries do not obtain the revenue to provide for socio-economic projects like education, healthcare, or to maintain infrastructure. Accordingly, protecting the tax base is fundamental to government's role in promoting socio-economic rights.

[52] SARS (2023). *Discussion Paper: Value-Added Tax Modernisation* at 7. Available at https://www.sars.gov.za/wp-content/uploads/Docs/VAT/Discussion-Paper-on-Value-Added-Tax-Modernisation.pdf. Accessed 4 October 2023.

[53] **Figure 1** reveals the tax revenue composition sources in South Africa from 2020/2021 to 2023/2024. **Figure 1** is extracted from the 2023 SARS statistics at page 11 and the 2023/24 tax collection figures. The 2023 SARS statistics is available at https://www.sars.gov.za/wp-content/uploads/2023-Tax-Statistics-Main-Publication-compressed.pdf. Accessed 7 June 2024.

One of the fundamental prospects of applying technology in VAT administration is the reduction of time spent on VAT collection and a significant reduction in compliance costs for online businesses.[54] Although technology is not rigid and has the propensity to evolve in unparalleled ways, Bardopoulos correctly states that the implementation of a technological solution for the collection of VAT should be conducive for the development of future technology.[55]

For technology to be used as an effective tool to administer VAT, international co-operation at the highest level will be required. Gjems-Onstand states that it is not necessary for countries to share precise online sale figures relating to e-commerce transactions but rather, countries should look at exchanging information like revenue statistics.[56] One factor that impedes co-operation at international level is political will, or the lack thereof. Currently, only a handful of countries impose taxes on cross-border e-commerce transactions.[57] A country's right to impose taxes is based on the principle of sovereignty and territorial integrity. Thus, every sovereign country exercises this right. Basu states the following:

> "The application of state law requires that a territorial connection can be made between the legal question and this physical or conceptual state place."[58]

Countries must implement international guidelines and legal frameworks that can assist tax authorities to maximise the use of technology to collect VAT. Without

[54] PWC (2017). *VAT compliance: the impact on business and how technology can help* at 22. Available at https://www.pwc-tls.it/it/assets/docs/pwc-vat-compliance-paying-taxes-2017.pdf. Accessed 17 November 2017.

[55] Bardopoulos, A., M., (2015). *eCommerce and the effects of technology on taxation: could VAT be the eTax solution?* Springer International Publishing Switzerland at 277.

[56] Gjems-Onstad, O. (2013). Cross-border electronic services and the need for international cooperation: the Norwegian experience *World Journal of VAT/GST Law* 2(3): 251.

[57] According to the website https://quaderno.io/blog/digital-taxes-around-world-know-new-tax-rules/,the following countries impose taxes on e-commerce transactions (colloquially referred to as 'digital tax'): Albania, Australia, Belarus, the European Union, Iceland, Japan, India, New Zealand, Norway, Russia, Saudi Arabia, Serbia, South Africa, South Korea, Switzerland, Taiwan, Turkey, United Arab Emirates (UAE). According to the same website, the following countries are considering imposing taxes on e-commerce transactions: Bahrain, Bangladesh, Canada, China, Israel, Kuwait, Malaysia, Oman, Qatar, Singapore, and Thailand. Accessed 19 March 2018. KPMG compiled a report in 2017 entitled *VAT/GST treatment of cross-border services*. Available at https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2017/11/ess-survey-13-nov-17.pdf. Accessed 19 March 2018. According to the KPMG report Egypt, Ghana, Kenya, Liechtenstein, Tanzania, the United Kingdom (UK) impose taxes on cross-border e-commerce transactions.

[58] Basu, S. (2007). *Global perspectives on e-commerce taxation law* (Routledge, UK) at 98.

international cooperation, it will be challenging for countries to maximise the use of technology for the collection of VAT.

I believe that blockchain technology should be used to collect VAT on the cross-border online trade in digital goods.[59] The onus rests on tax authorities to ensure that there is a legal framework in place for the collection and administration of VAT on the cross-border online trade in digital goods.

This thesis explores the use of blockchain technology for the purposes of collecting VAT on the cross-border online trade in digital goods. This study also explores how blockchain technology can be used effectively to administer VAT.

1.2 Objective of study and research questions

The aim of this thesis is to explore the nature and mechanics of blockchain to enable tax authorities to use blockchain for the collection of VAT on the cross-border trade in digital goods. In doing so, this thesis critically examines the positive and the negative aspects of using blockchain for the collection of VAT on the cross-border trade in digital goods. In this thesis, reference is made to business entities, brands, trademarks, or well-known goods or services. These references are for illustrative purposes only unless indicated otherwise.

To achieve this objective, the following questions are asked:

i) What are the interjurisdictional aspects, if any, that must be considered when implementing blockchain for the collection of VAT on cross-border trade in digital goods?

[59] In this regard, see the views by the following authors who argue for the use of technology in the administration of taxes: Kabwe, K., R. (2017). *Consumption tax collection models in online trade in digital goods* unpublished LLM mini-dissertation at UNISA at 100; Basu, S. (2007). *Global perspectives on e-commerce taxation law* (Routledge, UK) at 308; See also Bird, M., R., and Zolt M., E. (2008). Technology and taxation in developing countries: from hand to mouse *National Tax Journal* 61(4): 791 – 821; Cockfield, J., A (2002). The law and Economics of digital taxation: challenges to traditional tax laws and principles *Bulletin for international fiscal Documentation* Vol 56(12): 619.

ii) What are the advantages and disadvantages of using blockchain to collect and administer VAT?

iii) How and to what extent can blockchain be used to collect VAT on cross-border trade in digital goods?

iv) What are the legal considerations, if any, that must be considered as a result of implementing blockchain for VAT collection?

v) What enforcement measures can SARS have after implementing blockchain for VAT administration?

1.3 Research methodology

This thesis uses a qualitative research methodology, by collecting and analysing data from a wide range of academic legal sources and other material. A significant part of this thesis relies on published and statistical data with specific reference to textbooks, journals, legislation, statistical reports, case law, and Internet sources. Blockchain is a relatively new concept and as such, all reasonable steps have been taken to ensure that relevant and updated sources have been used and referenced accordingly. To my knowledge, and at the time of finalising this thesis, no country has adopted blockchain technology in its entirety for the collection of VAT for the cross-border supply of digital goods.[60] Since blockchain technology changes rapidly, newer sources and opposing views may have been published since the publication of this thesis.

In the main, the thesis looks at the use of blockchain to collect VAT on the cross-border supply of digital goods from the perspective of a tax authority. This is because the collection of VAT is a function of SARS. There are instances where the discussion shifts to the collection of VAT from the perspective of the supplier of digital goods. The change is necessary to highlight the benefits of using blockchain for VAT collection from a supplier's perspective. Moreover, where the application of blockchain for VAT

[60] It should be mentioned that some countries are testing blockchain technology unofficially.

collection is discussed from a consumer's perspective, it is for completion because it emphasises the socio-economic challenges that all parties can encounter.

1.4 Limitations of thesis

From the outset, it must be noted that this thesis does not seek to reinvent the wheel in so far as the various VAT collection mechanisms are concerned. Thus, an in-depth discussion of all the VAT collection mechanisms is not considered in this study because such an extensive discussion has been done already.[61]

The study discusses blockchain and all its facets from a legal perspective only. A technical or scientific analysis of the operation and application of blockchain falls outside the scope of this study. This thesis does not discuss blockchain elements from a computer science perspective. Therefore, a detailed technical discussion regarding cryptography, application programming interface, digital signatures (including the types of digital signatures), or blockchain mathematics falls outside the scope of this study. Rather, the discussion of blockchain technology in this thesis is intended to be holistic in nature to provide an abridged overview of the technology for purposes of reviewing the consideration factors for policymakers in implementing blockchain as a VAT collection tool. Moreover, it is not the aim of this thesis to focus on the development and testing of blockchain and related software systems on the collection of VAT on the cross-border supply of digital goods. Since the technology has not been tested in an African context, I neither advocate for nor against the application of blockchain technology as a VAT collection tool in South Africa.

[61] Van Zyl, S. P. (2013). *The collection of Value Added Tax on online cross-border trade in Digital Goods*. Unpublished LLD thesis (UNISA) at 205 – 228, 280 – 300; Kabwe, K., R. (2017). *Consumption tax collection models in online trade in digital goods* unpublished LLM mini-dissertation (UNISA) at 47 – 57; Lubbe, H. (2015). *Alternatives to the enforceability of VAT on imported digital purchases in South Africa*. Unpublished LLM mini dissertation (North-West University of South Africa) at 49 – 59; OECD (2005). *Facilitating collection of consumption taxes on business-to-consumer cross-border e-commerce transactions* at 7. Available at http://www.oecd.org/tax/consumption/34422641.pdf. Accessed on 10 June 2017. OECD (2000); *Report by the Technology Technical Advisory Group* at 51 - 66. Available at http://www.oecd.org/tax/consumption/1923248.pdf . Accessed on 8 March 2017.

A comprehensive study involving the application of blockchain on B2B e-commerce transactions[62] is not conducted. This study focuses on the application of blockchain for VAT collection purposes on B2C transactions only. However, in some instances, there are VAT collection challenges that occur in B2C and B2B transactions. For this reason, this thesis discusses B2B transactions in limited cases.

Although certain cryptocurrencies are issued on blockchain, this study does not go into an in-depth discussion of the application and use of the various cryptocurrencies. This study does not consider whether it is viable to tax cryptocurrencies because such a study has already been done.[63] This thesis discusses bitcoin transactions in limited cases to show how blockchain transactions operate.

A discussion on the possible effects or implications of using blockchain technology on corporate and individual income tax falls outside the scope of this study. This study does not provide a detailed discussion on how blockchain can be used to exchange tax information with other jurisdictions. It is not the purpose of this study to discuss how blockchain can improve the *place of supply* rules. A comprehensive discussion on the use of central bank digital currencies and artificial intelligence in the administration of taxes falls outside the scope of this study.

An in-depth discussion of the banking crisis is excluded from the study. Thus, a historical examination of the origins and development of the banking crisis falls outside the scope of this study. However, to set the scene for the development of cryptocurrency, a brief analysis of the 2008 financial crisis is included.

[62] The VAT Act does not specifically distinguish between B2C and B2B e-commerce transactions. However, there are instances where the VAT differentiates between B2B and B2C transactions. A foreign supplier of electronic services must register as a VAT vendor in South Africa if the taxable supplies exceed R1 million. In B2B setting, the recipient of the imported services is required to remit VAT to SARS in terms of the reverse-charge mechanism. This is because the supply of advertising services and computer programmes were excluded from the definition of 'electronic services' in the VAT Act Regulations. There was a perception that these services were consumed in B2B market. Kabwe and van Zyl argue that B2B and B2C transactions should not be treated differently. See Kabwe, R. & van Zyl, S.P. (2021). "The value-added tax in the digital economy: a fresh look at the South African dispensation" *Obiter* 42(3): 499 – 528.

[63] Bal, M., A. (2014). *Taxation of virtual currency* PhD thesis University of Leiden at https://openaccess.leidenuniv.nl/bitstream/handle/1887/29963/000-5-Bal-14-10-2014.pdf. Accessed 19 March 2019.

The statistics that depict the precise amount of revenue collected on e-commerce transactions and foregone as a result of e-commerce transactions not taxed constitute SARS confidential information. Accordingly, this thesis does not proffer an analysis of VAT foregone as a result of weak or inappropriate VAT collection models. Similarly, the thesis does not make revenue collection forecasts where blockchain technology is applied as a VAT collection tool.

Blockchain technology is constantly evolving. As such, since the publication of this thesis, newer publications or dissenting views may have been published. Lastly, this thesis does not constitute a blueprint for the implementation of blockchain technology as a VAT collection tool.

1.5 Exposition of thesis

This study is structured as follows:

Chapter 1: Introduction

This is the introductory chapter to the thesis. It sets out the background to this thesis and the research questions. This chapter also highlights why this thesis was undertaken and the significance it can have on e-commerce and tax law.

Chapter 2: What is blockchain?

Chapter 2 looks at the origins of blockchain. It also discusses the uses and components of blockchain technology.

Chapter 3: The collection of value-added tax on blockchain

This chapter discusses the various ways in which VAT can be collected on blockchain. The chapter also discusses the benefits and risks of adopting blockchain for the administration of VAT.

Chapter 4: Privacy and blockchain

This chapter critically analyses the privacy concerns associated with the use of blockchain technology.

Chapter 5: The protection of personal information on blockchain – The EU

This chapter discusses the relevant provisions of the European Union's ('EU') General Data Protection Regulation ('GDPR') that pertains to the processing of personal data on blockchain.

Chapter 6: The protection of personal information on blockchain – South Africa

Chapter 6 discusses how the relevant provisions of the Protection of Personal Information Act ('the POPI Act') affect the processing of personal information on blockchain from a South African perspective.

Chapter 7: Recommendations and conclusion

Conclusions are drawn from the findings of this study. Recommendations are then tabled to enable SARS and National Treasury to implement legislative framework and policy to facilitate blockchain for the cross-border supply of digital goods.

1.6 Conceptualisation

For purposes of this study, the following concepts are used and described below.

'API' – this is interface that enables a user or supplier to access data.

'B2B' (business-to-business) – the online cross-border supply of goods or services from one business to another.[64]

[64] See Van der Merwe, B. A. (2003). VAT and e-commerce *South African Mercantile Law Journal* 15(3): 373.

'B2C' (business-to-consumer) – the online cross-border supply of services or digital goods from business to consumer.[65]

'Consensus mechanism' – this is a system of validating transactions on a blockchain.

'Digital platform' – this is an e-commerce marketplace that provides goods or services to consumers.

'Fiat money' – this is money or legal tender that is issued by the government of a country.

'Hard fork' – this is a change to the blockchain software which is not backwards compatible with older versions of the blockchain software.[66]

'ICT' – or information and communications technology, is a combination of manufacturing and services industries that capture, transmit and display data and information electronically.[67]

'K-anonymity' – is a data anonymisation technique that is used to protect individual's privacy in a dataset.[68]

'Place of supply' – these are rules that determine whether a specific transaction can be taxed in a country.[69]

[65] See Van der Merwe, B. A. (2003). VAT and e-commerce *South African Mercantile Law Journal* 15(3): 373.

[66] Van der Laan, J., *Understanding Blockchain* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 40.

[67] OECD, (2002). *Measuring the Information Economy* OECD Publishing Paris at 81. Available at https://www.oecd.org/digital/ieconomy/1835738.pdf. Accessed 3 June 2023.

[68] Trotino, G. (2024). *What is k anonymity and why data pros care*. Available at https://www.k2view.com/blog/what-is-k-anonymity. Accessed 6 June 2024.

[69] Millar, R. (2008) Jurisdictional Reach of VAT *University of Sydney Law School*: Legal research paper 8(64): 175. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1162510. Accessed on 2 April 2017.

'Private blockchain' – this is a type of blockchain that allows a set of identified participants to participate in the network.[70]

'Public blockchain' – this is a type of blockchain that allows anyone to participate in the network without providing identification.[71]

'Soft fork' – this is a change to blockchain software which is backwards compatible with older versions of blockchain software.[72]

'Technique' – the way of doing an activity that needs skill.[73]

'Technology' – the practical industrial use of scientific discoveries.[74]

'Turing complete' – for purposes of this thesis, Turing complete refers to a system that can simulate any computational task.[75]

'Validator' – a person or entity that is responsible for verifying transactions on blockchain.[76]

[70] Van der Laan, J., *Understanding Blockchain* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 56.

[71] Van der Laan, J., *Understanding Blockchain* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 56.

[72] Van der Laan, J., *Understanding Blockchain* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 40.

[73] Cambridge Online Dictionary https://dictionary.cambridge.org/dictionary/english/technique. Accessed 2 October 2023.

[74] Cambridge Online Dictionary https://dictionary.cambridge.org/dictionary/english/technology. Accessed 2 October 2023.

[75] See Turing completeness. Available at https://coinmarketcap.com/academy/glossary/turing-completeness. Accessed 6 October 2023.

[76] Kurahashi-Sofue, J. *What is a blockchain validator?* Available at https://support.avax.network/en/articles/4064704-what-is-a-blockchain-validator. Accessed 6 October 2023.

‘VATCoin’ – a digital currency denominated in fiat money that is issued by a government for the sole purpose of paying VAT.

‘Zero-knowledge Proof’ – this is method or a way of proving the validity of a statement without revealing the statement itself.[77]

[77] See definition provided by Ethereum.org at https://ethereum.org/en/zero-knowledge-proofs/. Accessed 12 August 2023.

CHAPTER 2: BLOCKCHAIN

2.1 Introduction

There is a common misconception that blockchain and bitcoin are one and the same thing. This is primarily because of the close association that bitcoin has with blockchain. The misconception often translates into misinformation about the capabilities and possible uses of bitcoin as a payment system and blockchain as an operation system. While it is true that bitcoin cannot function without blockchain, the same cannot be said about blockchain. Blockchain is the standalone technology application that brings bitcoin into existence. While blockchain application is mostly renowned for its proficiency in the bitcoin domain, the conceptual framework behind its existence extends beyond bitcoin as a payment system; to a platform for sharing the economy; and to renovating the financial system.[78] Blockchain has intrigued academics, lawyers, health practitioners, governments, and even major corporations around the world. Although blockchain application has many benefits, its use and application raise several questions that underpin the doubt and scepticism borne by cynics. For this reason, it becomes important to undertake a study of this magnitude in order to explore and understand the concept that is blockchain. A clearer picture can help formulate a better understanding for regulators and institutions that seek to adopt blockchain. In this chapter, I trace the origins of blockchain system. Any attempt at adopting blockchain may prove fruitless if an understanding of its genesis is not considered. In this chapter, I also consider the nature and characteristics of blockchain. The dynamics of blockchain coupled with its uses and potential benefits are also briefly discussed. Having considered its attributes, I consider a premise on its potential application for the collection of VAT on e-commerce transactions.

[78] Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the technology behind bitcoin is changing money, business and the world* Portfolio Penguin at 17 – 19.

2.2 A brief history of blockchain

2.2.1 The 2008 global financial crisis

The 2008 global financial crisis (the financial crisis) was the precursor to the eventual development of bitcoin and blockchain. Originating in the United States of America (USA), the financial crisis highlighted the deficiencies that was prevalent in banks and other financial institutions.[79] The financial crisis began when consumers in the USA borrowed money from banks without the necessary checks and balances taking place prior to any subsequent loan approval. Often, these loans were obtained from financial institutions with the intention of purchasing houses.[80] The bankers did not conduct the appropriate background checks on borrowers to determine if the income earners could afford to repay the loans. This was precipitated by the United States government's backing of bankers to make home loans available to low income earners.[81] The home loans given to income earners were then sold off to pension funds, public saving institutions, and insurance firms in a process called securitisation.[82] The sale of these securities was not limited to institutions in America but also to financiers around the world.[83] The demand for the securities intensified to such an extent that borrowing was expanded to low income earners.[84] Interestingly, these loans originated from depositor's funds made by individuals who entrusted their savings and deposits into banks and other financial institutions.[85]

[79] Baghla, S. (2017). "Origin of Bitcoin: A brief history from 2008 crisis to present times." Available at https://www.analyticsindiamag.com/origin-bitcoin-brief-history/. Accessed 7 September 2019.

[80] Kolb, W. R. (ed) (2010). *Lessons from the financial crisis: causes, consequences and our economic future* John Wiley & Sons Inc (New Jersey) at 33.

[81] Kolb, W. R. (ed) (2010). *Lessons from the financial crisis: causes, consequences and our economic future* John Wiley & Sons Inc (New Jersey) at 69.

[82] Kolb, W. R. (ed) (2010). *Lessons from the financial crisis: causes, consequences and our economic future* John Wiley & Sons Inc (New Jersey) at 199. See also Vigna, P., & Casey, M., J. (2016). *The Age of Cryptocurrency: How Bitcoin and the Blockchain are Challenging the Global Economic order* Picador USA at 62.

[83] Kolb, W. R. (ed) (2010). *Lessons from the financial crisis: causes, consequences and our economic future* John Wiley & Sons Inc (New Jersey) at 199.

[84] Vigna, P., & Casey, M., J. (2016). *The Age of Cryptocurrency: How Bitcoin and the Blockchain are Challenging the Global Economic order* Picador USA at 62.

[85] Baghla, S. (2017). "Origin of Bitcoin: A brief history from 2008 crisis to present times." Available at https://www.analyticsindiamag.com/origin-bitcoin-brief-history/. Accessed 7 September 2019.

In addition to the above, the bankers lent money to borrowers without demanding an initial deposit on the loans.[86] Bankers held the belief that the prices in the housing market would rise. As a result, bankers were confident that they would obtain significant rewards and bonuses.[87] However, this did not materialize, and the house prices decreased while interest rates increased. With little or no money available, consumer spending declined. As a result of reduced consumer spending, the American economy shrunk. A shrinking economy led to further disparity in the financial markets.[88] The rise in interest rates coupled with the reduction in consumer lending led to borrowers defaulting on their mortgages. Home foreclosures became prevalent due to borrowers' inability to pay off their loans. As more foreclosures took place, the housing market collapsed.[89]

Banks and other financial institutions' inability to raise sufficient capital as a countermeasure against the collapsing housing market and the turmoil in the financial markets led to a liquidity crisis. The financial crisis caused a chain reaction around the world resulting in the collapse of international markets. The chain reaction can be attributed to banks' interconnectedness on a global scale.[90] Financial reputable institutions such as *Bear Sterns* and *Lehman Brothers* crumbled. Other financial institutions avoided total collapse and subsequent bankruptcy because of interventions from the Unites States government.[91] The bailouts from the Unites States government were necessary to avert a total collapse of the American financial system.[92]

[86] Kolb, W. R. (ed) (2010). *Lessons from the financial crisis: causes, consequences and our economic future* John Wiley & Sons Inc (New Jersey) at 34.

[87] Kolb, W. R. (ed) (2010). *Lessons from the financial crisis: causes, consequences and our economic future* John Wiley & Sons Inc (New Jersey) at 34. See also Werbach, K. (2018). *The Blockchain and the New Architecture of Trust* Massachusetts Institute of Technology Press (US) at 37 – 38.

[88] Kolb, W. R. (ed) (2010). *Lessons from the financial crisis: causes, consequences and our economic future* John Wiley & Sons Inc (New Jersey) at 105.

[89] Kolb, W. R. (ed) (2010). *Lessons from the financial crisis: causes, consequences and our economic future* John Wiley & Sons Inc (New Jersey) at 127.

[90] Vigna, P., & Casey, M., J. (2016). *The Age of Cryptocurrency: How Bitcoin and the Blockchain are Challenging the Global Economic order* Picador USA at 62.

[91] Werbach, K. (2018). *The Blockchain and the New Architecture of Trust* Massachusetts Institute of Technology Press (US) at 37.

[92] Vigna, P., & Casey, M., J. (2016). *The Age of Cryptocurrency: How Bitcoin and the Blockchain are Challenging the Global Economic order* Picador USA at 62.

Due to the collapse of banks and other financial institutions, individuals' savings and deposits diminished owing to questionable investment practices by the same banks and financial institutions.[93] Moreover, individual deposits could not be recovered from the same banks that were tasked with keeping the funds safe.

Fannie Mae and *Freddie Mac* also played a crucial role in the financial crisis. *Fannie Mae* and *Freddie Mac* were created by the United States Congress with the aim of establishing a liquid secondary mortgage market that would provide low-income families with an alternative to funding mortgages with deposits.[94] *Fannie Mae* and *Freddie Mac* had assumed a reputation as "too big to fail" because if the institutions ran into trouble, they would be bailed out by the US government.[95] Both institutions seemed to be less risky investments, enabling them to have a favourable treatment in the bond market. This also enabled them to borrow trillion of dollars more cheaply.[96] *Fannie Mae* and *Freddie Mac* bankrolled the US home finance system in the years leading to the financial crisis by buying mortgages on the secondary market resulting in a housing bubble.[97] The lack of oversight resulted in many people getting mortgage loans who would not ordinarily qualify for home loans. The unwinding of the housing bubble and the subsequent financial crisis nearly caused the collapse of *Fannie Mae* and *Freddie* Mac before they were rescued by the Federal Housing Finance Agency by putting the two institutions into conservatorship.[98]

[93] Baghla, S. (2017). "Origin of Bitcoin: A brief history from 2008 crisis to present times." Available at https://www.analyticsindiamag.com/origin-bitcoin-brief-history/. Accessed 7 September 2019.

[94] Pelouze, F. A. (2009). "Fannie Mae and Freddie Mac and the 2008 Financial Crisis" at 4. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1424456. Accessed 21 June 2024; Marquit, M. & Adams, M. (2022). *Fannie Mae and Freddie Mac*. Available at https://www.forbes.com/advisor/investing/fannie-mae-and-freddie-mac/#:~:text=Fannie%20Mae%20and%20Freddie%20Mac%20played%20a%20starring%20role%20in,functioning%20of%20the%20mortgage%20market. Accessed 21 June 2024.

[95] Marquit, M. & Adams, M. (2022). *Fannie Mae and Freddie Mac*. Available at https://www.forbes.com/advisor/investing/fannie-mae-and-freddie-mac/#:~:text=Fannie%20Mae%20and%20Freddie%20Mac%20played%20a%20starring%20role%20in,functioning%20of%20the%20mortgage%20market. Accessed 21 June 2024.

[96] Marquit, M. & Adams, M. (2022). *Fannie Mae and Freddie Mac*. Available at https://www.forbes.com/advisor/investing/fannie-mae-and-freddie-mac/#:~:text=Fannie%20Mae%20and%20Freddie%20Mac%20played%20a%20starring%20role%20in,functioning%20of%20the%20mortgage%20market. Accessed 21 June 2024.

[97] Marquit, M. & Adams, M. (2022). *Fannie Mae and Freddie Mac*. Available at https://www.forbes.com/advisor/investing/fannie-mae-and-freddie-mac/#:~:text=Fannie%20Mae%20and%20Freddie%20Mac%20played%20a%20starring%20role%20in,functioning%20of%20the%20mortgage%20market. Accessed 21 June 2024.

[98] Marquit, M. & Adams, M. (2022). *Fannie Mae and Freddie Mac*. Available at https://www.forbes.com/advisor/investing/fannie-mae-and-freddie-

2.3 A new payment system

2.3.1 A lack of trust

The financial sector industry is one of the most important sectors in the world.[99] In addition to offering financial services to people, it transfers substantial amounts of money daily while underwriting the global economy.[100] It stands to reason that the financial sector figures as an important industry for people, the latter relying on the former for their livelihoods. What is more, the financial sector underpins the functionality of commercial and e-commerce transactions.

Since the financial sector resounds with society, the financial crisis exposed the deficiencies in the centralised model of operation. A centralised model is a model where operations and major decisions are orchestrated by a single party. The single party is often the leader of the organisation and a central authority. The leader has all the power, control, and authority to make decisions. Often, the leader makes rules for the organisation to thrive. If people in the organisation do not adhere to these rules, the system fails.[101]

As central authorities increase in size and become more multifaceted, more people are required to ensure that the network functions smoothly. In the context of the financial industry, intermediaries are hired to offer financial services to people. The challenge arises when intermediaries stop providing services to people. It can also happen that an intermediary indiscriminately, and irrationally gives the wrong advice for the sole benefit of making a profit. Potential civil liability aside, the central authorities find it difficult to operate without these intermediaries. Basically, the central

mac/#:~:text=Fannie%20Mae%20and%20Freddie%20Mac%20played%20a%20starring%20role%20in,functioning%20of%20the%20mortgage%20market. Accessed 21 June 2024.

[99] See Mishra, M. (2023). *List of 10 Biggest and Largest Industries in the World*. Available at https://www.edudwar.com/biggest-industries-in-the-world/. Accessed 22 August 2023.

[100] Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the technology behind bitcoin is changing money, business and the world* Portfolio Penguin at 55.

[101] See Brafman, O., & Beckstrom, A., R., (2006). *The Starfish and the Spider: The unstoppable power of leaderless organizations* Portfolio Penguin (USA) at 19.

authorities and financial institutions become more influential because they rely on the efforts made by intermediaries.[102]

The other challenges that characterised the financial industry during the financial crisis included the administration of outdated rules, a lack of transparency, and lengthy transactions.[103] These shortcomings came to the fore during the 2008 financial crisis. As Tapscott and Tapscott state:

> “Excess leverage, a lack of transparency, and a sense of complacency driven by skewed incentives prevented anyone from identifying the problem until it was nearly too late.”[104]

What was evident during the financial crisis was the perception that banks and other financial institutions conducted risky transactions often misguided by irritational behaviour, without any significant repercussions. The irreprehensible behaviour of banks and other financial institutions led to financial losses for consumers. Moreover, there was a possibility that these events would be repeated in the future.[105]

It was necessary to change the domination that the financial industry had on businesses, merchants, consumers, commerce, corporations, and markets.[106] In order to make changes to a monopoly that lacked the attributes to inspire trust, it was necessary to introduce a system that had all the attributes that the financial sector did not possess.

[102] Vigna, P., & Casey, M., J. (2016). *The Age of Cryptocurrency: How Bitcoin and the Blockchain are Challenging the Global Economic order* Picador USA at 5.

[103] Vigna, P., & Casey, M., J. (2016). *The Age of Cryptocurrency: How Bitcoin and the Blockchain are Challenging the Global Economic order* Picador USA at 18.

[104] Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the technology behind bitcoin is changing money, business and the world* Portfolio Penguin at 56.

[105] Werbach, K. (2018). *The Blockchain and the New Architecture of Trust* Massachusetts Institute of Technology Press (US) at 38.

[106] See Vigna, P., & Casey, M., J. (2016). *The Age of Cryptocurrency: How Bitcoin and the Blockchain are Challenging the Global Economic order* Picador USA at 57.

2.3.2 Defining trust

For society to function, trust is required. Often, trust is predicated by one's experiences, ties to people, and beliefs.[107] These ideologies stem from day-to-day interaction with other people, the public, work, and more recently, social media. If these interactions lead to positive outcomes, then trust is gradually built until it is maintained. Negative experiences have the opposite effect on trust. Negative experiences break the chain of trust and, depending on the severity of the fallout, it has the potential to render trust non-existent.

It is generally accepted that trust consists of three distinct elements: risk, control, and uncertainty.[108] Consider the following example:

<u>Example 1</u>

> X decides to acquire his first item online. X purchases a tangible copy of a book on *Amazon.com*. X effects the necessary payment by credit card. X selects his preferred delivery destination as South Africa. Amazon.com duly informs X of the expected delivery date of the item.

In the above example, X is familiar with *Amazon.com* because of its reputation and because of positive experiences from friends and colleagues. Although X is acquainted with *Amazon.com*, X does not necessarily trust *Amazon.com*. X's trust in *Amazon.com* can be influenced by the potential success and outcome of his first online order. X's continued use of *Amazon.com* can be determined by their trust in *Amazon.com*.[109] However, there is uncertainty with regards to the exact date of delivery. In addition, there is also a risk that the item may not be delivered at all even

[107] Knittel, M., Pitts, S., & Wash R. (2019) "*The Most Trustworthy Coin: How Ideology Builds and Maintains Trust in Bitcoin*" Proceedings of the ACM Human Computer Interact Vol 3, CSCW, Article 36 (November 2019) at 1. https://doi.org/10.1145/3359138. Accessed 15 December 2019.

[108] See Manrique, S. (2018). *Blockchain: A Proof of Trust* Master thesis (Delft University of Technology) at 1 – 71. Available at https://repository.tudelft.nl/islandora/object/uuid%3Ac1996e12-1462-4683-8716-72110c665d4c. Accessed 14 January 2020.

[109] Manrique, S. (2018). *Blockchain: A Proof of Trust* Master thesis (Delft University of Technology) at 11. Available at https://repository.tudelft.nl/islandora/object/uuid%3Ac1996e12-1462-4683-8716-72110c665d4c. Accessed 14 January 2020.

though payment has been effected. X has little or no influence on the outcome because he does not have control of the situation. And yet, he may elect to trust *Amazon.com* because trust occurs where uncertainty is present.[110] If X receives the book within the projected timeframe, there is a greater chance that they can make additional orders on *Amazon.com*. Hence, trust has been built.

It is not easy to define trust. Trust is relative because people ascribe different connotations to it. Generally, trust can be defined as:

> "The expectation that a person or an institution will perform an action that is beneficial and not detrimental to us without the need to monitor or engage with them."[111]

Trust is vital if growth and consistency is to be maintained. For example, trust is required in the financial industry where financial investment establishments and money is exchanged on a regular basis.[112] Without trust, it is difficult to consistently make investments in the financial industry. As a result, a person is inclined to make use of alternative investment vehicle.

As a variant, it is possible to create trust through a social order containing peers. This is so because peers generally share common rules and standards. It is possible for peers to interact with each other in a communal environment because of the social setup.[113] In order for the setup to be flexible, peers determine rules upon which their

[110] Knittel, M., Pitts, S., & Wash R. (2019) "*The Most Trustworthy Coin: How Ideology Builds and Maintains Trust in Bitcoin*" Proceedings of the ACM Human Computer Interact Vol 3, CSCW, Article 36 (November 2019) at 3. https://doi.org/10.1145/3359138. Accessed 15 December 2019.

[111] Gambetta, D. (1988). "Can We Trust Trust?" in Gambetta, Diego (ed.) *Trust: Making and Breaking Cooperative Relations* Basil Blackwell Ltd (UK) at 217; Sapienza, P., & Zingales, L., (2012). "A Trust crisis" *International Review of Finance* 12(2):124. Available at https://doi.org/10.1111/j.1468-2443.2012.01152.x. Accessed 2 March 2020; Manrique, S. (2018). *Blockchain: A Proof of Trust* Master thesis (Delft University of Technology) at 15. Available at https://repository.tudelft.nl/islandora/object/uuid%3Ac1996e12-1462-4683-8716-72110c665d4c. Accessed 14 January 2020; Werbach, K. (2018). *The Blockchain and the New Architecture of Trust* Massachusetts Institute of Technology Press (US) at 25; Mayer, R., C., Davis, J., H., and Schoorman, F., D. (1995). "An Integrative Model of Organizational Trust" *The Academy of Management Review* Vol 20(3)712. Available at https://www.jstor.org/stable/pdf/258792.pdf. Accessed 3 March 2020.

[112] Sapienza, P., & Zingales, L., (2012). "A Trust crisis" *International Review of Finance* 12(2):124. Available at https://doi.org/10.1111/j.1468-2443.2012.01152.x. Accessed 2 March 2020.

[113] Werbach, K. (2018). *The Blockchain and the New Architecture of Trust* Massachusetts Institute of Technology Press (US) at 26.

autonomy is exercised.[114] Under these circumstances, trust is spread amongst the peers in that setup.[115] More importantly, there is no oversight by a central authority. The effect is that there is no principal point of failure or distrust. In contrast, trust placed in a central authority can be easily broken if the central authority collapses or fails. The challenge is amplified if the central authority is governed by obscure bureaucratic rules and practices that make trust problematic.

2.3.3 The introduction of Bitcoin

To address the inefficiencies of a centralised model deployed by banks and other financial institutions, it became necessary to adopt a system that was decentralised. The system also required a form of money that was not controlled by a central authority.[116] More importantly, that system had to be controlled and managed by peers without the need for trust. That system is what is known today as Bitcoin.

2.3.3.1 What is Bitcoin?

Bitcoin[117] is a form of decentralised digital currency that operates on an operating system known as the Bitcoin protocol.[118] Bitcoin was launched in 2009 when an individual with the pseudonym of *Satoshi Nakamoto* released a white paper detailing a new payment system that did not rely on trust but on cryptography.[119] Transactions can take place between people who do not know each other. Crucially, these

[114] Werbach, K. (2018). *The Blockchain and the New Architecture of Trust* Massachusetts Institute of Technology Press (US) at 26.

[115] Manrique, S. (2018). *Blockchain: A Proof of Trust* Master thesis (Delft University of Technology) at 16. Available at https://repository.tudelft.nl/islandora/object/uuid%3Ac1996e12-1462-4683-8716-72110c665d4c. Accessed 14 January 2020.

[116] This form of money had to be digital in nature as opposed to physical to prevent control from governments and financial institutions.

[117] When written with a small letter, 'bitcoin' refers to the virtual currency units. Written with a capital letter, 'Bitcoin' refers the network. See https://bitcoin.org/en/vocabulary#bit. Accessed 23 August 2022; see also Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 3; Brito, J. (2015) *et al The Law of Bitcoin* iUniverse at 10 – 11.

[118] According to Vigna and Casey, a protocol is "set of programming instructions that allows computers to communicate with each other." See Vigna, P., & Casey, M., J. (2016). *The Age of Cryptocurrency: How Bitcoin and the Blockchain are Challenging the Global Economic order* Picador USA at 9.

[119] See Nakamoto, S. (2008) "Bitcoin: A Peer-to-Peer Electronic Cash System" at 1. Available at https://bitcoin.org/bitcoin.pdf. Accessed 7 December 2019.

transactions can be conducted without the assistance of a third party, reducing transaction costs in the process.[120]

To process payment transactions, Bitcoin uses a public ledger to record all the transactions that are facilitated on the Bitcoin protocol. The public ledger substitutes third parties by making transactions visible and verifiable to everyone.[121] As opposed to relying on financial institutions, trust and accountability is placed on peers who run and transact on the Bitcoin protocol. This form of organisation seeks to redress the inefficiencies of central authorities by transferring the control of current assets like money from central authorities to people.[122]

Bitcoin's public nature helps facilitate access to areas of the economy that was previously inaccessible.[123] Accessibility is made possible because the Bitcoin protocol can run on any Internet enabled computer network that extends to any location around the world. All participants on the network are charged with preserving the public ledger and the payment system.[124]

For a person to make use of the Bitcoin payment system, they must have access to a Bitcoin wallet. A Bitcoin wallet[125] is a password protected software that functions as an account with which users can send bitcoins to other users anywhere around the world.[126] Transactions that take place on the Bitcoin protocol are made secure by means of cryptography.[127] Cryptography works by converting plaintext and scrambling

[120] Nakamoto, S. (2008) "Bitcoin: A Peer-to-Peer Electronic Cash System" at 1. Available at https://bitcoin.org/bitcoin.pdf. Accessed 7 December 2019.

[121] Vigna, P., & Casey, M., J. (2016). *The Age of Cryptocurrency: How Bitcoin and the Blockchain are Challenging the Global Economic order* Picador USA at 5.

[122] Vigna, P., & Casey, M., J. (2016). *The Age of Cryptocurrency: How Bitcoin and the Blockchain are Challenging the Global Economic order* Picador USA at 6.

[123] Vigna, P., & Casey, M., J. (2016). *The Age of Cryptocurrency: How Bitcoin and the Blockchain are Challenging the Global Economic order* Picador USA at 8.

[124] Vigna, P., & Casey, M., J. (2016). *The Age of Cryptocurrency: How Bitcoin and the Blockchain are Challenging the Global Economic order* Picador USA at 9.

[125] A Bitcoin wallet contains a person's private key. The private key enables a person to send bitcoins on the blockchain. A Bitcoin wallet can also show the total amount of bitcoins available. See https://bitcoin.org/en/vocabulary#bit. Accessed 23 August 2022.

[126] Vigna, P., & Casey, M., J. (2016). *The Age of Cryptocurrency: How Bitcoin and the Blockchain are Challenging the Global Economic order* Picador USA at 124; De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 21.

[127] Cryptography is "the branch of mathematics that lets us create mathematical proofs that provide high levels of security." With cryptography, a person can make it difficult for anyone to spend funds from another person's wallet. A person's Bitcoin wallet can also be encrypted to ensure

it into ciphertext, so that the encoded output can be understood by the intended recipient.[128] Once the text has been converted to ciphertext, information is only readable to the intended recipient only.[129] Generally, encryption is often used to scramble plaintext to ciphertext.[130] Blockchain uses three types of cryptography techniques: symmetric cryptography; asymmetric cryptography; and cryptographic hashing. Symmetric cryptography is a technique that involves using an encrypted code or key to translate information into cipher.[131] In other words, symmetric cryptography "is an encryption system where the same secret key is used to both encrypt and decrypt the data".[132] In symmetric cryptography, the parties communicate via symmetric encryption and exchange the key with recipients so that the data can be decrypted.[133] Asymmetric cryptography is a technique that uses "different keys between a sender and a receiver to encrypt and decrypt information respectively".[134] Here, a sender uses a key to encrypt and a different key is used to decrypt the data.[135] Cryptographic hashing converts plain text into a unique string of data by using

that it cannot be used without a password. See https://bitcoin.org/en/vocabulary#bit. Accessed 23 August 2022.

[128] Ghimiray, D. (2022). *What is cryptography and how does it work?* Available at https://www.avast.com/c-cryptography#:~:text=How%20does%20cryptography%20work%3F,all%20except%20the%20intended%20recipient. Accessed 22 August 2023.

[129] Ghimiray, D. (2022). *What is cryptography and how does it work?* Available at https://www.avast.com/c-cryptography#:~:text=How%20does%20cryptography%20work%3F,all%20except%20the%20intended%20recipient. Accessed 22 August 2023.

[130] Ghimiray, D. (2022). *What is cryptography and how does it work?* Available at https://www.avast.com/c-cryptography#:~:text=How%20does%20cryptography%20work%3F,all%20except%20the%20intended%20recipient. Accessed 22 August 2023.

[131] Spydra (2023). *Everything you need to know about cryptography in blockchain*. Available at https://www.linkedin.com/pulse/everything-you-need-know-cryptography-blockchain-spydra. Accessed 22 August 2023.

[132] Techskill Brew (2022). *Cryptography in Blockchain (Part 6-Blockchain series)*. Available at https://medium.com/techskill-brew/cryptography-in-blockchain-part-6-blockchain-basics-129ec058c574. Accessed 7 June 2024; see also Okafor, C. *Unveiling the depths of blockchain cryptography*. Available at https://www.linkedin.com/pulse/unveiling-depths-blockchain-cryptography-collins-okafor. Accessed 7 June 2024.

[133] Techskill Brew (2022). *Cryptography in Blockchain (Part 6-Blockchain series)*. Available at https://medium.com/techskill-brew/cryptography-in-blockchain-part-6-blockchain-basics-129ec058c574. Accessed 7 June 2024.

[134] Spydra (2023). *Everything you need to know about cryptography in blockchain*. Available at https://www.linkedin.com/pulse/everything-you-need-know-cryptography-blockchain-spydra. Accessed 22 August 2023.

[135] Techskill Brew (2022). *Cryptography in Blockchain (Part 6-Blockchain series)*. Available at https://medium.com/techskill-brew/cryptography-in-blockchain-part-6-blockchain-basics-129ec058c574. Accessed 7 June 2024; see also Okafor, C. *Unveiling the depths of blockchain cryptography*. Available at https://www.linkedin.com/pulse/unveiling-depths-blockchain-cryptography-collins-okafor. Accessed 7 June 2024.

cryptographic algorithms.[136] Simply put, hashing "is a technique or process of generating a fixed-length output hash for any input data irrespective of its size and length".[137] Once data is sent through a hash, it cannot be reversed. Hashing compresses data into small string text and can make large chunks of data smaller.[138] Currently, blockchain uses asymmetric cryptography and cryptographic hashing only.[139]

In a Bitcoin protocol, a user combines his unique private key, which is an address consisting of numbers, with a public key in a rigorous and accurate manner that creates a digital signature.[140] Once the transaction has been signed with a private key, a directive is sent to transfer the designated value to the recipient's address.[141] The recipient uses the sender's public key in order to decipher the transaction or message and confirm that indeed it was sent by the original sender. Interestingly, the sender's public key is made known to everyone on the Bitcoin network.[142] Transactions are stacked up together into blocks. The blocks are connected to each other using a timestamped sequence.[143] Every block on the network contains a hash. The purpose of a hash is to store large amounts of data into a smaller and compact size. This is achieved to organize and grade transactions in a hierarchal manner.[144]

[136] Spydra (2023). *Everything you need to know about cryptography in blockchain*. Available at https://www.linkedin.com/pulse/everything-you-need-know-cryptography-blockchain-spydra. Accessed 22 August 2023.

[137] Techskill Brew (2022). *Cryptography in Blockchain (Part 6-Blockchain series)*. Available at https://medium.com/techskill-brew/cryptography-in-blockchain-part-6-blockchain-basics-129ec058c574. Accessed 7 June 2024.

[138] Spydra (2023). *Everything you need to know about cryptography in blockchain*. Available at https://www.linkedin.com/pulse/everything-you-need-know-cryptography-blockchain-spydra. Accessed 22 August 2023.

[139] Techskill Brew (2022). *Cryptography in Blockchain (Part 6-Blockchain series)*. Available at https://medium.com/techskill-brew/cryptography-in-blockchain-part-6-blockchain-basics-129ec058c574. Accessed 7 June 2024.

[140] Nakamoto, S. (2008) "Bitcoin: A Peer-to-Peer Electronic Cash System" at 2. Available at https://bitcoin.org/bitcoin.pdf. Accessed 7 December 2019; Vigna, P., & Casey, M., J. (2016). *The Age of Cryptocurrency: How Bitcoin and the Blockchain are Challenging the Global Economic order* Picador USA at 125 – 126.

[141] Vigna, P., & Casey, M., J. (2016). *The Age of Cryptocurrency: How Bitcoin and the Blockchain are Challenging the Global Economic order* Picador USA at 124 – 125; Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 44.

[142] Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 44.

[143] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 22; Nakamoto, S. (2008) "Bitcoin: A Peer-to-Peer Electronic Cash System" at 2. Available at https://bitcoin.org/bitcoin.pdf. Accessed 7 December 2019.

[144] Vigna, P., & Casey, M., J. (2016). *The Age of Cryptocurrency: How Bitcoin and the Blockchain are Challenging the Global Economic order* Picador USA at 128 – 129; Kianieff, M. (2019) *Blockchain Technology and the Law Opportunities and Risks* Routledge Publishing (UK) at 11.

The next step is to validate the transaction to ensure that no one on the Bitcoin network has spent or used that bitcoin on previous occasions. This is done by a group of users on the Bitcoin network called miners. Miners solve a puzzle in a difficult process that requires computational power and large amounts of electricity. The process, which is essentially guesswork, ends when a single miner succeeds in validating the transaction. For their effort, that victorious miner is rewarded with new bitcoins.[145] Once the validation process is complete, the block is added to the other blocks. The process of authentication coupled with the addition of the new blocks to blockchain is known as consensus.[146]

2.4 Blockchain

When *Satoshi Nakatomo* released the white paper on Bitcoin, it was difficult to imagine that Bitcoin would bring about a revolutionary technological application capable of processing data. In fact, nowhere in the white paper does *Nakatomo* mention the term 'blockchain'.[147] Blockchain[148] is the innovative technological structure that facilitates the Bitcoin system.[149] As such, blockchain is a critical component of the Bitcoin system. As has been shown, the Bitcoin system's existence is predicated on blockchain technology. In its simplest form, a blockchain is a ledger registry that is shared anonymously on a computer network between two different entities with the main purpose of recording transactions.[150] For this reason, blockchains are often

[145] Nakamoto, S. (2008) "Bitcoin: A Peer-to-Peer Electronic Cash System" at 2 – 4. Available at https://bitcoin.org/bitcoin.pdf. Accessed 7 December 2019; Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 44; De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 23 – 26; Vigna, P., & Casey, M., J. (2016). *The Age of Cryptocurrency: How Bitcoin and the Blockchain are Challenging the Global Economic order* Picador USA at 129.

[146] See also Bacon, J., *et al* (2017). "Blockchain Demystified" *Queen Mary University of London, School of Law Legal Studies Research Paper No. 268/2017* at 11 - 15. Available https://papers.ssrn.com/sol3/papers.cfm?Abstract_id=3091218. Accessed 5 January 2020.

[147] See Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. Available at https://bitcoin.org/bitcoin.pdf. Accessed 7 December 2019; See also Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 8.

[148] According to Finck, the term 'blockchain' was adopted because transactions are recorded on 'blocks' that form a chain. See Finck, M. (2018). "Blockchains: Regulating the Unknown" *German Law Journal* 19(4): 668.

[149] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 8. See also Kiviat, T. I. (2015). Beyond bitcoin: Issues in regulating blockchain transactions *Duke Law Journal* 65(3): 573.

[150] Kianieff, M. (2019) *Blockchain Technology and the Law Opportunities and Risks* Routledge Publishing (UK) at 8; Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 10.

referred to as distributed ledger technology (DLT).[151] It is my view that the description is primarily due to the multiplicity of blockchain's reach and its application on a global scale.

Blockchain was primarily 'created' to transmit digital currencies in a peer-to-peer network.[152] The peer-to-peer network consists of 'nodes'[153] that store precise copies of a blockchain that is automatically synchronised by a software protocol.[154] Each node contains a copy of blockchain. A node contains a record of every transaction executed on the block since its inception up to the most recent entry.[155] The types of transactions recorded on blockchain is not limited to cryptographic transactions. Due to its technical nature, it is possible to record information and digital assets on a blockchain without the assistance of a third party.[156] This facet promotes new ways of information dissemination particularly if this information can be propagated anonymously.[157] The advent of blockchain technology facilitates dissemination of

[151] A distributed ledger is type of archive divided across a network of multiple sites, jurisdictions, or institutions. See UK Government Chief Scientific Adviser (2016). *Distributed Ledger Technology: Beyond Block Chain*
(London: Government Office for Science) (Blackett Review) at 5. Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 9 (footnote 14). The United Kingdom's Financial Conduct Authority defines a DLT as: "a set of technological solutions that enables a single, sequenced, standardised, and cryptographically secured record of activity to be safely distributed to, and acted upon by, a network of varied participants. This record could contain for example, transactions, asset holdings or identity data." See Financial Conduct Authority (2017). *Discussion Paper on distributed ledger technology* at 10. Available at https://www.fca.org.uk/publication/discussion/dp17-03.pdf. Accessed 23 August 2022; see also Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 9 (footnote 14).

[152] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 2; Alexander, G. (2022). "Blocking the Gap: The Potential for Blockchain Technology to secure VAT Compliance" *EC Tax Review* 31(3): 149.

[153] Nodes are computers that store a full or partial copy of a blockchain. Some nodes participate in the validation of new blocks. See Artzt, M., (ed) Determann, L., Long, W., *Blockchain and Data Privacy* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 205.

[154] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 2. See also Werbach, K. (2018). *The Blockchain and the New Architecture of Trust* Massachusetts Institute of Technology Press (US) at 7; See also Bacon, J., *et al* (2017). "Blockchain Demystified" *Queen Mary University of London, School of Law Legal Studies Research Paper No. 268/2017* at 11 – 12. Available https://papers.ssrn.com/sol3/papers.cfm?Abstract_id=3091218. Accessed 5 January 2020.

[155] Swan, M. (2015). *Blockchain: Blueprint for a new economy* O'Reilly Publishing (US) at ix; Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 10.

[156] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 8; De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 3.

[157] Kianieff, M. (2019) *Blockchain Technology and the Law Opportunities and Risks* Routledge Publishing (UK) at 7.

information between: countries, private individuals, organisations, or institutions on a global scale. Since intermediaries are not required, transactions occur at a faster rate because only two parties are involved in a typical transaction.[158] This potentially reduces transaction costs, whilst improving efficiency.[159]

Since no central authority or entity has control over blockchain,[160] the network can be accessed by any party provided they are connected to the network with a node. It is possible for the ledger to be updated at different times to replicate any new transaction between the parties.[161] It is important to note that once a new transaction is recorded on the ledger, it is automatically updated on all the computers in the network.[162] This results in the public display of information ensuring that everyone can view and scrutinize the information that is displayed on blockchain. For example, a party or entity in one jurisdiction can access blockchain network and record information using a node. Once that person or entity records the information, it is duplicated in every other node on blockchain network irrespective of the location or jurisdiction of the user.[163]

In addition to creating trust between parties, blockchain system demonstrates that transparency can be achieved.[164] These attributes make blockchain conducive for a variety of possible uses. These include the health sector for the storage of health

[158] In a Bitcoin blockchain, average processing time is 10 minutes.

[159] Kianieff, M. (2019) *Blockchain Technology and the Law Opportunities and Risks* Routledge Publishing (UK) at 7. See also Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 7. See also Kiviat, T. I. (2015). Beyond bitcoin: Issues in regulating blockchain transactions *Duke Law Journal* 65(3): 573.

[160] See Kiviat, T. I. (2015). Beyond bitcoin: Issues in regulating blockchain transactions *Duke Law Journal* 65(3): 573. See Finck, M. (2018). Blockchains: Regulating the Unknown *German Law Journal* 19(4): 668.

[161] Kianieff, M. (2019) *Blockchain Technology and the Law Opportunities and Risks* Routledge Publishing (UK) at 7.

[162] Kianieff, M. (2019) *Blockchain Technology and the Law Opportunities and Risks* Routledge Publishing (UK) at 7.

[163] Werbach, K. (2018). *The Blockchain and the New Architecture of Trust* Massachusetts Institute of Technology Press (US) at 7.

[164] Kianieff, M. (2019) *Blockchain Technology and the Law: Opportunities and Risks* Routledge Publishing (UK) at 7.

data,[165] for genomic sequencing,[166] mining,[167] community supercomputing,[168] notary type of work,[169] cloud storage,[170] car sharing and private transport,[171] archival and backup,[172] for learning and literacy,[173] financial services,[174] government services,[175] money market,[176] e-commerce transactions,[177] supply chain management,[178] crowdfunding,[179] mobile banking,[180] social networks,[181] the tracking of goods in international trade,[182] tax compliance,[183] value chain analysis,[184] VAT fraud detection,[185] sharing economy platforms,[186] peer-to-peer file sharing applications,[187] and public administration.[188] The potential uses illustrates that blockchain's reach has

[165] Swan, M. (2015). *Blockchain: Blueprint for a new economy* O'Reilly Publishing (US) at 59. See also Hacker, P., Lianos, L., Dimitropoulos, G., Eich, S., (eds) (2019) *Regulating Blockchain: Techno-social and Legal challenges* Oxford University Press (UK) at 5.

[166] Swan, M. (2015). *Blockchain: Blueprint for a new economy* O'Reilly Publishing (US) at 58.

[167] Swan, M. (2015). *Blockchain: Blueprint for a new economy* O'Reilly Publishing (US) at 53.

[168] Swan, M. (2015). *Blockchain: Blueprint for a new economy* O'Reilly Publishing (US) at 54.

[169] Swan, M. (2015). *Blockchain: Blueprint for a new economy* O'Reilly Publishing (US) at 60.

[170] Hacker, P., Lianos, L., Dimitropoulos, G., Eich, S., (eds) (2019) *Regulating Blockchain: Techno-social and Legal challenges* Oxford University Press (UK) at 5.

[171] Hacker, P., Lianos, L., Dimitropoulos, G., Eich, S., (eds) (2019) *Regulating Blockchain: Techno-social and Legal challenges* Oxford University Press (UK) at 5.

[172] Swan, M. (2015). *Blockchain: Blueprint for a new economy* O'Reilly Publishing (US) at 61.

[173] Swan, M. (2015). *Blockchain: Blueprint for a new economy* O'Reilly Publishing (US) at 61.

[174] Swan, M. (2015). *Blockchain: Blueprint for a new economy* O'Reilly Publishing (US) at 11.

[175] Hacker, P., Lianos, L., Dimitropoulos, G., Eich, S., (eds) (2019) *Regulating Blockchain: Techno-social and Legal challenges* Oxford University Press (UK) at 5; Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 20.

[176] Swan, M. (2015). *Blockchain: Blueprint for a new economy* O'Reilly Publishing (US) at 11. See also Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 20 – 22.

[177] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 5. See also Hacker, P., Lianos, L., Dimitropoulos, G., Eich, S., (eds) (2019) *Regulating Blockchain: Techno-social and Legal challenges* Oxford University Press (UK) at 5.

[178] Hacker, P., Lianos, L., Dimitropoulos, G., Eich, S., (eds) (2019) *Regulating Blockchain: Techno-social and Legal challenges* Oxford University Press (UK) at 5. See also Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 22 – 24.

[179] Swan, M. (2015). *Blockchain: Blueprint for a new economy* O'Reilly Publishing (US) at 12.

[180] See https://www.bitpesa.co/. Accessed 17 December 2019. See also Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 9.

[181] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 5.

[182] See https://www.everledger.io/about-us/about. Accessed 17 December 2019. See also Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 9.

[183] Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 24.

[184] Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 24 – 25.

[185] Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 25 – 27.

[186] Huckle, S. *et al* (2016). Internet of things, Blockchain and Shared Economy applications *Procedia Computer Science* 98:461. See also See also Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 9.

[187] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 5.

[188] Melnyk, R., & Barikova, A., (2019). "Cross-border public administration: Prospects for introducing blockchain jurisdiction" *Informatologia* 52 1-2, 74 – 89.

developed beyond the facilitation of a payment system and the financial sector[189] to a multi-purpose technological application.

A discussion of all the above-mentioned potential uses of blockchain is beyond the scope of this thesis. Instead, what follows is a discussion of the characteristics of blockchain. This discussion is important because it can assist to determine the relevant facets that the technology possesses for VAT collection purposes.

2.5 The characteristics of blockchain

It is imperative to understand and discuss the various characteristics of blockchain. What follows is an exposition of each of blockchain's characteristics.

2.5.1 An embodiment of trust architecture

From the outset, it must be noted that blockchain system functions on trust. From a business perspective, trust functions on the anticipation that a contracting party will act according to the four principles of integrity: accountability, honesty, transparency, and consideration.[190] Ordinarily, trust derived from organisations, intermediaries, or individuals.[191] With blockchain, trust is derived from the network and the material on the network.[192] Tapscott and Tapscott describe 'trust' as not necessarily having confidence in a business and its affairs, but rather trusting the integrity and protection of information once goods and services are bought.[193] Simply put, a party to a transaction on blockchain relies on the accuracy of the information. Once this information has been verified by other parties on blockchain system, trust is created.

[189] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 3.

[190] Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the technology behind bitcoin is changing money, business and the world* Portfolio Penguin at 10.

[191] Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the technology behind bitcoin is changing money, business and the world* Portfolio Penguin at 11.

[192] Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the technology behind bitcoin is changing money, business and the world* Portfolio Penguin at 11.

[193] Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the technology behind bitcoin is changing money, business and the world* Portfolio Penguin at 11.

Prior to the 2008 financial crisis, trust in the business sector predominantly originated from central authorities like banks and the government.[194] However, since the events of the 2008 financial crisis, trust in centralised institutions has diminished. South Africa has not been immune to the eschewed trust traditionally placed in the government and other centralised institutions.[195] For instance, it was shown that only 21 per cent of South Africans trusted their government in 2019.[196]

It can be argued that the use of the term 'trust' is a misnomer[197] because transactions on blockchain are generally pseudonymous in nature. Parties on blockchain are often unaware of each other's identity.[198] However, Finck argues that there are mechanisms currently in the works that can reveal the identities of parties on blockchain network.[199] In the absence of the implementation of these new mechanisms, it remains difficult to independently establish the identity of parties on a public blockchain.

Trust is not necessarily placed on the parties but rather on the veracity of the entries on blockchain registry. To be more precise, parties on blockchain system trust the entries recorded on the distributed ledger although no single individual can validate the entries.[200] However, it must be noted that trust is not dependent on the frequency of the transactions recorded on blockchain system but rather on the system's infrastructure. For example, the Bitcoin blockchain does not rely on a central authority or middleman but rather on the underlying code and the miners on the network.[201]

[194] Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the technology behind bitcoin is changing money, business and the world* Portfolio Penguin at 11.

[195] See 2019 Edelman Trust Barometer. Available at https://www.edelman.com/trust-barometer. Accessed 19 December 2019. See also https://www.corruptionwatch.org.za/trust-inequality-at-all-time-high/. Accessed 19 December 2019.

[196] See 2019 Edelman Trust Barometer. Available at https://www.edelman.com/trust-barometer. Accessed 19 December 2019.

[197] See also Werbach, K. (2018). *The Blockchain and the New Architecture of Trust* Massachusetts Institute of Technology Press (US) at 29.

[198] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 38.

[199] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 63.

[200] Werbach, K. (2018). *The Blockchain and the New Architecture of Trust* Massachusetts Institute of Technology Press (US) at 3.

[201] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 26.

Due to the reliance and trust that parties have on blockchain system, blockchains are often referred to as 'trustless' systems.[202] It has been argued that the description of blockchain as a 'trustless' system is vague and unclear because blockchain does not remove trust in the peer to peer network.[203] It is more accurate to state that the trust in blockchain system has been reduced because information on blockchain system has been disseminated to various parties.[204] The reduction in trust does not necessarily mean that trust has been eliminated in its entirety.[205] The form of trust that emerges from the use of blockchain is newfound.[206]

2.5.2 Consensus mechanism

Generally, parties to a contract reach an agreement by accepting the terms and conditions of the contract. This process is often known as meeting of the minds. In the context of blockchain, it is almost inconceivable for parties to reach agree on anything because their identities are unknown. However, consensus in blockchain is reached through trust.[207] Finck defines 'consensus' as:

[202] Nakamoto, S. (2008) *Bitcoin: A Peer-to-Peer Electronic Cash System* at 8. Available at https://bitcoin.org/bitcoin.pdf. Accessed 7 December 2019. De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 26. See also https://medium.com/@preethikasireddy/eli5-what-do-we-mean-by-blockchains-are-trustless-aa420635d5f6. Accessed 15 December 2019. Kiviat, T. I. (2015). Beyond bitcoin: Issues in regulating blockchain transactions *Duke Law Journal* 65(3): 574. De Filippi, P., & Hassan, S. (2016) *Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code* at 3**.** Available at https://arxiv.org/ftp/arxiv/papers/1801/1801.02507.pdf. Accessed 19 December 2019. Fairfield, J. (2014). Smart Contracts, Bitcoin Bots, and Consumer Protection *Washington and Lee Law Review Online* 71: 36. Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 12. De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 26. Werbach, K. (2018). *The Blockchain and the New Architecture of Trust* Massachusetts Institute of Technology Press (US) at 28 – 31. Rodrigues, U., R. (2019). Law and the Blockchain *Iowa Law Review* 104: 729.

[203] See https://medium.com/@preethikasireddy/eli5-what-do-we-mean-by-blockchains-are-trustless-aa420635d5f6. Accessed 15 December 2019.

[204] See https://medium.com/@preethikasireddy/eli5-what-do-we-mean-by-blockchains-are-trustless-aa420635d5f6. Accessed 15 December 2019.

[205] Werbach, K. (2018). *The Blockchain and the New Architecture of Trust* Massachusetts Institute of Technology Press (US) at 3. See Finck, M. (2018). Blockchains: Regulating the Unknown *German Law Journal* 19(4): 669.

[206] Werbach, K. (2018). *The Blockchain and the New Architecture of Trust* Massachusetts Institute of Technology Press (US) at 3.

[207] Werbach, K. (2018). *The Blockchain and the New Architecture of Trust* Massachusetts Institute of Technology Press (US) at 136. See also Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 20.

> "The mechanism that coordinates data held by various nodes, providing assurance to network participants that their versions of the ledger are consistent and accurate."[208]

Adam describes a consensus mechanism as "a protocol that ensures that all nodes of the corresponding blockchain network are synchronised with each other and on the basis of which it is decided which of the transactions made in the network are legitimate and thus to be attached to the existing blockchain."[209] Simply put, consensus occurs when everyone on blockchain system obtains their own copy of the ledger and rely on the fact that copies will remain consistent without the assistance of a central authority.[210] A party that joins blockchain after consensus has taken place, can merely access the entire registry to check all the transactions recorded since the inception of blockchain system.[211] One of the benefits of a using a consensus mechanism is determining whether a particular transaction is legitimate and managing conflicts between multiple simultaneous competing entities.[212]

As has been mentioned,[213] trust in blockchain system is created by means of a validation process.[214] This is done by solving complex mathematical puzzles in a process called 'mining'.[215] Once the 'mining' process has been completed, a new block is added to blockchain through a set of rules that determines how the new blocks can be shared on the database.[216] Once the blocks have been validated, a hash is produced and then added to the network. When other users verify the authenticity of the hash, trust is created because everyone acknowledges that work has been done

[208] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 7.

[209] Adam, K. (2022). *Blockchain Technology for Business Processes: Meaningful use of the new technology in business* Springer Nature at 25.

[210] Werbach, K. (2018). *The Blockchain and the New Architecture of Trust* Massachusetts Institute of Technology Press (US) at 7. See also Swan, M. (2015). *Blockchain: Blueprint for a new economy* O'Reilly Publishing (US) at 95.

[211] Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the technology behind bitcoin is changing money, business and the world* Portfolio Penguin at 34.

[212] Owens, J. & Hodžić, S. (2022). "Blockchain technology: potential for digital tax administration" *Intertax* Vol 50(11): 815.

[213] Paragraph 2.4.3.1 above.

[214] UK Government Chief Scientific Adviser (2016). *Distributed Ledger Technology: Beyond Block Chain* (US: Government Office for Science) (Blackett Review) at 17.

[215] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 23 – 24.

[216] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 23. See also UK Government Chief Scientific Adviser (2016). *Distributed Ledger Technology: Beyond Block Chain* (London: Government Office for Science) (Blackett Review) at 17.

to reach the outcome.[217] This process is often known as *proof-of-work*.[218] *Proof-of-work* is a decentralised consensus mechanism that solves complicated asymmetrical mathematical puzzles to produce new blocks during mining.[219] According to Bains, the *proof-of-work* mechanism allows a large number of nodes to participate in the blockchain network potentially making the network scalable. Bains also notes that "the larger the network of nodes, the less likely it is for a single node to hold power over the network and engage in fraudulent transactions".[220] *Proof-of-work* consensus mechanism helps prevent the double-spend problem. The double-spend problem occurs when users spend the same units or cryptocurrencies in different places before the transactions are recorded on the system.[221] To prevent this, *proof-of-work* incentivises miners to verify the integrity of new transactions before adding them to a blockchain.[222] Other than bitcoin, the other cryptocurrencies that currently use the *proof-of-work* consensus mechanism include *dogecoin*, *bitcoin cash*, *Litecoin*, and *Monero*.[223]

There are various consensus mechanisms currently available. It is possible that, as time goes by, more consensus mechanisms will be developed. Here, I discuss a select few for purposes of completion. *Proof-of-Importance* is a mechanism where the network participants are chosen to add a block to the blockchain. One of the features of this mechanism is that the validators have a sufficient number of cryptocurrency before they take part in the process.[224] Proof-of-Elapsed-Time is a mechanism where each participating node must wait for a randomly chosen period of time. Once the time

[217] Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the technology behind bitcoin is changing money, business and the world* Portfolio Penguin at 31.

[218] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 23.

[219] Bains, P. (2022). "Blockchain Consensus Mechanisms: A Primer for Supervisors" *International Monetary Fund* at 8.

[220] Bains, P. (2022). "Blockchain Consensus Mechanisms: A Primer for Supervisors" *International Monetary Fund* at 9.

[221] Napoletano, E. & Curry, B. (2024). *Proof of work explained*. Available at https://www.forbes.com/advisor/investing/cryptocurrency/proof-of-work/. Accessed 9 June 2024.

[222] Napoletano, E. & Curry, B. (2024). *Proof of work explained*. Available at https://www.forbes.com/advisor/investing/cryptocurrency/proof-of-work/. Accessed 9 June 2024.

[223] Napoletano, E. & Curry, B. (2024). *Proof of work explained*. Available at https://www.forbes.com/advisor/investing/cryptocurrency/proof-of-work/. Accessed 9 June 2024.

[224] Adam, K. (2022). *Blockchain Technology for Business Processes: Meaningful use of the new technology in business* Springer Nature at 37.

has elapsed or when the first one to fulfil the specifies waiting time wins the new block.[225] *Proof-of-authority* is a mechanism where the validators are named and chosen by system authorities. A 'mining leader' proposes new blocks and the majority of the other authorities must confirm the new block before it is attached to the previous block.[226]

Due to the rigorous nature of formulating consensus on blockchain, it is difficult for users to alter the transactions recorded on blockchain.[227] In general, a single party on blockchain system cannot alter the transactions. In order for changes to occur, consensus is required from 51 per cent of the users on blockchain network.[228] However, it is possible to make changes to relax the 51 per cent rule.[229] According to Hertig, a blockchain can be programmed so that 95 per cent of users make changes to blockchain network.[230] This change is effected by making upgrades to blockchain software through a process called *soft fork*.[231] Changes made through a *soft fork* is backward compatible on blockchain network.[232] This simply means that the updated version can be compatible with the older version of blockchain system. Interestingly, a *soft fork* does not require all the nodes on blockchain system to be upgraded for the change to take effect.[233] This implies that a change can only be made on a single

[225] Adam, K. (2022). *Blockchain Technology for Business Processes: Meaningful use of the new technology in business* Springer Nature at 38.

[226] Adam, K. (2022). *Blockchain Technology for Business Processes: Meaningful use of the new technology in business* Springer Nature at 36.

[227] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 25.

[228] Werbach, K. (2018). *The Blockchain and the New Architecture of Trust* Massachusetts Institute of Technology Press (US) at 136. See also Kianieff, M. (2019) *Blockchain Technology and the Law Opportunities and Risks* Routledge Publishing (UK) at 105.

[229] Hertig, A., (2017). *Why Are Miners Involved in Bitcoin Code Changes Anyway?* Available at https://www.coindesk.com/miners-involved-bitcoin-code-changes-anyway. Accessed 17 December 2019. See also Kianieff, M. (2019) *Blockchain Technology and the Law Opportunities and Risks* Routledge Publishing (UK) at 105.

[230] Hertig, A., (2017). *Why Are Miners Involved in Bitcoin Code Changes Anyway?* Available at https://www.coindesk.com/miners-involved-bitcoin-code-changes-anyway. Accessed 17 December 2019. See also Kianieff, M. (2019) *Blockchain Technology and the Law Opportunities and Risks* Routledge Publishing (UK) at 105.

[231] Hertig, A., (2017). *Why Are Miners Involved in Bitcoin Code Changes Anyway?* Available at https://www.coindesk.com/miners-involved-bitcoin-code-changes-anyway. Accessed 17 December 2019. See also Kianieff, M. (2019) *Blockchain Technology and the Law Opportunities and Risks* Routledge Publishing (UK) at 104 – 105.

[232] Hertig, A., (2017). *Why Are Miners Involved in Bitcoin Code Changes Anyway?* Available at https://www.coindesk.com/miners-involved-bitcoin-code-changes-anyway. Accessed 17 December 2019. See also Kianieff, M. (2019) *Blockchain Technology and the Law Opportunities and Risks* Routledge Publishing (UK) at 104.

[233] Hertig, A., (2017). *Why Are Miners Involved in Bitcoin Code Changes Anyway?* Available at https://www.coindesk.com/miners-involved-bitcoin-code-changes-anyway. Accessed 17

computer node to effect a change to the entire blockchain system. With a *soft fork*, a blockchain's code can be modified to have any number of users reach consensus.[234]

It is important to highlight how transactions are recorded on blockchain. A sender creates a transaction and transmits it to the network. The transaction contains the recipient's public address, the value of the transaction, and a cryptographic digital signature that authenticates the transaction.[235] The nodes receive a message and authenticate and validate it by decrypting the digital signature. Then, the transaction is placed in pool of pending transactions.[236] The transactions are then placed in a block by one of the nodes. Thereafter, the validator nodes receive the block and valid it by using the respective consensus mechanism.[237] Once all the transactions have been validated, the new block is chained to the current blockchain, and the new state of the ledger is transmitted to the network.[238]

December 2019. See also Kianieff, M. (2019) *Blockchain Technology and the Law Opportunities and Risks* Routledge Publishing (UK) at 105.

[234] Hertig, A., (2017). *Why Are Miners Involved in Bitcoin Code Changes Anyway?* Available at https://www.coindesk.com/miners-involved-bitcoin-code-changes-anyway. Accessed 17 December 2019. See also Kianieff, M. (2019) *Blockchain Technology and the Law Opportunities and Risks* Routledge Publishing (UK) at 105.

[235] Frøstad, P. & Holm, J. (2015). "Blockchain: Powering the Internet of Value" *White Paper Evry Labs* at 11. Available at https://blockchainlab.com/pdf/bank-2020---blockchain-powering-the-internet-of-value---whitepaper.pdf. Accessed 25 June 2024; Adam, K. (2022). *Blockchain Technology for Business Processes: Meaningful use of the new technology in business* Springer Nature at 26.

[236] Frøstad, P. & Holm, J. (2015). "Blockchain: Powering the Internet of Value" *White Paper Evry Labs* at 11. Available at https://blockchainlab.com/pdf/bank-2020---blockchain-powering-the-internet-of-value---whitepaper.pdf. Accessed 25 June 2024; Adam, K. (2022). *Blockchain Technology for Business Processes: Meaningful use of the new technology in business* Springer Nature at 26.

[237] Frøstad, P. & Holm, J. (2015). "Blockchain: Powering the Internet of Value" *White Paper Evry Labs* at 11. Available at https://blockchainlab.com/pdf/bank-2020---blockchain-powering-the-internet-of-value---whitepaper.pdf. Accessed 25 June 2024; Adam, K. (2022). *Blockchain Technology for Business Processes: Meaningful use of the new technology in business* Springer Nature at 26 – 27.

[238] Frøstad, P. & Holm, J. (2015). "Blockchain: Powering the Internet of Value" *White Paper Evry Labs* at 11. Available at https://blockchainlab.com/pdf/bank-2020---blockchain-powering-the-internet-of-value---whitepaper.pdf. Accessed 25 June 2024; Adam, K. (2022). *Blockchain Technology for Business Processes: Meaningful use of the new technology in business* Springer Nature at 26 – 27.

2.5.3 Decentralisation and disintermediation

Blockchain systems are decentralised peer-to-peer technology that do not require the use of intermediaries.[239] The use of an intermediary or central entity has been made redundant because blockchain system does not require a central entity for governance.[240] According to Werbach, systems are often decentralised because of practical restrictions as opposed to government interference.[241] While this may be factual, it is submitted that the inception of Bitcoin as a payment system was to limit intrusion and control from the government. In practical terms, no single authority, including the government, can 'shut down' blockchain system.[242] If a single node malfunctions or is hacked, the ledger can be accessed on the other nodes on blockchain system.[243] Access on the nodes is subject to having on an Internet connection and a PC.[244]

Due to its decentralised nature, blockchain system can operate across multiple jurisdictions. Due to the feasibility of cross-border blockchain application, international cooperation will be required.[245] For this reason, countries may have to enter into international agreements to facilitate cooperation and coordination for the use of blockchain technology at a global scale.

[239] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 60. See also Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the technology behind bitcoin is changing money, business and the world* Portfolio Penguin at 35.

[240] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 34. See also Werbach, K. (2018). *The Blockchain and the New Architecture of Trust* Massachusetts Institute of Technology Press (US) at 74. Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the technology behind bitcoin is changing money, business and the world* Portfolio Penguin at 33; Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 29; Bal, A. (2018). "Does the Tax Sector Need Blockchain?" *White Paper IBFD* at 6.

[241] Werbach, K. (2018). *The Blockchain and the New Architecture of Trust* Massachusetts Institute of Technology Press (US) at 76.

[242] Vigna, P., & Casey, M., J. (2016). *The Age of Cryptocurrency: How Bitcoin and the Blockchain are Challenging the Global Economic order* Picador USA at 253.

[243] Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the technology behind bitcoin is changing money, business and the world* Portfolio Penguin at 33.

[244] Werbach, K. (2018). *The Blockchain and the New Architecture of Trust* Massachusetts Institute of Technology Press (US) at 77.

[245] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 59 – 60.

Bal questions whether there is a need for disintermediation in the tax sector.[246] Bal notes that there is nothing wrong with having a trusted intermediary, like a tax administrator, manage and verify the correctness of tax information.[247] In a private blockchain,[248] an arrangement can be made to ensure that a tax authority manages and verifies the accuracy of tax information. Moreover, the tax administrator can solely retain the rights to these functions. The taxpayers (suppliers) merely use blockchain to record their supplies. For this reason, I agree with Bal that a tax administrator is essential for the effective administration of taxes.

2.5.4 Immutability

When transactions are recorded on blockchain, they cannot be altered.[249] The immutability feature creates permanency and unalterable records.[250] This ensures that information is not susceptible to unauthorised modifications.[251] Blockchain immutability is beneficial for tax authorities because taxpayer records can be accessed at any time.[252] Consider the following example:

Example 2:

Party A in country C can use blockchain as an entry to store information about e-commerce transactions. **Party B** in country Q can access those records in real time.

In the example above, even if Party A deletes all the entries made from its node, Party B can still access those entries at any time. Party A cannot unilaterally alter the

[246] Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 29; Bal, A. (2018). "Does the Tax Sector Need Blockchain?" *White Paper IBFD* at 6.
[247] Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 29; Bal, A. (2018). "Does the Tax Sector Need Blockchain?" *White Paper IBFD* at 6.
[248] See discussion in paragraph 2.7.2 below.
[249] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 30. De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 35. Kianieff, M. (2019) *Blockchain Technology and the Law Opportunities and Risks* Routledge Publishing (UK) at 8. Werbach, K. (2018). *The Blockchain and the New Architecture of Trust* Massachusetts Institute of Technology Press (US) at 101.
[250] Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 30; Bal, A. (2018). "Does the Tax Sector Need Blockchain?" *White Paper IBFD* at 7.
[251] Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 30; Bal, A. (2018). "Does the Tax Sector Need Blockchain?" *White Paper IBFD* at 7.
[252] See discussion in chapter 3.

information on blockchain system.[253] Once an entry has been made on blockchain system, that entry is duplicated on every node on blockchain system irrespective of the location or jurisdiction of the node.[254]

In a public blockchain[255] where multiple parties exist, the destruction or loss of one node on the system does not result in the loss of data on the entire blockchain system.[256] In fact, the remaining parties on the system can retrieve the information provided they have access to the Internet.[257] The party that lost its node for whatever reason, can re-access blockchain system once they have an Internet connection. That party can then proceed to update the entries that were previously inaccessible.[258]

Since information stored on blockchain cannot be changed so easily, a party can consistently audit and track the original source of a transaction.[259] This aspect is particularly useful for tax authorities because information relating to a specific transaction can be retrieved at any time. Furthermore, tax authorities can rely on the information displayed on blockchain system because information cannot be altered[260] without the knowledge of all the relevant parties.[261]

[253] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 35.

[254] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 35. See also Hacker, P., Lianos, L., Dimitropoulos, G., Eich, S., (eds) (2019) *Regulating Blockchain: Techno-social and Legal challenges* Oxford University Press (UK) at 4.

[255] See discussion under paragraph 2.7.1 below.

[256] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 36. See also Hacker, P., Lianos, L., Dimitropoulos, G., Eich, S., (eds) (2019) *Regulating Blockchain: Techno-social and Legal challenges* Oxford University Press (UK) at 4.

[257] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 36.

[258] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 36.

[259] Kianieff, M. (2019) *Blockchain Technology and the Law Opportunities and Risks* Routledge Publishing (UK) at 8.

[260] Bal notes that the immutable feature can be detrimental for tax purposes because a situation may arise where tax related corrections need to be made. Due to blockchain's immutability, changes cannot be effected retroactively, especially in a public blockchain. See Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 30; Bal, A. (2018). "Does the Tax Sector Need Blockchain?" *White Paper IBFD* at 7.

[261] Kianieff, M. (2019) *Blockchain Technology and the Law Opportunities and Risks* Routledge Publishing (UK) at 8.

Bal argues that blockchains are not perfectly immutable.[262] In a public blockchain, if a certain amount of participants decide to rebel against the system rules, they cannot be stopped.[263] If 51 per cent[264] of the participants control the majority of a blockchain network's mining power, they can control the whole blockchain network.[265]

2.5.5 Transparency

Another important characteristic of blockchain system is transparency. Simply put, a party on the public blockchain can access and validate the extent and nature of a transaction.[266] Transparency enables a person to establish the source of the transaction and the location where the transaction was conveyed.[267] Importantly, obtaining the location and the source of the transaction creates trust between the parties on blockchain system.[268]

The transparency aspect of transactions also creates accountability. Parties' information becomes openly accessible making it possible for other parties to verify and audit the authenticity of the information.[269] Since information on blockchain cannot be altered, parties are always compelled to provide accurate information which can reduce fraud.

[262] Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 29; Bal, A. (2018). "Does the Tax Sector Need Blockchain?" *White Paper IBFD* at 6.

[263] Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 29; Bal, A. (2018). "Does the Tax Sector Need Blockchain?" *White Paper IBFD* at 6.

[264] This is commonly referred to as a 51 per cent attack. See De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 25; See Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 29; Bal, A. (2018). "Does the Tax Sector Need Blockchain?" *White Paper IBFD* at 6.

[265] Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 29; Bal, A. (2018). "Does the Tax Sector Need Blockchain?" *White Paper IBFD* at 6.

[266] Hacker, P., Lianos, L., Dimitropoulos, G., Eich, S., (eds) (2019) *Regulating Blockchain: Techno-social and Legal challenges* Oxford University Press (UK) at 335. De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 37; Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 28.

[267] Hacker, P., Lianos, L., Dimitropoulos, G., Eich, S., (eds) (2019) *Regulating Blockchain: Techno-social and Legal challenges* Oxford University Press (UK) at 335. De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 38.

[268] Hacker, P., Lianos, L., Dimitropoulos, G., Eich, S., (eds) (2019) *Regulating Blockchain: Techno-social and Legal challenges* Oxford University Press (UK) at 335. De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 37 – 38.

[269] Kianieff, M. (2019) *Blockchain Technology and the Law Opportunities and Risks* Routledge Publishing (UK) at 7.

Bal opines that a blockchain's transparent feature can have positive and negative effects.[270] Transparency allows persons to verify their functionality and gain the trust of other users.[271] The downside to having a transparent blockchain is that people can identify errors and vulnerabilities in blockchain code.[272] In chapter 4, I discuss the issue of transparency of a blockchain from a South African perspective.

2.5.6 Pseudonymous

Transactions on blockchain are pseudonymous in nature. Parties on blockchain network can perform transactions without necessarily revealing their true identities.[273] This is made possible through cryptography, allowing users to make use of a public key infrastructure (PKI).[274] Finck defines PKI as:

> "a means of authenticating identities in order to identify the parties associated with each transaction in a pseudonymous manner."[275]

The 'means' that Finck is referring to in the definition above is the private and public keys. These two keys execute different functions: the public key is used to encrypt data while the private key is used to decrypt data.[276] A public key works like an

[270] See Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 28; Bal, A. (2018). "Does the Tax Sector Need Blockchain?" *White Paper IBFD* at 5.

[271] See Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 28; Bal, A. (2018). "Does the Tax Sector Need Blockchain?" *White Paper IBFD* at 5.

[272] See Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 28; Bal, A. (2018). "Does the Tax Sector Need Blockchain?" *White Paper IBFD* at 5.

[273] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 38.

[274] Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the technology behind bitcoin is changing money, business and the world* Portfolio Penguin at 39. Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 28 – 30. See De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 14 – 16 & 38 – 39.

[275] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 28. See also Bacon, J., *et al* (2017). "Blockchain Demystified" *Queen Mary University of London, School of Law Legal Studies Research Paper No. 268/2017* at 9. Available https://papers.ssrn.com/sol3/papers.cfm?Abstract_id=3091218. Accessed 5 January 2020.

[276] Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the technology behind bitcoin is changing money, business and the world* Portfolio Penguin at 39. Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 28. See also Bacon, J., *et al* (2017). "Blockchain Demystified" *Queen Mary University of London, School of Law Legal Studies Research Paper No. 268/2017* at 9. Available https://papers.ssrn.com/sol3/papers.cfm?Abstract_id=3091218. Accessed 5 January 2020.

individual's 'address'[277] consisting of numbers and letters ranging between 26 and 34 characters.[278] Before sending data to another person, a private key is exclusively generated to a particular address. A private key is identical to a passcode.[279] Once the public key and private key are combined through a mathematical process, they form what is known as a digital signature.[280] The recipient of the data transmission can use the sender's public key to verify that the data originated from the sender.[281] This feature makes transactions on blockchain highly secure.[282] See **Figure 2** below.

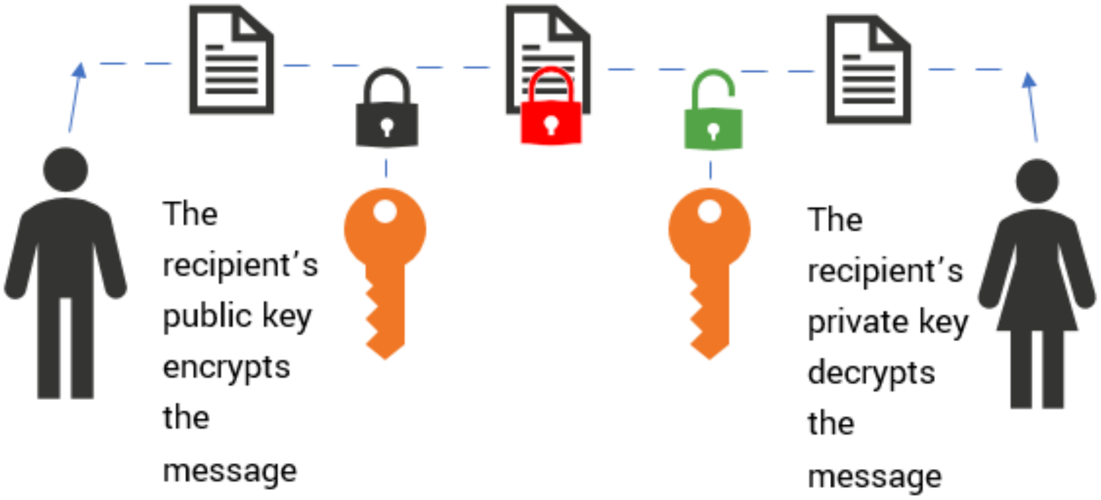

The recipient's public key encrypts the message
The recipient's private key decrypts the message

Figure 2[283]

[277] The reason why a public key can be used as an 'address' is because a public key can be shared with anyone. See Vigna, P., & Casey, M., J. (2016). *The Age of Cryptocurrency: How Bitcoin and the Blockchain are Challenging the Global Economic order* Picador USA at 125.

[278] Vigna, P., & Casey, M., J. (2016). *The Age of Cryptocurrency: How Bitcoin and the Blockchain are Challenging the Global Economic order* Picador USA at 125.

[279] Vigna, P., & Casey, M., J. (2016). *The Age of Cryptocurrency: How Bitcoin and the Blockchain are Challenging the Global Economic order* Picador USA at 125.

[280] Vigna, P., & Casey, M., J. (2016). *The Age of Cryptocurrency: How Bitcoin and the Blockchain are Challenging the Global Economic order* Picador USA at 125 – 126. See also Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 28 – 29. Bacon, J., *et al* (2017). "Blockchain Demystified" *Queen Mary University of London, School of Law Legal Studies Research Paper No. 268/2017* at 9. Available https://papers.ssrn.com/sol3/papers.cfm?Abstract_id=3091218. Accessed 5 January 2020.

[281] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 28 – 29. See also De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 14 – 16.

[282] Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the technology behind bitcoin is changing money, business and the world* Portfolio Penguin at 39 – 41.

[283] **Figure 2** illustrates how a private and public key work. **Figure 2** source from RapidSSonline. Available at https://www.rapidsslonline.com/ssl/difference-between-public-and-private-key/. Accessed 5 January 2020.

In addition to the private and public key, blockchain makes use of a hash function. A hash function is a string of alpha numerals that maintain the reliability of data on blockchain.[284] The use of a hash function makes the data on blockchain secure and tamper evident.[285] A hash function can demonstrate that a person had a specific document.[286]

I discussed the characteristics of blockchain system. What follows are the types of blockchains. Distinctions are drawn between the various types of blockchains to ascertain the most appropriate blockchain for VAT collection purposes.

2.6 Types of blockchain

2.6.1 Public blockchains

Public blockchains, as the name suggests, are available to the public and any person can obtain access to that blockchain provided they have an Internet connection.[287] Generally, public blockchains are permissionless, non-restrictive and distributed allowing anyone to join the network.[288] Since a person can obtain access without any form of approval from a central authority, public blockchains are sometimes known as

[284] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 7, 29. See also Kianieff, M. (2019) *Blockchain Technology and the Law Opportunities and Risks* Routledge Publishing (UK) at 11; Artzt, M., (ed) Determann, L., Long, W., *Blockchain and Data Privacy* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 197.

[285] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 7, 29. Bacon, J., *et al* (2017). "Blockchain Demystified" *Queen Mary University of London, School of Law Legal Studies Research Paper No. 268/2017* at 4, 6 – 7. Available https://papers.ssrn.com/sol3/papers.cfm?Abstract_id=3091218. Accessed 5 January 2020. Vigna, P., & Casey, M., J. (2016). *The Age of Cryptocurrency: How Bitcoin and the Blockchain are Challenging the Global Economic order* Picador USA at 128 – 129. Kianieff, M. (2019) *Blockchain Technology and the Law Opportunities and Risks* Routledge Publishing (UK) at 11.

[286] Werbach, K. (2018). *The Blockchain and the New Architecture of Trust* Massachusetts Institute of Technology Press (US) at 155.

[287] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 31. See also Hacker, P., Lianos, L., Dimitropoulos, G., Eich, S., (eds) (2019) *Regulating Blockchain: Techno-social and Legal challenges* Oxford University Press (UK) at 335; Herian, R., (2019). *Regulating Blockchain: Critical perspectives in law and technology* Routledge publishing at 14.

[288] Sharma, T. K. (2024). *Types of blockchains explained – public vs private vs consortium*. Available at https://www.blockchain-council.org/blockchain/types-of-blockchains-explained-public-vs-private-vs-consortium/. Accessed 9 June 2024.

'permissionless' blockchains.[289] See **Figure 3** below. Examples of public blockchains include *Ethereum*, *Bitcoin*, *Solana* and *Avalanche*.[290] Due to its openness and unrestricted access, the use of public blockchains for the exchange and storage of sensitive information (like a taxpayers' information) is unsuitable because of privacy concerns.[291]

In addition to decentralisation, transparency, and immutability, public blockchains open access nature encourages interoperability and collaboration across different platforms and applications.[292] The unrestricted access of public blockchains can promote innovation and a wider range of use cases.[293] Public blockchains also support the creation of tokens. The openness of public blockchains allows for the development of different assets on a blockchain.[294] Security on a public blockchain is managed by using consensus mechanisms. The consensus mechanisms make it difficult for malicious or unauthorised parties to alter the transactions on the network or

[289] This aspect relates to whether private or public blockchain may be joined freely, without the specific decision of admission (permissionless) or if a dedicated admission is applied (permissioned). See Richter, T., *Blockchain Regulation* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 127.

[290] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 31. See also Hacker, P., Lianos, L., Dimitropoulos, G., Eich, S., (eds) (2019) *Regulating Blockchain: Techno-social and Legal challenges* Oxford University Press (UK) at 335; Sharma, T. K. (2024). *Types of blockchains explained – public vs private vs consortium*. Available at https://www.blockchain-council.org/blockchain/types-of-blockchains-explained-public-vs-private-vs-consortium/. Accessed 9 June 2024.

[291] See Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 28. From a South African perspective, it is not prudent to use a public blockchain due to issues around privacy. See also discussion in chapter 4.

[292] Sharma, T. K. (2024). *Types of blockchains explained – public vs private vs consortium*. Available at https://www.blockchain-council.org/blockchain/types-of-blockchains-explained-public-vs-private-vs-consortium/. Accessed 9 June 2024.

[293] Sharma, T. K. (2024). *Types of blockchains explained – public vs private vs consortium*. Available at https://www.blockchain-council.org/blockchain/types-of-blockchains-explained-public-vs-private-vs-consortium/. Accessed 9 June 2024.

[294] Sharma, T. K. (2024). *Types of blockchains explained – public vs private vs consortium*. Available at https://www.blockchain-council.org/blockchain/types-of-blockchains-explained-public-vs-private-vs-consortium/. Accessed 9 June 2024.

compromise network security.[295] Currently, public blockchains use *proof-of-work*, *proof-of-stake*,[296] and *delegated proof-of-stake*[297] as consensus mechanisms.[298]

One of the challenges associated with using public blockchains is the apparent difficulty in its regulation.[299] This can be attributed to the extended reach that a decentralised blockchain possesses.[300] In simple terms, it is unrealistic to establish the identity and location of every person who accesses the open public peer-to-peer network.[301] These regulatory challenges can lead to legal uncertainty, which in turn, impede global acceptance and adoption.[302]

However, it is beneficial to use a public blockchain because of its network safety features.[303] These include digital certificates, PKI, and cryptography.[304] A single individual attempting to hack the network will require significant amounts of

[295] Sharma, T. K. (2024). *Types of blockchains explained – public vs private vs consortium*. Available at https://www.blockchain-council.org/blockchain/types-of-blockchains-explained-public-vs-private-vs-consortium/. Accessed 9 June 2024.

[296] *Proof-of-stake* is a consensus mechanism where "senior participants with higher stakes (more crypto coins) validate transactions assuming their intrinsic interest in the integrity of the network for the sake of their stakes". See Richter, T., *Blockchain Regulation* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 129; see also Bains, P. (2022). "Blockchain Consensus Mechanisms: A Primer for Supervisors" *International Monetary Fund* at 10.

[297] According to Bains, a *delegated proof-of-stake* is mechanism that "operates a voting system where the stakeholders chosen to validate a block can outsource their work to third party. These third parties are known as 'witnesses' and are responsible for achieving consensus during the generation and validation of new blocks. Rewards are shared between the witnesses and the stakeholders." See Bains, P. (2022). "Blockchain Consensus Mechanisms: A Primer for Supervisors" *International Monetary Fund* at 12.

[298] See Bains, P. (2022). "Blockchain Consensus Mechanisms: A Primer for Supervisors" *International Monetary Fund* at 8.

[299] Hacker, P., Lianos, L., Dimitropoulos, G., Eich, S., (eds) (2019) *Regulating Blockchain: Techno-social and Legal challenges* Oxford University Press (UK) at 31; Sharma, T. K. (2024). *Types of blockchains explained – public vs private vs consortium*. Available at https://www.blockchain-council.org/blockchain/types-of-blockchains-explained-public-vs-private-vs-consortium/. Accessed 9 June 2024.

[300] Hacker, P., Lianos, L., Dimitropoulos, G., Eich, S., (eds) (2019) *Regulating Blockchain: Techno-social and Legal challenges* Oxford University Press (UK) at 31.

[301] It is unrealistic from the perspective of SARS to identify all the participants on a public permissionless blockchain. This could hamper the VAT administration process.

[302] Sharma, T. K. (2024). *Types of blockchains explained – public vs private vs consortium*. Available at https://www.blockchain-council.org/blockchain/types-of-blockchains-explained-public-vs-private-vs-consortium/. Accessed 9 June 2024.

[303] Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the technology behind bitcoin is changing money, business and the world* Portfolio Penguin at 39.

[304] Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 11. See also Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the technology behind bitcoin is changing money, business and the world* Portfolio Penguin at 39 – 41.

computational power. Even if a person succeeds by hacking the system through a single node, other nodes maintain the same copy of the entire ledger. As a result, information is not lost. Another concern related to the use of public blockchains is the lack of governance structures.[305] The decision-making processes and protocol upgrades may be disputed by the members on the network, which can lead to forks and division.[306] Generally public blockchains struggle to handle several transactions resulting in slower processing times and higher fees during network congestion.[307] Despite this, it should be noted that *Solana* blockchain is currently the fastest blockchain with a record of 91 million transactions processed in a single day.[308] According to Senga, this translates to an average rate of 1500 crypto transactions per second (TSP).[309] From a blockchain perspective, transaction speed "refers to the amount of time it takes for a transaction to be processed and recorded on a blockchain network".[310] In other words, transaction speed determines how quickly a transaction can be completed from the moment it is instigated by the sender to the moment it is confirmed on a blockchain.[311] According to Lalav, there are several factors that influence the transaction speed on a blockchain. These include the size of the transaction, the fee attached to the transaction, and network congestion.[312] Furthermore, Lalav opines that a favourable transaction speed provides better user

[305] Sharma, T. K. (2024). *Types of blockchains explained – public vs private vs consortium*. Available at https://www.blockchain-council.org/blockchain/types-of-blockchains-explained-public-vs-private-vs-consortium/. Accessed 9 June 2024.

[306] Sharma, T. K. (2024). *Types of blockchains explained – public vs private vs consortium*. Available at https://www.blockchain-council.org/blockchain/types-of-blockchains-explained-public-vs-private-vs-consortium/. Accessed 9 June 2024.

[307] Sharma, T. K. (2024). *Types of blockchains explained – public vs private vs consortium*. Available at https://www.blockchain-council.org/blockchain/types-of-blockchains-explained-public-vs-private-vs-consortium/. Accessed 9 June 2024.

[308] Senga, E. (2024). *Crypto: here is the fastest blockchain in the world!* Available at https://www.cointribune.com/en/crypto-here-is-the-fastest-blockchain-in-the-world/#:~:text=Solana%20stands%20out%20as%20the,5%20times%20faster%20than%20Polygon. Accessed 9 June 2024.

[309] Senga, E. (2024). *Crypto: here is the fastest blockchain in the world!* Available at https://www.cointribune.com/en/crypto-here-is-the-fastest-blockchain-in-the-world/#:~:text=Solana%20stands%20out%20as%20the,5%20times%20faster%20than%20Polygon. Accessed 9 June 2024.

[310] Lalav, R. (2023). *Blockchain with the highest transaction speed*. Available at https://bitpowr.com/blog/blockchains-with-the-highest-transaction-speeds. Accessed 9 June 2024.

[311] Lalav, R. (2023). *Blockchain with the highest transaction speed*. Available at https://bitpowr.com/blog/blockchains-with-the-highest-transaction-speeds. Accessed 9 June 2024.

[312] Lalav, R. (2023). *Blockchain with the highest transaction speed*. Available at https://bitpowr.com/blog/blockchains-with-the-highest-transaction-speeds. Accessed 9 June 2024.

experience and allows for a wider range of use cases for blockchain technology. As a result, Lalav notes that it is important to strike a balance between security and speed, as a faster transaction speed may come at the cost of decreased security.[313]

2.6.2 Private blockchains[314]

A private blockchain is a type of blockchain that is administered by a central authority.[315] A central authority has control of the flow of data stored on blockchain system.[316] The central authority can permit certain entities to join blockchain system at any given time. The central authority can also limit access to a selected number of participants.[317] Parties on the private blockchain are responsible for adding blocks and authenticating transactions on blockchain system.[318] The limited access to participants on the network implies that private blockchains are not open to the public. For these reasons, a private blockchain is often known as a 'permissioned' blockchain.[319] One of the most important differences between a private and a public blockchain is that the latter is highly accessible while the former is confined to a group of entities or persons.[320] Private blockchains are highly centralised because a single authority is

[313] Lalav, R. (2023). *Blockchain with the highest transaction speed*. Available at https://bitpowr.com/blog/blockchains-with-the-highest-transaction-speeds. Accessed 9 June 2024.

[314] Compare paragraph 3.3 where I discuss the suitability of private blockchains as a VAT collection tool for South Africa.

[315] In a public blockchain, anyone can gain access to the network. From SARS' perspective, this is not ideal because of privacy issues. If anyone gains access to the network, then taxpayer confidentiality can be breached. A private blockchain is optimal due to policy and privacy considerations. See also discussion in chapter 4.

[316] Hacker, P., Lianos, L., Dimitropoulos, G., Eich, S., (eds) (2019) *Regulating Blockchain: Techno-social and Legal challenges* Oxford University Press (UK) at 16, 334.

[317] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 31.

[318] Hacker, P., Lianos, L., Dimitropoulos, G., Eich, S., (eds) (2019) *Regulating Blockchain: Techno-social and Legal challenges* Oxford University Press (UK) at 334; De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 31.

[319] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 31; Kianieff, M. (2019) *Blockchain Technology and the Law Opportunities and Risks* Routledge Publishing (UK) at 36; Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the technology behind bitcoin is changing money, business and the world* Portfolio Penguin at 67; Herian, R., (2019). *Regulating Blockchain: Critical perspectives in law and technology* Routledge publishing at 14.

[320] Sharma, T. K. (2024). *Types of blockchains explained – public vs private vs consortium*. Available at https://www.blockchain-council.org/blockchain/types-of-blockchains-explained-public-vs-private-vs-consortium/. Accessed 9 June 2024.

responsible for managing the network.[321] Examples of private blockchains include *Hyperledger Sawtooth*, *Hyperledger Fabric*, *IBM*, and *R3 Corda*.[322]

Type of blockchain	Admission model	Operated by	Certain legal key considerations
Public	Permissionless	All nodes and miners (no control)	Focus on how legal compliance can be achieved without a responsible party
Public	Permissioned	All nodes and miners (no control), permission process (partially) controlled by coders/initiators/third parties/oracle	Focus on how legal compliance can be ensured through design of the code and the permission process allows to introduce terms and conditions (T&Cs) between participants, but difficulties in surveillance of adherence to the T&Cs
Private	Permissionless	Specified operator retaining control over writing transactions, but open to anyone for reading considerations	Focus on legal implications of ledger being readable by anyone
Private	Permissioned	Specified operator retaining control over reading and writing transactions; may be fully or partially private network	Focus on the T&Cs that are agreed between the participants

[321] Sharma, T. K. (2024). *Types of blockchains explained – public vs private vs consortium*. Available at https://www.blockchain-council.org/blockchain/types-of-blockchains-explained-public-vs-private-vs-consortium/. Accessed 9 June 2024.

[322] Sharma, T. K. (2024). *Types of blockchains explained – public vs private vs consortium*. Available at https://www.blockchain-council.org/blockchain/types-of-blockchains-explained-public-vs-private-vs-consortium/. Accessed 9 June 2024.

Figure 3[323]

One of the benefits of a private blockchain is the ability to establish the identities of the participants beforehand.[324] By allowing access to the network, a central authority can confirm the identity of the participants. If the identity of the participants is known, trust can be built.[325] This view is not shared by De Filippi and Wright who argue that trust in a private blockchain is volatile because participants may elect to conspire with others to interfere with and undermine blockchain system.[326] It should be noted that a blockchain system can be compromised if a certain number of conspirators[327] decide to undermine the system. That is to say, the private blockchain can be at risk if most of the participants decide to collude together. Collusion can lead to manipulative practices or biased decision-making in a blockchain network.[328] For instance, if there are a total of ten participants on a private blockchain and six participants decide to make changes to the infrastructure of the network, changes can be made. For this reason, Bal submits that immutability is not absolute in private blockchains.[329] According to Bal, a private blockchain's immutability depends on the behaviour and reliability of the participants.[330] A counter argument is to decrease the number of participants on the network, thereby minimising the chances of collusion.[331]

[323] **Figure 3** courtesy of Richter, T., *Blockchain Regulation* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 129.

[324] Kianieff, M. (2019) *Blockchain Technology and the Law Opportunities and Risks* Routledge Publishing (UK) at 37.

[325] In contrast, a public blockchain is not suitable from a tax authority perspective because anyone can access the blockchain. It will be difficult for tax authorities to identify all the persons on the public blockchain. From a taxpayer perspective, it is not in the public interest for every person to access a blockchain where sensitive information is stored.

[326] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 32.

[327] This can be 51 per cent of the participants.

[328] Sharma, T. K. (2024). *Types of blockchains explained – public vs private vs consortium*. Available at https://www.blockchain-council.org/blockchain/types-of-blockchains-explained-public-vs-private-vs-consortium/. Accessed 9 June 2024.

[329] Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 29; Bal, A. (2018). "Does the Tax Sector Need Blockchain?" *White Paper IBFD* at 6. In the absence of academic text discrediting Bal, statement must be considered correct. Additionally, there are projects in place to make blockchain editable. See chapter 4.

[330] Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 29; Bal, A. (2018). "Does the Tax Sector Need Blockchain?" *White Paper IBFD* at 6.

[331] Buterin, V., (2015). "*On Public and Private Blockchains*". Available at https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/. Accessed 8 January 2020.

While the possibility of collusion can materialise, it does not entirely negate the benefits that come with use of a private blockchain. While some authors argue that transactions on a private blockchain are quicker than on a public blockchain,[332] this is not entirely correct because public blockchains have proven to be faster.[333] The underlying reason why some authors argue that private blockchains are faster may be attributed to the reduced number of participants that are required in order to reach consensus on a private blockchain.[334] According to De Filippi and Wright, it can take up to ten minutes for a transaction to be processed on a public blockchain.[335] With a private blockchain, that number can be reduced significantly due to the reduced number of participants on the network.[336] Bal notes that a consensus mechanism such as *proof-of-work* or *proof-of-stake* are unnecessary in a private blockchain because these are complicated and expensive since blocks are created by identified parties.[337] However, it should be noted that the consensus mechanisms used on a private blockchain differ to those on a public blockchain. Currently, the consensus mechanisms used in a private blockchain include *proof-of-authority*,[338] *proof-of-*

[332] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 31 – 32; Buterin, V., (2015). "*On Public and Private Blockchains*". Available at https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/. Accessed 8 January 2020; Kianieff, M. (2019) *Blockchain Technology and the Law Opportunities and Risks* Routledge Publishing (UK) at 37; Bacon, J., *et al* (2017). "Blockchain Demystified" *Queen Mary University of London, School of Law Legal Studies Research Paper No. 268/2017* at 21. Available https://papers.ssrn.com/sol3/papers.cfm?Abstract_id=3091218. Accessed 5 January 2020; see also Blockchain Smart Solutions (2023). *Public vs Private Blockchains: Which one id the best for your business?* Available at https://www.linkedin.com/pulse/public-vs-private-blockchains-which-one-best#:~:text=Transaction%20speed%3A,limited%20number%20of%20authorized%20entities. Accessed 4 October 2023.

[333] See Lalav, R. (2023). *Blockchain with the highest transaction speed*. Available at https://bitpowr.com/blog/blockchains-with-the-highest-transaction-speeds. Accessed 9 June 2024; Senga, E. (2024). *Crypto: here is the fastest blockchain in the world!* Available at https://www.cointribune.com/en/crypto-here-is-the-fastest-blockchain-in-the-world/#:~:text=Solana%20stands%20out%20as%20the,5%20times%20faster%20than%20Polygon. Accessed 9 June 2024.

[334] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 31.

[335] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 31.

[336] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 31.

[337] Bal, A. (2018). "Does the Tax Sector Need Blockchain?" *White Paper IBFD* at 3.

[338] *Proof-of-authority* is a consensus mechanism that uses identity as the sole verification of the authority to validate. Here, no mining is required. See Batmunkh, D. (2018). *Private blockchain consensus mechanisms*. Available at https://medium.com/@arigatodl/private-blockchain-consensus-mechanisms-8e6fc48c8fb. Accessed 10 June 2024.

elapsed time,[339] *proof-of-importance*,[340] *practical byzantine fault tolerance*,[341] *federated byzantine agreement*,[342] and *Raft*.[343]

Even if a central authority in a private blockchain controls the participants on the network, the integrity of the data must be assured.[344] To reach consensus in a private blockchain, transactions are added to the network by the relevant users. Thereafter, the pre-selected validators verify the transactions to ensure that they are accurate.[345] Once verified, the transactions are compiled into blocks and a group of validators agree by a "supermajority" on the order of the transactions to reach consensus regarding a blockchain.[346] The benefit of using pre-approved validators in a private

[339] *Proof-of-elapsed time* is a consensus mechanism that enables each participating node in the network to wait for a randomly chose time period, and the first one to complete the designed waiting time wins the new block. See Batmunkh, D. (2018). *Private blockchain consensus mechanisms*. Available at https://medium.com/@arigatodl/private-blockchain-consensus-mechanisms-8e6fc48c8fb. Accessed 10 June 2024; see also Bains, P. (2022). "Blockchain Consensus Mechanisms: A Primer for Supervisors" *International Monetary Fund* at 16.

[340] *Proof-of-importance* is a consensus mechanism that allows accounts with a higher importance score will have a higher probability of being chosen to create a block. See Batmunkh, D. (2018). *Private blockchain consensus mechanisms*. Available at https://medium.com/@arigatodl/private-blockchain-consensus-mechanisms-8e6fc48c8fb. Accessed 10 June 2024.

[341] Practical byzantine fault tolerance is a consensus mechanism where all the nodes are ordered in a sequence with one node being the primary node and the others referred to as the backup nodes. See Batmunkh, D. (2018). *Private blockchain consensus mechanisms*. Available at https://medium.com/@arigatodl/private-blockchain-consensus-mechanisms-8e6fc48c8fb. Accessed 10 June 2024.

[342] In a *federated byzantine agreement*, each node does not have to be known and verified ahead of time. Here, membership is open, and control of the network is decentralised. See Batmunkh, D. (2018). *Private blockchain consensus mechanisms*. Available at https://medium.com/@arigatodl/private-blockchain-consensus-mechanisms-8e6fc48c8fb. Accessed 10 June 2024.

[343] Batmunkh, D. (2018). *Private blockchain consensus mechanisms*. Available at https://medium.com/@arigatodl/private-blockchain-consensus-mechanisms-8e6fc48c8fb. Accessed 10 June 2024; Bains, P. (2022). "Blockchain Consensus Mechanisms: A Primer for Supervisors" *International Monetary Fund* at 12. Batmunkh explains the Raft consensus mechanism as follows: "there are three roles, leader (only 1), follower (others) and a candidate (intermediate status). Time is divided into terms of arbitrary length. Terms are numbered with consecutive integers starting from 0. Each term begins with an election, the winner becomes a leader and will make block and send to followers. In order to avoid split vote, election timeouts are chosen randomly from a fixed interval." See Batmunkh, D. (2018). *Private blockchain consensus mechanisms*. Available at https://medium.com/@arigatodl/private-blockchain-consensus-mechanisms-8e6fc48c8fb. Accessed 10 June 2024.

[344] Vashishtha, G. (2023). *Consensus mechanism for permissioned blockchain protocols*. Available at https://www.zeeve.io/blog/consensus-mechanisms-for-permissioned-blockchain-protocols/. Accessed 10 June 2024.

[345] Vashishtha, G. (2023). *Consensus mechanism for permissioned blockchain protocols*. Available at https://www.zeeve.io/blog/consensus-mechanisms-for-permissioned-blockchain-protocols/. Accessed 10 June 2024.

[346] Vashishtha, G. (2023). *Consensus mechanism for permissioned blockchain protocols*. Available at https://www.zeeve.io/blog/consensus-mechanisms-for-permissioned-blockchain-protocols/. Accessed 10 June 2024.

blockchain is that it increases network security because the validators are known to the central authority.[347]

Second, a private blockchain offers more flexibility than a public blockchain. This is because the rules on a private blockchain can be changed by the central authority.[348] The prospect of rule changes is beneficial because participants can agree to use different mechanisms to verify and approve transactions.[349] Moreover, the participants have control over the consensus mechanism, governance, and the rules. This form of control allows faster decision-making and adaptation to specific business requirements.[350] From a VAT collection viewpoint, a tax authority can prescribe the rules and consensus mechanism on the network. In addition, a tax authority can customise a blockchain according to its specific needs.[351] Since private blockchains are more flexible than public blockchains, private blockchains can be designed to seamlessly integrate with existing systems.[352]

One of the most important features of a private blockchain is the fact that it promotes privacy.[353] A central authority can determine the rights of all the participants and can

[347] Vashishtha, G. (2023). *Consensus mechanism for permissioned blockchain protocols*. Available at https://www.zeeve.io/blog/consensus-mechanisms-for-permissioned-blockchain-protocols/. Accessed 10 June 2024.

[348] Buterin, V., (2015). "*On Public and Private Blockchains*". Available at https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/. Accessed 8 January 2020; Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the technology behind bitcoin is changing money, business and the world* Portfolio Penguin at 67. This is not necessarily a trust destroyer because one must consider the context in which the private blockchain is used. It is not a trust destroyer if the private blockchain is used to administer taxes and the jurisdiction in question values taxpayer privacy. A central authority can make changes to the blockchain code to make it conducive for taxpayer privacy. Moreover, a tax authority can determine the rules and access rights so that only the relevant role players obtain access to the network which solidifies privacy considerations.

[349] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 32. See also Buterin, V., (2015). "*On Public and Private Blockchains*". Available at https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/. Accessed 8 January 2020.

[350] Sharma, T. K. (2024). *Types of blockchains explained – public vs private vs consortium*. Available at https://www.blockchain-council.org/blockchain/types-of-blockchains-explained-public-vs-private-vs-consortium/. Accessed 9 June 2024.

[351] Sharma, T. K. (2024). *Types of blockchains explained – public vs private vs consortium*. Available at https://www.blockchain-council.org/blockchain/types-of-blockchains-explained-public-vs-private-vs-consortium/. Accessed 9 June 2024.

[352] Sharma, T. K. (2024). *Types of blockchains explained – public vs private vs consortium*. Available at https://www.blockchain-council.org/blockchain/types-of-blockchains-explained-public-vs-private-vs-consortium/. Accessed 9 June 2024.

[353] Buterin, V., (2015). "*On Public and Private Blockchains*". Available at https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/. Accessed 8 January

determine who gains access to sensitive content.[354] It is also easier to hold parties accountable because a breach in privacy is frowned upon by the public. In contrast, public blockchains can be accessed by any person around the world making the sharing of sensitive information impractical. From a VAT collection perspective, the dissemination of sensitive information is more plausible if the disseminator trusts and identifies the recipients of the information.[355] It is important to note that a private blockchain remains transparent. All transactions can be viewed and controlled by the central authority. All the parties on blockchain have the exact same copy of blockchain.[356]

According to Bal, private blockchains can use cryptography to safeguard data.[357] Bal also notes that private blockchains "do not employ mathematical guarantees at the validation level or with respect to the irreversibility of transactions."[358] Moreover, Bal further argues that the security of a private blockchain is dependent on the honesty of the entities that validate the transactions.[359]

There are several drawbacks to using private blockchains. First, a private blockchain is highly centralised. Only a few participants control the network which, in essence, undermines the decentralised nature of a blockchain.[360] Private blockchains depend on a central authority to run the network. The collapse or failure of the central authority can put the entire blockchain network at risk.[361] Second, and closely connected to the fist drawback, are the security risks associated with a private blockchain. If a participant is compromised or acts with malice, it can severely jeopardise the security

2020. See also Kianieff, M. (2019) *Blockchain Technology and the Law Opportunities and Risks* Routledge Publishing (UK) at 37.

[354] See Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 28; Bal, A. (2018). "Does the Tax Sector Need Blockchain?" *White Paper IBFD* at 5.

[355] See Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 28; Bal, A. (2018). "Does the Tax Sector Need Blockchain?" *White Paper IBFD* at 7.

[356] Hacker, P., Lianos, L., Dimitropoulos, G., Eich, S., (eds) (2019) *Regulating Blockchain: Techno-social and Legal challenges* Oxford University Press (UK) at 334.

[357] Bal, A. (2018). "Does the Tax Sector Need Blockchain?" *White Paper IBFD* at 2.

[358] Bal, A. (2018). "Does the Tax Sector Need Blockchain?" *White Paper IBFD* at 2.

[359] Bal, A. (2018). "Does the Tax Sector Need Blockchain?" *White Paper IBFD* at 2 – 3.

[360] Sharma, T. K. (2024). *Types of blockchains explained – public vs private vs consortium*. Available at https://www.blockchain-council.org/blockchain/types-of-blockchains-explained-public-vs-private-vs-consortium/. Accessed 9 June 2024.

[361] Sharma, T. K. (2024). *Types of blockchains explained – public vs private vs consortium*. Available at https://www.blockchain-council.org/blockchain/types-of-blockchains-explained-public-vs-private-vs-consortium/. Accessed 9 June 2024.

of the network.[362] Third, a private blockchain may encounter difficulties communicating and exchanging data with other blockchain networks.[363] Fourth, setting up and maintaining a private blockchain is costly because it requires significant resources.[364] Lastly, without the necessary incentive structures, participants may lack the motivation to maintain and contribute to a network's security.[365]

2.6.3 Consortium/Hybrid blockchain

A consortium blockchain consists of pre-determined participants who are responsible for the control and access of blockchain.[366] No single authority has control over the network. Instead, several participants are involved in the selecting the nodes, reading, auditing, and writing on a blockchain.[367] Consensus in a consortium or hybrid blockchain system is set and determined by pre-selected participants.[368] Typically, participants in the closed network control the entries made on blockchain system. If enquiries are made regarding the nature and contents of blockchain, then such information can subsequently be made available to the public.[369] Since there is shared control on a consortium blockchain, it is suitable for industries where multiple

[362] Sharma, T. K. (2024). *Types of blockchains explained – public vs private vs consortium*. Available at https://www.blockchain-council.org/blockchain/types-of-blockchains-explained-public-vs-private-vs-consortium/. Accessed 9 June 2024.

[363] Sharma, T. K. (2024). *Types of blockchains explained – public vs private vs consortium*. Available at https://www.blockchain-council.org/blockchain/types-of-blockchains-explained-public-vs-private-vs-consortium/. Accessed 9 June 2024.

[364] Sharma, T. K. (2024). *Types of blockchains explained – public vs private vs consortium*. Available at https://www.blockchain-council.org/blockchain/types-of-blockchains-explained-public-vs-private-vs-consortium/. Accessed 9 June 2024.

[365] Sharma, T. K. (2024). *Types of blockchains explained – public vs private vs consortium*. Available at https://www.blockchain-council.org/blockchain/types-of-blockchains-explained-public-vs-private-vs-consortium/. Accessed 9 June 2024.

[366] Hacker, P., Lianos, L., Dimitropoulos, G., Eich, S., (eds) (2019) *Regulating Blockchain: Techno-social and Legal challenges* Oxford University Press (UK) at 334. See also Buterin, V., (2015). "*On Public and Private Blockchains*". Available at https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/. Accessed 8 January 2020.

[367] Sharma, T. K. (2024). *Types of blockchains explained – public vs private vs consortium*. Available at https://www.blockchain-council.org/blockchain/types-of-blockchains-explained-public-vs-private-vs-consortium/. Accessed 9 June 2024.

[368] Hacker, P., Lianos, L., Dimitropoulos, G., Eich, S., (eds) (2019) *Regulating Blockchain: Techno-social and Legal challenges* Oxford University Press (UK) at 334. See also Buterin, V., (2015). "*On Public and Private Blockchains*". Available at https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/. Accessed 8 January 2020.

[369] Herian, R., (2019). *Regulating Blockchain: Critical perspectives in law and technology* Routledge publishing at 14.

stakeholders need to collaborate.[370] Although consortium blockchains do not offer the same level of privacy as private blockchains, the participants maintain a certain degree of control regarding who has access to the network, providing a certain level of confidentiality in the process.[371] Consortium blockchains also present several customisation options for blockchain participants.[372]

An apparent difficulty that arises from the use of the consortium or hybrid blockchain is that changes to blockchain system can only be effected if all the participants in the consortium agree to the changes. For example, suppose that a consortium consists of four distinct participants. If two participants agree to change the rules on blockchain, change cannot take place unless the two remaining participants agree to the changes. In the absence of a majority or a central authority, it is difficult for changes to be made. This speaks to the complex governance structures required to manage the decision-making process among the participants on the network.[373] It is difficult to develop and maintain effective governance on a consortium blockchain potentially leading to delays in decision-making.[374] Like a private blockchain, a consortium blockchain relies on the key members of the network. If the key members do not participate or leave the network, the stability of the consortium blockchain may be compromised.[375]

A consortium or hybrid blockchain can simultaneously possess features of a private blockchain and a public blockchain. Participants can be selected to manage the entire

[370] Sharma, T. K. (2024). *Types of blockchains explained – public vs private vs consortium*. Available at https://www.blockchain-council.org/blockchain/types-of-blockchains-explained-public-vs-private-vs-consortium/. Accessed 9 June 2024.

[371] Sharma, T. K. (2024). *Types of blockchains explained – public vs private vs consortium*. Available at https://www.blockchain-council.org/blockchain/types-of-blockchains-explained-public-vs-private-vs-consortium/. Accessed 9 June 2024.

[372] Sharma, T. K. (2024). *Types of blockchains explained – public vs private vs consortium*. Available at https://www.blockchain-council.org/blockchain/types-of-blockchains-explained-public-vs-private-vs-consortium/. Accessed 9 June 2024.

[373] Sharma, T. K. (2024). *Types of blockchains explained – public vs private vs consortium*. Available at https://www.blockchain-council.org/blockchain/types-of-blockchains-explained-public-vs-private-vs-consortium/. Accessed 9 June 2024.

[374] Sharma, T. K. (2024). *Types of blockchains explained – public vs private vs consortium*. Available at https://www.blockchain-council.org/blockchain/types-of-blockchains-explained-public-vs-private-vs-consortium/. Accessed 9 June 2024.

[375] Sharma, T. K. (2024). *Types of blockchains explained – public vs private vs consortium*. Available at https://www.blockchain-council.org/blockchain/types-of-blockchains-explained-public-vs-private-vs-consortium/. Accessed 9 June 2024.

blockchain network by a central authority.[376] It is possible for a consortium blockchain to be made open to the public.[377] However, it can be argued that once a consortium blockchain has been made public, private information can be made available to unauthorised parties. Unauthorised parties can use sensitive information to commit fraud and identity theft. For this reason, and in my view, it is unlikely that a consortium blockchain can be used for cross-border VAT collection.

2.7 Ethereum

2.7.1 Background

The spread and popularity of Bitcoin gained momentum to the extent that the price of a single bitcoin climbed to just above United States of America Dollars ('USD') 13 000 in 2017.[378] With increased popularity, users began exploring alternative blockchain applications resulting in the establishment of cryptocurrencies such as Tether and Bitcoin cash.[379]

Despite the popularity and relative success of Bitcoin, it later became apparent that Bitcoin had significant drawbacks. One drawback was Bitcoin's inability to facilitate transactional exchanges. In other words, the Bitcoin blockchain could only be used to exchange virtual currencies.[380] The Bitcoin blockchain was initially designed to cater for online financial transactions. One could simply not operate any other program of functionality on the Bitcoin blockchain because that would have led to system vulnerabilities such as hacks and bugs.[381]

[376] Hacker, P., Lianos, L., Dimitropoulos, G., Eich, S., (eds) (2019) *Regulating Blockchain: Techno-social and Legal challenges* Oxford University Press (UK) at 334.

[377] Buterin, V., (2015). "*On Public and Private Blockchains*". Available at https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/. Accessed 8 January 2020.

[378] Blake Finucane (2019) "Bitcoin Market Cycles and Price Swings – What You Need to Know". Available at https://financial-news-now.com/bitcoin-market-cycles-and-price-swings-what-you-need-to-know/. Accessed 24 February 2020.

[379] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 27; see also https://coinmarketcap.com/. Accessed 11 March 2020.

[380] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 27.

[381] Werbach, K. (2018). *The Blockchain and the New Architecture of Trust* Massachusetts Institute of Technology Press (US) at 65.

As a result of this, a programmer by the name of *Vitalik Buterin* released a white paper in December 2013 detailing an alternative platform to the Bitcoin blockchain.[382] The alternative platform is known as Ethereum.

2.7.2 What is Ethereum?

Ethereum is a platform distinct from the Bitcoin blockchain in the sense that it can run and develop decentralised applications (*dApps*).[383] *dApps* can be defined as "smart contracts which interact with an off-chain interface to enable applications which users can access, usually through a browser-based interface."[384] Ethereum is written in a programming language called *Turing complete*.[385] *Turing complete* enables Ethereum's functionality to evolve beyond storing information. Ethereum creates a user-friendly platform (like an application interface) that facilitates the implementation of applications.[386] In simple terms, Ethereum is equivalent to the Android Operating System (Android). The Android system runs an interface that enables a multiplicity of applications (Apps) that function on the system. Similarly, all manner of applications can be programmed on Ethereum.[387]

The extended functionality of Ethereum supports the implementation of smart contracts.[388] This implies that smart contracts cannot operate on the traditional Bitcoin

[382] Buterin, V., (2013). "Ethereum White Paper: a next generation smart contract & decentralized application platform". Available at https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf. Accessed 24 February 2020; see also Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the technology behind bitcoin is changing money, business and the world* Portfolio Penguin at 87.

[383] Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 45; De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 27; Werbach, K. (2018). *The Blockchain and the New Architecture of Trust* Massachusetts Institute of Technology Press (US) at 87.

[384] Van der Laan, J., *Understanding Blockchain* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 47.

[385] Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 46.

[386] Vigna, P., & Casey, M., J. (2016). *The Age of Cryptocurrency: How Bitcoin and the Blockchain are Challenging the Global Economic order* Picador USA at 231.

[387] Vigna, P., & Casey, M., J. (2016). *The Age of Cryptocurrency: How Bitcoin and the Blockchain are Challenging the Global Economic order* Picador USA at 231; Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 45.

[388] Buterin, V., (2013). "Ethereum White Paper: a next generation smart contract & decentralized application platform" at 1. Available at https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf. Accessed 24 February 2020; Tapscott, D., & Tapscott, A. (2016). *Blockchain*

blockchain. The reason for this is that the Bitcoin blockchain was primarily created for transactional exchanges in virtual currencies.[389]

2.7.3 How does Ethereum work?

Initially, Ethereum used a *proof-of-work* mechanism. *Proof-of-work* is a consensus mechanism that enables miners on blockchain to compete by making use of computational power to validate transactions.[390] In September 2022, Ethereum changed to a *proof-of-stake* mechanism since it is less energy-intensive, more secure, and has better scalability compared to *proof-of-work*.[391]

Ethereum also makes use of a 'virtual machine' known as the Ethereum Virtual Machine (EMV).[392] The EMV is akin to a decentralised virtual machine that facilitates the implementation of smart contract.[393] Due to the fact that Ethereum is open to the public, any person can generate a smart contract by transferring the computer code to the EMV.[394] A smart contract is initiated by transmitting an ether to a recipient's account on the Ethereum blockchain.[395] An ether is an Ethereum based digital currency that operates similarly to a bitcoin.[396] An ether can also be used to purchase

Revolution: How the technology behind bitcoin is changing money, business and the world Portfolio Penguin at 87; De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 27; Werbach, K. (2018). *The Blockchain and the New Architecture of Trust* Massachusetts Institute of Technology Press (US) at 63.

[389] Werbach, K. (2018). *The Blockchain and the New Architecture of Trust* Massachusetts Institute of Technology Press (US) at 65.

[390] Narayanan, A., *et al* (2016). *Bitcoin and Cryptocurrency technologies: A comprehensive introduction* Princeton University Press (US) at 41; Richter, T., *Blockchain Regulation* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 129.

[391] See Ethereum (2023). *Proof-of-stake (POS)*. Available https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/. Accessed 21 August 2023.

[392] Narayanan, A., *et al* (2016). *Bitcoin and Cryptocurrency technologies: A comprehensive introduction* Princeton University Press (US) at 265; De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 28 – 29.

[393] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 28.

[394] Narayanan, A., *et al* (2016). *Bitcoin and Cryptocurrency technologies: A comprehensive introduction* Princeton University Press (US) at 264 – 265; De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 28; Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 45.

[395] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 28.

[396] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 28

an asset known as *gas*. With *gas*, a user can supplement additional patterns on the Ethereum network.[397]

In as much as Ethereum has similar properties to the Bitcoin blockchain, there are distinct differences. First, transactions on the Ethereum blockchain are faster than those processed on the Bitcoin blockchain. Currently, and in terms of speed, Ethereum can processes 30 transactions per second.[398] With Ethereum's change to a *proof-of-stake* consensus mechanism, up to 100 000 transactions could be processed per second.[399] In contrast, a Bitcoin blockchain processes seven transactions per second.[400] A transaction on the Ethereum blockchain can take between fifteen seconds and five minutes to process[401] whereas it takes ten minutes to complete a transaction on the Bitcoin blockchain.[402] Second, a user on Ethereum has access to two accounts as opposed to a single account on the Bitcoin blockchain. If a user wants to initiate a smart contract, they can use a 'contract account'. Should a user require to conduct day to day transactions on the Ethereum blockchain, they can make use of

[397] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 28; Werbach, K. (2018). *The Blockchain and the New Architecture of Trust* Massachusetts Institute of Technology Press (US) at 66.

[398] Worldcoin (2023). *What's Ethereum 2.0? A complete guide*. Available at https://worldcoin.org/articles/whats-ethereum-2-0#:~:text=In%20terms%20of%20processing%20speed,which%20is%20a%20massive%20jump. Accessed 21 August 2023.

[399] Worldcoin (2023). *What's Ethereum 2.0? A complete guide*. Available at https://worldcoin.org/articles/whats-ethereum-2-0#:~:text=In%20terms%20of%20processing%20speed,which%20is%20a%20massive%20jump. Accessed 21 August 2023.

[400] Hyson, P. & Ancrum, S. (2023). *Unleashing the power of cryptocurrency: Exploring Transactions per second (TPS) and its impact*. Available at https://www.miamiherald.com/software-business/article274817896.html#:~:text=Bitcoin%2C%20the%20first%20cryptocurrency%2C%20has,around%207%20transactions%20per%20second. Accessed 21 August 2023.

[401] Deer, M. (2023). *How to check an Ethereum transaction*. Available at https://cointelegraph.com/news/how-to-check-an-ethereum-transaction#:~:text=How%20long%20does%20an%20Ethereum,at%20the%20time%20of%20processing. Accessed 21 August 2023.

[402] Dog, D. (2021). *How long does a Bitcoin Transaction Take?* Available at https://coinmarketcap.com/alexandria/article/how-long-does-a-bitcoin-transaction-take#:~:text=little%20bit*%20longer.-,How%20Long%20Does%20Bitcoin%20Take%20to%20Send%3F,activity%2C%20hashrate%20and%20transaction%20fees. Accessed 21 August 2023.

an externally owned account.[403] Finally, ether enables applications to run on Ethereum while bitcoin can only be used as a virtual currency.[404]

2.8 Blockchain and smart contracts

Blockchain infrastructure permits parties to conclude self-executing contracts. While conventional contracts are decided verbally or in writing, self-executing contracts can only be concluded digitally.[405] These self-executing contracts, or smart contracts,[406] run on a software program or code on blockchain and once all the conditions in the software program are met,[407] the contract automatically executes.[408] Before the execution of a smart contract, parties must first negotiate the terms of the agreement

[403] Buterin, V., (2013). "Ethereum White Paper: a next generation smart contract & decentralized application platform" at 13. Available at https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf. Accessed 24 February 2020; De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 28.

[404] Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 46.

[405] Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 12.

[406] The term 'smart contract' was initialled coined by Nick Szabo. Nick Szabo defined a smart contract as "a set of promises, specified in digital form, including protocols within which the parties perform on these promises." See Szabo, N. (1996). "Smart Contracts: Building Blocks for the Digital Markets". Available at https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html. Accessed 8 September 2022. Finck notes that a smart contract is neither 'smart' nor a 'contract' but an agent that can "alter how we think of law." Finck also notes that smart contracts "are not able to understand natural language or to independently verify whether an execution-relevant event occurred." See Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 24 – 25, 75. Van der Laan also argues that smart contracts are "neither smart nor legal contracts. Instead, they are simply bits of computer code committed to the Ethereum or similar blockchain. Smart contracts are nothing more than a series of programmed steps, like any other computer program, and are not imbued with any specific properties just because they are called 'smart'. The perception by many that these program code snippets have some sort of artificial intelligence capability, particularly now that artificial intelligence is top of mind for many, is unfortunate." Van der Laan, J., *Understanding Blockchain* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 45.

[407] It can be argued that a self-executing contract uses 'suspensive conditions' styled programmed mechanism to take place and once all the conditions have been realised, then a smart contract comes into existence. This principle is well established in the law of contract where a contract can only be enforced once a specified event materialises. Often, this specified event is uncertain because it is dependent on the performance by one of the parties to the agreement. In the context of VAT and e-commerce transactions, the implementation and execution of a smart contract may be contingent on a supplier of digital goods receiving funds from a purchaser of the said goods.

[408] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 74; Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 24.

until they agree.[409] Once consensus has been reached, the agreement can be converted into code.[410] Parties can identify each other using the other's wallet.[411] Upon reaching consensus, parties share a common goal to have the conditions fulfilled and any subsequent obligation met.[412] After the parties' agreement has been codified using a programming language, the smart contract is inserted into a specific block inside blockchain system.[413] Thereafter, the participants on blockchain assess the smart contract to determine whether the conditions attached to the agreement have been complied with.[414]

The next stage in the process is the execution phase. During this process, the participants on blockchain peruse the smart contract. An analysis of the smart contract occurs to ascertain its authenticity. After a smart contract has been authenticated, the participants examine the conditions of the contract. Once satisfied that all the conditions have been complied with, the contract is then executed through the consensus protocol.[415] When the contract has been realised, the outcome of any dealings associated with that contract is subsequently stored on blockchain.[416]

[409] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 74. Sillaber, C., & Waltl, B., (2017). "Life Cycle of Smart Contracts in Blockchain Ecosystems" at 3. Available at https://csillaber.q-e.at/pdfs/SW_DuD_SmartContracts_preprint.pdf. Accessed 21 February 2020.

[410] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 74. Sillaber, C., & Waltl, B., (2017). "Life Cycle of Smart Contracts in Blockchain Ecosystems" at 3. Available at https://csillaber.q-e.at/pdfs/SW_DuD_SmartContracts_preprint.pdf. Accessed 21 February 2020.

[411] Sillaber, C., & Waltl, B., (2017). "Life Cycle of Smart Contracts in Blockchain Ecosystems" at 3. Available at https://csillaber.q-e.at/pdfs/SW_DuD_SmartContracts_preprint.pdf. Accessed 21 February 2020.

[412] Sillaber, C., & Waltl, B., (2017). "Life Cycle of Smart Contracts in Blockchain Ecosystems" at 3. Available at https://csillaber.q-e.at/pdfs/SW_DuD_SmartContracts_preprint.pdf. Accessed 21 February 2020.

[413] Sillaber, C., & Waltl, B., (2017). "Life Cycle of Smart Contracts in Blockchain Ecosystems" at 3 – 4. Available at https://csillaber.q-e.at/pdfs/SW_DuD_SmartContracts_preprint.pdf. Accessed 21 February 2020; see also De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 74.

[414] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 74. See also Sillaber, C., & Waltl, B., (2017). "Life Cycle of Smart Contracts in Blockchain Ecosystems" at 3 – 4. Available at https://csillaber.q-e.at/pdfs/SW_DuD_SmartContracts_preprint.pdf. Accessed 21 February 2020.

[415] Sillaber, C., & Waltl, B., (2017). "Life Cycle of Smart Contracts in Blockchain Ecosystems" at 3 – 4. Available at https://csillaber.q-e.at/pdfs/SW_DuD_SmartContracts_preprint.pdf. Accessed 21 February 2020. See also Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 26; Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 13.

[416] Sillaber, C., & Waltl, B., (2017). "Life Cycle of Smart Contracts in Blockchain Ecosystems" at 4. Available at https://csillaber.q-e.at/pdfs/SW_DuD_SmartContracts_preprint.pdf. Accessed 21 February 2020.

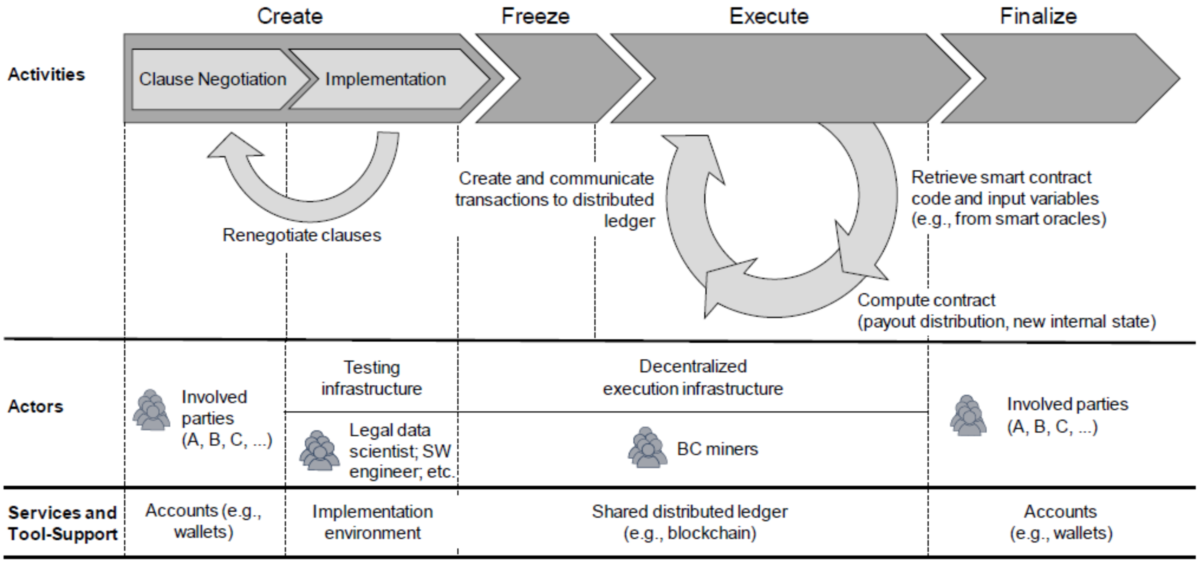

Create
Freeze
Execute
Finalize
Activities
Clause Negotiation
Implementation
Renegotiate clauses
Create and communicate transactions to distributed ledger
Retrieve smart contract code and input variables (e.g., from smart oracles)
Compute contract (payout distribution, new internal state)
Actors
Involved parties (A, B, C, ...)
Testing infrastructure
Legal data scientist; SW engineer; etc.
Decentralized execution infrastructure
BC miners
Involved parties (A, B, C, ...)
Services and Tool-Support
Accounts (e.g., wallets)
Implementation environment
Shared distributed ledger (e.g., blockchain)
Accounts (e.g., wallets)

Figure 4[417]

Ordinarily, smart contracts do not have artificial intelligence (AI) capabilities that enable them to read and understand natural language or to independently verify if an execution has been orchestrated correctly.[418] For this reason, an *oracle* can be used.[419] An *oracle* is a program, multiple groups or persons that store and transmit information from the outside world into the smart contract (code).[420] Essentially, an *oracle* acts as a nexus between the real world and blockchain-based transactions in

[417] **Figure 4** illustrates how smart contracts are formulated. **Figure 4** source from Sillaber, C., & Waltl, B., (2017). "Life Cycle of Smart Contracts in Blockchain Ecosystems" at 4. Available at https://csillaber.q-e.at/pdfs/SW_DuD_SmartContracts_preprint.pdf. Accessed 21 February 2021.

[418] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 24 – 25.

[419] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 25; De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 75; Werbach, K. (2018). *The Blockchain and the New Architecture of Trust* Massachusetts Institute of Technology Press (US) at 213; Van der Laan, J., *Understanding Blockchain* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 46 – 47; Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 19.

[420] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 25; De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 75; Werbach, K. (2018). *The Blockchain and the New Architecture of Trust* Massachusetts Institute of Technology Press (US) at 213; Van der Laan, J., *Understanding Blockchain* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 46 – 47.

the absence of artificial intelligence.[421] When the real world and blockchain-based transactions interact, smart contracts can be enhanced by adjusting performance obligations during the term of an agreement.[422] During this process, smart contracts can react to external events.[423] For example, if the VAT rate in South Africa[424] changes, a SARS official can merely use a data feed to input the relevant data into the smart contract to convey the new VAT rate.[425] This ensures that a smart contract can respond to changing events in real-time.[426] Moreover, the *oracle* can facilitate the insight of human beings or facilitate dispute resolution or arbitration.[427]

There are different types of oracles depending on several qualities.[428] A software oracle is an oracle that retrieves data from online databases, websites, and on the web. By connecting to the Internet, oracles supply data to smart contracts in real-time.[429] A hardware oracle is an oracle that retrieves information from the physical world through devices like electronic sensors, barcodes, or any other reading devices.[430] A hardware oracle retrieves information by conveying real-world events into digital values that can be interpreted by a smart contract.[431] A human oracle is a person that verifies information from multiple sources before conveying the information

[421] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 75; Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 25; Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 19.

[422] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 75.

[423] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 75.

[424] Currently at fifteen per cent.

[425] See De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 75; see also Post, D. & Cipollini, C. (2022). Fundamental elements of a blockchain-based tax system – when to use blockchain for tax? *World Tax Journal* 14(4): 532.

[426] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 75; see also Post, D. & Cipollini, C. (2022). Fundamental elements of a blockchain-based tax system – when to use blockchain for tax? *World Tax Journal* 14(4): 532.

[427] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 75.

[428] Beniiche, A. (2020). *A study of blockchain oracles* at 1. Available at https://arxiv.org/pdf/2004.07140.pdf. Accessed 18 October 2023. According to Beniiche, some of these qualities include (i) Source: whether the data originates from a software, hardware or human; (ii) direction of information: whether the data is inbound or outbound; (iii) whether the oracle is centralised or decentralised.

[429] Beniiche, A. (2020). *A study of blockchain oracles* at 1. Available at https://arxiv.org/pdf/2004.07140.pdf. Accessed 18 October 2023.

[430] Beniiche, A. (2020). *A study of blockchain oracles* at 1. Available at https://arxiv.org/pdf/2004.07140.pdf. Accessed 18 October 2023.

[431] Beniiche, A. (2020). *A study of blockchain oracles* at 1. Available at https://arxiv.org/pdf/2004.07140.pdf. Accessed 18 October 2023.

to smart contracts.[432] A computation oracle is an oracle that performs off-chain computations and returns the input result on-chain.[433] Inbound oracles convey information from external sources to smart contracts while outbound oracles relay information from a smart contract to the real world.[434] A consensus-based oracle are decentralised oracles are multiple oracles that are often used in prediction market. They provide accurate information if a certain oracle is not trusted. However, they are slower because they take longer to reach consensus.[435] Last, a contract-specific oracle is an oracle that specifically designed by a single smart contract.[436]

It should be noted that no single authority has control over a smart contract. Furthermore, a smart contract operates without human intervention or any third party.[437] The exception to this rule is where *oracle*s are used.[438] Once a smart contract has been activated, it cannot be interrupted.[439] Changes to a smart contract cannot be readily effected unless an alternative smart contract is created to rectify the error or omission.[440] Bal posits that it is possible to make changes to the smart contract after its execution provided that the smart contract was programmed to incorporate change from the onset.[441] The inability to make changes to a smart contract suggests that parties may not have any remedy available at their disposal should an error occur in the execution of the original contract. An aggrieved party may not sue a 'defaulting' party for 'breach of contract' if a smart contract does not come into existence.

[432] Beniiche, A. (2020). *A study of blockchain oracles* at 1. Available at https://arxiv.org/pdf/2004.07140.pdf. Accessed 18 October 2023.

[433] Beniiche, A. (2020). *A study of blockchain oracles* at 2. Available at https://arxiv.org/pdf/2004.07140.pdf. Accessed 18 October 2023.

[434] Beniiche, A. (2020). *A study of blockchain oracles* at 2. Available at https://arxiv.org/pdf/2004.07140.pdf. Accessed 18 October 2023.

[435] Beniiche, A. (2020). *A study of blockchain oracles* at 2. Available at https://arxiv.org/pdf/2004.07140.pdf. Accessed 18 October 2023.

[436] Beniiche, A. (2020). *A study of blockchain oracles* at 2. Available at https://arxiv.org/pdf/2004.07140.pdf. Accessed 18 October 2023.

[437] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 25; De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 29; Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 13.

[438] See discussion above.

[439] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 74; Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 24; Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 16 – 17.

[440] Sillaber, C., & Waltl, B., (2017). "Life Cycle of Smart Contracts in Blockchain Ecosystems" at 4. Available at https://csillaber.q-e.at/pdfs/SW_DuD_SmartContracts_preprint.pdf. Accessed 21 February 2020.

[441] Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 17.

However, this view is not shared by Bal who states that parties can breach a smart contract if the conditions that led to the creation of the contract have changed or if a contracting party desires a more lucrative option.[442]

Smart contracts do not necessarily qualify as conventional contracts.[443] As such, they are not subject to review and enforcement by a competent court. The lack of oversight by a competent court into the nature and outcome of smart contracts presupposes that parties must address a desired outcome from the beginning to avoid disappointment. Thus, it is important for parties to understand the nature and the extent of an agreement and manage expectations accordingly. For this reason, parties can renegotiate an agreement should they fail to agree during the creation phase.[444]

Since smart contracts are essentially self-executing software, they do not understand natural language or contractual terms.[445] Contractual terms are often drafted by experienced lawyers who possess knowledge of the law of contract. Since lawyers do not program smart contracts, ordinary parties formulate conditions and obligations into a computer program.[446] Despite this drawback, smart contracts execute automatically without human intervention and institutional trust which lowers transaction costs, interpretative uncertainty, and counterparty risk.[447] To put this into context, e-commerce businesses tasked with collecting and remitting VAT to the relevant tax authority often experience delays because funds are processed by financial institutions. Financial institutions usually process the transfer of funds for a fee.[448] The role of a financial institution can be limited if smart contracts are used. A smart contract can automatically transfer funds to the tax authority without any delays. Furthermore,

[442] Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 17.

[443] Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 12 – 15; Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 25.

[444] See **Figure 4** above. See also Sillaber, C., & Waltl, B., (2017). "Life Cycle of Smart Contracts in Blockchain Ecosystems" at 3 – 4. Available at https://csillaber.q-e.at/pdfs/SW_DuD_SmartContracts_preprint.pdf. Accessed 21 February 2020.

[445] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 24 – 25.

[446] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 74.

[447] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 25; see also Vigna, P., & Casey, M., J. (2016). *The Age of Cryptocurrency: How Bitcoin and the Blockchain are Challenging the Global Economic order* Picador USA at 217.

[448] For example, financial institution can impose charges for the remittance.

the payment received by the tax authority occurs in real-time.[449] E-commerce businesses do not incur any transaction fees due to the absence of a financial institutions.[450] This can reduce compliance costs borne by e-commerce businesses.

Blockchain and smart contracts can build trust between taxpayers and tax authorities. For example, Alexander notes that tax authorities can engender trust with taxpayers by treating taxpayers fairly and by ensuring that taxpayer privacy and security in relation to processed data is always maintained.[451]

2.8.1 Challenges associated with the use of smart contracts

2.8.1.1 Programming errors

Smart contracts are run by computer code. Thus, it is possible for programming errors to occur.[452] It must be noted that faults in programming occur because of human error. Van der Laan notes that although smart contracts can execute instructions as coded, it does not necessarily mean that the smart contract will perform the intended functionality of its designer and coder.[453] Werbach correctly states that smart contracts require the "reduction of human-readable language to machine-readable code."[454] Werbach also notes that "this limits their scope to those subjects and activities that can readily be specified precisely."[455] As a result, it is possible for smart contracts to contain bugs and execution errors on a blockchain.[456] If code errors cause the

[449] See discussion in chapter 3.

[450] See De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 76.

[451] Alexander, G. (2022). "Blocking the Gap: The Potential for Blockchain Technology to secure VAT Compliance" *EC Tax Review* 31(3): 144.

[452] Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 17; See also Werbach, K. (2018). *The Blockchain and the New Architecture of Trust* Massachusetts Institute of Technology Press (US) at 124.

[453] Van der Laan, J., *Understanding Blockchain* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 45.

[454] Werbach, K. (2018). *The Blockchain and the New Architecture of Trust* Massachusetts Institute of Technology Press (US) at 125.

[455] Werbach, K. (2018). *The Blockchain and the New Architecture of Trust* Massachusetts Institute of Technology Press (US) at 125.

[456] Van der Laan, J., *Understanding Blockchain* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 45.

execution of the smart contract to fail, then the desired outcome cannot materialise on blockchain.[457]

Errors can potentially raise concerns around liability. For instance, suppose a supplier and a customer enter into a purchase agreement for the sale of digital goods. Both parties are situated in different jurisdictions. The parties agree that the digital goods can be downloaded by the customer subject to the receipt of the purchase price. If the customer renders full payment but the smart contract fails to remit VAT to the tax authority because of a programming error, the tax authority cannot hold the supplier liable.[458] For this reason, Bal states that parties should specify any eventuality that may ensue especially when these eventualities fall outside their control.[459] Parties can then mitigate the risks associated with any unforeseen event and plan accordingly.[460] Interestingly, it is possible for a programmer to insert a self-destruction functionality in a smart contract on a blockchain.[461] This is significant because a smart contract can be deleted and rendered inoperable.[462] Without a self-destruction code, a smart contract cannot be deleted.[463]

Another way to abate any potential loss by a party to a smart contract is to execute the smart contract on a private blockchain. It is difficult to remedy any contractual liability if an aggrieved party does not know the identity of the other party. Additionally, there is no central authority in a public blockchain that could potentially resolve any dispute between parties to a smart contract.[464] In a private blockchain, the chances of a recourse increase because a central authority knows the identities of the parties on

[457] Van der Laan, J., *Understanding Blockchain* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 45; See also Werbach, K. (2018). *The Blockchain and the New Architecture of Trust* Massachusetts Institute of Technology Press (US) at 125.

[458] This can be the case where neither the purchaser nor the seller programmed the smart contract. The purchaser can hold the third-party programmer liable.

[459] Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 17.

[460] See Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 17.

[461] Van der Laan, J., *Understanding Blockchain* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 45.

[462] Van der Laan, J., *Understanding Blockchain* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 45.

[463] Van der Laan, J., *Understanding Blockchain* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 45.

[464] Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 17.

blockchain network. Similarly, a central authority can intervene should a dispute arise between participants on the private blockchain.

It is difficult to know for sure what a smart contract will do until it runs.[465] It is advisable to check smart contracts before they are encoded on blockchain.[466] To do this, formal verification methods can be applied.[467] It should be noted that while smart contracts can operate as designed, there is a chance that they can produce sub-optimal outcomes.[468]

2.8.1.2 Illegal smart contracts

The decentralised and pseudonymous nature of blockchain increases online activities. Naturally, it is possible for people to take part in illegal online activities. Illegal transactions can be orchestrated using a smart contract. The reason for this is that it is possible to incorporate all kinds of agreements, legal and illegal, in the computer code that governs smart contracts.[469] Unlike humans, smart contracts (compute code) cannot distinguish between moral or immoral contracts. Consequently, if the conditions are complied with, irrespective of their moral nature, then the smart contract will automatically execute.[470] People with criminal intent can rely on smart contracts to conduct illegal activities.[471] For example, people can purposefully arrange unlawful economic arrangements in a manner that circumvents laws and regulations.[472] This challenge can be compounded by using smart contracts in public blockchains because no central authority is available to halt the potential illegal activity.[473]

[465] Werbach, K. (2018). *The Blockchain and the New Architecture of Trust* Massachusetts Institute of Technology Press (US) at 125.
[466] Werbach, K. (2018). *The Blockchain and the New Architecture of Trust* Massachusetts Institute of Technology Press (US) at 125.
[467] Werbach, K. (2018). *The Blockchain and the New Architecture of Trust* Massachusetts Institute of Technology Press (US) at 125.
[468] Werbach, K. (2018). *The Blockchain and the New Architecture of Trust* Massachusetts Institute of Technology Press (US) at 125.
[469] Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 17.
[470] Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 17 – 18.
[471] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 86 – 87.
[472] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 86 – 87.
[473] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 86 – 87.

I believe that a central authority can act on potential illegal activities if the activities are concluded on a private blockchain. If two parties on blockchain conclude and execute an illegal contract, the central authority can theoretically identify the transgressors. Furthermore, other participants on blockchain can view the transaction and recognise the actors by searching for their public keys. To mitigate the risks associated with illegal smart contracts, private blockchain participants can impose sanctions, hefty penalties, or even report them to the relevant authorities should any of the participants contravene the law.

2.8.1.3 Smart contract coding

Computer programmers design computer code. Programmers play a crucial role in blockchain since they are responsible for the smooth operation of blockchain system. It would be difficult for blockchain participants to conduct transactions without the full support of programmers. When errors occur, it is the task of programmers to maintain and fix bugs on blockchain system. Unsurprisingly, it requires a sophisticated level of skill and understanding to program code for a complex system such as blockchain. Additional levels of skill and sophistication is required to implement code that runs autonomously without any human intervention.[474] It is the role of programmers to convert agreements between parties into computer code. There is an inherent risk that programmers may misinterpret a provision or a meaning in an agreement because these agreements are often drafted by lawyers in complex legal terminology. If a programmer is not familiar with the terms or meaning of the agreement, incorrect programming language could be embedded in the computer code.[475] As Bal correctly states:

> “Not all legal language is capable of reduction into an algorithm and omitting a single word in legal documents may give rise to unintended legal consequences and prolonged disputes. Some contracts rely on abstract concepts such as ‘reasonable steps’ or ‘good faith’, that do not lend themselves to encoding as they involve value judgments and are a question of degree. As words are ambiguous and capable of

[474] Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 18.
[475] Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 18.

> multiple interpretations, they may be incorrectly interpreted by those converting a particular obligation into code."[476]

Consequently, it may be necessary for legal practitioners to draft legal agreements in tandem with programmers and in a language that is comprehensible to allow programmers to translate the agreements into code.[477]

2.8.1.4 Concerns regarding privacy[478]

It is not uncommon for parties to insert privacy clauses (confidentiality clauses) in a contractual agreement to safeguard the nature and contents of their agreement. Smart contracts are publicly visible to all participants on blockchain system. As a result, the nature of agreements concluded on smart contracts are not private.[479] De Filippi and Wright opine that blockchain's transparent nature increases these privacy risks especially when the accounts of blockchain participants are linked to known entities.[480] De Filippi and Wright reason that transactions executed via smart contracts are conducted on a peer-to-peer network, making them publicly visible to all the nodes.[481] In a blockchain, there is a risk that the identity of parties can be determined through the continuous use of blockchain.[482] The reason for this is clear. Participants on blockchains use pseudonymous accounts which, although not entirely anonymous, can be discerned to reveal their true identities using the appropriate identification techniques.[483] As a result, if a party's identity has been established, all operations performed with the same account can be associated with a participant's identity.[484]

[476] Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 18.
[477] Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 18.
[478] Compare chapter 4 where I discuss the legal consequences of privacy in South Africa.
[479] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 83.
[480] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 83.
[481] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 83.
[482] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 83.
[483] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 83.
[484] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 83.

2.9 Decentralised autonomous organisations

Blockchain and smart contracts can be used to create a decentralised autonomous organisation (DAO). A DAO can also be characterised as a crowdfunding digital investment vehicle.[485] A DAO consists of a combination of smart contracts that form an interconnected system of technically enforced relationships that collectively define the rules of an organisation.[486] According to De Filippi and Wright, the smart contracts' interconnectedness enables blockchain to create decentralised organisations consisting of people who collaborate on a peer-to-peer basis and transact value without the assistance of a central authority.[487]

DAOs use tokens[488] and smart contracts to grant people direct or indirect control of an organisation's assets.[489] A token can be allocated by the organisation as a reward in exchange for capital or resources.[490] A token grants an individual specific rights, such as the right to transfer an organisation's resources.[491] Tokens can give people access to an organisation's decision-making process.[492] There is no hierarchy in a DAO. Instead, a DAO's management is run by a group consensus which relies on smart contracts to aggregate votes or preferences of token holders.[493]

[485] Richter, T., *Blockchain Regulation* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 150; See also Werbach, K. (2018). *The Blockchain and the New Architecture of Trust* Massachusetts Institute of Technology Press (US) at 67.

[486] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 136.

[487] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 156.

[488] Van de Laan defines a token as "smart contract based encapsulated entitlement tracking functionality for a particular purpose. Contract based tokens allow the use of a distributed ledger for record-keeping without the necessity to create a new and separate blockchain." see Van der Laan, J., *Understanding Blockchain* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 48.

[489] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 136.

[490] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 136.

[491] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 136 – 137.

[492] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 137.

[493] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 137.

A key feature of a DAO is its high degree of autonomy.[494] In other words, once a DAO is programmed and deployed on a blockchain, the coders have no control of the DAO.[495] The coders only retain voting rights linked to the tokens purchased from the DAO.[496] The DAO governance is automated with little human intervention, the latter required when members have to vote regarding the DAO's organisational structure or investment decisions.[497] Members can invest in a DAO using cryptocurrencies.[498] The cryptocurrencies are held by the DAO and not the members.[499]

2.10 The challenges associated with blockchain use

2.10.1 Electricity costs

It is important to note that using blockchain can consume significant amounts of electricity. The high electricity costs can be attributed to bitcoin mining and the *proof-of-work* consensus mechanism.[500] Bitcoin mining requires computational power for miners to validate transactions.[501] If the demand for bitcoins increases, there will be increased competition between miners to release new bitcoins in the network.[502] Tapscott and Tapscott argue that the use of blockchain may not be sustainable in the

[494] Richter, T., *Blockchain Regulation* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 151.

[495] Richter, T., *Blockchain Regulation* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 151.

[496] Richter, T., *Blockchain Regulation* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 151.

[497] Richter, T., *Blockchain Regulation* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 151.

[498] Richter, T., *Blockchain Regulation* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 151.

[499] Richter, T., *Blockchain Regulation* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 151.

[500] See Deutsche Energie-Agentur (Publisher) (dena, 2023) "Rethinking Blockchain's Electricity Consumption – A Guide to Electricity- Efficient Design of Decentralized Data-Infrastructure" at 6. Available at https://www.dena.de/fileadmin/dena/Publikationen/PDFs/2023/Guide_Rethinking_Blockchain_s_Energy_Consumption.pdf. Accessed 22 June 2024.

[501] Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the technology behind bitcoin is changing money, business and the world* Portfolio Penguin at 260.

[502] Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the technology behind bitcoin is changing money, business and the world* Portfolio Penguin at 259 – 260.

long run due to high electricity costs and the effects of prolonged hardware use on the environment.[503] The German Energy Agency (the Agency) has released a report on the reduction of energy consumption on blockchain.[504] In the report, the Agency identified that Ethereum's shift from using *proof-of-work* to *proof-of-stake* can significantly reduce electricity consumption on a blockchain network.[505] This implies that the use of an alternative consensus mechanism can be more energy efficient. The Agency has proposed that a suitable network design can also significantly reduce electricity consumption.[506] In this context, a suitable network design involves selecting the appropriate blockchain type, identifying a suitable blockchain platform and designing the network.[507] First, an entity must decide whether to use a permissionless or permissioned blockchain for the specific use case. Second, an entity must identify the right blockchain platform. For example, a permissioned blockchain can be designed to be more efficient. The reason for this is that, generally, permissioned blockchains have fewer participants than a permissionless blockchain making it easier to reach consensus.[508] Designing a permissionless blockchain from scratch can be more expensive because it requires significant amounts of investments.[509] According

[503] See Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the technology behind bitcoin is changing money, business and the world* Portfolio Penguin at 259 – 263.

[504] Deutsche Energie-Agentur (Publisher) (dena, 2023) "Rethinking Blockchain's Electricity Consumption – A Guide to Electricity- Efficient Design of Decentralized Data-Infrastructure". Available at https://www.dena.de/fileadmin/dena/Publikationen/PDFs/2023/Guide_Rethinking_Blockchains_Energy_Consumption.pdf. Accessed 22 June 2024.

[505] Deutsche Energie-Agentur (Publisher) (dena, 2023) "Rethinking Blockchain's Electricity Consumption – A Guide to Electricity- Efficient Design of Decentralized Data-Infrastructure" at 75. Available at https://www.dena.de/fileadmin/dena/Publikationen/PDFs/2023/Guide_Rethinking_Blockchains_Energy_Consumption.pdf. Accessed 22 June 2024.

[506] Deutsche Energie-Agentur (Publisher) (dena, 2023) "Rethinking Blockchain's Electricity Consumption – A Guide to Electricity- Efficient Design of Decentralized Data-Infrastructure" at 6. Available at https://www.dena.de/fileadmin/dena/Publikationen/PDFs/2023/Guide_Rethinking_Blockchains_Energy_Consumption.pdf. Accessed 22 June 2024.

[507] Deutsche Energie-Agentur (Publisher) (dena, 2023) "Rethinking Blockchain's Electricity Consumption – A Guide to Electricity- Efficient Design of Decentralized Data-Infrastructure" at 47. Available at https://www.dena.de/fileadmin/dena/Publikationen/PDFs/2023/Guide_Rethinking_Blockchains_Energy_Consumption.pdf. Accessed 22 June 2024.

[508] Deutsche Energie-Agentur (Publisher) (dena, 2023) "Rethinking Blockchain's Electricity Consumption – A Guide to Electricity- Efficient Design of Decentralized Data-Infrastructure" at 49. Available at https://www.dena.de/fileadmin/dena/Publikationen/PDFs/2023/Guide_Rethinking_Blockchains_Energy_Consumption.pdf. Accessed 22 June 2024.

[509] Deutsche Energie-Agentur (Publisher) (dena, 2023) "Rethinking Blockchain's Electricity Consumption – A Guide to Electricity- Efficient Design of Decentralized Data-Infrastructure" at 48. Available at

to the Agency, reducing electricity consumption in a permissionless blockchain is restricted to choosing a network with low electricity consumption.[510] Third, and if a permissioned blockchain is used, it is important to for an entity to design a network that provides the desired properties and effectively meets the requirements.[511] For instance, a network design for a permissioned blockchain should consider aspects such as data security, performance, and environment impact.[512] Furthermore, the Agency has proposed measures to further enhance electricity efficiency and sustainability in blockchain technology. The Agency highlights the need for standardisation and regulation of blockchain technology. This can assist by providing metrics for the electricity consumption or carbon emissions associated with blockchain technology to allow entities using the technology to calculate their carbon footprint.[513] The blockchain developers can consider the electricity consumption aspect of the software. If the developers consider this, they can incorporate features aimed at reducing electricity consumption. This contributes to blockchain sustainability because it provides practical guidelines for electricity-efficient designs and creating tools to monitor a network's electricity consumption.[514] Last, the blockchain operators should consider a conscious network design. This design, described above, can reduce the

https://www.dena.de/fileadmin/dena/Publikationen/PDFs/2023/Guide_Rethinking_Blockchains_Energy_Consumption.pdf. Accessed 22 June 2024.

[510] Deutsche Energie-Agentur (Publisher) (dena, 2023) "Rethinking Blockchain's Electricity Consumption – A Guide to Electricity- Efficient Design of Decentralized Data-Infrastructure" at 49. Available at https://www.dena.de/fileadmin/dena/Publikationen/PDFs/2023/Guide_Rethinking_Blockchains_Energy_Consumption.pdf. Accessed 22 June 2024.

[511] Deutsche Energie-Agentur (Publisher) (dena, 2023) "Rethinking Blockchain's Electricity Consumption – A Guide to Electricity- Efficient Design of Decentralized Data-Infrastructure" at 50. Available at https://www.dena.de/fileadmin/dena/Publikationen/PDFs/2023/Guide_Rethinking_Blockchains_Energy_Consumption.pdf. Accessed 22 June 2024.

[512] Deutsche Energie-Agentur (Publisher) (dena, 2023) "Rethinking Blockchain's Electricity Consumption – A Guide to Electricity- Efficient Design of Decentralized Data-Infrastructure" at 50 – 52. Available at https://www.dena.de/fileadmin/dena/Publikationen/PDFs/2023/Guide_Rethinking_Blockchains_Energy_Consumption.pdf. Accessed 22 June 2024.

[513] Deutsche Energie-Agentur (Publisher) (dena, 2023) "Rethinking Blockchain's Electricity Consumption – A Guide to Electricity- Efficient Design of Decentralized Data-Infrastructure" at 76. Available at https://www.dena.de/fileadmin/dena/Publikationen/PDFs/2023/Guide_Rethinking_Blockchains_Energy_Consumption.pdf. Accessed 22 June 2024.

[514] Deutsche Energie-Agentur (Publisher) (dena, 2023) "Rethinking Blockchain's Electricity Consumption – A Guide to Electricity- Efficient Design of Decentralized Data-Infrastructure" at 76. Available at https://www.dena.de/fileadmin/dena/Publikationen/PDFs/2023/Guide_Rethinking_Blockchains_Energy_Consumption.pdf. Accessed 22 June 2024.

impact of electricity consumption while ensuring that the network is suitable for the specific use case.[515]

A critical question that must be posed is whether developing countries such as South Africa, can meet the demands of a blockchain electricity-efficient design.[516] It can be argued that the implementation of a blockchain electricity-efficient design in South Africa may struggle for sustainability due to perennial electricity price increases and an unstable electricity grid. The success of a blockchain electricity-efficient design is thus contingent on a reliable, consistent, and cheap source of energy supply. Another important factor to consider is the support, or the lack thereof, from the government. If a tax authority is to consider using blockchain or any other technological advancement to administer tax, political backing will be required.[517]

It should be noted that high electricity costs and high energy consumption associated with permission blockchains, and bitcoin mining has forced countries to reposition mining facilities in cooler environments.[518] This is primarily due to the apparent inexpensive electricity costs and the reduced energy consumption in cooler environments.[519] The viability of extending mining facilities to cooler environments is a decision that is not readily available to developing countries. In my view, it is more realistic for developing countries to adopt and implement permissioned blockchains as opposed to using permissionless blockchains. Delmotte supports this view.[520]

[515] Deutsche Energie-Agentur (Publisher) (dena, 2023) “Rethinking Blockchain’s Electricity Consumption – A Guide to Electricity- Efficient Design of Decentralized Data-Infrastructure” at 76. Available at https://www.dena.de/fileadmin/dena/Publikationen/PDFs/2023/Guide_Rethinking_Blockchain_s_Energy_Consumption.pdf. Accessed 22 June 2024.

[516] This may prove problematic for developing countries that rely on neighbouring countries for electricity supply. The increased electricity costs of bitcoin mining coupled with an unreliable electricity supply could prove to be a hurdle too great for most developing countries. Having said that, the implementation of blockchain technology will depend on political will and a state’s ability to balance the potential benefits of blockchain against electricity costs. It may be necessary for states to adopt renewable energy as alternative sources of energy in order to facilitate blockchain transactions.

[517] Bird, M., R., and Zolt M., E. (2008). “Technology and taxation in developing countries: from hand to mouse” *National Tax Journal* at 796 – 797. See also extended discussion in chapter 3 below.

[518] Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the technology behind bitcoin is changing money, business and the world* Portfolio Penguin at 261.

[519] Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the technology behind bitcoin is changing money, business and the world* Portfolio Penguin at 261.

[520] Delmotte, C. (2022). “The Promises and Pitfalls of a Blockchain Driven Tax System” at 31. Available at https://ssrn.com/abstract=4187919. Accessed 6 October 2022.

Delmotte uses the example of possibly introducing a blockchain driven sales tax[521] in the US. For this to succeed, Delmotte argues that it may be necessary to introduce blockchain at state level than federal level because it is easier to work on a smaller scale.[522]

Countries can consider renewable energy as an alternative source of energy. For example, suitable locations that have an abundant water supply can be used to source bitcoin mining.[523] The use of renewable energy can reduce the burden on the electricity grid while also maintaining a sustainable and environmentally friendly means of energy production. Moreover, and as discussed above, electricity costs can be alleviated by using a *proof-of-stake* mechanism in permissionless blockchains.[524] *Proof-of-stake* is an alternative consensus mechanism that depends on the amount of coins that a participant stores at any given time.[525] The more 'stake' (coins) that a participant holds, the higher the chances of authenticating transactions. Once a participant has authenticated a transaction, they are rewarded with transaction fees.[526] Since no computational power takes place during *proof-of-stake*, energy[527] is

[521] Sales tax is equivalent to VAT.

[522] Delmotte, C. (2022). "The Promises and Pitfalls of a Blockchain Driven Tax System" at 31. Available at https://ssrn.com/abstract=4187919. Accessed 6 October 2022.

[523] Alternative renewable energy sources such as solar power, hydro power, and wind energy can be considered.

[524] Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 10. Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the technology behind bitcoin is changing money, business and the world* Portfolio Penguin at 40.

[525] Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 10; Kianieff, M. (2019) *Blockchain Technology and the Law Opportunities and Risks* Routledge Publishing (UK) at 102; Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the technology behind bitcoin is changing money, business and the world* Portfolio Penguin at 32; Vigna, P., & Casey, M., J. (2016). *The Age of Cryptocurrency: How Bitcoin and the Blockchain are Challenging the Global Economic order* Picador USA at 158; Hacker, P., Lianos, L., Dimitropoulos, G., Eich, S., (eds) (2019) *Regulating Blockchain: Techno-social and Legal challenges* Oxford University Press (UK) at 338.

[526] Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 10; Kianieff, M. (2019) *Blockchain Technology and the Law Opportunities and Risks* Routledge Publishing (UK) at 102; Hacker, P., Lianos, L., Dimitropoulos, G., Eich, S., (eds) (2019) *Regulating Blockchain: Techno-social and Legal challenges* Oxford University Press (UK) at 338.

[527] It should be pointed that sub–Saharan Africa is currently experiencing rolling blackouts. Zambia and Zimbabwe currently have rolling blackouts because of drought. No rain means the hydroelectric plants cannot operate optimally. South Africa's rolling blackouts have been well documented. South Africa has been experiencing load shedding for 14 years. The load shedding cripples businesses and negatively impacts on the economy. See Sguazzin, A. (2022). *Who unplugged South Africa?* Available at https://www.washingtonpost.com/business/energy/who-unplugged-south-africa/2022/12/13/33128cb8-7aac-11ed-bb97-f47d47466b9a_story.html. Accessed 13

conserved.[528] While the use of *proof-of-stake* use significantly lower energy compared to *proof-of-work* blockchains, the overall consumption of electricity of networks that do not use *proof-of-work* will vary depending on the computational load each node supports and the number of active nodes on the network.[529]

To summarise, there are measures in place to reduce the costs of electricity from a tax administration perspective. First, tax authorities can use a permissioned blockchain to administer taxes. Using a permissioned blockchain reduces the number of participants on blockchain. If there are fewer participants, fewer nodes will be required to validate transactions thereby reducing electricity costs.[530] Interestingly, Delmotte notes that a public blockchain can be used to administer taxes.[531] Delmotte argues that taxpayers can join a public network to automate their tax payments. In this public network, data on the nature of the sales is not shared with the world.[532] According to Delmotte, no tax data is stored on blockchain. Additionally, a public blockchain can use *zero-knowledge proof*[533] to encrypt tax information.[534] Second, permissioned blockchains reduce a blockchain's energy consumption.[535] Permissioned blockchains do not use the *proof-of-work*[536] consensus mechanism. Permissioned blockchains can be programmed to have one node (for example a tax authority runs the node) that validates tax payments, which avoids thousands of

December 2022. Currently, Taiwan and the American states of California and Texas are experiencing blackouts.

[528] Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 10.

[529] Deutsche Energie-Agentur (Publisher) (dena, 2023) "Rethinking Blockchain's Electricity Consumption – A Guide to Electricity- Efficient Design of Decentralized Data-Infrastructure" at 29. Available at https://www.dena.de/fileadmin/dena/Publikationen/PDFs/2023/Guide_Rethinking_Blockchain_s_Energy_Consumption.pdf. Accessed 22 June 2024.

[530] Kianieff, M. (2019) *Blockchain Technology and the Law Opportunities and Risks* Routledge Publishing (UK) at 37. See also Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the technology behind bitcoin is changing money, business and the world* Portfolio Penguin at 67.

[531] Delmotte, C. (2022). "The Promises and Pitfalls of a Blockchain Driven Tax System" at 23. Available at https://ssrn.com/abstract=4187919. Accessed 6 October 2022.

[532] Delmotte, C. (2022). "The Promises and Pitfalls of a Blockchain Driven Tax System" at 23. Available at https://ssrn.com/abstract=4187919. Accessed 6 October 2022.

[533] See definition and explanation of *zero-knowledge proof* at paragraph 4.8.2.

[534] Delmotte, C. (2022). "The Promises and Pitfalls of a Blockchain Driven Tax System" at 23. Available at https://ssrn.com/abstract=4187919. Accessed 6 October 2022.m

[535] Delmotte, C. (2022). "The Promises and Pitfalls of a Blockchain Driven Tax System" at 24. Available at https://ssrn.com/abstract=4187919. Accessed 6 October 2022.

[536] It should be noted that there are different types of consensus mechanisms. As such, blockchains can use consensus mechanism other than *proof-of-work*.

participants using electricity to validate transactions.[537] This reduces energy consumption in the process.[538] Third, a layer-two protocol[539] solution allows a participant to store data offline and ensures hashes that represent the exchanges are stored online.[540] According to Delmotte, non-tax transactions do not run on a blockchain but on a secondary framework or protocol that is built on top of any existing blockchain.[541] Fourth, governments can privatise blockchains so that the costs associated with running blockchain is spread among users.[542] Last, innovations in energy can be applied to blockchain and new ways to run blockchain with less energy can be uncovered.[543]

2.10.2 Scalability

As already mentioned,[544] blockchains are decentralised in nature. Participants on blockchain network process and validate all the transactions while maintaining a copy of those transactions.[545] This creates challenges for blockchain system. First, the time for validation is extended to ten minutes because each participant must authenticate a transaction.[546] As more transactions continue to be authenticated, blockchain ledger

[537] Delmotte, C. (2022). "The Promises and Pitfalls of a Blockchain Driven Tax System" at 24. Available at https://ssrn.com/abstract=4187919. Accessed 6 October 2022.

[538] Delmotte, C. (2022). "The Promises and Pitfalls of a Blockchain Driven Tax System" at 24. Available at https://ssrn.com/abstract=4187919. Accessed 6 October 2022.

[539] A two-layer protocol is a protocol that "allows transactions between users through the exchange of authenticated messages via a medium which is outside of, but tethered to, a layer-one blockchain. Authenticated assertions are submitted to the parent-chain only in cases of a dispute, with the parent-chain deciding the outcome of the dispute. Security and non-custodial properties of a layer-two protocol rely on the consensus algorithm of the parent-chain." See Gudgeon, L. *et al*, *SoK: Layer-Two Blockchain Protocols* in Bonneau, J. & Heninger, N. (eds) (2020) *Financial Cryptography and Data Security* (Springer Nature, Switzerland) at 204.

[540] Delmotte, C. (2022). "The Promises and Pitfalls of a Blockchain Driven Tax System" at 26 – 27. Available at https://ssrn.com/abstract=4187919. Accessed 6 October 2022.

[541] Delmotte, C. (2022). "The Promises and Pitfalls of a Blockchain Driven Tax System" at 28. Available at https://ssrn.com/abstract=4187919. Accessed 6 October 2022.

[542] Delmotte, C. (2022). "The Promises and Pitfalls of a Blockchain Driven Tax System" at 29. Available at https://ssrn.com/abstract=4187919. Accessed 6 October 2022.

[543] Delmotte, C. (2022). "The Promises and Pitfalls of a Blockchain Driven Tax System" at 29. Available at https://ssrn.com/abstract=4187919. Accessed 6 October 2022.

[544] See paragraph 2.5 above.

[545] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 31; Kasireddy, P., (2017). "*Fundamental challenges with public blockchains*". Available at https://medium.com/@preethikasireddy/fundamental-challenges-with-public-blockchains-253c800e9428. Accessed 13 January 2020.

[546] Kasireddy, P., (2017). "*Fundamental challenges with public blockchains*". Available at https://medium.com/@preethikasireddy/fundamental-challenges-with-public-blockchains-253c800e9428. Accessed 13 January 2020.

increases in size which increases the time to validate transactions.[547] This reduces the number of transactions that can be conducted in a day.[548] Second, information stored on a blockchain cannot be deleted. Data that is continuously added gets stored on every computer node on blockchain.[549] The need for storage space poses a burden on participants because they can be expected to continuously store data.[550] As blockchain continues to grow, the more likely it is for participants to increase their storage capabilities and their computational power.[551] De Fillipi and Wright correctly point out that strenuous requirements may lead to fewer participants partaking in transactions on blockchain.[552]

In the context of blockchain, scalability "refers to its scale capability with the increase of the number of users."[553] Practically, the factors that affect blockchain's scalability include the time required to confirm a transaction, the time consumed when validating a transaction, and the cost generated per confirmed transactions.[554] The need to store large amounts of data on blockchain also affects a blockchain's efficiency.[555] Some of the ways of increasing blockchain scalability include increasing the block size, reducing the hash time, and using different consensus mechanisms.[556] Marwala and Xing posit that artificial intelligence algorithms (such as federated learning) can

[547] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 31 – 32.

[548] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 56.

[549] Kasireddy, P., (2017). "*Fundamental challenges with public blockchains*". Available at https://medium.com/@preethikasireddy/fundamental-challenges-with-public-blockchains-253c800e9428. Accessed 13 January 2020. See also Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 32. De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 56.

[550] Kasireddy, P., (2017). "*Fundamental challenges with public blockchains*". Available at https://medium.com/@preethikasireddy/fundamental-challenges-with-public-blockchains-253c800e9428. Accessed 13 January 2020.

[551] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 56.

[552] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 56.

[553] Marwala, T. & Xing, B. (2018). "Blockchain and Artificial Intelligence" at 7. Available at https://arxiv.org/pdf/1802.04451.pdf. Accessed 8 September 2022.

[554] Marwala, T. & Xing, B. (2018). "Blockchain and Artificial Intelligence" at 7. Available at https://arxiv.org/pdf/1802.04451.pdf. Accessed 8 September 2022.

[555] Van der Laan, J., *Understanding Blockchain* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 70.

[556] Van der Laan, J., *Understanding Blockchain* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 70.

improve the efficiency of blockchain system.[557] According to Gudgeon *et al*, the layer-two protocol can scale blockchains by enabling users to perform off-chain transactions through private and authenticated communication as opposed to storing transactions on the main blockchain.[558] This process reduces transaction load on the main blockchain and is fully backward compatible.[559] Another way to make blockchains scalable is by making them permissioned.[560] This is because permissioned blockchains can designed for specific purposes with different consensus mechanisms.[561] Permissioned blockchains have different levels of control, visibility, and security.[562]

2.10.3 Adoption

Another challenge that arises with the use of blockchain is its adoption in social and government settings.[563] While it is true that blockchain is in its infancy, the social impediments pertaining to its perceived complexity remains one of the biggest hurdles for its adaptation.[564] Blockchain's perceived complexity, coupled with its association with cryptocurrencies, creates the impression that blockchain's use is limited to facilitate cryptocurrency transactions. In addition, major scams leading to financial losses and theft of cryptocurrencies has not improved public image. It can be argued that the hype and excitement around blockchain can influence people to have expectations. If these expectations are not met, people can lose trust in blockchain.[565]

[557] Marwala, T. & Xing, B. (2018). "Blockchain and Artificial Intelligence" at 7. Available at https://arxiv.org/pdf/1802.04451.pdf. Accessed 8 September 2022.

[558] Gudgeon, L. *et al*, *SoK: Layer-Two Blockchain Protocols* in Bonneau, J. & Heninger, N. (eds) (2020) *Financial Cryptography and Data Security* (Springer Nature, Switzerland) at 202.

[559] Gudgeon, L. *et al*, *SoK: Layer-Two Blockchain Protocols* in Bonneau, J. & Heninger, N. (eds) (2020) *Financial Cryptography and Data Security* (Springer Nature, Switzerland) at 202.

[560] Atzori, M. (2017). "Blockchain technology and decentralized governance: is the states still necessary?" *Journal of Governance and Regulation* 6(1): 53.

[561] Atzori, M. (2017). "Blockchain technology and decentralized governance: is the states still necessary?" *Journal of Governance and Regulation* 6(1): 53.

[562] Atzori, M. (2017). "Blockchain technology and decentralized governance: is the states still necessary?" *Journal of Governance and Regulation* 6(1): 53.

[563] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 32. De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 57.

[564] Hacker, P., Lianos, L., Dimitropoulos, G., Eich, S., (eds) (2019) *Regulating Blockchain: Techno-social and Legal challenges* Oxford University Press (UK) at 33.

[565] Manrique, S. (2018). *Blockchain: A Proof of Trust* Master thesis (Delft University of Technology) at 32. Available at https://repository.tudelft.nl/islandora/object/uuid%3Ac1996e12-1462-4683-8716-72110c665d4c. Accessed 14 January 2020.

The growth of blockchains and its potential uses will ultimately depend on the role the government plays in its adoption and regulation.[566] It is likely that governments will inevitably pass laws aimed at regulating blockchain. The way blockchain laws and regulations are promulgated can influence people's perceptions towards blockchain. Laws that are too cumbersome and complex can affect interest and general levels of compliance. If laws are too lenient or passive, participants and other important role players can easily manipulate blockchain system. Finding the right balance is key because a balanced blockchain-based regulatory framework can encourage blockchain use cases.[567]

2.10.4 Blockchain specialists

Due to blockchain's novelty, it is possible to have little or no personnel specializing in blockchain technology from a legal and information technology (IT) perspective.[568] The presence or absence of blockchain specialists can influence a government's approach towards blockchain regulation. A lack of competent and qualified blockchain advisers can also delay governments' efforts to implement and adopt blockchain technology.

From a legal perspective, various issues pertaining to consumer protection, law of contract, international law, criminal law, tax law, competition law, privacy, and law of copyright are some of the laws that interplay with the application of blockchain technology in society.[569] Generally, lawyers and legal scholars have an advanced understanding of the law. It can be said that the role of lawyers and legal scholars can revolve around the interaction between code (blockchain) and the law. It seems

[566] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 4. See also De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 57.

[567] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 57; Finck, M. (2018). Blockchains: Regulating the Unknown *German Law Journal* 19(4): 667; Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the technology behind bitcoin is changing money, business and the world* Portfolio Penguin at 264.

[568] Deloitte (2017). "Blockchain technology and its potential in taxes" at 18. Available https://www2.deloitte.com/content/dam/Deloitte/pl/Documents/Reports/pl_Blockchain-technology-and-its-potential-in-taxes-2017-EN.PDF. Accessed 14 January 2020.

[569] See Deloitte (2019). "Blockchain: Legal implications, questions, opportunities and risks" at 10 – 11. Available at https://www2.deloitte.com/content/dam/Deloitte/za/Documents/legal/za_legal_implications_of_blockchain_14052019.pdf. Accessed 14 January 2020.

plausible that authorities will look to legal experts for expertise on the continued advancements of the technology and its effects on law and society.

The role played by IT specialists cannot be overstated. Blockchain technology's underlying infrastructure is computer code. Blockchain and its subservient applications require the services of IT specialists with expertise in cryptography, computer programming, and coding.[570] Like all computer systems, it is possible for blockchain to have coding errors. Coding errors can only be rectified by specialists who possess an advanced understanding of cryptography and blockchain system's mechanics.[571] IT specialists can identify any coding and programming errors and advise the relevant officials on how these errors can be rectified.[572] In the absence of individual IT specialists, it may be necessary for governments to request assistance from entities that develop code for blockchain.[573]

2.11 Conclusion

Blockchain is one of the most important technological discoveries post the 2008 financial crisis. While it is true that the bitcoins have received a lot of attention, blockchain is the system that enables users to transfer bitcoins on a peer-to-peer network. One of blockchain's heralded features is transparency. Transparency promotes trust because all the participants on blockchain can view all the transactions if they are granted viewing rights on blockchain. Transparency can build trust between tax authorities and foreign suppliers of digital goods.[574] Immutability is an essential feature of blockchain. Foreign supplier's data on blockchain can engender data reliability. Data can be made available to tax authorities in real-time.

This chapter has shown that a private blockchain is the most suitable type of blockchain for the collection of VAT on the cross-border supply of digital goods. Privacy can be provided by ensuring that only vetted participants can have access to

[570] Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 31.
[571] See Werbach, K. (2018). *The Blockchain and the New Architecture of Trust* Massachusetts Institute of Technology Press (US) at 118.
[572] Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 31.
[573] See De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 181.
[574] See extensive discussion in chapter 3 below.

the network. Moreover, the dissemination of information, if applicable, is limited to the participants on the network.

This chapter has shown that a smart contract can be programmed to remit VAT to the relevant tax authorities in real-time. *Oracles* can be deployed where human intervention is required. It was also established that smart contracts can be susceptible to programming errors. This can be resolved by conducting rigorous testing before smart contracts are deployed.

The next chapter discusses how VAT can be collected and administered on blockchain.

CHAPTER 3: THE COLLECTION OF VALUE-ADDED TAX ON BLOCKCHAIN

3.1 Introduction

The previous chapter discusses blockchain and its various characteristics. Blockchain has the necessary characteristics that are conducive for the collection of VAT on the cross-border supply of digital goods and services. Currently, tax authorities rely on businesses (suppliers),[575] intermediaries,[576] and consumers[577] for the collection and remittance of VAT. The reliance on businesses, intermediaries, and natural persons creates unintended consequences for all the parties involved in the VAT administration process. For example, natural persons may not be aware of their tax obligation when importing digital goods or services from a foreign non-vendor supplier.[578] A natural person's lack of awareness in the collection and remittance of VAT leads to little or no VAT collection.

Where intermediaries are tasked with the collection of VAT on the cross-border supply of digital goods, a compliance burden is imposed on them. Often, an intermediary's obligation to collect and remit VAT stems from legislation or it may stem from an agreement concluded between the intermediary and the principal supplier.[579] However, if there is no incentive for the intermediary to collect and remit VAT on behalf of the principal supplier, then it is likely that VAT will go uncollected.

Tax authorities incur administrative costs when VAT is administered. The administrative costs are increased if natural persons, suppliers, and intermediaries fail to comply with VAT laws. This creates pressure on the *fiscus*. Tax authorities do not

[575] The supplier is the VAT registered vendor or the person/entity that is required to register as a VAT vendor.
[576] Where the VAT legislation makes provision for a VAT intermediary in the form of an agent or platform. In the case of a platform, see for example the OECD 2023 *VAT Digital Toolkit for Africa* chapter 4.
[577] In the reverse-charge mechanism.
[578] See section 14 of the VAT Act.
[579] See section 54(2B) of the VAT Act.

have the resources available to ensure that every taxpayer complies with the VAT laws. Other factors that burden the VAT administrative process include delays in remittance, the inability to identify taxpayers, a lack of trust between taxpayers and tax authorities, the lack of co-operation from taxpayers, tax fraud, tax evasion, and the inability to audit suppliers.[580]

The adoption of blockchain technology for the collection VAT offers much promise. For starters, blockchain's infrastructure simplifies the recording of transactions. Once recorded, transactions can no longer be deleted on a blockchain. The presence of a tax authority on a blockchain network is beneficial because tax audits can take place.[581] Tax audits are made possible because blockchain is transparent in nature. All transactions can be stored and recorded on blockchain. Tax authorities can verify the accuracy of the data processed by suppliers. Whenever a tax authority wants to access tax related data, it can merely do so by accessing the records stored on blockchain.[582]

In this chapter, I briefly outline the VAT collection processes on the online cross-border trade of digital goods in South Africa. I also highlight how and to what extent blockchain addresses some of the issues with the current VAT collection process. Then, I discuss how blockchain technology can be used to collect VAT on the cross-border supply of digital goods and services.[583] To achieve this, I discuss how a tax authority can set-up a blockchain for VAT collection purposes. I then discuss the various ways in which blockchain can be used to collect VAT. Second, I discuss the benefits of using blockchain as a model for collecting VAT. Third, I look at the challenges associated with the collection of VAT on blockchain.

[580] This is not an exhaustive list. See also Van Zyl, S. P. (2013). *The collection of Value Added Tax on online cross-border trade in Digital Goods*. Unpublished LLD thesis (UNISA) at 304.

[581] Merkx, M. (2019). "VAT and Blockchain: Challenges and Opportunities ahead" *EC Tax Review* 28(2): 88.

[582] PWC (2016). "How blockchain technology could improve the tax system" at 2. Available at https://www.pwc.co.uk/issues/futuretax/assets/documents/how-blockchain-could-improve-the-tax-system.pdf. Accessed 24 March 2021.

[583] While this study primarily looks at blockchain technology and its possible adoption for the collection of VAT on the cross-border supply of digital goods, it must be noted that blockchain technology can also be implemented to collect VAT at a local sphere. Importantly, it is possible for SARS to implement blockchain for the administration of income tax and withholding tax.

3.2 The collection of VAT on B2C online trade in digital goods in South Africa: The current position

In this section, I demonstrate how the current VAT collection process works in South Africa.

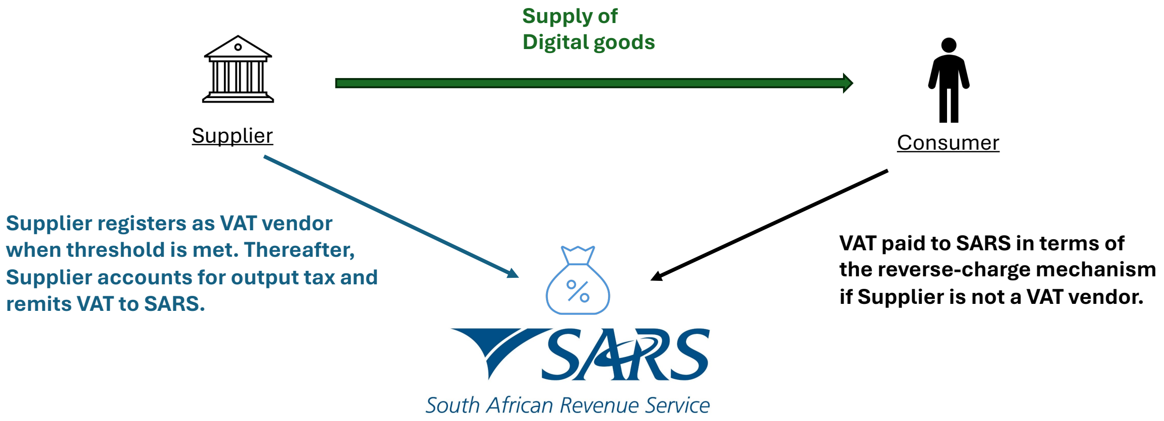

Supply of
Digital goods
Supplier
Consumer
Supplier registers as VAT vendor when threshold is met. Thereafter, Supplier accounts for output tax and remits VAT to SARS.
VAT paid to SARS in terms of the reverse-charge mechanism if Supplier is not a VAT vendor.
%
SARS
South African Revenue Service

Figure 5[584]

In South Africa, a transaction is susceptible to VAT if it conforms to the provisions of the VAT Act.[585] The VAT Act provides that VAT is levied[586] on the supply of imported services; the importation of goods into South Africa; and on the supply of goods and services by a vendor in the course or furtherance of an enterprise.[587] If a person imports goods into South Africa, they must pay VAT to SARS. If a person imports services, they must also pay VAT to SARS. A vendor is liable to pay VAT once they supply goods or services in the course or furtherance of any enterprise.[588]

[584] **Figure 5** demonstrates the current position in South Africa regarding the collection of VAT from the cross-border supply of digital goods. Authors own work.

[585] Kabwe, R. & van Zyl, S.P. (2021). "The value-added tax in the digital economy: a fresh look at the South African dispensation" *Obiter* 42(3): 501.

[586] Currently at fifteen per cent.

[587] Section 7(1) of the VAT Act.

[588] Section 7(2) of the VAT Act.

The supply of digital goods in South Africa forms part of the definition of 'services',[589] particularly 'electronic services'.[590] The definition of 'electronic services' in the VAT Regulations[591] include any services supplied on the Internet for a consideration. The definition of 'electronic services' is broad enough to include all forms of services that can be bought on the Internet.[592] According to Kabwe and van Zyl, there are instances where the possibility of double taxation of a service arises in the jurisdiction of origin and in South Africa.[593] Kabwe and van Zyl provide an example where a service, such as consulting, is physically rendered, used and consumed in a foreign jurisdiction but can also be subject to VAT in South Africa if the advice is emailed to a South African consumer.[594] This is issue is compounded by the lack of clear *place of supply* rules in the VAT Act. Since South Africa follows the destination principle, all economic activities used and consumed in South Africa should be taxed in South Africa.[595] Consequently, the VAT Act applies to South African residents and to the supply of electronic services to South African consumers by foreign suppliers.[596]

The problem that tax authorities face is identifying the consumer of digital goods or ascertaining whether the digital goods are consumed in South Africa.[597] Having *place of supply* rules helps establish where the supply is made or where the digital goods

[589] Section 1 of the definition of services reads: "means anything done or to be done, including the granting, assignment, cession or surrender of any right or the making available of any facility or advantage, but excluding a supply of goods, money or any stamp, form or card contemplated in paragraph (c) of the definition of "goods".

[590] The definition of 'electronic services' has been provided above. See chapter 1, footnote 3.

[591] Regulations Prescribing electronic services for the purpose of the definition of "electronic services" in section 1 of the Value-Added Tax Act, 1991.

[592] The definition of electronic services specifically excludes: "educational services supplied from a place in an export country and regulated by an educational authority in terms of the laws of that export country; or telecommunications services; or services supplied from a place in an export country by a company that is not a resident of the Republic to a company that is a resident of the Republic if: both those companies form part of the same group of companies; and the company that is not a resident of the Republic itself supplies those services exclusively for the purposes of consumption of those services by the company that is a resident of the Republic." See section 2of the definition of 'electronic services' in the VAT Regulations.

[593] Kabwe, R. & van Zyl, S.P. (2021). "The value-added tax in the digital economy: a fresh look at the South African dispensation" *Obiter* 42(3): 506.

[594] Kabwe, R. & van Zyl, S.P. (2021). "The value-added tax in the digital economy: a fresh look at the South African dispensation" *Obiter* 42(3): 506.

[595] See Kabwe, R. & van Zyl, S.P. (2021). "The value-added tax in the digital economy: a fresh look at the South African dispensation" *Obiter* 42(3): 507.

[596] Kabwe, R. & van Zyl, S.P. (2021). "The value-added tax in the digital economy: a fresh look at the South African dispensation" *Obiter* 42(3): 507.

[597] Kabwe, R. & van Zyl, S.P. (2021). "The value-added tax in the digital economy: a fresh look at the South African dispensation" *Obiter* 42(3): 507.

are consumed. In doing so, tax authorities can collect the right amount of tax.[598] If VAT laws do not provide for specific *place of supply* rules, proxies are used. For purposes of VAT, a proxy can be defined as "a deemed place of consumption that assists in establishing the jurisdiction of taxation."[599] In South Africa, the *place of supply* rules is closely linked to whether a supplier of electronic services carries on an 'enterprise'. In terms of the VAT Act, an 'enterprise' is defined as:

> "in the case of any vendor, any enterprise or activity which is carried on continuously or regularly by any person in the Republic or partly in the Republic and in the course or furtherance of which goods or services are supplied to any other person for a consideration, whether or not for profit, including any enterprise or activity carried on in the form of a commercial, financial, industrial, mining, farming, fishing, municipal or professional concern or any other concern of a continuing nature or in the form of an association or club"[600]

The definition of 'enterprise' is broad enough to include the supply of digital goods to a South African consumer. Furthermore, the VAT Act provides proxies to ascertain whether a supply of electronic services is taxable in South Africa. A supplier of electronic services carries on an enterprise in South Africa if: (i) the recipient of electronic services resides in South Africa; (ii) the payment originates from a bank in South Africa; and (iii) the recipient of the electronic services has a postal, residential, or business address in South Africa.[601] It should be noted that two of the three requirements mentioned above must be present in order to establish the residency of the consumer.[602] It should be further noted that the onus rests on the supplier of electronic services to ascertain the residency of the consumer.[603] This creates an unnecessary compliance burden on suppliers of electronic services. In other words, foreign suppliers must use all available resources to identify the consumer of digital goods. Since the VAT Act does not indicate the effort required to determine the

[598] Kabwe, R. & van Zyl, S.P. (2021). "The value-added tax in the digital economy: a fresh look at the South African dispensation" *Obiter* 42(3): 508.

[599] Kabwe, R. & van Zyl, S.P. (2021). "The value-added tax in the digital economy: a fresh look at the South African dispensation" *Obiter* 42(3): 508 at footnote 53.

[600] Section 1(a) of the definition of "enterprise" in the VAT Act.

[601] Section 1(b)(vi) of the definition of "enterprise" in the VAT Act.

[602] Section 1(b)(vi) of the definition of "enterprise" in the VAT Act.

[603] Kabwe, R. & van Zyl, S.P. (2021). "The value-added tax in the digital economy: a fresh look at the South African dispensation" *Obiter* 42(3): 511.

residency of the consumer, Kabwe and van Zyl submit that a supplier of electronic services must corroborate the consumer's credit card details, IP address, and billing address with the residency address.[604]

3.2.1 Foreign vendor registration

Foreign suppliers of electronic services[605] that meet the threshold[606] and carry on an enterprise, must register as VAT vendors in South Africa. The registration process has been streamlined to make it simpler for foreign suppliers to register in South Africa. A foreign supplier must register on the SARS website and download a VAT 101 form. Once the form has been filled, it must be emailed together with supporting documents to SARS at eCommerceRegistration@sars.gov.za.[607] A foreign supplier is not required to have a physical presence in South Africa. This poses challenges for tax authorities in South Africa because it is difficult to verify the existence of a foreign supplier. As a result, a foreign supplier may submit fake invoices to benefit from an input VAT deduction.[608]

Once a foreign supplier receives confirmation of registration, a foreign supplier must issue a tax invoice to a consumer withing 21 days of supply.[609] The invoice must contain: (i) the name and VAT registration number of the electronic services supplier; (ii) the name and address of the electronic services recipient; (iii) a individualised serial number; (iv) date of issue; (v) description of the electronic services supplied; (vi) the consideration in money for the supply in the currency of any country; and (vii) the exchange rate used.[610] The foreign supplier of electronic services must account for

[604] Kabwe, R. & van Zyl, S.P. (2021). "The value-added tax in the digital economy: a fresh look at the South African dispensation" *Obiter* 42(3): 511.

[605] See definition at paragraph 1.1, footnote 3 above.

[606] Currently R1 million per annum.

[607] SARS (2023). *Supply of electronic services by foreign suppliers and foreign intermediaries* at 4. Available at https://www.sars.gov.za/wp-content/uploads/Ops/Guides/VAT-REG-02-G02-Supply-of-Electronic-Services-by-Foreign-Suppliers-and-Foreign-Intermediaries-External-Guide.pdf. Accessed 12 October 2023; see also Kabwe, R. & van Zyl, S.P. (2021). "The value-added tax in the digital economy: a fresh look at the South African dispensation" *Obiter* 42(3): 514 – 515.

[608] Kabwe, R. & van Zyl, S.P. (2021). "The value-added tax in the digital economy: a fresh look at the South African dispensation" *Obiter* 42(3): 514 – 515.

[609] Section 20(1) of the VAT Act.

[610] SARS (2016). *Binding General Ruling (VAT) No 28 Issue 2* at 1 – 2. Available at https://www.sars.gov.za/wp-content/uploads/Legal/Rulings/BGR/LAPD-IntR-R-BGR-2015-03-BGR28-Electronic-Services.pdf. Accessed 15 July 2021.

and remit VAT to SARS. It should be noted that if a consumer purchases digital goods from a non-registered foreign supplier, the recipient must obtain and fill the necessary forms prescribed by SARS and calculate the tax payable on the value of the imported services at a rate of fifteen per cent.[611] Even if a foreign supplier is liable to pay VAT on a supply, but fails to do so, the recipient consumer becomes responsible to collect and remit VAT to SARS.[612] As mentioned above,[613] the reverse-charge mechanism relies on the integrity of the recipient of imported services. Without the recipient's compliance, VAT goes uncollected because the recipient is often unaware of their tax liability.[614]

SARS inserted a proviso in section 23(1A) of the VAT Act that provides that if a foreign supplier of electronic services or a foreign intermediary exceeds the compulsory registration threshold in a consecutive period of 12 months due to a consequence of abnormal circumstances of a temporary nature, then the foreign supplier or foreign intermediary will not be liable for VAT.[615] According to SARS, this amendment reduces the administrative burden on foreign suppliers of electronic services and it aims at "achieving parity with the concession granted to domestic vendors."[616]

Kabwe and van Zyl correctly state that there are no provisions in the VAT Act that permit SARS to monitor the compliance of foreign suppliers of electronic services.[617] In fact, it can be argued that SARS relies on the honesty of foreign suppliers to comply with the provisions of the VAT Act. Moreover, and in the absence of international

[611] Section 14(1) of the VAT Act.

[612] Kabwe, R. & van Zyl, S.P. (2021). "The value-added tax in the digital economy: a fresh look at the South African dispensation" *Obiter* 42(3): 516.

[613] See discussion in chapter 1.1.

[614] Kabwe, R. & van Zyl, S.P. (2021). "The value-added tax in the digital economy: a fresh look at the South African dispensation" *Obiter* 42(3): 526.

[615] Section 23(1A) of the VAT Act; see also SARS (2023). *Supply of electronic services by foreign suppliers and foreign intermediaries* at 3. Available at https://www.sars.gov.za/wp-content/uploads/Ops/Guides/VAT-REG-02-G02-Supply-of-Electronic-Services-by-Foreign-Suppliers-and-Foreign-Intermediaries-External-Guide.pdf. Accessed 12 October 2023.

[616] SARS (2023). *VAT Connect Issue 16 (August 2023)*. Available at https://www.sars.gov.za/businesses-and-employers/my-business-and-tax/newsletters/vat-connect-issue-16-august-2023/#:~:text=Registration%20of%20foreign%20electronic%20service,any%20consecutive%2012%2Dmonth%20period. Accessed 12 October 2023.

[617] Kabwe, R. & van Zyl, S.P. (2021). "The value-added tax in the digital economy: a fresh look at the South African dispensation" *Obiter* 42(3): 516.

agreements, SARS does not have extra-territorial powers to impose penalties on non-compliant foreign suppliers of electronic services.[618]

3.3 How VAT can be collected on blockchain

3.3.1 Setting up blockchain

From the outset, it is important to note that the establishment of a blockchain varies from one institution to another. Thus, the needs and requirements for each institution adopting blockchain will likely differ at structural and organisational level.[619] As such, there is no "one size fits all." For example, it is unlikely that a tax authority will make use of a public blockchain to collect VAT due to the risks associated with unrestricted accessibility and the *proof-of-work* consensus mechanism.[620] As discussed earlier,[621] it is prudent for a tax authority to consider a private blockchain for the collection of VAT. In a private blockchain, identified suppliers (participants) can be required to join the private blockchain network to record, and remit the VAT amount to the tax authority. Access on the private blockchain can be granted to participants only if blockchain is permissioned.[622] In other words, only identified participants can join the network at any given time. This also ensures that the supplier is identified and known to the relevant tax authority beforehand. For access to be granted, blockchain's code must be programmed in such a way that only pre-selected participants are admitted inside the network subject to a vetting process.[623] It is also possible to admit participants on a case-by-case basis depending on the tax authority's discretion.[624]

[618] Kabwe, R. & van Zyl, S.P. (2021). "The value-added tax in the digital economy: a fresh look at the South African dispensation" *Obiter* 42(3): 516.

[619] Iredale, G. (2019). "Introduction to Permissioned Blockchains." Available at https://101blockchains.com/permissioned-blockchain/. Accessed 3 May 2021.

[620] See Chapter 2, paragraph 2.6 above.

[621] See Chapter 2, paragraph 2.6 above.

[622] The view that permissioned blockchains is conducive for the administration of VAT is also supported by Ainsworth and Alwohaibi. See Ainsworth, R., T. & Alwohaibi, M. (2017). "Blockchain, Bitcoin and VAT in the GCC: The Missing Trader Example" *Boston University School of Law, Law & Economics Working Paper No. 17-05* at 8. Available at http://www.bu.edu/law/files/2017/03/BLOCKCHAIN-BITCOIN-VAT-in-the-GCC.pdf. Accessed 21 May 2021.

[623] Richter, T., *Blockchain Regulation* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 127.

[624] Richter, T., *Blockchain Regulation* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 127.

A tax authority can either build (program)[625] its own blockchain or it can have blockchain built and licenced by a third party.[626] In my view, it is beneficial for a tax authority to program its own blockchain for several reasons. This view is supported by Mazur.[627] The first reason is that the tax authority must avoid paying licensing fees to the third-party owner of blockchain. The funds that would have been paid to the third-party owner can be channelled to other sectors such as blockchain training and education. Second, the creation of blockchain by a third-party implies that the tax authority does not own that specific blockchain. A tax authority can use that blockchain subject to any Intellectual Property (IP) agreement with the third-party.[628] If a tax authority creates its own blockchain, it retains ownership (and copyright in the process) of blockchain in addition to allocating Intellectual Property Rights (IPRs) to any potential user or participant.[629] Third, blockchain can be programmed by the tax authority in a manner that it sees fit. In other words, there is room for flexibility on the overall design of blockchain. Additionally, blockchain can be upgraded and updated when the need arises whilst also considering the possibility of new technical

[625] Section 2 of the South African Copyright Act 98 of 1978 defines a 'computer program' as: "a set of instructions fixed or stored in any manner and which, when used directly or indirectly in a computer, directs its operation to bring about a result."

[626] Bird & Bird. "Private Blockchains" at 1. Available at https://www.twobirds.com/~/media/pdfs/in-focus/blockchain/private-blockchain-briefing-note.pdf. Accessed 26 April 2021.

[627] Mazur, O. (2021). "Can Blockchain Revolutionize Tax Administration?" SMU Dedman School of Law Legal Studies Research Paper No. 510 at 41. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3841785. Accessed 23 June 2021.

[628] See Bird & Bird. "Private Blockchains" at 3. Available at https://www.twobirds.com/~/media/pdfs/in-focus/blockchain/private-blockchain-briefing-note.pdf. Accessed 26 April 2021.

[629] In South Africa, if a person (or group of persons) creates a computer program they obtain copyright over that computer program. Ownership of the copyright vests with the author (creator) of that computer program. Section 2 of the Copyright Act 98 of 1978 defines an 'author' as: "(a) a literary, musical or artistic work, means the person who first makes or creates the work; (b) a photograph, means the person who is responsible for the composition of the photograph; (c) a sound recording, means the person by whom the arrangements for the making of the sound recording were made; (d) a cinematograph film, means the person by whom the arrangements for the making of the film were made; (e) a broadcast, means the first broadcaster; (f) a programme-carrying signal, means the first person emitting the signal to a satellite; (g) a published edition, means the publisher of the edition; (h) a literary, dramatic, musical or artistic work or computer program which is computer-generated, means the person by whom the arrangements necessary for the creation of the work were undertaken; and (i) a computer program, the person who exercised control over the making of the computer program." Furthermore, section 21(1)(a) of the Copyright Act reads: "Subject to the provisions of this section, the ownership of any copyright conferred by section 3 or 4 on any work shall vest in the author or, in the case of a work of joint authorship, in the co-authors of the work." Interestingly, if a public servant (author) creates a computer program whilst working with the state, then the copyright vests with the state. See section 21(2) of the Copyright Act 98 of 1978. See also https://businesstech.co.za/news/it-services/257135/what-you-need-to-know-before-writing-or-developing-code-in-south-africa/. Accessed 3 May 2021.

advancements to blockchain technology. Fourth, the creator of blockchain can have a bearing on the level of trust afforded by participants, creating the perception of legality.[630] It is possible for the participants to trust blockchain network if blockchain has been created by a government.[631] Fifth, if tax authorities are at the forefront of blockchain's development, it is possible that the tax authority's ability to automate the tax process and further improve the administration of tax, will be enhanced.[632] Last, the creation of a blockchain can potentially be a means for a tax authority to encode and subsequently apply its rules and regulations in an orderly and automatic manner.[633] Put it differently, a tax authority can enforce its respective rules and regulations on VAT through code embedded in blockchain.

It is important to note that a blockchain has five layers.[634] The hardware infrastructure layer contains physical resources like nodes that are required to run a blockchain.[635] The data layer is the part of blockchain where data is stored. The network layer is responsible for connecting the nodes together on blockchain network.[636] The consensus or protocol layer is the layer that defines and regulates how nodes come to an agreement on a blockchain.[637] The application layer consists of applications that interact with blockchain. For example, the application layer runs smart contracts, dApps, and the user interface.[638]

[630] Richter, T., *Blockchain Regulation* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 128.

[631] See Richter, T., *Blockchain Regulation* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 128.

[632] Mazur, O. (2021). "Can Blockchain Revolutionize Tax Administration?" SMU Dedman School of Law Legal Studies Research Paper No. 510 at 41. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3841785. Accessed 23 June 2021.

[633] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 193; Richter, T., *Blockchain Regulation* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 137.

[634] See Binamite (2023). *5 blockchain layers you should know in 2023*. Available at https://binamite.com/blockchain-layers/. Accessed 16 October 2023.

[635] Binamite (2023). *5 blockchain layers you should know in 2023*. Available at https://binamite.com/blockchain-layers/. Accessed 16 October 2023.

[636] Binamite (2023). *5 blockchain layers you should know in 2023*. Available at https://binamite.com/blockchain-layers/. Accessed 16 October 2023.

[637] John, F., Oleh, M. & Luciano, C. (2023). *Blockchain architecture layers: a comprehensive guide*. Available at https://hacken.io/discover/blockchain-architecture-layers/. Accessed 16 October 2023.

[638] John, F., Oleh, M. & Luciano, C. (2023). *Blockchain architecture layers: a comprehensive guide*. Available at https://hacken.io/discover/blockchain-architecture-layers/. Accessed 16 October 2023.

There are at least two types of software code that must be programmed in the context of blockchain.[639] In the first instance, the upper layer of code consists of a program designed for blockchain itself (operating system). The second code that must be embedded is the smart contract code. This is a separate code, referred to as the "app" (application), that can be executed on blockchain.[640] Depending on the model used, a tax authority can create a form of digital tax currency exclusively for VAT collection.[641]

There are different rights that can be made available on a blockchain. Access rights are rights given to access blockchain network and to read data on the ledger.[642] Users given access rights only view what happens on a blockchain but do not take part in the development of the network and the writing of new data.[643] Typically, entities or persons with access rights have limited roles such as monitoring and auditing.[644] In the VAT collection context, foreign suppliers can be granted access rights for purposes of VAT remittance and data storage. Foreign suppliers do not have monitoring and auditing roles on blockchain because that role is reserved for the tax authority. Control rights grant users the capability to ratify and monitor decisions on a blockchain.[645] Control rights should be reserved for tax authorities since they are ultimately responsible for blockchain. Management rights authorise the decision proposals and implementation of decisions.[646] Last, decision rights are conferred on users that "have

[639] Richter, T., *Blockchain Regulation* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 137.

[640] Richter, T., *Blockchain Regulation* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 137.

[641] See paragraphs 3.3.3, 3.3.4 and 3.3.5 below.

[642] Post, D & Cipollini, C. (2023). "Fundamental Elements of a Blockchain-Based Tax System: Governance, Legal and Technology Aspects" *World Tax Journal* 15(3): 3. [unpublished version].

[643] Post, D & Cipollini, C. (2023). "Fundamental Elements of a Blockchain-Based Tax System: Governance, Legal and Technology Aspects" *World Tax Journal* 15(3): 3. [unpublished version].

[644] Post, D & Cipollini, C. (2023). "Fundamental Elements of a Blockchain-Based Tax System: Governance, Legal and Technology Aspects" *World Tax Journal* 15(3): 3. [unpublished version].

[645] Honkanen, P. Nylund, M. Westerlund, M. (2021). "Organizational Building Blocks for Blockchain Governance: A Survey of 241 Blockchain White Papers" *Frontiers in Blockchain* 4 (2021) at 5. Available at https://www.theseus.fi/bitstream/handle/10024/510748/Blockchain_Nylund_et_al.pdf?sequence=1. Accessed 12 November 2023; Post, D & Cipollini, C. (2023). "Fundamental Elements of a Blockchain-Based Tax System: Governance, Legal and Technology Aspects" *World Tax Journal* 15(3): 4. [unpublished version].

[646] Honkanen, P. Nylund, M. Westerlund, M. (2021). "Organizational Building Blocks for Blockchain Governance: A Survey of 241 Blockchain White Papers" *Frontiers in Blockchain* 4 (2021) at 5.

the right to participate in the voting process and contribute to adding a new block."[647] Decision right holders manage the consensus process and determine whether a transaction should be added to blockchain. Once a transaction has been added, they are allowed to write data on blockchain through the consensus mechanism.[648] In my view, the decision right holders should be reserved for the SARS officials since their task will be to ensure that new tax data is audited before it is added to a new block on blockchain.

3.3.1.1 The distributed ledger model

Currently, there are currently two ways to setup a private blockchain.[649] In the first scenario (see **Figure 6** below), a tax authority runs various validator nodes on the network.[650] Validator nodes are a group of computers interconnected to each other via the Internet according to a defined and immutable software protocol.[651] The validator nodes are manned by tax officials responsible for validating transactions before they are recorded on blockchain.[652] A tax authority creates a software app, a smart contract in the context of VAT collection, that communicates with the validator nodes. The software app can be accessed by external participants, subject to identification verification, enabling them to send transactions on blockchain for purposes of

Available at https://www.theseus.fi/bitstream/handle/10024/510748/Blockchain_Nylund_et_al.pdf?sequence=1. Accessed 12 November 2023; Post, D & Cipollini, C. (2023). "Fundamental Elements of a Blockchain-Based Tax System: Governance, Legal and Technology Aspects" *World Tax Journal* 15(3): 4. [unpublished version].

[647] Post, D & Cipollini, C. (2023). "Fundamental Elements of a Blockchain-Based Tax System: Governance, Legal and Technology Aspects" *World Tax Journal* 15(3): 4. [unpublished version].

[648] Post, D & Cipollini, C. (2023). "Fundamental Elements of a Blockchain-Based Tax System: Governance, Legal and Technology Aspects" *World Tax Journal* 15(3): 4. [unpublished version]; see also Honkanen, P. Nylund, M. Westerlund, M. (2021). "Organizational Building Blocks for Blockchain Governance: A Survey of 241 Blockchain White Papers" *Frontiers in Blockchain* 4 (2021) at 5. Available at https://www.theseus.fi/bitstream/handle/10024/510748/Blockchain_Nylund_et_al.pdf?sequence=1. Accessed 12 November 2023.

[649] This is based on a report compiled by Bird & Bird LLP. See "Bird & Bird & Private Blockchains". Available at https://www.twobirds.com/~/media/pdfs/in-focus/blockchain/private-blockchain-briefing-note.pdf. Accessed 26 April 2021.

[650] Bird & Bird. "Private Blockchains" at 2. Available at https://www.twobirds.com/~/media/pdfs/in-focus/blockchain/private-blockchain-briefing-note.pdf. Accessed 26 April 2021.

[651] Richter, T., *Blockchain Regulation* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 152 – 153.

[652] Bird & Bird. "Private Blockchains" at 1. Available at https://www.twobirds.com/~/media/pdfs/in-focus/blockchain/private-blockchain-briefing-note.pdf. Accessed 26 April 2021.

recording.[653] Alternatively, a participant can gain access to the private blockchain network by making use of a computer node. The computer node contains a partial copy of blockchain ledger. A participant gains access to the private blockchain via the app but access is restricted to the part of the ledger that is relevant to the participant.[654]

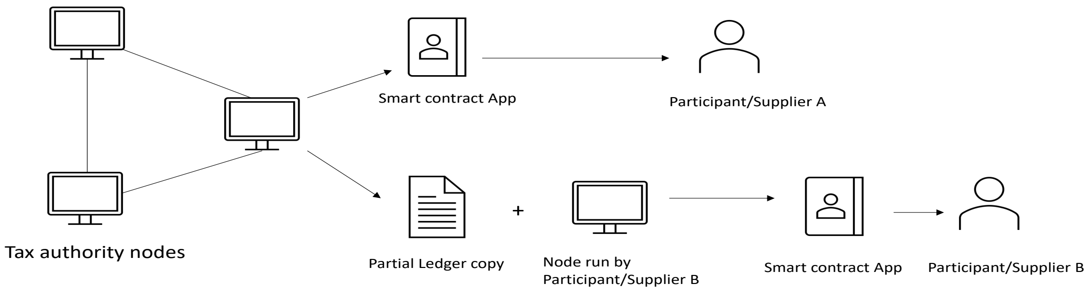


Figure 6[655]

3.3.1.2 Shared ledger model

In this model, a tax authority runs a single node that has the full copy of blockchain ledger. A participant gains access to the private blockchain network by operating a node that contains the app. Once inside the network, the participant accesses a partial copy of the ledger.[656] Regardless of which model is used, if a VAT payment is made, the ledger automatically authenticates the supplier and verifies the qualities of the VAT amount.[657] The tax authority and the supplier are "presented by a unique node that

[653] Bird & Bird. "Private Blockchains" at 1. Available at https://www.twobirds.com/~/media/pdfs/in-focus/blockchain/private-blockchain-briefing-note.pdf. Accessed 26 April 2021.

[654] Bird & Bird. "Private Blockchains" at 1. Available at https://www.twobirds.com/~/media/pdfs/in-focus/blockchain/private-blockchain-briefing-note.pdf. Accessed 26 April 2021.

[655] **Figure 6** is adapted from Bird & Bird. "Private Blockchains" at 2. Available at https://www.twobirds.com/~/media/pdfs/in-focus/blockchain/private-blockchain-briefing-note.pdf. Accessed 26 April 2021.

[656] Bird & Bird. "Private Blockchains" at 2. Available at https://www.twobirds.com/~/media/pdfs/in-focus/blockchain/private-blockchain-briefing-note.pdf. Accessed 26 April 2021.

[657] See Delmotte, C. (2022). "The Promises and Pitfalls of a Blockchain Driven Tax System" at 20. Available at https://ssrn.com/abstract=4187919. Accessed 6 October 2022.

enables seamless identity verification."[658] If a supplier uses blockchain to pay VAT, they can send data about the amount of VAT paid and the date payment was made.[659] The supplier can encrypt the data in the form of a hash while the tax authority can decrypt the hash value with the supplier's public key.[660] Once a tax authority validates the tax payment, a new block is added to blockchain.[661]

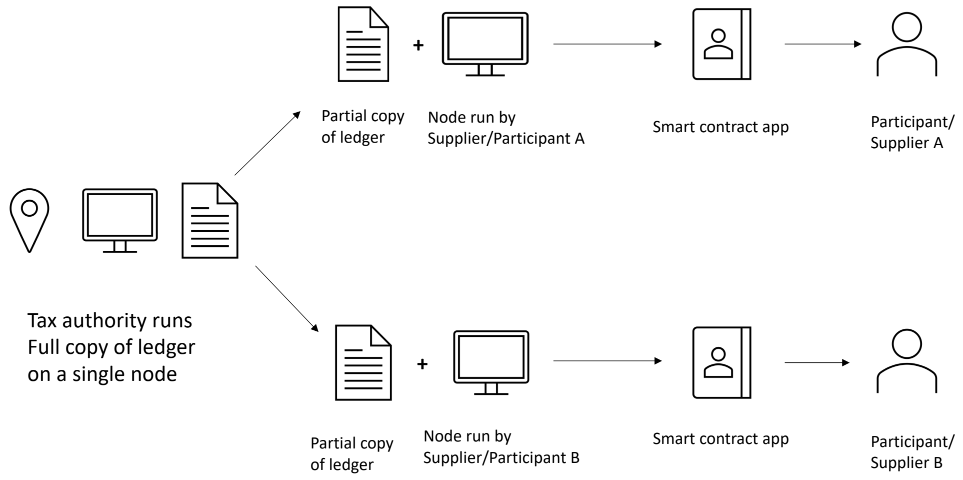


Figure 7[662]

3.3.2 Blockchain frontend and backend

It is important to understand how a supplier can manage the connection to a tax authority's blockchain. The first option requires an IT partner to connect to blockchain

[658] Delmotte, C. (2022). "The Promises and Pitfalls of a Blockchain Driven Tax System" at 20. Available at https://ssrn.com/abstract=4187919. Accessed 6 October 2022.
[659] Delmotte, C. (2022). "The Promises and Pitfalls of a Blockchain Driven Tax System" at 12. Available at https://ssrn.com/abstract=4187919. Accessed 6 October 2022.
[660] Delmotte, C. (2022). "The Promises and Pitfalls of a Blockchain Driven Tax System" at 12. Available at https://ssrn.com/abstract=4187919. Accessed 6 October 2022.
[661] Delmotte, C. (2022). "The Promises and Pitfalls of a Blockchain Driven Tax System" at 12. Available at https://ssrn.com/abstract=4187919. Accessed 6 October 2022.
[662] **Figure 7** is adapted from Bird & Bird. "Private Blockchains" at 2. Available at https://www.twobirds.com/~/media/pdfs/in-focus/blockchain/private-blockchain-briefing-note.pdf. Accessed 26 April 2021.

system on the supplier's behalf.[663] The second option requires the supplier to manage the connection to blockchain themselves.[664] According to Gries *et al*, the first option enables easy onboarding and is cost-efficient while the second option enables maximum control and allows access to blockchain infrastructure.[665] In my view, a tax authority should develop the frontend and backend of blockchain. The frontend is the part of a website that a user sees in a browser and interacts with when data is entered.[666] The tax authority ensures that user interface of the website, applications, or any other software performs optimally.[667] For example, a supplier can access a smart contract on the website interface because the smart contract would have been bound from blockchain developers and then connected to the interface.[668] The backend is the part of blockchain system that runs the database which, in turn, stores the Apps and instructions. The backend connects to the frontend to provide the necessary function.[669] The tax authority runs the backend and ensures that the backend is secured. The tax authority can build an application programming interface (API). The API is an interface that enables a user or supplier to access data on blockchain.[670] The API enables a supplier to transmit or store data on blockchain.

[663] Gries, M., Gurges, K., & Tobai, M. *Blockchain in Tax and Customs Processes* in Owens, J., & Risse, R. (eds) (2021). *Tax Law and Digitalization: The New Frontier for Government and Business: Principles, Use Cases and Outlook* Kluwer Law International at 65.

[664] Gries, M., Gurges, K., & Tobai, M. *Blockchain in Tax and Customs Processes* in Owens, J., & Risse, R. (eds) (2021). *Tax Law and Digitalization: The New Frontier for Government and Business: Principles, Use Cases and Outlook* Kluwer Law International at 65.

[665] Gries, M., Gurges, K., & Tobai, M. *Blockchain in Tax and Customs Processes* in Owens, J., & Risse, R. (eds) (2021). *Tax Law and Digitalization: The New Frontier for Government and Business: Principles, Use Cases and Outlook* Kluwer Law International at 65.

[666] Crypton Studio (2022). *Frontend developer on a blockchain project*. Available at https://medium.com/coinmonks/frontend-developer-on-a-blockchain-project-9d0c496fd38. Accessed 20 August 2023.

[667] Crypton Studio (2022). *Frontend developer on a blockchain project*. Available at https://medium.com/coinmonks/frontend-developer-on-a-blockchain-project-9d0c496fd38. Accessed 20 August 2023.

[668] Crypton Studio (2022). *Frontend developer on a blockchain project*. Available at https://medium.com/coinmonks/frontend-developer-on-a-blockchain-project-9d0c496fd38. Accessed 20 August 2023.

[669] Sharma, T. K. (2018). *How To Architect A Blockchain Application?* Available at https://www.blockchain-council.org/blockchain/how-to-architect-a-blockchain-application/#:~:text=Frontend%20–%20This%20is%20typically%20written,use%20for%20conventional%20web%20applications. Accessed 20 August 2023.

[670] According to Amazon Web Services (AWS), an API is a "mechanism that enables two software components to communicate with each other using a set of definitions and protocols." See AWS (2023). *What is an API (Application Programming Interface)?* Available at https://aws.amazon.com/what-is/api/#:~:text=API%20stands%20for%20Application%20Programming,of%20service%20between%20two%20applications. Accessed 24 August 2023.

Moreover, a supplier can retrieve data from blockchain if they have permission to do so.

3.3.3 VAT collection using blockchain smart contracts

A consumer purchases digital goods or services from a supplier's platform (*supplier A*). The supplier generates an electronic invoice. The invoice forms the basis upon which the purchase price and the VAT amount is determined by the supplier. The supplier creates an account where all transactions are received (receivable account). The smart contract calculates and divides the purchase price into two separate amounts: the VAT amount and the non-VAT amount. The VAT amount is then transferred to the relevant tax authority's smart contract account in real time.[671] The non-VAT amount is transferred to the supplier's second account (payable account).[672] If a *supplier A* owes a payment to a third-party supplier (*supplier B*), then *supplier A* can pay *supplier B* from the second smart contract account. That account transfers the amount due to *supplier B*. The smart contract calculates the VAT payable and remits the VAT to *supplier A's* tax authority.[673] See **Figure 8** below.

[671] Owens, J. & De Jong, J. (2017). "Taxation on the Blockchain: Opportunities and Challenges" *Tax Notes International* 87(6): 606.

[672] Demirhan, H. *Effective Taxation System by Blockchain Technology* in Hacioglu, U., (ed) (2019). *Blockchain Economics and Financial Market Innovation: Financial Innovations in the Digital Age* (Springer) at 354 – 355; see also Deloitte (2019). "*Business Blockchains*" at 7. Available at https://www2.deloitte.com/content/dam/Deloitte/dk/Documents/strategy/Business%20Blockchain%20in%20Finance.pdf. Accessed 5 April 2021; Rikken, O. (2017). "Blockchain Real Time Tax". Available at https://www.linkedin.com/pulse/blockchain-real-time-tax-olivier-rikken. Accessed 6 April 2021; Deloitte (2017). "Blockchain Technology and its potential in taxes" at 13. Available at https://www2.deloitte.com/content/dam/Deloitte/pl/Documents/Reports/pl_Blockchain-technology-and-its-potential-in-taxes-2017-EN.PDF. Accessed 6 May 2021.

[673] Rikken, O. (2017). "Blockchain Real Time Tax". Available at https://www.linkedin.com/pulse/blockchain-real-time-tax-olivier-rikken. Accessed 6 April 2021.

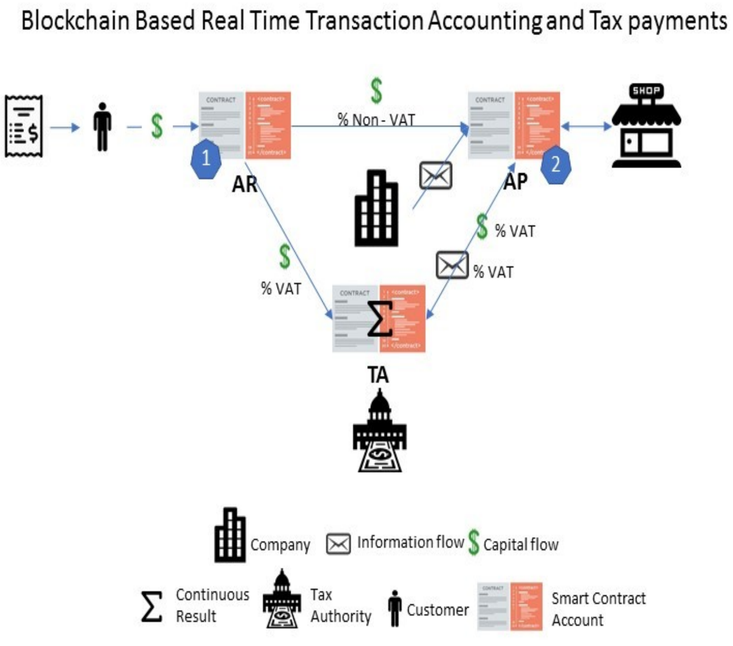


Figure 8[674]

A supplier can store a copy of a digital VAT invoice on blockchain. In my view, the supplier must sign the VAT invoice. This can be done by making use of a digital signature. The purpose of the digital signature is to ensure integrity and authorship of the data on the invoice.[675] This view is supported by Azam and Mazur.[676] Once stored on blockchain, the tax authority can access the digital invoice at any time to verify the accuracy of the VAT remitted by that supplier. Thus, it should be made compulsory for suppliers to issue a digital VAT invoice.[677] In South Africa, it is a statutory requirement

[674] **Figure 8** illustrates how VAT can be collected by means of a blockchain smart contract. **Figure 8** source: Rikken, O. (2017). “Blockchain Real Time Tax”. Available at https://www.linkedin.com/pulse/blockchain-real-time-tax-olivier-rikken. Accessed 6 April 2021.

[675] Ainsworth, R., T. & Todorov, G. (2013). “DICE – Digital Invoice Customs Exchange” Boston University School of Law Working Paper No 13-40. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2314478. Accessed 15 July 2021.

[676] Azam, R. & Mazur, O. (2019). “Cloudy with a chance of taxation” *Florida Tax Review* 22(2): 552.

[677] See Azam, R. & Mazur, O. (2019). “Cloudy with a chance of taxation” *Florida Tax Review* 22(2): 559.

for a VAT vendor[678] to issue a tax invoice containing the necessary particulars whenever a taxable supply is made to a consumer.[679] The particulars of a digital invoice include, among others, the name, address and the VAT registration number of the supplier.[680]

According to SARS *Binding General Ruling 28*,[681] (BGR 28) a supplier of electronic services is required to have their name and VAT registration number; the name and address of the recipient of the electronic services; the date of issue; an individual serialised number; a description of the electronic services supplied and the consideration in money for the supply on an invoice.[682] Interestingly, BGR 28 also states that a supplier of electronic services must contain the exchange rate used.[683] In my view, and in order to simplify matters for suppliers of electronic services, a smart contract can be programmed to consider the appropriate exchange rate[684] into account

[678] See definition in footnote 38 under chapter 1.1 above.

[679] Section 20(1) of the VAT Act. See also section 20(5B) of the VAT Act.

[680] Section 20(4) of the VAT Act. Section 20(4) reads: "except as the Commissioner may otherwise allow, and subject to this section, a tax invoice (full tax invoice) shall be in the currency of the Republic and shall contain the following particulars: (a) The words 'tax invoice', 'VAT invoice' or 'invoice'; (b) the name, address and VAT registration number of the supplier; (c) the name, address and where the recipient is a registered vendor, the VAT registration number of the recipient; (d) an individual serialized number and the date upon which the tax invoice is issued; (e) full and proper description of the goods (indicating, where applicable, that the goods are second-hand goods) or services supplied; (f) the quantity or volume of the goods or services supplied; (g) either (i) the value of the supply, the amount of tax charged and the consideration for the supply or (ii) where the amount of tax charged by applying the tax fraction to the consideration, the consideration for the supply and either the amount of the tax charged, or a statement that it includes a change in respect of the tax and the rate at which the tax was charged: provided that the requirement that the consideration or the value of the supply, as the case may be, shall be in the currency of the Republic shall not apply to a supply that is charged with tax under section 11." *VAT News 20* lists the following information that must be contained in a tax invoice: (1) The name and address and the VAT registration number of the seller; (2) the name and address of the purchaser; (3) a serialised invoice number; (4) the date; (5) the words "tax invoice"; (6) a proper description of the goods or services supplied; (7) the date of issue; (8) the volume or mass of the goods (9) the consideration for the supply and the VAT charged or a statement that VAT is included in the price charged and the rate of VAT charged. See https://www.sars.gov.za/wp-content/uploads/Docs/VATNews/LAPD-IntR-VATN-Arc-2013-20-VATNews-20-September-2002.pdf. Accessed 14 May 2021.

[681] SARS (2016). *Binding General Ruling (VAT) No 28 Issue 2.* Available at https://www.sars.gov.za/wp-content/uploads/Legal/Rulings/BGR/LAPD-IntR-R-BGR-2015-03-BGR28-Electronic-Services.pdf. Accessed 15 July 2021.

[682] SARS (2016). *Binding General Ruling (VAT) No 28 Issue 2* at 1 – 2. Available at https://www.sars.gov.za/wp-content/uploads/Legal/Rulings/BGR/LAPD-IntR-R-BGR-2015-03-BGR28-Electronic-Services.pdf. Accessed 15 July 2021.

[683] SARS (2016). *Binding General Ruling (VAT) No 28 Issue 2* at 2. Available at https://www.sars.gov.za/wp-content/uploads/Legal/Rulings/BGR/LAPD-IntR-R-BGR-2015-03-BGR28-Electronic-Services.pdf. Accessed 15 July 2021.

[684] When establishing the value of a supply, a supplier of electronic services must convert the amount of tax charged to South African Rand. A supplier of electronic services can look at the exchange rate published by the South African Reserve Bank, Bloomberg or the European

when VAT remittance is conducted. This can be achieved by making use of an *oracle*.[685] Merkx correctly opines that a smart contract can be programmed to take the applicable VAT rate[686] into account.[687]

In my view, the information contained in a tax invoice constitutes personal (taxpayer) information which must be protected. The need for protection stems from the fact that information contained in a tax invoice can be used to identify a natural person and a juristic person (supplier).[688] Additionally, information contained in a tax invoice constitutes taxpayer information which is confidential in nature and must not be accessed by prohibited users.[689] For this reason, information contained in a tax invoice must not be in plain text but must rather be encrypted.[690] SARS in *VAT News 20*[691]

Central Bank. The applicable exchange rate is the daily exchange rate on the day the supply occurs; the daily exchange rate on the last day of the month preceding the time of the supply or the monthly average rate for the month preceding the month during which the time of supply occurs. See SARS (2016). *Binding General Ruling (VAT) No 28 Issue 2* at 3. Available at https://www.sars.gov.za/wp-content/uploads/Legal/Rulings/BGR/LAPD-IntR-R-BGR-2015-03-BGR28-Electronic-Services.pdf. Accessed 15 July 2021.

[685] See discussion at paragraph 2.8 above.

[686] South Africa's current VAT rate is fifteen per cent.

[687] Merkx, M. (2019). "VAT and Blockchain: Challenges and Opportunities ahead" *EC Tax Review* 28(2): 89.

[688] In terms of the Protection of Personal Information Act (POPI Act), the following information constitutes 'personal information' for purposes of the POPI Act:
"(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person; (b) information relating to the education or the medical, financial, criminal or employment history of the person; (c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person; (d) the biometric information of the person; (e) the personal opinions, views or preferences of the person; (f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; (g) the views or opinions of another individual about the person; and (h) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person." It must be borne in mind that the protection of personal information is not limited to natural persons only but extends to juristic person.

[689] Section 67(1)(b) of the Tax Administration Act 28 of 2011 defines 'taxpayer information' as "any information provided by a taxpayer or obtained by SARS in respect of the taxpayer including biometric information." See also Setyowati, M., S. *et al* (2020). "Blockchain Technology Application for Value-Added Tax Systems" *Journal of Open Innovation: Technology, Market and Complexity* 6(156): 17.

[690] Nguyen, V-C. *et al* (2019). "*Digitizing Invoice and Managing VAT payment Using Blockchain Smart Contract*" at 75. Available at https://www.researchgate.net/profile/Pham-Hoai-Luan/publication/334167437_Digitizing_Invoice_and_Managing_VAT_Payment_Using_Blockchain_Smart_Contract/links/5f50ac6992851c250b8c5aac/Digitizing-Invoice-and-Managing-VAT-Payment-Using-Blockchain-Smart-Contract.pdf. Accessed 5 April 2021.

[691] *VAT News* are documents used as communication tools to inform the relevant stakeholders of any new developments in the VAT Act. From August 2011, VAT News was replaced by *VAT*

also mentions that digital (electronic) invoices may be issued by VAT vendors and that those digital invoices *must*[692] be encrypted over a secure line or contain an electronic signature.[693]

Currently, the VAT Act does not make provision for a foreign supplier to issue a digital invoice. Moreover, the VAT Act does not require a VAT vendor or a foreign supplier to sign a digital invoice. In my view, it is important for a foreign supplier to sign a digital invoice using their private key. By signing with a private key, a supplier creates a digital signature which, in turn, establishes that the invoice originated from that supplier.[694] The use of PKI[695] ensures authenticity on a blockchain system. The use of PKI can also determine whether a digital signature is correct.[696] It is almost impossible to falsify a digital signature especially if the process takes place on a blockchain. It is my view that the VAT Act should be amended to make provision for the use of digital invoices, PKI, and digital signatures by foreign suppliers of digital goods.

Moreover, I propose that a digital invoice should be stored on a blockchain. The anonymised invoice should contain: i) the name and VAT registration number of the foreign supplier; ii) the name and address of the recipient of the electronic services; iii) an individual serialised number; iv) the date of issue; v) description of the electronic services supplied; vi) value of the supply, and vii) exchange rate.[697] This is to ensure that SARS has data that shows that the taxpayer complied with the provisions of the VAT Act and paid the correct amount of tax.

connect. See https://www.sars.gov.za/legal-counsel/legal-counsel-archive/vatnews/. Accessed 14 May 2021.

[692] My own emphasis.

[693] *SARS VAT News 20* – September 2002. Available at https://www.sars.gov.za/wp-content/uploads/Docs/VATNews/LAPD-IntR-VATN-Arc-2013-20-VATNews-20-September-2002.pdf. Accessed 14 May 2021.

[694] Bacon, J., Millard, C., & Singh, J. (2018). "Blockchain Demystified: A technical and Legal Introduction to Distributed and Centralised Ledgers" *Richmond Journal of Law & Technology* 25(1): 14 – 15.

[695] Public key infrastructure. A user sends encrypted data using their public and private keys. The recipient decrypts the data using the sender's public key.

[696] Bacon, J., Millard, C., & Singh, J. (2018). "Blockchain Demystified: A technical and Legal Introduction to Distributed and Centralised Ledgers" *Richmond Journal of Law & Technology* 25(1): 14.

[697] See Kabwe, R. & van Zyl, S.P. (2021). "The value-added tax in the digital economy: a fresh look at the South African dispensation" *Obiter* 42(3): 515; see also section 20(4) of the VAT Act.

3.3.4 VAT collection using VATCoin

The second way VAT can be collected on a blockchain is by using VATCoin.[698] Ainsworth *et al* originally proposed to use VATCoin for the collection of VAT in an intra-state community like the Gulf Cooperation Council (GCC).[699] Although not explicitly mentioned by Ainsworth *et al*, the concept of VATCoins is predominantly intended to be used for B2B in intra-community supplies of goods and services. A VATCoin is a digital currency that is only issued by a government for the purposes of tax compliance.[700] All VATCoins are stored in the cloud.[701] VATCoin is not a new form of tax nor is it fiat money. VATCoin is a non-redeemable currency, and it is only the government that can convert VATCoin into fiat money.[702] Moreover, a VATCoin can only be issued on a private blockchain increasing its suitability for collecting taxes such as VAT.[703] It is possible for VATCoin to be denominated in the currency that was originally used to acquire it.[704]

VATCoins are issued centrally in one of the GCC's member countries. Suppliers purchase VATCoins from the government for use in commercial transactions. Once

[698] The idea of VATCoin was developed by Richard Ainsworth, Musaad Alwohaibi, and Mike Cheetham for the EU and the Gulf Cooperation Council (GCC). The GCC currently consists of Kuwait, Bahrain, Oman, Qatar, Saudi Arabia and United Arab Emirates (UAE). See https://www.gcc-sg.org/en-us/Pages/default.aspx. Accessed 10 April 2021.

[699] See Ainsworth, R., T. & Alwohaibi, M. (2017). "Blockchain, Bitcoin and VAT in the GCC: The Missing Trader Example" *Boston University School of Law, Law & Economics Working Paper No. 17-05* at 1 – 18. Available at http://www.bu.edu/law/files/2017/03/BLOCKCHAIN-BITCOIN-VAT-in-the-GCC.pdf. Accessed 21 May 2021; Ainsworth, R., T., Alwohaibi, M., & Cheetham, M. (2016). "VATCOIN: The GCC's Cryptotaxcurrency" at 1 – 23. Available at https://www.law.upenn.edu/live/files/5955-gcc-vatcoin.pdf. Accessed 9 April 2021.

[700] Ainsworth, R., T., Alwohaibi, M., & Cheetham, M. (2016). "VATCOIN: The GCC's Cryptotaxcurrency" at 1. Available at https://www.law.upenn.edu/live/files/5955-gcc-vatcoin.pdf. Accessed 9 April 2021.

[701] Ainsworth, R., T., Alwohaibi, M., & Cheetham, M. (2016). "VATCOIN: The GCC's Cryptotaxcurrency" at 7. Available at https://www.law.upenn.edu/live/files/5955-gcc-vatcoin.pdf. Accessed 9 April 2021; Merkx, M., & Verbaan, N. (2019). "Technology: A key to solve VAT Fraud?" *EC Tax Review* 28(6) at 303; Merkx, M. (2019). "VAT and Blockchain: Challenges and Opportunities ahead" *EC Tax Review* 28(2): 85.

[702] Ainsworth, R., T., Alwohaibi, M., & Cheetham, M. (2016). "VATCOIN: The GCC's Cryptotaxcurrency" at 2. Available at https://www.law.upenn.edu/live/files/5955-gcc-vatcoin.pdf. Accessed 9 April 2021.

[703] Ainsworth, R., T., Alwohaibi, M., & Cheetham, M. (2016). "VATCOIN: The GCC's Cryptotaxcurrency" at 1. Available at https://www.law.upenn.edu/live/files/5955-gcc-vatcoin.pdf. Accessed 9 April 2021.

[704] Ainsworth, R. T., Alwohaibi, M., Cheetham, M., & Tirand, C., V. (2018). "A VATCoin Solution to MTIC Fraud: Past Efforts, Present Technology and the EU's 2017 Proposal" *Boston University Scool of Law, Law and Economics Research Paper No. 18-08* at 17. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3151394. Accessed 24 May 2021.

purchased, VATCoins can be stored in the supplier's account located in the cloud until it is needed.[705] All VATCoin based transactions are stored and registered on the GCC blockchain. The tax authorities in each jurisdiction verify the validity of each transaction by means of government operated nodes. The operational nodes of a country within the GCC are determined by the country's Gross Domestic Product (GDP). The GDP of a member state is relative to the combined GDP of the GCC.[706] All the suppliers can gain access to blockchain to view all their respective VATCoin transactions.[707]

Once a transaction takes place, it is recorded on the GCC blockchain. It should be noted that all VAT is paid in VATCoin facilitated by a smart contract. Once a transaction has been validated, it is cryptographically sealed and added to the next block in blockchain every ten minutes.[708] The member countries in the GCC use *Proof of Identity*[709] (PoI) as a consensus mechanism. Once the active nodes in the GCC reach 75 per cent consensus, the verification process is complete, and the transaction is sealed.[710]

At no point does a supplier hold VAT (in fiat money) on behalf of the government. It is difficult for a supplier to escape their VAT liability. Furthermore, it is difficult for any supplier to commit VAT fraud due to non-payment because VAT, in the form of VATCoins, is remitted to the tax authority in real-time.[711] The sale or unlawful

[705] Ainsworth, R., T., Alwohaibi, M., & Cheetham, M. (2016). "VATCOIN: The GCC's Cryptotaxcurrency" at 7. Available at https://www.law.upenn.edu/live/files/5955-gcc-vatcoin.pdf. Accessed 9 April 2021.

[706] Ainsworth, R., T., Alwohaibi, M., & Cheetham, M. (2016). "VATCOIN: The GCC's Cryptotaxcurrency" at 6. Available at https://www.law.upenn.edu/live/files/5955-gcc-vatcoin.pdf. Accessed 9 April 2021.

[707] Ainsworth, R., T., Alwohaibi, M., & Cheetham, M. (2016). "VATCOIN: The GCC's Cryptotaxcurrency" at 6. Available at https://www.law.upenn.edu/live/files/5955-gcc-vatcoin.pdf. Accessed 9 April 2021.

[708] It must be noted that validation on a Bitcoin blockchain takes 10 minutes to complete. If a private or consortium blockchain is used, then the validation times will differ.

[709] According to Ainsworth and Alwohaibi, Proof-of-Identity is a consensus mechanism where the identities of the persons manning the computer nodes are known. In the context of VATCoin, the nodes are manned by government employees. The employees are responsible and accountable to their respective governments. See Ainsworth, R., T., Alwohaibi, M., & Cheetham, M. (2016). "VATCOIN: The GCC's Cryptotaxcurrency" at 18. Available at https://www.law.upenn.edu/live/files/5955-gcc-vatcoin.pdf. Accessed 9 April 2021.

[710] Ainsworth, R., T., Alwohaibi, M., & Cheetham, M. (2016). "VATCOIN: The GCC's Cryptotaxcurrency" at 6 – 7. Available at https://www.law.upenn.edu/live/files/5955-gcc-vatcoin.pdf. Accessed 9 April 2021.

[711] Ainsworth, R., T., Alwohaibi, M., & Cheetham, M. (2016). "VATCOIN: The GCC's Cryptotaxcurrency" at 9 – 11. Available at https://www.law.upenn.edu/live/files/5955-gcc-vatcoin.pdf. Accessed 9 April 2021.

appropriation of VATCoins will be immediately identified by blockchain. Any attempts to resell the VATCoins will be declined on blockchain. Any unauthorised transaction will be refused and the VATCoins will be cancelled in the process.[712] Any person trying to repossess and reuse stolen VATCoins cannot do so because blockchain would have categorized those VATCoins as worthless.[713] Any purchase or disposal of a VATCoin will be illegal and any person involved must be criminally charged.[714]

According to the authors, for VATCoin to work efficiently certain rules must be put in place in each member state. First, and as mentioned above, VAT is paid in VATCoin by a smart contract. A supplier issues a digital invoice which forms the basis upon which a smart contract is paid. All VATCoins must be acknowledged as a non-redeemable currency that can only be converted by the government. If a supplier's input tax exceeds his output tax, the government can issue a refund in fiat money (cash). Additionally, refunds are paid out after a brief waiting period.[715] Second, VATCoins paid as input tax and VATCoins received as output tax are verified in real-time before the transactions are added to blockchain.[716]

It should be noted that the VATCoin is not attached to a specific currency. Simply put, a VATCoin is not a denomination of a specific currency. As was mentioned above, a VATCoin is a digital currency issued by a government for VAT administration purposes. Since the VATCoin is government issued, only the government, and by

[712] Merkx, M. (2019). "VAT and Blockchain: Challenges and Opportunities ahead" *EC Tax Review* 28(2): 85; Ainsworth, R., T., Alwohaibi, M., & Cheetham, M. (2016). "VATCOIN: The GCC's Cryptotaxcurrency" at 13. Available at https://www.law.upenn.edu/live/files/5955-gcc-vatcoin.pdf. Accessed 9 April 2021.

[713] Merkx, M., & Verbaan, N. (2019). "Technology: A key to solve VAT Fraud?" *EC Tax Review* 28(6) at 303; Merkx, M. (2019). "VAT and Blockchain: Challenges and Opportunities ahead" *EC Tax Review* 28(2): 85; Ainsworth, R., T., Alwohaibi, M., & Cheetham, M. (2016). "VATCOIN: The GCC's Cryptotaxcurrency" at 13. Available at https://www.law.upenn.edu/live/files/5955-gcc-vatcoin.pdf. Accessed 9 April 2021.

[714] Merkx, M., & Verbaan, N. (2019). "Technology: A key to solve VAT Fraud?" *EC Tax Review* 28(6) at 303; Merkx, M. (2019). "VAT and Blockchain: Challenges and Opportunities ahead" *EC Tax Review* 28(2): 85; Ainsworth, R., T., Alwohaibi, M., & Cheetham, M. (2016). "VATCOIN: The GCC's Cryptotaxcurrency" at 13. Available at https://www.law.upenn.edu/live/files/5955-gcc-vatcoin.pdf. Accessed 9 April 2021.

[715] Ainsworth, R., T., Alwohaibi, M., & Cheetham, M. (2016). "VATCOIN: The GCC's Cryptotaxcurrency" at 8. Available at https://www.law.upenn.edu/live/files/5955-gcc-vatcoin.pdf. Accessed 9 April 2021.

[716] Ainsworth, R., T., Alwohaibi, M., & Cheetham, M. (2016). "VATCOIN: The GCC's Cryptotaxcurrency" at 8. Available at https://www.law.upenn.edu/live/files/5955-gcc-vatcoin.pdf. Accessed 9 April 2021.

implication tax authorities, can determine the amount of VATCoins issued at any time. As a result, it is possible for every country to issue VATCoins. For this to happen, countries must agree on international standards for the creation and issue of VATCoins. It is impractical for countries to insist on the denomination of VATCoin in a specific currency. What is important is for tax authorities to convert the VATCoin into their respective currencies for the purpose of VAT administration.

This technology remains to be tested. As such, I do not proffer an express view for or against its implementation.

3.3.5 VAT collection using TVACoin

The collection of VAT through TVACoin is a concept developed by Bitjoka and Edoa.[717] In terms of this model, tax authorities run and operate a consortium blockchain to ensure that information relating to the taxpayers and consumers is known to the tax authorities.[718] All the transactions recorded on blockchain are validated by nodes run by tax authorities.[719] TVACoin is a type of cryptocurrency only issued by a tax authority. TVACoin can be exchanged for normal fiat currency provided the exchange is authorised by a tax authority.[720] In addition to tax authorities, TVACoin is intended for use by consumers and suppliers.[721] To illustrate how VAT can be collected through TVACoin, the following example is used:

Example 3

> Y is a local supplier of digital goods. Y is a registered VAT vendor. Y purchases digital goods from W, a foreign registered VAT vendor (B2B), for R8 000 inclusive of VAT. W supplies digital goods to Y. **(scenario 1)**

[717] Bitjoka, G., B., & Edoa, M., M., N. (2020). "Blockchain in the Implementation of VAT Collection" *American Journal of Computer Science and Technology* 3(2): 18 – 26.

[718] Bitjoka, G., B., & Edoa, M., M., N. (2020). "Blockchain in the Implementation of VAT Collection" *American Journal of Computer Science and Technology* 3(2): 20.

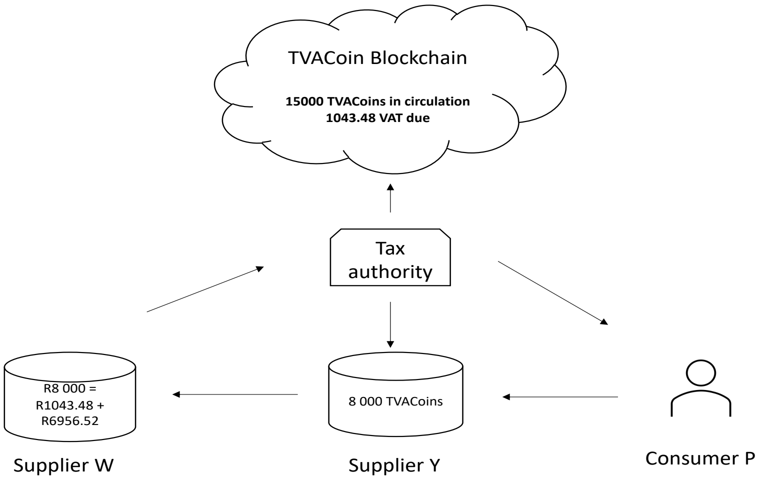
[719] Bitjoka, G., B., & Edoa, M., M., N. (2020). "Blockchain in the Implementation of VAT Collection" *American Journal of Computer Science and Technology* 3(2): 20.

[720] Bitjoka, G., B., & Edoa, M., M., N. (2020). "Blockchain in the Implementation of VAT Collection" *American Journal of Computer Science and Technology* 3(2): 20.

[721] Bitjoka, G., B., & Edoa, M., M., N. (2020). "Blockchain in the Implementation of VAT Collection" *American Journal of Computer Science and Technology* 3(2): 20.

P, a consumer, purchases the same digitals goods from business Y for a purchase price of R10 000 inclusive of VAT. **(scenario 2)**

In **scenario 1** above (see **Figure 9** below), business Y accounts for VAT to a tax authority by means of the reverse-charge mechanism. With TVACoin, business Y submits a request to a tax authority wherein the latter issues the equivalent value of R8 000 worth of TVACoins to the former. The request made by business Y is recorded on blockchain. Blockchain also contains a record of the total amount of VAT that is stored at any given time. The tax authority also creates a value of R8 000 worth of TVACoins on blockchain. At the same time, the tax authority increases the total value of VAT stored on blockchain by R1 043.48 which is the VAT amount of the current purchase price (R8 000 x 15/115). The amount of R1 043.48 recorded on blockchain also acts as a "credit" indicating the amount of VAT owed to the tax authority. Business Y pays R8 000 to the tax authority in exchange for R8 000 worth of TVACoins. Business Y then uses R8 000 TVACoins to purchase digital goods from business W. Business W transfers 1 043.48 TVACoins (which is the total VAT collected) from the 8 000 TVACoins received to the tax authority. All the transactions are recorded on blockchain.[722]



[722] See Bitjoka, G., B., & Edoa, M., M., N. (2020). "Blockchain in the Implementation of VAT Collection" *American Journal of Computer Science and Technology* 3(2): 23 – 24.

Figure 9[723]

In **scenario 2** above, the total value of the digital goods is R10 000 which amounts to a price of R8 695.65 exclusive of VAT. The VAT amount is R1 304.35. Consumer P makes a request to the tax authority for 10 000 TVACoins. The tax authority creates 10 000 TVACoins on blockchain network before accepting R10 000 from Consumer P. The total amount of VAT in circulation at the time increases to R1 304.35 (the amount of R1 304.35 also indicates the VAT owed to the tax authority). Consumer P purchases the digital goods from business Y with 10 000 TVACoins. Business Y transfers R1 304.35 worth of TVACoins to the tax authority for recording purposes.[724] The tax authority withdraws the VAT amount (R1 304.35) from blockchain representing the amount of VAT collected. Should Business Y wish to claim the amount of VAT paid to Business W, then the tax authority can refund that VAT amount through fiat currency or through TVACoins.[725]

This technology remains to be tested. As such, I do not proffer an express view for or against its implementation.

3.3.6 DICE on blockchain

The concept of a Digital Invoice Customs Exchange (DICE) was developed by Ainsworth and Todorov.[726] The authors define 'DICE' as:

> "A technology-intensive tax compliance regimen for VAT/GST that utilizes invoice encryption to safeguard transactional data exchanged between seller and buyer in

[723] **Figure 9** adapted from Bitjoka, G., B., & Edoa, M., M., N. (2020). "Blockchain in the Implementation of VAT Collection" *American Journal of Computer Science and Technology* 3(2): 23 – 25.

[724] Bitjoka, G., B., & Edoa, M., M., N. (2020). "Blockchain in the Implementation of VAT Collection" *American Journal of Computer Science and Technology* 3(2): 24 – 25.

[725] Bitjoka, G., B., & Edoa, M., M., N. (2020). "Blockchain in the Implementation of VAT Collection" *American Journal of Computer Science and Technology* 3(2): 26.

[726] See Ainsworth, R., T. & Todorov, G. (2013). "DICE – Digital Invoice Customs Exchange" Boston University School of Law Working Paper No 13-40. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2314478. Accessed 15 July 2021.

> both domestic and import/export contexts while simultaneously notifying concerned jurisdictions of the transaction details."[727]

DICE aims to replace paper invoices with digital invoices.[728] With DICE, digital invoices are encrypted and signed by means of a digital signature. Invoices are exchanged between tax authorities, sellers, and buyers. These parties verify the digital invoices by making use of public access keys. The access keys enable the parties to examine the data on the invoice. An AI controls the exchange of data and conducts risk analysis on the transactions to prevent any asymmetries.[729]

One of the benefits of using DICE is that it can be implemented in B2B and B2C transactions.[730] In a B2B setting where both the seller and buyer are in the **same** jurisdiction, the seller generates an invoice containing all the necessary particulars of the transactions. The seller signs the invoice with a digital signature. The invoice is transmitted to the tax authority for authorisation. The authorisation process is automatic. Once verified, the tax authority signs the invoice with a different digital signature.[731] A copy of this invoice is stored by the tax authority. Upon receipt of the signed digital invoice, the seller sends a copy of that invoice to the buyer. The buyer accesses the tax authority's public key to ascertain the authenticity of the invoice. Once authenticated, the buyer signs the invoice received from the seller and transmits that invoice to the tax authority. The tax authority verifies the invoice a second time, stores it and returns the invoice to the buyer with a second public key. The buyer keeps

[727] Ainsworth, R., T. & Todorov, G. (2013). "DICE – Digital Invoice Customs Exchange" Boston University School of Law Working Paper No 13-40 at 2. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2314478. Accessed 15 July 2021.

[728] Ainsworth, R., T. & Todorov, G. (2013). "DICE – Digital Invoice Customs Exchange" Boston University School of Law Working Paper No 13-40 at 3. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2314478. Accessed 15 July 2021; Ainsworth, R., T., Alwohaibi, M., & Cheetham, M. (2016). "VATCOIN: The GCC's Cryptotaxcurrency" at 16. Available at https://www.law.upenn.edu/live/files/5955-gcc-vatcoin.pdf. Accessed 9 April 2021.

[729] Ainsworth, R., T., Alwohaibi, M., & Cheetham, M. (2016). "VATCOIN: The GCC's Cryptotaxcurrency" at 16. Available at https://www.law.upenn.edu/live/files/5955-gcc-vatcoin.pdf. Accessed 9 April 2021; Merkx, M., & Verbaan, N. (2019). "Technology: A key to solve VAT Fraud?" *EC Tax Review* 28(6) at 303.

[730] Ainsworth, R., T. & Todorov, G. (2013). "DICE – Digital Invoice Customs Exchange" Boston University School of Law Working Paper No 13-40 at 4 – 9. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2314478. Accessed 15 July 2021.

[731] Ainsworth, R., T. & Todorov, G. (2013). "DICE – Digital Invoice Customs Exchange" Boston University School of Law Working Paper No 13-40 at 4 – 5. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2314478. Accessed 15 July 2021.

a copy of the invoice and sends the original version to the seller. An original invoice is produced containing two public keys. The seller can now transact with the buyer. VAT can also be remitted to the tax authority as and when due. The tax authority is aware of the transaction and the amount of VAT due.[732]

Using the same example above, let us assume that the buyer sells the goods or services to a consumer (B2C). After making the supply, the seller submits a file to the tax authority requesting permission to issue a tax invoice. The file contains the required information, including the description of the goods or services sold and the value of the supply.[733] Once the tax authority authenticates the accuracy of the data on the file, a copy is saved, and the tax authority signs the file. The seller issues a signed receipt to the consumer. The consumer can access the tax authority's database to verify the accuracy of the receipt.[734]

DICE can also be applied to cross-border transactions.[735] The supplier (located in a foreign jurisdiction) generates an electronic file containing the necessary information pertaining to the supply. The file is signed by the supplier. The file is sent to the **destination** tax authority. The tax authority authenticates and saves a copy of that file. The tax authority signs the file with a public key and sends it to the seller. Based on this, the seller sends the invoice containing data from the original file and the public key signed by the destination tax authority to the consumer.[736] The consumer uses the public key to ascertain the validity of the invoice. Then, the consumer signs the invoice before it is sent back to the tax authority. The tax authority re-verifies and stores a copy of that invoice. The tax authority signs with a second public key and returns the

[732] Ainsworth, R., T. & Todorov, G. (2013). "DICE – Digital Invoice Customs Exchange" Boston University School of Law Working Paper No 13-40 at 4 – 5. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2314478. Accessed 15 July 2021.

[733] Ainsworth, R., T. & Todorov, G. (2013). "DICE – Digital Invoice Customs Exchange" Boston University School of Law Working Paper No 13-40 at 6. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2314478. Accessed 15 July 2021.

[734] Ainsworth, R., T. & Todorov, G. (2013). "DICE – Digital Invoice Customs Exchange" Boston University School of Law Working Paper No 13-40 at 6. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2314478. Accessed 15 July 2021.

[735] Ainsworth, R., T. & Todorov, G. (2013). "DICE – Digital Invoice Customs Exchange" Boston University School of Law Working Paper No 13-40 at 7. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2314478. Accessed 15 July 2021.

[736] Ainsworth, R., T. & Todorov, G. (2013). "DICE – Digital Invoice Customs Exchange" Boston University School of Law Working Paper No 13-40 at 8. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2314478. Accessed 15 July 2021.

invoice to the consumer. The consumer retains a copy of the invoice and thereafter becomes responsible for remitting VAT to the tax authority.[737] This is a form of self-assessment or reverse-charge mechanism. The only difference with the conventional reverse-charge mechanism is that the destination tax authority is aware that a transaction has occurred or is about to take place. A tax authority is aware that the consumer has a tax obligation since all transactions are recorded.[738] Hence, even if a consumer does not report their tax liability, the tax authority is aware that a supply took place making enforcement easier.

It is possible for DICE to be used in conjunction with blockchain.[739] If that is the case, all transactions can be recorded on blockchain. Blockchain can also be used to link the supply of goods and services to buyers and sellers.[740] This can greatly improve the cross-border supply of goods and services.[741]

According to the authors,[742] the combination of DICE, blockchain and VATCoin can make the administration of VAT highly efficient and eliminate VAT fraud in its entirety.[743] The combination of blockchain and DICE can be beneficial because: i) there will be no cash-flow burden on businesses and suppliers, ii) tax payments are instantaneous, secure, verifiable, and transparent, iii) no entity incurs transaction costs, iv) recordkeeping can be facilitated by government using Cloud services and

[737] Ainsworth, R., T. & Todorov, G. (2013). “DICE – Digital Invoice Customs Exchange” Boston University School of Law Working Paper No 13-40 at 8. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2314478. Accessed 15 July 2021.

[738] Ainsworth, R., T. & Todorov, G. (2013). “DICE – Digital Invoice Customs Exchange” Boston University School of Law Working Paper No 13-40 at 8 – 9. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2314478. Accessed 15 July 2021.

[739] Ainsworth, R., T., Alwohaibi, M., & Cheetham, M. (2016). “VATCOIN: The GCC’s Cryptotaxcurrency” at 17. Available at https://www.law.upenn.edu/live/files/5955-gcc-vatcoin.pdf. Accessed 9 April 2021.

[740] Ainsworth, R., T., Alwohaibi, M., & Cheetham, M. (2016). “VATCOIN: The GCC’s Cryptotaxcurrency” at 17. Available at https://www.law.upenn.edu/live/files/5955-gcc-vatcoin.pdf. Accessed 9 April 2021.

[741] Ainsworth, R., T., Alwohaibi, M., & Cheetham, M. (2016). “VATCOIN: The GCC’s Cryptotaxcurrency” at 17. Available at https://www.law.upenn.edu/live/files/5955-gcc-vatcoin.pdf. Accessed 9 April 2021.

[742] Ainsworth, R., T., Alwohaibi, M., & Cheetham, M. (2016). “VATCOIN: The GCC’s Cryptotaxcurrency”. Available at https://www.law.upenn.edu/live/files/5955-gcc-vatcoin.pdf. Accessed 9 April 2021.

[743] Ainsworth, R., T., Alwohaibi, M., & Cheetham, M. (2016). “VATCOIN: The GCC’s Cryptotaxcurrency” at 18 – 19. Available at https://www.law.upenn.edu/live/files/5955-gcc-vatcoin.pdf. Accessed 9 April 2021; See also Merkx, M. (2019). “VAT and Blockchain: Challenges and Opportunities ahead” *EC Tax Review* 28(2): 85.

blockchain, v) VAT returns can be done by the government, and vi) there is no compliance burden on suppliers and businesses.[744]

This technology remains to be tested. As such, I do not proffer an express view for or against its implementation.

3.3.7 Automated VAT collection mechanism

The automated VAT collection mechanism (AVCM) is a concept proposed by Muller.[745] According to Muller, the AVCM can work effectively if the following measures are in place. First, it is crucial to establish a reliable network that is sustainable and efficient.[746] Second, VAT is collected in real-time during the payment process.[747] Third, the supplier must be connected to the consumer's payment service provider (this can be a bank or financial institution).[748]

Tax authorities run blockchain to ensure that transaction costs are low and only the relevant participants are granted access to submit information.[749] A smart contract contains two sets of information: (1) VAT information from the supplier and, (2) consumer information[750] (recipient of goods or services) provided by the bank.[751] The smart contract must be validated by the consumer's bank before execution to ensure

[744] Ainsworth, R., T., Alwohaibi, M., & Cheetham, M. (2016). "VATCOIN: The GCC's Cryptotaxcurrency" at 19 – 20. Available at https://www.law.upenn.edu/live/files/5955-gcc-vatcoin.pdf. Accessed 9 April 2021.

[745] Muller, R. (2020). "Proposal for an Automated Real-Time VAT Collection Mechanism in B2C E-Commerce Using Blockchain Technology" *International VAT Monitor* 31(3): 135 – 138.

[746] Muller, R. (2020). "Proposal for an Automated Real-Time VAT Collection Mechanism in B2C E-Commerce Using Blockchain Technology" *International VAT Monitor* 31(3): 135.

[747] Muller, R. (2020). "Proposal for an Automated Real-Time VAT Collection Mechanism in B2C E-Commerce Using Blockchain Technology" *International VAT Monitor* 31(3): 135.

[748] Muller, R. (2020). "Proposal for an Automated Real-Time VAT Collection Mechanism in B2C E-Commerce Using Blockchain Technology" *International VAT Monitor* 31(3): 135.

[749] Muller, R. (2020). "Proposal for an Automated Real-Time VAT Collection Mechanism in B2C E-Commerce Using Blockchain Technology" *International VAT Monitor* 31(3): 136 – 137.

[750] Consumer information can include credit card details and the name of the consumer. This information is readily available to suppliers. Authorising a bank or financial institution to provide this information to a supplier is not different from ordinary credit card transactions orchestrated by the consumer. In the latter case, the consumer consents to the sharing of their personal information.

[751] Muller, R. (2020). "Proposal for an Automated Real-Time VAT Collection Mechanism in B2C E-Commerce Using Blockchain Technology" *International VAT Monitor* 31(3): 137.

that the information provided by the supplier is collaborated.[752] During the payment process, the smart contract calculates the correct amount of VAT using information provided by the supplier and the consumer's bank. The VAT amount is transferred to a special bank account of the supplier. Thereafter, the VAT is transmitted to the relevant tax authority.[753]

The AVCM can be used by countries in regional communities such as the EU.[754] In this setting, tax authorities store, and validate all VAT related information. Trust is also built between tax authorities and suppliers to ensure that accurate data is stored on blockchain, and the correct amount of VAT is collected.[755] Muller proposes that a public-permissioned blockchain is used to ensure that suppliers have written permission for new transactions.[756] The consumer's bank has reading and writing permissions to approve transactions, identify payments, and to complete information on a smart contract.[757]

Muller's model highlights the need for a reliable payment system. Since a smart contract can be programmed to split the VAT amount and the non-VAT amount, the VAT amount should be paid to the tax authority instantaneously. Bal correctly argues that if blockchain is to be used to collect taxes, blockchain must support money transfers.[758] In other words, blockchain should be programmed to transfer the monetary value of VAT collected to the relevant tax authority. Bal also points out that distributed ledgers are programmed to transfer cryptocurrency and tokenised assets, but fiat currency relies on financial institutions.[759] Hence, Bal argues that a blockchain-

[752] Muller, R. (2020). "Proposal for an Automated Real-Time VAT Collection Mechanism in B2C E-Commerce Using Blockchain Technology" *International VAT Monitor* 31(3): 137.

[753] Muller, R. (2020). "Proposal for an Automated Real-Time VAT Collection Mechanism in B2C E-Commerce Using Blockchain Technology" *International VAT Monitor* 31(3): 137.

[754] See Muller, R. (2020). "Proposal for an Automated Real-Time VAT Collection Mechanism in B2C E-Commerce Using Blockchain Technology" *International VAT Monitor* 31(3): 135 – 138.

[755] Muller, R. (2020). "Proposal for an Automated Real-Time VAT Collection Mechanism in B2C E-Commerce Using Blockchain Technology" *International VAT Monitor* 31(3): 137.

[756] Muller, R. (2020). "Proposal for an Automated Real-Time VAT Collection Mechanism in B2C E-Commerce Using Blockchain Technology" *International VAT Monitor* 31(3): 137.

[757] Muller, R. (2020). "Proposal for an Automated Real-Time VAT Collection Mechanism in B2C E-Commerce Using Blockchain Technology" *International VAT Monitor* 31(3): 137.

[758] Bal, A. (2023). *Tax management through blockchain – will this be possible?* Available at https://www.forbes.com/sites/aleksandrabal/2023/02/09/tax-management-through-blockchainwill-this-ever-be-possible/. Accessed 20 June 2024.

[759] Bal, A. (2023). *Tax management through blockchain – will this be possible?* Available at https://www.forbes.com/sites/aleksandrabal/2023/02/09/tax-management-through-blockchainwill-this-ever-be-possible/. Accessed 20 June 2024.

based tax collection system requires a proper integration of payment facilities.[760] While this argument has merit, it is possible to collect VAT on blockchain using a crypto tax currency like VATCoin. The use of a VATCoin on blockchain does not require a financial institution or the transfer of fiat currency.[761] Moreover, the use of a VATCoin does not necessarily require an integration of payment facilities.[762] For this reason, it may be viable to use VATCoin as an alternative method to collect VAT on blockchain.

This method remains to be tested. As such, I do not proffer an express view for or against its implementation.

3.4 The benefits of collecting VAT on blockchain

3.4.1 Submission of tax returns and rectification of taxpayer errors/omissions

One of the most important aspects of a good tax administration is the filing of tax returns.[763] Here, I differentiate between income tax returns and VAT returns. One area that can greatly benefit from the adoption of blockchain is the submission of income tax returns. SARS requires taxpayers to submit tax returns.[764] Thus, the tax system relies on data provided by the taxpayer (self-assessment) and data provided by third parties. Data provided by third parties can originate from employers, or persons who has control over the of assets of the taxpayer to submit returns on the taxpayer's behalf.[765] Generally, the submission of tax returns[766] can be done electronically on the SARS e-filling system.[767] The adoption of blockchain can simplify the submission of

[760] Bal, A. (2023). *Tax management through blockchain – will this be possible?* Available at https://www.forbes.com/sites/aleksandrabal/2023/02/09/tax-management-through-blockchainwill-this-ever-be-possible/. Accessed 20 June 2024.

[761] See paragraphs 3.3.4 and 3.3.5 above.

[762] In my view, the decision to use blockchain for tax collection can hinge on the reliability of a country's payment system. If the payment system is dysfunctional, then it will be very difficult to use blockchain for tax collection unless a crypto tax currency is used.

[763] Bird, R. M. & Gendron, P. P. (2007). *The VAT in developing and transitional countries* (Cambridge University Press, New York) at 167.

[764] See section 25 of the Tax Administration Act.

[765] See section 26 of the Tax Administration Act.

[766] Although a discussion of income tax returns falls outside the scope of the study, a brief mention of the benefits of blockchain in respect of income tax returns in the South African context is necessary.

[767] See SARS eFiling page at https://www.sarsefiling.co.za. Accessed 12 December 2022. See also Van Zyl, S. P. (2013). *The collection of Value Added Tax on online cross-border trade in Digital Goods*. Unpublished LLD thesis (UNISA) at 118.

tax returns. With blockchain, individual taxpayers can submit their returns instantaneously using a smart contract. If an individual taxpayer fails to submit their income tax returns on time, SARS can automatically send a notification to that taxpayer.[768] A smart contract can be used to notify the taxpayer. If the individual taxpayer fails to submit an income tax return or fails to pay the necessary tax required by any tax Act,[769] SARS can issue an assessment to the taxpayer and the estimated tax payment can be sent to the taxpayer instantaneously.[770] No delays are anticipated, and the taxpayer can view the tax payable on blockchain.

In the context of VAT, the conventional process of submitting VAT returns is often characterised by periodic returns and long delays. At times, suppliers can spend more time filing returns than making taxable supplies.[771] Due to the complexity around the VAT filing process, errors can occur. However, errors are not limited to the submission of VAT returns. For example, it is possible for a supplier to make an error when issuing a tax invoice. In terms of the VAT Act, a supplier is required to make corrections to a tax invoice within 21 days from the date of request provided that the time of the supply remains unchanged, and the supplier must also retain sufficient information to identify the transaction to which the tax invoice refers.[772] Ordinarily, rectifying errors requires additional time for suppliers which results in delays in the remittance and collection of VAT. From a supplier's perspective, blockchain can make errors easier to detect. This can reduce the supplier's compliance burden. Blockchain's transparent nature makes it easier for taxpayers and tax authorities to identify omissions that may have been made. Additionally, the payment of VAT to the relevant tax authorities can easily be tracked on the network.[773] With blockchain, a supplier can merely reissue a new digital

[768] See Bird, R. M. & Gendron, P. P. (2007). *The VAT in developing and transitional countries* (Cambridge University Press, New York) at 168.

[769] Section 91(4) of the Tax Administration Act.

[770] Section 91(4) read with section 95 of the Tax Administration Act; see also Bird, R. M. & Gendron, P. P. (2007). *The VAT in developing and transitional countries* (Cambridge University Press, New York) at 168.

[771] Van Zyl, S. P. (2013). *The collection of Value Added Tax on online cross-border trade in Digital Goods*. Unpublished LLD thesis (UNISA) at 118.

[772] Section 20(1B)(i) and (ii) of the VAT Act. See also SARS (2019). VAT 404 – Guide for Vendors at iv. Available at https://www.sars.gov.za/wp-content/uploads/Ops/Guides/LAPD-VAT-G02-VAT-404-Guide-for-Vendors.pdf. Accessed 14 May 2021.

[773] PWC (2016). "How blockchain technology could improve the tax system" at 3. Available at https://www.pwc.co.uk/issues/futuretax/assets/documents/how-blockchain-could-improve-the-tax-system.pdf. Accessed 24 March 2021.

invoice and store it on blockchain in a matter of minutes. This can be done using a smart contract.

In my view, the use of blockchain to collect VAT can theoretically eliminate the need for VAT vendors and suppliers to submit VAT returns. This view is also supported by Delmotte[774] and Merkx.[775] Merkx argues that the recording of transactions on blockchain can abolish the requirement for suppliers to submit VAT returns.[776] Delmotte argues that a blockchain can be programmed to automatically calculate and apply the right amount of tax without human intervention hence rendering tax returns unnecessary.[777] Eliminating the obligation to file VAT returns can further reduce compliance costs for VAT vendors and suppliers. Ainsworth *et al* correctly point out that if the VAT system works properly then suppliers and businesses should not incur a heavy burden to pay tax.[778] By making use of a blockchain, all the transactions are recorded and made accessible to tax authorities. Tax officials can, therefore, complete and file returns on behalf of foreign suppliers by means of an administrative assessment system.[779] Contextually, the administrative assessment system can be used to "nudge"[780] foreign suppliers into using blockchain technology as the preferred approach for VAT collection and tax compliance.

[774] Delmotte, C. (2022). "The Promises and Pitfalls of a Blockchain Driven Tax System" at 12. Available at https://ssrn.com/abstract=4187919. Accessed 6 October 2022.

[775] Merkx, M. (2019). "VAT and Blockchain: Challenges and Opportunities Ahead" *EC Tax Review* 28(2): 83 – 89.

[776] Merkx, M. (2019). "VAT and Blockchain: Challenges and Opportunities Ahead" *EC Tax Review* 28(2): 86.

[777] Delmotte, C. (2022). "The Promises and Pitfalls of a Blockchain Driven Tax System" at 12. Available at https://ssrn.com/abstract=4187919. Accessed 6 October 2022.

[778] Ainsworth, R., T., Alwohaibi, M., & Cheetham, M. (2016). "VATCOIN: The GCC's Cryptotaxcurrency" at 11. Available at https://www.law.upenn.edu/live/files/5955-gcc-vatcoin.pdf. Accessed 9 April 2021.

[779] Ainsworth, R., T., Alwohaibi, M., & Cheetham, M. (2016). "VATCOIN: The GCC's Cryptotaxcurrency" at 19. Available at https://www.law.upenn.edu/live/files/5955-gcc-vatcoin.pdf. Accessed 9 April 2021.

[780] A nudge is a concept that is adopted in behavioural economics. Nudges seek to positively influence the decision of individuals. Thaler and Sunstein define a nudge as "any aspect of the choice architecture that alters people's behaviour in a predictable way without forbidding any options or significantly changing their economic incentives." See Thaler, R. & Sunstein, C. (2008). *Nudge: Improving decisions about health, wealth and happiness* Penguin Books at 6.

3.4.2 Reduction of compliance costs

Businesses often contend with different VAT laws across multiple jurisdictions. It is difficult for businesses to comply with all the different VAT laws. The application and interpretation of VAT rules leads to a heavy compliance burden for businesses across the world. This process is often time consuming and costly for businesses.[781]

It is trite that for a tax to be successfully administered, time and money must be spent.[782] Generally, established suppliers have the upper hand in so far as compliance with tax laws is concerned because they have resources at their disposal. New and smaller suppliers do not necessarily possess the same resources as their established counterparts. For this reason, it can be said that the compliance costs incurred by new and smaller suppliers is disproportionally higher to those incurred by established suppliers.[783] In fact, it is likely that the compliance costs borne by new suppliers can outweigh the number of sales at any given time. New and smaller businesses are more likely to spend additional time and resources to comply with their tax obligations.[784] Moreover, the cross-border supply of goods and services poses difficulties for VAT systems. It also poses a heavy compliance burden on businesses,[785] particularly new and smaller businesses.

Usually, VAT compliance is a complex process for companies due to the periodic VAT returns, frequent payments, and the invoice system.[786] According to a study conducted

[781] PWC (2017). "*VAT Compliance: The impact on business and how technology can help*" at 2. Available at https://www.pwc.com/gx/en/tax/pdf/pwc-vat-compliance-paying-taxes-2017.pdf. Accessed 12 April 2021; Mazur, O. (2021). "Can Blockchain Revolutionize Tax Administration?" SMU Dedman School of Law Legal Studies Research Paper No. 510 at 10. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3841785. Accessed 23 June 2021; Azam, R. & Mazur, O. (2019). "Cloudy with a chance of taxation" *Florida Tax Review* 22(2): 564.

[782] Basu, S. (2007). *Global perspectives on e-commerce taxation law* (Routledge, UK publishing) at 306 footnote 53; Rikken, O. (2017). "*Blockchain Real Time Tax"*. Available at https://www.linkedin.com/pulse/blockchain-real-time-tax-olivier-rikken. Accessed 6 April 2021.

[783] Cnossen, S. (2019). Modernizing VATs in Africa *Oxford University Press* (UK) at 40.

[784] Rikken, O. (2017). "*Blockchain Real Time Tax"*. Available at https://www.linkedin.com/pulse/blockchain-real-time-tax-olivier-rikken. Accessed 6 April 2021.

[785] PWC (2017). "*VAT Compliance: The impact on business and how technology can help*" at 10. Available at https://www.pwc.com/gx/en/tax/pdf/pwc-vat-compliance-paying-taxes-2017.pdf. Accessed 12 April 2021.

[786] Rikken, O. (2017). "*Blockchain Real Time Tax"*. Available at https://www.linkedin.com/pulse/blockchain-real-time-tax-olivier-rikken. Accessed 6 April 2021; Businesstech staff writer (2020). "*It's time to change the way our VAT system works*". Available

by *Price Waterhouse Coopers* (PwC), businesses tend to comply better in high earning economies due to the simplicity of the VAT systems.[787] PwC suggests that this may be due to automation which can be attributed to efficient IT systems and infrastructure which then reduces compliance times for businesses. It is also possible that if the amount of information required to submit VAT returns is reduced, more emphasis can be placed on a tax authority's ability to audit the taxpayer.[788]

Based on the findings by PwC, it can be concluded that if developing countries adopt the appropriate technology for the administration of VAT, compliance and administrative costs can be reduced. Contextually, the adoption of blockchain to collect VAT can significantly reduce the time spent by businesses when complying with VAT laws. As has been mentioned, blockchain offers the possibility of real-time reporting[789] and the possibility of eliminating VAT returns can reduce compliance costs for businesses. Blockchain can also reduce foreign suppliers' compliance burden if, for instance, smart contracts are programmed to calculate, collect, and remit VAT to the relevant tax authority.[790] In turn, the automatic remittal of VAT can significantly reduce the administrative burden borne by tax authorities.[791]

at https://businesstech.co.za/news/finance/386705/its-time-to-change-the-way-our-vat-system-works-tax-expert/. Accessed 6 April 2021.

[787] PWC (2017). "*VAT Compliance: The impact on business and how technology can help*" at 13. Available at https://www.pwc.com/gx/en/tax/pdf/pwc-vat-compliance-paying-taxes-2017.pdf. Accessed 12 April 2021.

[788] PwC (2017). "*VAT Compliance: The impact on business and how technology can help*" at 13. Available at https://www.pwc.com/gx/en/tax/pdf/pwc-vat-compliance-paying-taxes-2017.pdf. Accessed 12 April 2021.

[789] See PwC (2017). "*VAT Compliance: The impact on business and how technology can help*" at 8. Available at https://www.pwc.com/gx/en/tax/pdf/pwc-vat-compliance-paying-taxes-2017.pdf. Accessed 12 April 2021; Azam, R. & Mazur, O. (2019). "Cloudy with a chance of taxation" *Florida Tax Review* 22(2): 555 – 556.

[790] Azam, R. & Mazur, O. (2019). "Cloudy with a chance of taxation" *Florida Tax Review* 22(2): 555; Bossa, G. & de Paiva Gomes, E. (2019). "Blockchain: Technology as a Tool for Tax information Exchange or an instrument Threatening the Taxpayer's Privacy?" at 16. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3540277. Accessed 19 July 2019; Delmotte, C. (2022). "The Promises and Pitfalls of a Blockchain Driven Tax System" at 17. Available at https://ssrn.com/abstract=4187919. Accessed 6 October 2022.

[791] Bossa, G. & de Paiva Gomes, E. (2019). "Blockchain: Technology as a Tool for Tax information Exchange or an instrument Threatening the Taxpayer's Privacy?" at 16. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3540277. Accessed 19 July 2019.

3.4.3 Behavioural change in taxpayers

An important revolutionary step that can be brought by the adoption of blockchain is the behavioural change in taxpayer compliance.[792] Generally, tax compliance is low where enforcement measures are inefficient and lax. In other words, there is no incentive for taxpayers to comply with tax laws due to a lack of comprehensive enforcement mechanisms. Compliance can also be low where tax laws are unclear or ambiguous. To combat this, blockchain's transparent nature can be an important aid for tax authorities. Tax authorities can identify non-compliant taxpayers on blockchain. If a taxpayer has not extinguished their tax liability, a tax authority can send a communique to that taxpayer reminding them of their tax liability. If an assessment must be made, a tax authority can easily do so and communicate to the taxpayer accordingly. To avoid further delays, and if a tax authority does not receive correspondence from the taxpayer, a tax authority can elect to charge interest on the tax debt and send this information to the taxpayer by means of a smart contract.[793] This way, tax authorities can act swiftly on non-compliant taxpayers and prevent endemic practices such as tax fraud.[794] Depending on the type of blockchain used, a tax authority can elect to publish the name of a non-compliant taxpayer and the administration of penalties incurred on blockchain.[795]

In my view, this process can act as a deterrent to taxpayers. A taxpayer can experience some sort of discomfort once they realise that other taxpayers on blockchain are familiar with the former's transgressions with tax laws. This can act as an incentive for all taxpayers to fulfil their tax liability actively and positively.[796] Blockchain can also change a taxpayer's approach towards their responsibility in the payment, collection, and remittance of taxes. Should a taxpayer be non-compliant with

[792] PwC (2016). "How blockchain technology could improve the tax system" at 3. Available at https://www.pwc.co.uk/issues/futuretax/assets/documents/how-blockchain-could-improve-the-tax-system.pdf. Accessed 24 March 2021; Owens, J. & De Jong, J. (2017). "Taxation on the Blockchain: Opportunities and Challenges" *Tax Notes International* 87(6): 608; Merkx, M. (2019). "VAT and Blockchain: Challenges and Opportunities ahead" *EC Tax Review* 28(2): 85.

[793] See section 187 of the Tax Administration Act.

[794] See Bird, R. M. & Gendron, P. P. (2007). *The VAT in developing and transitional countries* (Cambridge University Press, New York) at 174.

[795] See Bird, R. M. & Gendron, P. P. (2007). *The VAT in developing and transitional countries* (Cambridge University Press, New York) at 174.

[796] See also Merkx, M. (2019). "VAT and Blockchain: Challenges and Opportunities ahead" *EC Tax Review* 28(2): 85.

the tax laws, that taxpayer can also be excluded from participating in blockchain network.[797]

It is also important to consider whether taxpayers will voluntarily join blockchain to remit tax to the relevant tax authority.[798] Since blockchain can be introduced to close the tax gap, it is important for taxpayers to voluntarily partake in tax remittance on blockchain so that society can benefit from an efficient tax system.[799] Delmotte proposes incentives for taxpayers to voluntarily pay taxes on blockchain.[800] One proposal is to make tax payments on blockchain obligatory. This proposal penalises non-compliant taxpayers with fines, interest, or even imprisonment.[801] Another proposal is for taxpayers to be issued with tokens.[802] A token[803] is cryptocurrency or unit of value that exists on another blockchain.[804] A taxpayer that uses blockchain for remitting taxes can receive tokens for paying their taxes.[805] The tokens can function as a form of ownership or rights in a particular service or company. In the tax context, taxpayers can receive ownership rights in public goods.[806] Taxpayers become partial

[797] PwC (2016). "How blockchain technology could improve the tax system" at 3. Available at https://www.pwc.co.uk/issues/futuretax/assets/documents/how-blockchain-could-improve-the-tax-system.pdf. Accessed 24 March 2021.

[798] Delmotte, C. (2022). "The Promises and Pitfalls of a Blockchain Driven Tax System" at 32. Available at https://ssrn.com/abstract=4187919. Accessed 6 October 2022.

[799] Delmotte, C. (2022). "The Promises and Pitfalls of a Blockchain Driven Tax System" at 32. Available at https://ssrn.com/abstract=4187919. Accessed 6 October 2022.

[800] Delmotte, C. (2022). "The Promises and Pitfalls of a Blockchain Driven Tax System" at 32 – 35. Available at https://ssrn.com/abstract=4187919. Accessed 6 October 2022.

[801] Delmotte, C. (2022). "The Promises and Pitfalls of a Blockchain Driven Tax System" at 34. Available at https://ssrn.com/abstract=4187919. Accessed 6 October 2022.

[802] Delmotte, C. (2022). "The Promises and Pitfalls of a Blockchain Driven Tax System" at 33. Available at https://ssrn.com/abstract=4187919. Accessed 6 October 2022.

[803] Generally, there are three types of tokens. These are currency tokens, utility tokens, and security tokens. According to Juenemann, a utility token is a "kind of digital voucher which can be redeemed against a promised service or issuer. They do not grant membership rights or similar financial relationship and do not substantiate monetary claims. Utility tokens are only accepted by the issuer but not third parties, and only the issuer can carry out the promised service." A currency token "functions as a unit of account that may or may not be backed by reserve, thus may or may not fluctuate in their nominal value against one or more fiat currencies." A security token is a form of security. "Securities are subject to capital markets law in all major economies." See Juenemann, M. *Capital markets* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 265 – 267. See also Momtaz, P. P., Rennertseder, K., and Schröder, H. (2019). *Token Offerings: A Revolution in Corporate Finance?* At 7. Available at https://ssrn.com/abstract=3346964. Accessed 24 December 2022.

[804] Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* Kluwer Law International at 39.

[805] Delmotte, C. (2022). "The Promises and Pitfalls of a Blockchain Driven Tax System" at 34. Available at https://ssrn.com/abstract=4187919. Accessed 6 October 2022.

[806] Delmotte, C. (2022). "The Promises and Pitfalls of a Blockchain Driven Tax System" at 34. Available at https://ssrn.com/abstract=4187919. Accessed 6 October 2022.

owners of the public goods[807] they help finance through the tokens they receive.[808] Token ownership can provide evidence that a taxpayer pays their taxes. Tokens can also be used as a virtual currency to purchase public goods that governments charge for.[809] The last incentive that can be provided to taxpayers is a tax credit.[810] For example, a taxpayer can receive a lump sum tax credit and a percentage in the total tax liability.[811]

3.4.4 The collection of VAT from small parcels

In South Africa, there is no VAT payable on the imported services where the value of the supply does not exceed R100 per invoice.[812] The import of services exceeding R100 remains susceptible to VAT. However, the import of services exceeding R100 often goes unreported due to a lack of compliance.[813] As a result, VAT due to the *fiscus* goes uncollected.[814]

Currently, there is an exemption on low value items (not exceeding R500) such as printed books and journals imported through the post office.[815] The import of low value items is centrally administered at OR Tambo International Airport in Johannesburg.[816] Upon arrival at OR Tambo International Airport, all imports are monitored and cleared by customs.[817] If the imported goods exceed R500, VAT is levied and the recipient of

[807] Examples of public goods include education, garbage collection, and train tickets. See Delmotte, C. (2022). “The Promises and Pitfalls of a Blockchain Driven Tax System” at 34. Available at https://ssrn.com/abstract=4187919. Accessed 6 October 2022.

[808] Delmotte, C. (2022). “The Promises and Pitfalls of a Blockchain Driven Tax System” at 34. Available at https://ssrn.com/abstract=4187919. Accessed 6 October 2022.

[809] Delmotte, C. (2022). “The Promises and Pitfalls of a Blockchain Driven Tax System” at 34. Available at https://ssrn.com/abstract=4187919. Accessed 6 October 2022.

[810] Delmotte, C. (2022). “The Promises and Pitfalls of a Blockchain Driven Tax System” at 32 – 33. Available at https://ssrn.com/abstract=4187919. Accessed 6 October 2022.

[811] Delmotte, C. (2022). “The Promises and Pitfalls of a Blockchain Driven Tax System” at 33. Available at https://ssrn.com/abstract=4187919. Accessed 6 October 2022.

[812] Section 14(5)(e) of the VAT Act.

[813] Kabwe, K., R. (2017). *Consumption tax collection models in online trade in digital goods* unpublished LLM mini-dissertation (UNISA) at 39.

[814] Kabwe, K., R. (2017). *Consumption tax collection models in online trade in digital goods* unpublished LLM mini-dissertation (UNISA) at 39.

[815] Section 13(3) of the VAT Act read with Schedule 1 of the VAT Act.

[816] Steyn, T. (2010). “VAT and e-commerce: still looking for answers?” *South African Mercantile Law Journal* 22(2): 233.

[817] Steyn, T. (2010). “VAT and e-commerce: still looking for answers?” *South African Mercantile Law Journal* 22(2): 233.

the goods pays VAT at the post office before the goods are collected.[818] Generally, a customs clearance fee of R67.60[819] is charged on all incoming parcels and the post office charges an administrative fee of R34.90.[820] It is unclear why the small parcel exemption was introduced in the VAT Act.[821] Van Zyl posits that the provision could have been "introduced to avoid potential bottleneck resulting from an increase in imports as a result of an increased popularity in e-commerce."[822] The importation of parcels into South Africa face numerous challenges. First, if information provided by the consumer is incorrect or outstanding, customs officials can decide to block the parcel until the requested information has been provided.[823] Second, if the custom clearance fee is exorbitant or unexpectedly high, the importer may be reluctant to pay. This can cause delays at OR Tambo International Airport. Third, labour strikes by post office workers or customs officials can cause delays during the clearance process. An importer can receive their parcel three or four months than originally planned due to the strikes. Fourth, if there are large quantities of goods entering the borders on a particular day, imports can take longer than anticipated. This is because the customs clearance process can take longer than expected.[824] Fifth, it can happen that a parcel is randomly chosen for inspection and screening. This is in addition to inspection done on suspicious or dangerous parcels. The inspection process can take up to several weeks since there are many parcels that are checked daily.[825]

[818] Steyn, T. (2010). "VAT and e-commerce: still looking for answers?" *South African Mercantile Law Journal* 22(2): 233; Van Zyl, S. P. (2013). *The collection of Value Added Tax on online cross-border trade in Digital Goods*. Unpublished LLD thesis (UNISA) at 61.

[819] This figure can change in the future.

[820] Post Office (2022). *"Rates Brochure"* at 19. Available at https://www.postoffice.co.za/questions/Postalrates.pdf. Accessed 24 September 2022. This figure can change in the future.

[821] Van Zyl, S. P. (2013). *The collection of Value Added Tax on online cross-border trade in Digital Goods*. Unpublished LLD thesis (UNISA) at 115.

[822] Van Zyl, S. P. (2013). *The collection of Value Added Tax on online cross-border trade in Digital Goods*. Unpublished LLD thesis (UNISA) at 115.

[823] See M6T (2021). "*How long does a shipment take to clear customs in South Africa?"* Available at https://www.m6t.co.za/how-long-does-a-shipment-take-to-clear-customs-in-south-africa/. Accessed 25 September 2022.

[824] See M6T (2021). "*How long does a shipment take to clear customs in South Africa?"* Available at https://www.m6t.co.za/how-long-does-a-shipment-take-to-clear-customs-in-south-africa/. Accessed 25 September 2022.

[825] See M6T (2021). "*How long does a shipment take to clear customs in South Africa?"* Available at https://www.m6t.co.za/how-long-does-a-shipment-take-to-clear-customs-in-south-africa/. Accessed 25 September 2022.

The OECD has noted that the collection of VAT from small parcels can be onerous, susceptible to non-compliance, and not cost effective.[826] The application of import VAT exemptions on small parcels has been untenable due to the rise in online purchases of low-value goods from foreign suppliers.[827] The OECD states that using traditional customs-based collection processes for countries that decide to collect VAT on small parcels could lead to disproportionate VAT collection costs, making detecting fraud challenging, and this could have detrimental effects on the tax collection on the importation of goods with higher value.[828] For these reasons, the OECD recommends the vendor collection model as a mechanism to collect VAT on small parcels or low-value goods. In terms of this model, the foreign supplier registers for and collects VAT on the supply of low-value imported goods to consumers in the jurisdiction of taxation.[829]

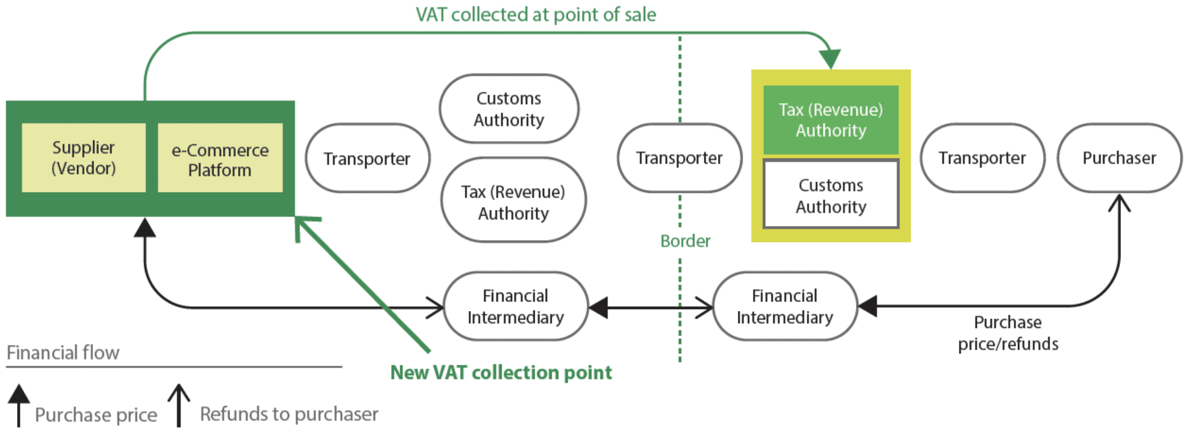


Figure 10[830]

[826] OECD/WBG/ATAF (2023). *VAT Digital Toolkit for Africa* OECD Paris at 114. Available at https://www.oecd.org/tax/consumption/vat-digital-toolkit-for-africa.pdf. Accessed 12 August 2023.

[827] OECD/WBG/ATAF (2023). *VAT Digital Toolkit for Africa* OECD Paris at 115. Available at https://www.oecd.org/tax/consumption/vat-digital-toolkit-for-africa.pdf. Accessed 12 August 2023.

[828] OECD/WBG/ATAF (2023). *VAT Digital Toolkit for Africa* OECD Paris at 115. Available at https://www.oecd.org/tax/consumption/vat-digital-toolkit-for-africa.pdf. Accessed 12 August 2023.

[829] OECD/WBG/ATAF (2023). *VAT Digital Toolkit for Africa* OECD Paris at 118. Available at https://www.oecd.org/tax/consumption/vat-digital-toolkit-for-africa.pdf. Accessed 12 August 2023.

[830] **Figure 10** demonstrates how the vendor collection mechanism works in the context of VAT collection on the importation of low-value goods. **Figure 10** is directly taken from OECD/WBG/ATAF (2023). *VAT Digital Toolkit for Africa* OECD Paris at 121. Available at https://www.oecd.org/tax/consumption/vat-digital-toolkit-for-africa.pdf. Accessed 12 August 2023.

In terms of the vendor collection for low-value goods, VAT on the supply of these goods by foreign suppliers is collected in the jurisdiction of importation at the point of sale by the foreign supplier or by the digital platform that facilitates the supply rather than at the border upon importation.[831] This means that the consumer is charged the gross amount inclusive of VAT and the foreign supplier or the digital platform collects and remits VAT to the tax authorities. When the goods arrive at the border, VAT has already been paid and the customs officials are not required to assess VAT.[832] In essence, the VAT collection burden on low-value goods shifts from customs officials at the border to the foreign supplier of digital goods or the digital platform.[833] The benefits of this collection model include: i) reduced administrative costs, ii) foreign suppliers and digital platforms apply VAT to the purchase price as opposed to customs officials, iii) maximise the tax base by levying VAT on previously untaxed low-value goods, iv) increasing the efficiency of compliance risk strategies and enforcement actions, v) faster customs clearance and shorter delivery times, and vi) improved consumer compliance.[834]

There are several benefits of using blockchain in the custom clearance process. First and foremost, customs officials can monitor the origin of the imported goods.[835] It is possible to store information relating to the production phase, verification, transport, and the customs clearance process.[836] During these processes, a unique identification code is assigned which promotes transparency in the logistics process.[837] Second, the

[831] OECD/WBG/ATAF (2023). *VAT Digital Toolkit for Africa* OECD Paris at 121. Available at https://www.oecd.org/tax/consumption/vat-digital-toolkit-for-africa.pdf. Accessed 12 August 2023.

[832] OECD/WBG/ATAF (2023). *VAT Digital Toolkit for Africa* OECD Paris at 121. Available at https://www.oecd.org/tax/consumption/vat-digital-toolkit-for-africa.pdf. Accessed 12 August 2023.

[833] OECD/WBG/ATAF (2023). *VAT Digital Toolkit for Africa* OECD Paris at 121. Available at https://www.oecd.org/tax/consumption/vat-digital-toolkit-for-africa.pdf. Accessed 12 August 2023.

[834] This is not a closed list. See fully OECD/WBG/ATAF (2023). *VAT Digital Toolkit for Africa* OECD Paris at 124 – 125. Available at https://www.oecd.org/tax/consumption/vat-digital-toolkit-for-africa.pdf Accessed 12 August 2023.

[835] Belu, G. M. (2020). “Blockchain Technology and Customs Procedures” *The Romanic Economic Journal* Year XXIII issue 78: at 19.

[836] Belu, G. M. (2020). “Blockchain Technology and Customs Procedures” *The Romanic Economic Journal* Year XXIII issue 78: at 19.

[837] Belu, G. M. (2020). “Blockchain Technology and Customs Procedures” *The Romanic Economic Journal* Year XXIII issue 78: at 19.

use of blockchain can reduce the waiting times at customs.[838] This is possible because the identities of the parties (the importer and the supplier) can be verified.[839] Once the identity of the parties have been verified, customs officials can have a better picture of international trade transactions subject to customs clearance.[840] Customs officials can obtain information on the nature, route, and the parties involved in commercial transactions.[841] This can facilitate successful risk management procedures related to customs clearance of goods, reducing the time required to obtain customs clearance.[842] Third, blockchain can digitise customs documents.[843] This makes it easier to manage documents required to obtain customs clearance.[844] Fourth, blockchain can help reduce the VAT gap. Blockchain's transparency and traceability features can help detect fraud and errors.[845] Customs officials, suppliers, importers, and any other relevant parties can exchange information in real-time. This can help customs officials to identify fraudulent practices and strengthen revenue collection.[846] Fifth, blockchain technology can assist customs officials and the relevant role players to improve their capacity to conduct risk analysis and management, thus contributing to international trade.[847] Blockchain technology can link customs officials and business entities to a common platform that enables exchange of information between all the

[838] Belu, G. M. (2020). "Blockchain Technology and Customs Procedures" *The Romanic Economic Journal* Year XXIII issue 78: at 18.

[839] Belu, G. M. (2020). "Blockchain Technology and Customs Procedures" *The Romanic Economic Journal* Year XXIII issue 78: at 18; Ganne, E. (2018). *"Can Blockchain revolutionize international trade?"* World Trade Organisation at 35. Available at https://theblockchaintest.com/uploads/resources/WTO%20-%20Can%20Blockchain%20revolutionize%20international%20trade%20-%202018.pdf. Accessed 25 September 2022.

[840] Belu, G. M. (2020). "Blockchain Technology and Customs Procedures" *The Romanic Economic Journal* Year XXIII issue 78: at 18.

[841] Belu, G. M. (2020). "Blockchain Technology and Customs Procedures" *The Romanic Economic Journal* Year XXIII issue 78: at 18.

[842] Belu, G. M. (2020). "Blockchain Technology and Customs Procedures" *The Romanic Economic Journal* Year XXIII issue 78: at 18.

[843] Belu, G. M. (2020). "Blockchain Technology and Customs Procedures" *The Romanic Economic Journal* Year XXIII issue 78: at 20.

[844] Belu, G. M. (2020). "Blockchain Technology and Customs Procedures" *The Romanic Economic Journal* Year XXIII issue 78: at 20.

[845] Belu, G. M. (2020). "Blockchain Technology and Customs Procedures" *The Romanic Economic Journal* Year XXIII issue 78: at 19.

[846] Belu, G. M. (2020). "Blockchain Technology and Customs Procedures" *The Romanic Economic Journal* Year XXIII issue 78: at 19; see also Chang, Y. *et al* (2020). "Blockchain in global supply chains and cross-border trade: a critical synthesis of the state-of-the-art, challenges and opportunities" International Journal of Production Research 58(7): 2093 – 2094. Available at https://doi.org/10.1080/00207543.2019.1651946. Accessed 25 September 2022.

[847] Belu, G. M. (2020). "Blockchain Technology and Customs Procedures" *The Romanic Economic Journal* Year XXIII issue 78: at 18.

relevant role players.[848] For example, information related to the seller, buyer, price, quantity, carrier, financing, and insurance can be used to track the location and the status of the goods in real-time.[849] Last, blockchain technology can improve compliance with product safety and conformity standards by providing a platform where manufacturers, logistics operators, regulators, and consumers can access information relating to the origins of the products.[850] Blockchain technology can also ensure that the products have been adequately tested for certification and that the correct export/import licence has been issued.[851]

From a tax authority perspective, the collection of VAT on blockchain can simplify the VAT system by addressing the challenges of small parcels.[852] Small parcels can be traced on blockchain by tax authorities.[853] Tax authorities can verify and determine whether the transactions are susceptible to VAT. Tax authorities can notify the supplier whenever a transaction is susceptible to VAT. The supplier can then remit the amount of VAT by making use of a smart contract. Additionally, traces of these transactions could provide a better picture of the frequency and nature of small transactions to tax authorities. The collection of VAT from small transactions that was previously untraceable and uncollected, could boost the revenue pool for emerging economies.[854] As mentioned above, the collection of VAT from these transactions can also bridge the VAT gap. The VAT gap is the difference between the projected VAT

[848] Belu, G. M. (2020). "Blockchain Technology and Customs Procedures" *The Romanic Economic Journal* Year XXIII issue 78: at 18. See also Chang, Y. *et al* (2020). "Blockchain in global supply chains and cross-border trade: a critical synthesis of the state-of-the-art, challenges and opportunities" International Journal of Production Research 58(7): 2093 – 2094. Available at https://doi.org/10.1080/00207543.2019.1651946. Accessed 25 September 2022.

[849] Belu, G. M. (2020). "Blockchain Technology and Customs Procedures" *The Romanic Economic Journal* Year XXIII issue 78: at 18.

[850] Belu, G. M. (2020). "Blockchain Technology and Customs Procedures" *The Romanic Economic Journal* Year XXIII issue 78: at 19.

[851] Belu, G. M. (2020). "Blockchain Technology and Customs Procedures" *The Romanic Economic Journal* Year XXIII issue 78: at 19.

[852] Merkx, M. (2019). "VAT and Blockchain: Challenges and Opportunities ahead" *EC Tax Review* 28(2): 85; PWC (2016). "How blockchain technology could improve the tax system" at 1 - 3. Available at https://www.pwc.co.uk/issues/futuretax/assets/documents/how-blockchain-could-improve-the-tax-system.pdf. Accessed 24 March 2021.

[853] PwC (2016). "How blockchain technology could improve the tax system" at 1 - 3. Available at https://www.pwc.co.uk/issues/futuretax/assets/documents/how-blockchain-could-improve-the-tax-system.pdf. Accessed 24 March 2021.

[854] From a South African perspective, it can result in the reduction of staff requirement. It can alleviate the qualified staffing shortage experienced by customs, or it can result in job losses. If job losses are anticipated, political will is required to implement. Due to the high unemployment rate in South Africa, it might not be feasible to implement without political will.

collection revenue figures and the actual amount of VAT collected.[855] Generally, the VAT gap is caused by tax evasion, tax avoidance and optimisation practices, bankruptcies, tax fraud, financial insolvencies, miscalculations, and administrative errors.[856]

3.4.5 Reduction in transaction costs

E-commerce facilitates the exchange of goods and services between a willing buyer and a willing seller. Purchases can be triggered when a buyer accesses the seller's online platform, selects the desired item(s) before paying the purchase price.[857] Due to the nature of e-commerce, both buyer and seller can be situated in different jurisdictions. Currently, tax remittance requires the presence of financial intermediaries to broker payments by checking that the important features are present.[858] A financial intermediary in the buyer's jurisdiction ascertains if funds are available in the latter's bank account. The financial intermediary in the buyer's jurisdiction transfers the funds to the seller's bank account.[859] During that exchange, it is possible for the financial intermediary to charge a fee. Intermediation costs are transaction costs typically borne by sellers and buyers when they cannot reliably establish the facets of a specific transaction.[860]

[855] Cnossen, S. (2019). Modernizing VATs in Africa *Oxford University Press* (UK) at 274; see also European Commission (2019). "*Taxation and Customs Union: VAT Gap*". Available at https://taxation-customs.ec.europa.eu/business/vat/vat-gap_en. Accessed 24 September 2022; see also Hoffman, M. R. (2018). "Can Blockchains and Linked Data Advance Taxation?" Available at https://dl.acm.org/doi/fullHtml/10.1145/3184558.3191555. Accessed 6 October 2022; See Delmotte, C. (2022). "The Promises and Pitfalls of a Blockchain Driven Tax System" at 15. Available at https://ssrn.com/abstract=4187919. Accessed 6 October 2022.

[856] European Commission (2019). "*Taxation and Customs Union: VAT Gap*". Available at https://taxation-customs.ec.europa.eu/business/vat/vat-gap_en. Accessed 24 September 2022.

[857] See Catalinin, C. & Gans, J., S. (2016). "Some Simple Economics of the Blockchain" at 2 – 3. Available at https://ccl.yale.edu/sites/default/files/files/SSRN%20--%20Some%20Simple%20Economics%20About%20Blockchain.pdf. Accessed 16 April 2021.

[858] Delmotte, C. (2022). "The Promises and Pitfalls of a Blockchain Driven Tax System" at 19. Available at https://ssrn.com/abstract=4187919. Accessed 6 October 2022.

[859] Catalinin, C. & Gans, J., S. (2016). "Some Simple Economics of the Blockchain" at 3. Available at https://ccl.yale.edu/sites/default/files/files/SSRN%20--%20Some%20Simple%20Economics%20About%20Blockchain.pdf. Accessed 16 April 2021; see also Delmotte, C. (2022). "The Promises and Pitfalls of a Blockchain Driven Tax System" at 19. Available at https://ssrn.com/abstract=4187919. Accessed 6 October 2022.

[860] Catalinin, C. & Gans, J., S. (2016). "Some Simple Economics of the Blockchain" at 3. Available at https://ccl.yale.edu/sites/default/files/files/SSRN%20--%20Some%20Simple%20Economics%20About%20Blockchain.pdf. Accessed 16 April 2021; see also Delmotte, C. (2022). "The Promises and Pitfalls of a Blockchain Driven Tax System" at 19. Available at https://ssrn.com/abstract=4187919. Accessed 6 October 2022.

Generally, if the seller is a VAT vendor, there is an obligation on them to remit VAT to the relevant tax authority. The VAT remittance must be verified and processed by a financial intermediary before it is transmitted to the tax authority's jurisdiction. Sellers often bear high transaction costs due to the continued obligation to remit VAT to tax authorities. The problem is compounded by the fact that a supplier must remit VAT to tax authorities in multiple jurisdictions. With the adoption of blockchain, sellers can potentially remit VAT instantaneously to the relevant tax authority without incurring transaction costs. In the process, VAT is remitted in real time and businesses' transaction costs are significantly reduced.[861]

Kim correctly points out that tax information originates from taxpayer activities, which is not always readily available to tax authorities.[862] Ordinarily, this information is obtained from taxpayers through self-reporting, or the information can be retrieved from third parties like financial institutions.[863] Kim argues that blockchain's transparency and immutability features can resolve the information asymmetry in the tax compliance system.[864] Currently, tax authorities rely on costly methods to verify a taxpayer's reported information.[865] Blockchain allows tax authorities to work with tax

[861] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 198; WU Net Team. (2017). "Blockchain: Taxation and Regulatory Challenges and Opportunities" *WU Global Tax Policy Centre of Vienna University of Business and Economics* at 8; Demirhan, H. *Effective Taxation System by Blockchain Technology* in Hacioglu, U., (ed) (2019). *Blockchain Economics and Financial Market Innovation: Financial Innovations in the Digital Age* (Springer) at 354; Catalinin, C. & Gans, J., S. (2016). "Some Simple Economics of the Blockchain" at 4. Available at https://ccl.yale.edu/sites/default/files/files/SSRN%20--%20Some%20Simple%20Economics%20About%20Blockchain.pdf. Accessed 16 April 2021; Owens, J. & De Jong, J. (2017). "Taxation on the Blockchain: Opportunities and Challenges" *Tax Notes International* 87(6): 607; Kim, R., C. (2021). "Blockchain Initiatives for Tax Administration" *University of Utah College of Law Research Paper No 427* at 25. Available at https://ssrn.com/abstract=3798136. Accessed 26 June 2021; Mazur, O. (2021). "Can Blockchain Revolutionize Tax Administration?" SMU Dedman School of Law Legal Studies Research Paper No. 510 at 21. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3841785. Accessed 23 June 2021.

[862] Kim, R., C. (2021). "Blockchain Initiatives for Tax Administration" *University of Utah College of Law Research Paper No 427* at 5. Available at https://ssrn.com/abstract=3798136. Accessed 26 June 2021.

[863] Kim, R., C. (2021). "Blockchain Initiatives for Tax Administration" *University of Utah College of Law Research Paper No 427* at 5. Available at https://ssrn.com/abstract=3798136. Accessed 26 June 2021.

[864] Kim, R., C. (2021). "Blockchain Initiatives for Tax Administration" *University of Utah College of Law Research Paper No 427* at 5. Available at https://ssrn.com/abstract=3798136. Accessed 26 June 2021.

[865] Mazur, O. (2021). "Can Blockchain Revolutionize Tax Administration?" SMU Dedman School of Law Legal Studies Research Paper No. 510 at 9. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3841785. Accessed 23 June 2021; see

information embedded in a transaction in real-time.[866] Since tax information cannot be modified if stored on a blockchain, the transactional burden of taxation is reduced while the reliability of data is improved.[867]

3.4.6 Blockchain and the sharing economy

The ‘sharing economy’ or the ‘collaborative economy’[868] is a “business model where activities are facilitated by collaborative platforms that create an open marketplace for the temporary usage of goods and services often provided by private individuals.”[869] Generally, the sharing economy is characterised by an online innovative business model where parties share certain common traits.[870] Second, transactions take place in a marketplace intermediated by digital platforms.[871] Third, the sharing economy generally has three actors: an online platform operating a virtual marketplace; customers receiving temporary access to products; and individuals supplying goods and services.[872] Fourth, the suppliers of goods and services and customers usually act in a business or private capacity.[873] Fifth, parties in the sharing economy can perform activities habitually and occasionally.[874] Last, at least two parties are required to perform transactions and the economic activities are carried out for profit or for free.[875]

There are three important role players in the sharing economy. The first role player is the digital platform. The digital platform can be a broker or intermediary that facilitates transactions between the supplier of goods and services and the consumer. The

also Delmotte, C. (2022). “The Promises and Pitfalls of a Blockchain Driven Tax System” at 19. Available at https://ssrn.com/abstract=4187919. Accessed 6 October 2022.

[866] Delmotte, C. (2022). “The Promises and Pitfalls of a Blockchain Driven Tax System” at 19. Available at https://ssrn.com/abstract=4187919. Accessed 6 October 2022.

[867] Delmotte, C. (2022). “The Promises and Pitfalls of a Blockchain Driven Tax System” at 19. Available at https://ssrn.com/abstract=4187919. Accessed 6 October 2022.

[868] These terms are often used interchangeably.

[869] European Commission (2016). *Communication from the commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the regions: A European agenda for the collaborative economy* at 3; see also Beretta, G. (2018). “VAT and the Sharing Economy” *World Tax Journal* 10(3): 386.

[870] Beretta, G. (2018). “VAT and the Sharing Economy” *World Tax Journal* 10(3): 386.

[871] Beretta, G. (2018). “VAT and the Sharing Economy” *World Tax Journal* 10(3): 386.

[872] Beretta, G. (2018). “VAT and the Sharing Economy” *World Tax Journal* 10(3): 387.

[873] Beretta, G. (2018). “VAT and the Sharing Economy” *World Tax Journal* 10(3): 387.

[874] Beretta, G. (2018). “VAT and the Sharing Economy” *World Tax Journal* 10(3): 387.

[875] Beretta, G. (2018). “VAT and the Sharing Economy” *World Tax Journal* 10(3): 387.

second role player is the supplier. The supplier dispenses their assets, time, or skills on the digital platform. It is possible for a supplier to act in a professional or private capacity.[876] The third role player is the consumer. The consumer is the person or business that receives goods or services from the digital platform and from other platform users or suppliers. However, it should be noted that consumers can also provide services in a barter transaction with other users.[877]

One of the key contributing factors to the growth of the sharing economy are the recent advancements in ICT, which has facilitated access to information.[878] ICT has reduced the cost of doing business by providing lower market entry barriers for service providers.[879] A central entity no longer supplies goods and services to customers. Rather, transactions take place directly between individuals through a digital platform.[880] Beretta submits that the financial crisis forced individuals to look for alternative sources of income, while a reduced need of capital investments can be alluring to businesses.[881]

While it is true that the sharing economy has had a positive economic impact on individuals and businesses, the sharing economy has also posed challenges to the tax sector. From a VAT perspective, it is difficult to ascertain the taxable person.[882] In the sharing economy, an individual can be a supplier and a consumer at the same time.[883] For example, a user on a sharing platform can act in their professional capacity (as a VAT vendor) or in their private capacity by exploiting their assets for personal or commercial reasons.[884] As a result, it is difficult to establish the capacity in which an individual is acting when performing economic transactions on the digital platforms. Additionally, Beretta correctly points out that it is difficult to establish the liability of the

[876] Beretta, G. (2018). "VAT and the Sharing Economy" *World Tax Journal* 10(3): 388.

[877] Beretta, G. (2018). "VAT and the Sharing Economy" *World Tax Journal* 10(3): 388 – 389.

[878] Cannas, F. (2017). "Sharing economy: Everyone can be an entrepreneur for two days…but what about a VAT taxable person?" *World Journal of VAT* 6(2): 82.

[879] Beretta, G. (2018). "VAT and the Sharing Economy" *World Tax Journal* 10(3): 387.

[880] Beretta, G. (2018). "VAT and the Sharing Economy" *World Tax Journal* 10(3): 387.

[881] Beretta, G. (2018). "VAT and the Sharing Economy" *World Tax Journal* 10(3): 388.

[882] In the South African context, VAT vendor is used.

[883] Cannas, F. (2017). "Sharing economy: Everyone can be an entrepreneur for two days…but what about a VAT taxable person?" *World Journal of VAT* 6(2): 82; Lidstrom, C. (2020). *EU VAT and the sharing economy: The relationship between the concept of "taxable person" and Airbnb and Uber* unpublished LLM thesis (Uppsala Universitet) at 14.

[884] Lidstrom, C. (2020). *EU VAT and the sharing economy: The relationship between the concept of "taxable person" and Airbnb and Uber* unpublished LLM thesis (Uppsala Universitet) at 14.

sharing platforms in so far as VAT compliance and collection is concerned, especially in cross-border situations.[885] Moreover, the OECD has highlighted the fact that the sharing economy has the potential to erode a jurisdiction's VAT base. According to the OECD, this can lead to a shift in economic activity from a small number of large tax compliant businesses to a large number of small business actors that may not necessarily be tax compliant because their activities remain below the VAT exempt/registration threshold.[886] The business model employed in the sharing economy makes it difficult to determine the VAT nature and status of the actors and to determine and implement the appropriate VAT treatment of the transactions.[887]

Adopting blockchain can resolve some of the issues associated with VAT collection in the sharing economy. For example, tax authorities can monitor the transactions and the VAT payments of the participants on blockchain. In doing so, tax authorities can ascertain the VAT liability of each participant in the sharing economy. Tax authorities can impose data reporting obligations on actors in the sharing economy supply chain.[888] With blockchain, the digital platform can assume responsibility by discharging the underlying VAT liability borne by the supplier.[889] A smart contract can be used to calculate the supplier's VAT liability. Remittance to the relevant tax authority is done in real-time. If the supplier is not VAT compliant, the joint and several liability (JSL) regime can provide for the tax authorities to declare the platform that facilitates the sharing economy jointly and severally liable for VAT.[890] A smart contract can be programmed to ensure that once a supplier is non-compliant, the hosting platform will automatically incur VAT liability and the proportionate VAT amount can be paid to the relevant tax authority in real-time. This process ensures that the VAT due to the respective tax authorities is paid on time. Alternatively, a full liability regime (FLR) stipulates that the digital platform is designated by law as the supplier for VAT liability

[885] Beretta, G. (2018). "VAT and the Sharing Economy" *World Tax Journal* 10(3): 390.

[886] OECD (2021). *The Impact of the Growth of the Sharing and Gig Economy on VAT/GST Policy and Administration* OECD Publishing, Paris at 27.

[887] OECD (2021). *The Impact of the Growth of the Sharing and Gig Economy on VAT/GST Policy and Administration* OECD Publishing, Paris at 27.

[888] OECD (2021). *The Impact of the Growth of the Sharing and Gig Economy on VAT/GST Policy and Administration* OECD Publishing, Paris at 35.

[889] OECD (2021). *The Impact of the Growth of the Sharing and Gig Economy on VAT/GST Policy and Administration* OECD Publishing, Paris at 60.

[890] OECD (2021). *The Impact of the Growth of the Sharing and Gig Economy on VAT/GST Policy and Administration* OECD Publishing, Paris at 60.

purposes.[891] Under this regime, the digital platform is solely liable for VAT to the respective tax authorities.[892] The assessment, collection, and remittance of VAT can be effected using a smart contract on a blockchain. Thus, blockchain can simplify administration of VAT in the sharing economy.

3.4.7 Improved auditing function

Performing an audit function remains one of the most crucial aspects of tax administration.[893] A tax audit is important for tax authorities because it enables them to sustain a good tax administration system.[894] According to Demirhan, conducting a tax audit is significant because it expands the tax base, reduces tax evasion, and minimises tax losses.[895] Generally, tax authorities verify filed VAT returns in order to determine the accuracy of the VAT remitted. Inconsistencies in the submission of VAT returns and the VAT remitted can be picked up by tax authorities through the audit process.[896] As a rule, the realisation of a successful audit is dependent on three aspects – i) the information processing capacity of tax authorities; ii) the collection of information from taxpayers and other third parties, and iii) the strategy adopted by the relevant tax authority.[897] In my view, the adoption of a suitable strategy can be used to enhance a tax authority's capacity to retrieve tax related data. If that strategy amplifies a tax authority's capacity to perform an audit function, then that strategy must also be adopted.

[891] OECD (2021). *The Impact of the Growth of the Sharing and Gig Economy on VAT/GST Policy and Administration* OECD Publishing, Paris at 77.

[892] This is in line with OECD's recommendations. See OECD (2019), *The Role of Digital Platforms in the Collection of VAT/GST on Online Sales*, OECD, Paris. Available at https://www.oecd.org/tax/consumption/the-role-of-digital-platforms-in-the-collection-of-vat-gst-on-online-sales.pdf. Accessed 17 August 2023.

[893] Bird, R. M. & Gendron, P. P. (2007). *The VAT in developing and transitional countries* (Cambridge University Press, New York) at 172; Bird, M., R., and Zolt M., E. (2008). "Technology and taxation in developing countries: from hand to mouse" *National Tax Journal* 61(4): Part 2 at 802.

[894] Bird, R. M. & Gendron, P. P. (2007). *The VAT in developing and transitional countries* (Cambridge University Press, New York) at 172.

[895] Demirhan, H. *Effective Taxation System by Blockchain Technology* in Hacioglu, U., (ed) (2019). *Blockchain Economics and Financial Market Innovation: Financial Innovations in the Digital Age* (Springer) at 357.

[896] Bird, M., R., and Zolt M., E. (2008). "Technology and taxation in developing countries: from hand to mouse" *National Tax Journal* 61(4) Part 2 at 802.

[897] Bird, M., R., and Zolt M., E. (2008). "Technology and taxation in developing countries: from hand to mouse" *National Tax Journal* 61(4) Part 2 at 802.

The audit function can be performed on a blockchain in two ways. Whenever transactions are recorded on blockchain, they can be viewed and accessed by a tax authority at any given time. Tax authorities can cross check information supplied on a tax invoice and the actual VAT remitted. All transactions remain immutable, further providing good audit trail for tax authorities. A transaction on blockchain contains transactional data (hashed data)[898] which can be used to identify a participant on a blockchain.[899] Transactions are also recorded on the address of the smart contracts enabling tax authorities to view all outgoing and incoming transactions.[900] According to Merkx, AI can be used to perform the audit function on blockchain where the smart contracts have been stored.[901]

Blockchain's transparent nature can aid tax authorities to ascertain a taxpayer's identity beforehand. Once identified, foreign suppliers can be audited at any time to ensure compliance with the VAT laws. In my view, foreign suppliers can be exempted from keeping records due to blockchain's immutability.[902] All transactions can be stored, accessed, and retrieved from blockchain at any given time by a tax authority. In my view, it is illogical for suppliers to maintain records for extended periods if a tax authority stores and accesses the same records on blockchain network. The records can be accessed in real-time.[903] A supplier's compliance burden is reduced in the process.[904]

[898] See discussion at paragraphs 5.4.4 below and 2.5.6 above.

[899] Artzt, M., (ed) Determann, L., Long, W., *Blockchain and Data Privacy* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 197 – 198.

[900] Rikken, O. (2017). "Blockchain Real Time Tax". Available at https://www.linkedin.com/pulse/blockchain-real-time-tax-olivier-rikken. Accessed 6 April 2021; Merkx, M. (2019). "VAT and Blockchain: Challenges and Opportunities Ahead" *EC Tax Review* 28(2): 88.

[901] Merkx, M. (2019). "VAT and Blockchain: Challenges and Opportunities ahead" *EC Tax Review* 28(2): 88.

[902] See section 29 of the Tax Administration Act 28 of 2011.

[903] Merkx, M. (2019). "VAT and Blockchain: Challenges and Opportunities ahead" *EC Tax Review* 28(2): 85.

[904] The Tax Administration Act allows for electronic record keeping. Thus, it is not necessary to make amendments since the Act allows for smooth implementation. For example, section 255 of the Tax Administration Act reads: "(1) The Commissioner may by public notice make rules prescribing - (a) the procedures for submitting a return in electronic format, electronic record retention and other electronic communications between SARS and other persons; (b) requirements for an electronic or digital signature of a return or communication; and (c) the procedures for electronic record retention by SARS. (2) SARS may, in the case of a return or other document submitted in electronic format, accept an electronic or digital signature of a person as a valid signature for purposes of a tax Act if a signature is required. (3) If in any proceedings under a tax Act, the question arises whether an electronic or digital signature of a

3.4.8 Reduction of VAT fraud

One of the most challenging aspects of taxing e-commerce transactions is the difficulty in establishing the identity of the taxpayer. If the taxpayer is unidentifiable or lacks any physical presence in the country of consumption, transactions can be concealed to evade paying taxes.[905] Tax authorities often lack the resources to locate taxpayers in order to enforce tax laws.[906] The advancement of technology brings new opportunities for the early prevention and detection of tax evasion and VAT fraud.[907]

From the onset, it must be noted that VAT evasion and VAT fraud are not similar. Generally, VAT fraud occurs when a taxpayer omits to pay VAT to the relevant tax authority.[908] VAT fraud constitutes the "coordinated and systemic actions, with varying levels of sophistication and organisation towards obtaining an unlawful extra VAT financial advantage, beyond the mere reduction of liability."[909] VAT evasion is "the deliberate refrainment from correctly reporting the taxable nature of transactions in order to reduce tax liability."[910] There are different types of VAT fraud. First, bogus traders occur when companies are set up solely to sale invoices that allow for the recovery of VAT.[911] Second, missing trader fraud (MTF) occurs when a registered

person referred to in subsection (2) was used with the authority of the person, it must be assumed, in the absence of proof to the contrary, that the signature was so used." Furthermore, the definition of 'document' in section 1 of the Tax Administration Act reads: "anything that contains a written, sound or pictorial record, or other record of information, whether in physical or electronic form."

[905] Basu, S. (2007). *Global perspectives on e-commerce taxation law* (Routledge, UK publishing) at 104.

[906] Bird, R. M. & Gendron, P. P. (2007). *The VAT in developing and transitional countries* (Cambridge University Press, New York) at 26.

[907] Merkx, M., & Verbaan, N. (2019). "Technology: A key to solve VAT Fraud?" *EC Tax Review* 28(6) at 301.

[908] Merkx, M., & Verbaan, N. (2019). "Technology: A key to solve VAT Fraud?" *EC Tax Review* 28(6) at 301; Van Zyl, S. P. (2013). *The collection of Value Added Tax on online cross-border trade in Digital Goods*. Unpublished LLD thesis (UNISA) at 315; Ainsworth, R. T. & Madzharova, B. (2012). "Real-Time Collection of the Value-Added Tax: Some Business and Legal Implications" *Boston University School of Law, Law and Economics Research paper* 12-51 at 7. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2166316. Accessed 26 March 2021.

[909] De la Feria, R. & Schoeman, A. (2019). "Addressing VAT fraud in developing countries: the tax policy-administration symbiosis" at 4. Available at https://repository.up.ac.za/bitstream/handle/2263/77923/DelaFeria_Addressing_2019.pdf?sequence=1. Accessed 29 December 2022.

[910] Alexander, G. (2022). "Blocking the Gap: The Potential for Blockchain Technology to secure VAT Compliance" *EC Tax Review* 31(3): 142.

[911] Alexander, G. (2022). "Blocking the Gap: The Potential for Blockchain Technology to secure VAT Compliance" *EC Tax Review* 31(3): 142; see also De la Feria, R. & Schoeman, A. (2019). "Addressing VAT fraud in developing countries: the tax policy-administration symbiosis" at 4 –

business charges VAT to their customers but disappears before paying tax to the tax authorities.[912] Third, carousel fraud or Missing Trading Intra-Community Fraud (MITC)[913] is a more sophisticated from of MTF that involves the movement of goods in and out of the EU. Several parties exploit VAT rules, leaving VAT imports unpaid.[914] Fourth, under-reported sales occurs when a business only reports a proportion of their sales, falsifies accounts, or keeps sales off-the-books by not issuing invoices.[915] Fifth, VAT fraud can occur when businesses generate sales above the registration threshold but fail to register.[916] Last, misclassification of sales takes place where a business reduces its tax liability by overestimating the proportion of sales in products subject to reduced rates of VAT.[917]

5. Available at https://repository.up.ac.za/bitstream/handle/2263/77923/DelaFeria_Addressing_2019.pdf?sequence=1. Accessed 29 December 2022.

[912] Keen, M. & Smith, S. (2007). "VAT fraud and evasion: what do we know, and what can be done?" IMF working paper WP/07/31 at 8. Available at https://www.imf.org/external/pubs/ft/wp/2007/wp0731.pdf. Accessed 29 December 2022; Alexander, G. (2022). "Blocking the Gap: The Potential for Blockchain Technology to secure VAT Compliance" *EC Tax Review* 31(3): 143.

[913] De le Feria and Schoeman explain carousel fraud as follows: "In its simplest form, a trader – the missing trader– collects VAT paid to him by a supplier without accounting or remitting to the tax authorities, disappearing soon after, and before the authorities realise what has occurred. There are numerous variations to this basic model: the same goods may move around different chains continuously, with all the traders in the chain, or its employees, involved, or at least aware that the fraud is occurring (carousel fraud); or different goods are sold by fraudsters to unsuspecting third parties, inserting themselves into legitimate production chains (missing trader fraud). A more recent version of the missing trader fraud is reportedly the insolvent trader, in which instead of a missing trader, the scheme includes an existing firm, which is stripped of any assets before the tax authorities reach it. Whilst these fraud schemes have traditionally been a great concern within the European Union, similar schemes have now developed in other countries, taking advantage of VAT temporary exemption rules on imports." See De la Feria, R. & Schoeman, A. (2019). "Addressing VAT fraud in developing countries: the tax policy-administration symbiosis" at 6. Available at https://repository.up.ac.za/bitstream/handle/2263/77923/DelaFeria_Addressing_2019.pdf?sequence=1. Accessed 29 December 2022.

[914] Alexander, G. (2022). "Blocking the Gap: The Potential for Blockchain Technology to secure VAT Compliance" *EC Tax Review* 31(3): 143; Merkx, M., & Verbaan, N. (2019). "Technology: A key to solve VAT Fraud?" *EC Tax Review* 28(6) at 301.

[915] De la Feria, R. & Schoeman, A. (2019). "Addressing VAT fraud in developing countries: the tax policy-administration symbiosis" at 5. Available at https://repository.up.ac.za/bitstream/handle/2263/77923/DelaFeria_Addressing_2019.pdf?sequence=1. Accessed 29 December 2022; Keen, M. & Smith, S. (2007). "VAT fraud and evasion: what do we know, and what can be done?" IMF working paper WP/07/31 at 7 – 8. Available at https://www.imf.org/external/pubs/ft/wp/2007/wp0731.pdf. Accessed 29 December 2022.

[916] De la Feria, R. & Schoeman, A. (2019). "Addressing VAT fraud in developing countries: the tax policy-administration symbiosis" at 5. Available at https://repository.up.ac.za/bitstream/handle/2263/77923/DelaFeria_Addressing_2019.pdf?sequence=1. Accessed 29 December 2022; Keen, M. & Smith, S. (2007). "VAT fraud and evasion: what do we know, and what can be done?" IMF working paper WP/07/31 at 8. Available at https://www.imf.org/external/pubs/ft/wp/2007/wp0731.pdf. Accessed 29 December 2022.

[917] De la Feria, R. & Schoeman, A. (2019). "Addressing VAT fraud in developing countries: the tax policy-administration symbiosis" at 5. Available at

Blockchain can reduce VAT fraud and VAT evasion. For example, a central bank digital currency (CBDC)[918] can eliminate VAT fraud and VAT evasion by streamlining the VAT collection process.[919] A CBDC is a government issued digital equivalent of fiat money.[920] A smart contract can be used to make automatic payments to tax authorities using programmable money.[921] Since a CBDC is issued by a government's central bank, a tax authority can trace the digital version of money throughout blockchain. In my view, suppliers and businesses can be obligated to transact only in government issued CBDC to prevent the risks associated with cash transactions. Once a supplier charges VAT on a transaction, a smart contract can automatically remit the CBDC to the tax authority in real-time. In my view, the use of a CBDC has the same effect as using a VATCoin/TVACoin.[922] It is also possible to prevent VAT fraud and VAT evasion by combining blockchain and DICE.[923]

Using blockchain for VAT collection can ensure that VAT is paid directly to the relevant tax authority using a smart contract.[924] The real time remission of VAT can improve the administration of VAT.[925] An effective administration can negate the possibility of cheating under a VAT system.[926]

https://repository.up.ac.za/bitstream/handle/2263/77923/DelaFeria_Addressing_2019.pdf?sequence=1. Accessed 29 December 2022; Keen, M. & Smith, S. (2007). "VAT fraud and evasion: what do we know, and what can be done?" IMF working paper WP/07/31 at 8. Available at https://www.imf.org/external/pubs/ft/wp/2007/wp0731.pdf. Accessed 29 December 2022.

[918] The issuing and regulation of CBDCs falls outside the scope of this study.

[919] Alexander, G. (2022). "Blocking the Gap: The Potential for Blockchain Technology to secure VAT Compliance" *EC Tax Review* 31(3): 153.

[920] Alexander, G. (2022). "Blocking the Gap: The Potential for Blockchain Technology to secure VAT Compliance" *EC Tax Review* 31(3): 153.

[921] Alexander, G. (2022). "Blocking the Gap: The Potential for Blockchain Technology to secure VAT Compliance" *EC Tax Review* 31(3): 153; see also Bank of England (2020). *Central bank digital currency: opportunities, challenges and design* Future of Money Discussion Paper at 18. Available at https://www.bankofengland.co.uk/-/media/boe/files/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design.pdf. Accessed 30 December 2022.

[922] See discussions at paragraphs 3.2.3 and 3.2.4 above.

[923] Merkx, M., & Verbaan, N. (2019). "Technology: A key to solve VAT Fraud?" *EC Tax Review* 28(6) at 303. See also discussion at paragraph 3.3.6 above.

[924] Merkx, M., & Verbaan, N. (2019). "Technology: A key to solve VAT Fraud?" *EC Tax Review* 28(6) at 303; WU Net Team. (2017). "Blockchain: Taxation and Regulatory Challenges and Opportunities" *WU Global Tax Policy Centre of Vienna University of Business and Economics* at 6 – 8; Merkx, M. (2019). "VAT and Blockchain: Challenges and Opportunities ahead" *EC Tax Review* 28(2): 84; PWC (2016). "How blockchain technology could improve the tax system" at 3. Available at https://www.pwc.co.uk/issues/futuretax/assets/documents/how-blockchain-could-improve-the-tax-system.pdf. Accessed 24 March 2021; Azam, R. & Mazur, O. (2019). "Cloudy with a chance of taxation" *Florida Tax Review* 22(2): 47.

[925] Azam, R. & Mazur, O. (2019). "Cloudy with a chance of taxation" *Florida Tax Review* 22(2): 47.

[926] Bird, R. M. & Gendron, P. P. (2007). *The VAT in developing and transitional countries* (Cambridge University Press, New York) at 178.

3.4.9 Eliminating the reverse-charge mechanism and raising revenue

The reverse-charge mechanism is a model used to collect VAT on the importation of goods and services. In terms of the destination principle,[927] imports are taxed in the destination country in a deferred payment or postponed accounting.[928] The taxpayers (consumers) self-assess. In other words, taxpayers must calculate and remit VAT to the tax authorities.[929] Taxpayers must complete their VAT returns and submit them with their payments to the tax authorities.[930]

It is trite that the reverse-charge mechanism is an ineffective mechanism for the collection of VAT on the cross-border trade in digital goods.[931] One of the fundamental issues plaguing the reverse-charge mechanism is the reliance on the recipient or consumer to collect and remit VAT to the relevant tax authority. Currently, South African consumers are obligated to collect and remit VAT to SARS whenever they receive imported services from a foreign supplier.[932] It is generally accepted that South African consumers are not aware of this statutory obligation. Furthermore, SARS does not have the resources to enforce the reverse-charge mechanism on consumers.[933] In my view, it is possible to eliminate the reverse-charge mechanism from VAT legislation if blockchain is adopted. This view is supported by Merkx.[934] Merkx questions the relevance of the application of the reverse-charge mechanism in international trade if VAT payments to tax authorities take place automatically.[935]

[927] The destination principle entails that tax is levied at all stages of production and must be fully credited in the country of consumption. See Ebrill, L. Keen, M. Bodin, J.P. Summers, V. (2001). *The Modern VAT* (International Monetary Fund, Washington DC) at 179.

[928] Ebrill, L. Keen, M. Bodin, J.P. Summers, V. (2001). *The Modern VAT* (International Monetary Fund, Washington DC) at 177; see also Van Zyl, S. P. (2013). *The collection of Value Added Tax on online cross-border trade in Digital Goods*. Unpublished LLD thesis (UNISA) at 57.

[929] Ebrill, L. Keen, M. Bodin, J.P. Summers, V. (2001). *The Modern VAT* (International Monetary Fund, Washington DC) at 138.

[930] Ebrill, L. Keen, M. Bodin, J.P. Summers, V. (2001). *The Modern VAT* (International Monetary Fund, Washington DC) at 138.

[931] See Paragraph 1.1 above.

[932] Section 14(a) & (b) of the VAT Act.

[933] See Kabwe, K., R. (2017). *Consumption tax collection models in online trade in digital goods* unpublished LLM mini-dissertation (UNISA) at 39 – 45.

[934] Merkx, M. (2019). “VAT and Blockchain: Challenges and Opportunities Ahead” *EC Tax Review* 28(2): 88.

[935] Merkx, M. (2019). “VAT and Blockchain: Challenges and Opportunities Ahead” *EC Tax Review* 28(2): 88.

Generally, the obligation to collect and remit VAT from the supply of imported services lies with the consumer.[936] However, the burden to collect and remit VAT can shift to a supplier (B2B transactions) if the supplier imports the services.[937] With blockchain, VAT can be remitted using a smart contract. The process is instantaneous and does not require the cooperation of the consumer.[938] Moreover, the administrative burden on SARS is minimised. The resources that SARS could have used to enforce the reverse-charge mechanism can be diverted elsewhere. VAT that could have been collected through the reverse-charge mechanism can be collected through blockchain. The additional VAT collected can raise surplus revenue for SARS.

3.4.10 Is there a need for the registration requirement?

In terms of the registration requirement, foreign suppliers are required to account for and remit VAT in the country of consumption. In South Africa, foreign suppliers must conduct an enterprise in South Africa.[939] Where the foreign supplier is a supplier of electronic services, there are other requirements that must be met. First, the recipient of the electronic services must reside in South Africa. Second, the payment to the supplier must originate from a bank registered in terms of the Bank's Act.[940] Third, the

[936] Section 14(a) & (b) of the VAT Act.

[937] Blockchain technology can be used on B2B transactions. Here, the business supplier identifies the business consumer beforehand. The business supplier uses blockchain to remit VAT to the tax authority. In this scenario, the business supplier knows the identity of the business supplier. Since the identity is known, the taxing jurisdiction is also known making it easier for the business supplier to remit VAT. However, a B2C still requires a foreign supplier to identify the consumer before remitting VAT to the appropriate jurisdiction. If businesses use a consortium blockchain run by a tax authority, it can make tax administration simpler because a tax authority can easily monitor and audit the transactions on the blockchain. Both supplier and consumer are known to all the participants on the blockchain. Other businesses can verify the transaction to determine if a particular business supplier is tax compliant. Hence, it is possible for B2B and B2C transactions to be treated differently on a blockchain in so far as VAT collection is concerned. Thus, it is important to treat B2B and B2C the same.

[938] It remains the responsibility of the supplier to identify the consumer and their jurisdiction. This can be done by making use of *place of supply* rules. Currently, the VAT Act prescribes a person's physical/residential address; residency and the location of the bank as *place of supply* rules for the importation of electronic services as defined. See section 1(b)(iv) of the definition of "enterprise" in the VAT Act.

[939] Section 1 of the VAT Act defines an 'enterprise' as: "in the case of any vendor, any enterprise or activity which is carried on continuously or regularly by any person in the Republic or partly in the Republic and in the course or furtherance of which goods or services are supplied to any other person for a consideration, whether or not for profit, including any enterprise or activity carried on in the form of a commercial, financial, industrial, mining, farming, fishing, municipal or professional concern or any other concern of a continuing nature or in the form of an association or club."

[940] Act 94 of 1990.

recipient of the electronic services must have a postal, residential, or business address in South Africa.[941] Thereafter, a foreign supplier of electronic services must register as VAT vendor when their taxable suppliers exceed R1 million in any consecutive twelve-month period.[942] Upon registration, a foreign supplier is required to account for and remit VAT to SARS. Despite the registration requirement's preference as a model for the collection of VAT on the cross-border supply of goods and services, it has shortcomings.

Some of those shortcomings include:

i) The opening of a bank account where applicable;

ii) Obtaining information about the local VAT registration process. This includes how to conduct VAT returns in a language that may not easily be understood;

iii) Understanding thresholds and how they work;

iv) Retaining documents in accordance with VAT legislation;

v) Understanding the VAT rates applicable in the consumption state and implement the necessary changes to cope with charging the relevant VAT rate;

vi) Understanding rules relating to invoicing;

vii) Monitoring changes in legislation and other administrative updates which require system changes;

viii) Grasping the applicable collection mechanisms.[943]

A supplier who is required to register as a VAT vendor in several jurisdictions must contend with these shortcomings. While established businesses may be willing to commit resources to comply with VAT laws and expand their international footprint, smaller businesses lack the funds, resources, and knowledge to do so. Established businesses are more likely to expand in jurisdictions that have the simplest tax compliance regime and where they are certain that their investment will yield returns.

[941] Section 1(b)(iv) of the definition of "enterprise" in the VAT Act.

[942] Section 23(1A) of the VAT Act.

[943] See OECD (2017). *Mechanisms for the effective collection of VAT/GST* at 19. https://www.oecd.org/tax/tax-policy/mechanisms-for-the-effective-collection-of-VAT-GST.pdf. Accessed 29 March 2019.

It should be noted that attempts are been made to simplify the registration mechanism. The simplification of the registration mechanism is necessary to lessen the compliance burden imposed on foreign suppliers, particularly where there are compliance burdens in multiple jurisdictions.[944] If the registration mechanism is too complex, foreign suppliers may be inclined to cease trading in jurisdictions that pose a heavy compliance burden. Additionally, a heavy compliance burden can generate an uneven playing field between local and foreign suppliers which can lead to market distortions.[945]

In my view, the registration requirement can be discarded if suppliers automatically remit VAT to the relevant tax authorities whenever supplies are made to a consumer. The adoption of blockchain for the collection of VAT can remove the registration thresholds currently imposed by VAT rules. With blockchain technology, it can be possible for small and established suppliers to use blockchain to collect and remit VAT to the tax authorities. All foreign suppliers can be treated the same irrespective of their stature. Furthermore, the risks associated with the registration mechanism can be removed altogether. However, it should be noted that the adoption of blockchain as a collection mechanism could lead to differentiation between foreign suppliers and local suppliers. The potential differentiation stems from the perception that foreign suppliers will be treated differently compared to local suppliers due to the latter's use of blockchain technology as a method for VAT collection. The differentiation can be removed if local and foreign suppliers use blockchain to remit VAT to tax authorities.

[944] OECD (2017). *Mechanisms for the effective collection of VAT/GST* at 20. https://www.oecd.org/tax/tax-policy/mechanisms-for-the-effective-collection-of-VAT-GST.pdf. Accessed 29 March 2019.

[945] OECD (2017). *Mechanisms for the effective collection of VAT/GST* at 20. https://www.oecd.org/tax/tax-policy/mechanisms-for-the-effective-collection-of-VAT-GST.pdf. Accessed 29 March 2019.

3.4.11 Improving e-commerce and trade

E-commerce is growing on the African continent. While developed countries like Switzerland, Netherlands, and Denmark[946] dominate the e-commerce landscape,[947] African countries like Ghana and Algeria have seen increased penetration in the e-commerce market.[948] However, e-commerce in Africa is largely dominated by Nigeria, South Africa, and Kenya.[949] Generally, e-commerce struggles to gain a foothold on the African continent due to a multitude of challenges. Some of these challenges can be attributed to people's scepticism towards online transactions, (low) Internet penetration,[950] high costs associated with Internet access, modest bank card

[946] These three countries provide very favourable income tax regimes for e-commerce companies ranging from tax incentives to tax holidays for skilled employees. As a result, these three countries attract e-commerce companies to set-up shop there. The hosting country benefits because highly skilled and high-income earners move to those countries contributing to the tax base in the process.

[947] This is according to the United Nations Conference on Trade and Development (UNCTAD) B2C E-commerce Index 2020. Available at https://unctad.org/system/files/official-document/tn_unctad_ict4d17_en.pdf. Accessed 21 April 2021.

[948] UNCTAD (2020). "The UNCTAD B2C E-commerce Index 2020: Spotlight on Latin America and the Caribbean" *UNCTAD Technical Notes on ICT for Development No 17* at 5. Available at https://unctad.org/system/files/official-document/tn_unctad_ict4d17_en.pdf. Accessed 21 April 2021.

[949] Masekesa, F. (2020). "Nigeria, South Africa and Kenya dominate the e-commerce industry in Sub-Saharan Africa." Available at https://www.theasianbanker.com/updates-and-articles/nigeria,-south-africa-and-kenya-dominate-the-e-commerce-industry-in-sub-saharan-africa. Accessed 21 April 2021.

[950] It should be noted that low Internet penetration was one of the reasons for the slow uptake of e-commerce. According to GSMA, 495 million people in Sub-Saharan Africa have access to mobile phones. This represents 46 per cent of the region's population. The same report states that at the end of 2020, 303 million people across Sub-Saharan Africa have access to mobile internet. As a result of the increase mobile penetration, Africa has become a major market for streaming service companies such as Netflix, Iroko, and Showmax. For example, Netflix and Showmax has recently launched mobile-only subscription plans to tap into the increasing uptake of smartphones. The market is saturated by young and tech savvy people who may not necessarily have access to large screen streaming devices or prefer lower subscription costs. See GSMA (2021). *The Mobile economy: Sub-Saharan Africa*. Available at https://www.gsma.com/mobileeconomy/wp-content/uploads/2021/09/GSMA_ME_SSA_2021_English_Web_Singles.pdf. Accessed 5 October 2022. Despite their presence in Sub-Saharan Africa, streaming services like Netflix are not available in all African countries because they are either too tax rigid or the uptake combined with strict tax laws make it difficult for the services to be rolled out. Affluent Africans have access to credit cards issued by foreign banks. These cards are used to subscribe to streaming services. It is then possible for the service to go untaxed or the service gets taxed in the incorrect jurisdiction. Currently, it is difficult to ascertain whether the use of blockchain can resolve this problem without identity management and access to the blockchain. Ordinarily, Netflix would remit VAT to the consumption state on the blockchain. However, if the taxpayer uses a virtual private network (VPN) or a foreign credit card or mask their location, Netflix cannot determine the consumption country. As a result, VAT goes uncollected. This problem can be resolved by implementing blockchain-based identity management systems. The identity management system can determine the identity of the consumer. An *oracle* can be programmed in the blockchain to accurately depict the real-time location of the consumer. This can be used

ownership, and limited online payment options.[951] It is also worrying to note that a significant portion of the African population remains unbanked.[952] Traditional credit card payments remain prevalent in developed countries, while this is not necessarily the case in African countries.[953] The lack of access to banking services has a negative impact on the growth of e-commerce on the African continent. Payment options such as *PayPal*, mobile money solutions and *M-Pesa*[954] are increasingly made available to African consumers. These payment options are provided by local e-commerce suppliers like *Jumia*.[955] Despite the popularity of *M-Pesa* and mobile money payments in certain African countries, major multinational e-commerce suppliers do not use such payment options at checkout. The availability of payment options significantly inhibits the growth of e-commerce on the African continent.[956] Having a small pool of e-

to determine the *place of supply*. As alluded to, it is necessary for the consumer to be a party on the blockchain. Without this requirement, it will be difficult to accurately depict the *place of supply*.

[951] Masekesa, F. (2020). "Nigeria, South Africa and Kenya dominate the e-commerce industry in Sub-Saharan Africa." Available at https://www.theasianbanker.com/updates-and-articles/nigeria,-south-africa-and-kenya-dominate-the-e-commerce-industry-in-sub-saharan-africa. Accessed 21 April 2021.

[952] Generally, a person who is unbanked is someone that does not own a bank account or a person who does not have access to a bank account and banking services. See Vigna, P., & Casey, M., J. (2016). *The Age of Cryptocurrency: How Bitcoin and the Blockchain are Challenging the Global Economic order* Picador USA at 8; Sharrock, R. (ed) *et al* (2016). *The Law of Banking and Payment in South Africa* Juta & Co at 3 – 4; Masekesa, F. (2020). "Nigeria, South Africa and Kenya dominate the e-commerce industry in Sub-Saharan Africa." Available at https://www.theasianbanker.com/updates-and-articles/nigeria,-south-africa-and-kenya-dominate-the-e-commerce-industry-in-sub-saharan-africa. Accessed 21 April 2021.

[953] See Masekesa, F. (2020). "Nigeria, South Africa and Kenya dominate the e-commerce industry in Sub-Saharan Africa." Available at https://www.theasianbanker.com/updates-and-articles/nigeria,-south-africa-and-kenya-dominate-the-e-commerce-industry-in-sub-saharan-africa. Accessed 21 April 2021. In South Africa, major e-commerce businesses such as *Takealot.com* and *BidorBuy* do offer credit cards as a payment option at checkout.

[954] M-Pesa is an African based mobile money service currently available in Kenya, Tanzania, Egypt, Ghana, Lesotho, Mozambique and the Democratic Republic of Congo (DRC). It enables people to make payments without needing a bank account. It also enables people to access financial services, purchase airtime, send and receive money, receive salaries, obtain short term loans and make bill payments. In order to make use of this service, consumers register at a local retailer and deposit cash in exchange for electronic money. Transactions are secured by means of a PIN number which is received by the sender and receiver once money is transferred. The recipient receives electronic money in real-time and redeems it for cash at an outlet. Once a person receives electronic money, they are notified by means of a short message service (SMS). See https://www.vodafone.com/what-we-do/services/m-pesa. Accessed 21 April 2021.

[955] See Masekesa, F. (2020). "Nigeria, South Africa and Kenya dominate the e-commerce industry in Sub-Saharan Africa." Available at https://www.theasianbanker.com/updates-and-articles/nigeria,-south-africa-and-kenya-dominate-the-e-commerce-industry-in-sub-saharan-africa. Accessed 21 April 2021.

[956] See Masekesa, F. (2020). "Nigeria, South Africa and Kenya dominate the e-commerce industry in Sub-Saharan Africa." Available at https://www.theasianbanker.com/updates-and-articles/nigeria,-south-africa-and-kenya-dominate-the-e-commerce-industry-in-sub-saharan-africa. Accessed 21 April 2021.

commerce suppliers to collect tax from impacts negatively on a tax authority's ability to raise revenue.

The adoption of blockchain in e-commerce has the potential to improve trade and e-commerce. Blockchain can facilitate the use of bitcoin (cryptocurrency) as a payment method in exchange for goods and services.[957] This is subject to suppliers accepting bitcoin or other cryptocurrencies as a payment method.[958] If suppliers do accept cryptocurrencies as a form of payment, cryptocurrency borne transactions can be treated as taxable supplies. The supplier will then account for VAT and use a smart contract to remit VAT instantaneously to the relevant tax authority.[959] In doing so, suppliers' transaction and compliance costs are reduced providing an incentive for suppliers to trade in developing countries where the cost of trading is low. A boost in trade and e-commerce transactions can also boost revenue. Second, the introduction of cryptocurrencies as a payment method can enable unbanked people to access the digital economy. Generally, before a person can open a bank account, he or she must be in possession of positive identification.[960] However, access to identification documents is not always possible for individuals residing in remote areas on the African continent. Obtaining identification requires a person to travel to a government office situated in a town or city far from a person's natural abode. Travelling to a town or city requires one to spend money he or she may not necessarily have.

The requirement to have positive identification to access the financial sector and other financial services is legislated in South Africa. For example, the Financial Intelligence Centre Act 38 of 2001 (the FICA Act) compels financial institutions to establish and verify the identity of a client before doing business or before conducting a transaction

[957] Schwab, J. & Ohnesorge, J. (2019). "Potential Blockchain Technology for Trade Integration of Developing Countries" *German Development Institute Briefing Paper 4/2019* at 3. Available at https://www.die-gdi.de/en/briefing-paper/article/potential-of-blockchain-technology-for-trade-integration-of-developing-countries/. Accessed 21 April 2021.

[958] Schwab, J. & Ohnesorge, J. (2019). "Potential Blockchain Technology for Trade Integration of Developing Countries" *German Development Institute Briefing Paper 4/2019* at 3. Available at https://www.die-gdi.de/en/briefing-paper/article/potential-of-blockchain-technology-for-trade-integration-of-developing-countries/. Accessed 21 April 2021.

[959] Kabwe, R. (2020). "The VAT Treatment of Cryptocurrencies in South Africa: Lessons from Australia" *Obiter* 41(4): 783.

[960] See Vigna, P., & Casey, M., J. (2016). *The Age of Cryptocurrency: How Bitcoin and the Blockchain are Challenging the Global Economic order* Picador USA at 190.

with such a person.[961] Additionally, if a person acts on behalf of someone else, the financial institution must establish the identity of the third party as well as the person's authority to act on behalf of the third party.[962] Often these laws, while justifiable,[963] can restrict persons to only conduct transactions in cash.[964] The exclusion from the e-commerce environment is also compounded by the fact that financial institutions do not open branches in remote areas where infrastructure and security is lacking.[965] To address the financial exclusion, the use of cryptocurrencies is key. In South Africa, about 24 per cent of the population is currently unbanked.[966] Currently, 90 per cent of South Africa's population has access to mobile phones.[967] These figures suggest that more people in South Africa have access to mobile phones than bank accounts. While conventional e-commerce transactions require the use of a PC and a stable Internet connection, more consumers use mobile devices to conduct e-commerce transactions. In my view, enabling consumers to use cryptocurrencies as a payment method when performing e-commerce transactions can significantly increase trade.[968] To simplify matters further, consumers can use blockchain enabled mobile phones to perform e-commerce transactions.[969] Blockchain's features can create trust between a consumer and supplier. If more people trust the suppliers, there is a chance that they are more likely to trade with them. More people can possess devices that facilitate trade without the necessary hassles of obtaining a bank account. An increase in these transactions can translate to additional VAT collection and remittance in real-time, increasing the revenue pool in the process.

[961] Section 21(1)(a) of the FICA Act.

[962] Section 21(1)(b)(i) and (ii) of the FICA Act.

[963] This is mostly done to detect and prevent fraud and money laundering.

[964] Vigna, P., & Casey, M., J. (2016). *The Age of Cryptocurrency: How Bitcoin and the Blockchain are Challenging the Global Economic order* Picador USA at 190.

[965] Vigna, P., & Casey, M., J. (2016). *The Age of Cryptocurrency: How Bitcoin and the Blockchain are Challenging the Global Economic order* Picador USA at 190.

[966] This figure is provided by the Oxford Business Group. Available at https://oxfordbusinessgroup.com/analysis/final-20-reaching-unbanked-population-complex-task. Accessed 22 April 2021.

[967] Mzekandaba, S. (2020). "SA's smartphone penetration surpasses 90%". Available at https://www.itweb.co.za/content/xA9PO7NZRad7o4J8. Accessed 22 April 2021.

[968] Kenya uses a bitcoin-based mobile device called BitPesa. BitPesa was introduced by Elizabeth Rosiello in 2013 as a digital foreign exchange platform. It was designed with blockchain technology in order to facilitate payments and remittance across countries such Ghana, Kenya and Nigeria. See Vigna, P., & Casey, M., J. (2016). *The Age of Cryptocurrency: How Bitcoin and the Blockchain are Challenging the Global Economic order* Picador USA at 213 – 218.

[969] HTC manufactured a blockchain enabled smartphone called *Exodus 1*. The *Exodus 1* has a pre-installed bitcoin app. See https://innovationatwork.ieee.org/blockchain-smartphones-going-mobile/. Accessed 22 April 2021. Another blockchain enabled smartphone, Finney, is currently on the market. It is developed by Sirin Labs.

It is worth pointing out that the success of blockchain adoption is, to a certain extent, dependent on the uptake/trust in the technology in Africa. For the most part, people associate blockchain with bitcoins and other forms of cryptocurrencies. Any negative connotation around bitcoins and other cryptocurrencies can transcend to blockchain technology, creating negative misconceptions in the process. It is important to educate the public about the differences between cryptocurrencies and blockchain technology. A better understanding of blockchain technology can greatly reduce public misconceptions. Having said that, it remains to be seen if Africans will trust blockchain technology in the future.

3.4.12 Enhanced international administrative cooperation

On a global scale, blockchain can facilitate the exchange of information (EOI) between different countries.[970] Currently, SARS is obligated to obtain and transmit information (taxpayer information) to a tax authority situated in another jurisdiction upon request by the latter.[971] This is a clear indication that SARS can exchange taxpayer information with other jurisdictions. At SARS' request, a tax authority in a foreign jurisdiction can also transmit tax related information to SARS.[972] Generally, EOI is governed by a Double Tax Agreement (DTA) or multinational agreements.[973] South Africa is also a

[970] Kim, R., C. (2021). "Blockchain Initiatives for Tax Administration" *University of Utah College of Law Research Paper No 427* at 52. Available at https://ssrn.com/abstract=3798136. Accessed 26 June 2021; Bossa, G. & de Paiva Gomes, E. (2019). "Blockchain: Technology as a Tool for Tax information Exchange or an instrument Threatening the Taxpayer's Privacy?" at 2. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3540277. Accessed 19 July 2019.

[971] Section 3(3)(a) of the Tax Administration Act.

[972] SARS (2021). "Automatic Exchange of Information". Available at https://www.sars.gov.za/businesses-and-employers/third-party-data-submission-platform/automatic-exchange-of-information/. Accessed 26 June 2021.

[973] See section 3(3) of the Tax Administration Act; see also SARS (2021). "Automatic Exchange of Information". Available at https://www.sars.gov.za/businesses-and-employers/third-party-data-submission-platform/automatic-exchange-of-information/. Accessed 26 June 2021.

member of the Multilateral Convention on Mutual Administrative Assistance in Tax Matters,[974] having signed the amended convention in 2011.[975]

To facilitate EOI or Automatic Exchange in Information (AOEI), countries rely on IT systems and good infrastructure.[976] However, the current methods of exchanging information are characterised by intermittent transmissions,[977] the lack of administrative capacity, and inadequate computing and technological advancements.[978] In other instances, the transmission of information is depicted by lengthy and cumbersome processes.[979]

Currently, the EOI and AOEI is overly reliant on financial institutions.[980] Financial institutions are obligated to collect and report a person's tax reference number, their bank account, account balance, name and address, date of birth and country of

[974] According to the OECD, the Mutual Convention on Administrative Assistance in Tax Matters "was developed jointly by the OECD and the Council of Europe in 1988 and amended by Protocol in 2010. The Convention is the most comprehensive multilateral instrument available for all forms of tax co-operation to tackle tax evasion and avoidance. The Convention facilitates international co-operation for a better operation of national tax laws, while respecting the fundamental rights of taxpayers. It provides for all possible forms of administrative co-operation between governments in the assessment and collection of taxes. This co-operation ranges from exchange of information, including automatic exchanges, to the recovery of foreign tax claims." Currently, the convention has 141 signatories. See https://www.oecd.org/tax/exchange-of-tax-information/convention-on-mutual-administrative-assistance-in-tax-matters.htm. Accessed 19 July 2021.

[975] See OECD (2021). "Jurisdictions Participating in The Convention on Mutual Administrative Assistance In Tax Matters Status – 15 July 2021." Available at https://www.oecd.org/tax/exchange-of-tax-information/Status_of_convention.pdf. Accessed 19 July 2021.

[976] Duperrut, J., Thevoz, P., Ilves, L., Migai, C. & Owens, J. (2019). "Why – and How – African Countries Should Use Technology for Automatic Information Exchange" *Tax Notes International* 96(2): 924.

[977] Kim, R., C. (2021). "Blockchain Initiatives for Tax Administration" *University of Utah College of Law Research Paper No 427* at 53. Available at https://ssrn.com/abstract=3798136. Accessed 26 June 2021.

[978] Duperrut, J., Thevoz, P., Ilves, L., Migai, C. & Owens, J. (2019). "Why – and How – African Countries Should Use Technology for Automatic Information Exchange" *Tax Notes International* 96(2): 921.

[979] See SARS (2021). "Automatic Exchange of Information". Available at https://www.sars.gov.za/businesses-and-employers/third-party-data-submission-platform/automatic-exchange-of-information/. Accessed 26 June 2021; Duperrut, J., Thevoz, P., Ilves, L., Migai, C. & Owens, J. (2019). "Why – and How – African Countries Should Use Technology for Automatic Information Exchange" *Tax Notes International* 96(2): 922.

[980] Duperrut, J., Thevoz, P., Ilves, L., Migai, C. & Owens, J. (2019). "Why – and How – African Countries Should Use Technology for Automatic Information Exchange" *Tax Notes International* 96(2): 920 – 924; SARS (2021). "Automatic Exchange of Information". Available at https://www.sars.gov.za/businesses-and-employers/third-party-data-submission-platform/automatic-exchange-of-information/. Accessed 26 June 2021.

residence.[981] Once collected, the financial institution processes this data. Thereafter, the data is sent to the financial institution's domestic tax authority. That tax authority processes the same data before making it available to other tax authorities in the jurisdiction where the taxpayer resides.[982] If the coordination between the tax authority and the financial institution is lacking or if the means of coordination lacks a sophisticated integrated system, it can be said that neither the financial institution nor the country can conduct AOEI effectively.[983] The reliance on financial institutions also implies that AOEI is dependent on a central authority.[984]

To make AOEI more seamless and secure,[985] blockchain can be adopted.[986] Blockchain has the capability of enhancing the storage of taxpayer information. Traditional methods of storing taxpayer information are outdated and less secure. Taxpayer information stored on a blockchain can be cryptographically secured and shared with pre-selected jurisdictions. Additionally, tax data can be transmitted seamlessly over blockchain network. Kim argues that a consortium blockchain can be used to exchange the data with specified countries.[987] In a consortium blockchain, a

[981] SARS (2021). "Automatic Exchange of Information". Available at https://www.sars.gov.za/businesses-and-employers/third-party-data-submission-platform/automatic-exchange-of-information/. Accessed 26 June 2021.

[982] Duperrut, J., Thevoz, P., Ilves, L., Migai, C. & Owens, J. (2019). "Why – and How – African Countries Should Use Technology for Automatic Information Exchange" *Tax Notes International* 96(2): 921.

[983] Duperrut, J., Thevoz, P., Ilves, L., Migai, C. & Owens, J. (2019). "Why – and How – African Countries Should Use Technology for Automatic Information Exchange" *Tax Notes International* 96(2): 921.

[984] Kim, R., C. (2021). "Blockchain Initiatives for Tax Administration" *University of Utah College of Law Research Paper No 427* at 54. Available at https://ssrn.com/abstract=3798136. Accessed 26 June 2021.

[985] Duperrut, J., Thevoz, P., Ilves, L., Migai, C. & Owens, J. (2019). "Why – and How – African Countries Should Use Technology for Automatic Information Exchange" *Tax Notes International* 96(2): 922.

[986] On 6 July 2021 SARS announced a joint venture with the Internal Revenue Service (IRS) to combat tax evasion and economic crimes. See SARS (2021). "IRS Criminal Investigation and SARS join forces to fight international crimes." Available at https://www.sars.gov.za/media-release/irs-criminal-investigation-and-sars-join-forces-to-fight-international-crimes/. Accessed 7 July 2021. While the move is welcomed, it must be noted that any successful intervention between the two nations can only be successful if information is shared. In my view, this is an opportune moment for blockchain to be used. With blockchain, SARS and the IRS can coordinate the exchange of information by making use of blockchain technology. All transactions and access can be facilitated with a smart contract. All taxpayer information can be secured through cryptography. Taxpayer information need not be stored in plain text. Anonymisation techniques can be used to protect the privacy of taxpayer information.

[987] Kim, R., C. (2021). "Blockchain Initiatives for Tax Administration" *University of Utah College of Law Research Paper No 427* at 54. Available at https://ssrn.com/abstract=3798136. Accessed 26 June 2021.

central administrator can manage, collect, and disseminate data to the relevant parties.[988] A smart contract can be used to automatically share the data with the relevant parties on blockchain network. Pre-selected countries access the data once the smart contract executes the instruction to exchange taxpayer data.[989] Moreover, blockchain's transparent nature has the potential to mitigate tax evasion and tax avoidance.[990] As pointed out by Owens and De Jong, blockchain can enhance country by country reporting real-time reporting which, in turn, can significantly reduce tax evasion and tax avoidance.[991] Blockchain has the potential to make international cooperation more effective.[992] This is because taxpayer information can easily be cross-checked, meaning that the appropriate jurisdictions could determine if it has the right to collect the tax.[993] As a result of blockchain's proficiency in cross-checking and synchronizing taxpayer information, Bossa and de Paiva Gomes correctly submit that blockchain can be an appropriate tool to give effect to international tax treaties.[994] This is in line with the current provisions of the Tax Administration Act.[995] In terms of the Tax Administration Act, SARS may disclose and transmit information to another competent tax authority if requested to do so.[996] SARS can retain information of a person and must treat the information as taxpayer information.[997] Blockchain can perform a dual purpose, promote tax transparency and modernising cooperation amongst countries.

[988] Kim, R., C. (2021). "Blockchain Initiatives for Tax Administration" *University of Utah College of Law Research Paper No 427* at 53. Available at https://ssrn.com/abstract=3798136. Accessed 26 June 2021.

[989] Kim, R., C. (2021). "Blockchain Initiatives for Tax Administration" *University of Utah College of Law Research Paper No 427* at 54. Available at https://ssrn.com/abstract=3798136. Accessed 26 June 2021.

[990] Owens, J. & De Jong, J. (2017). "Taxation on the Blockchain: Opportunities and Challenges" *Tax Notes International* 87(6): 607.

[991] Owens, J. & De Jong, J. (2017). "Taxation on the Blockchain: Opportunities and Challenges" *Tax Notes International* 87(6): 607.

[992] Bossa, G. & de Paiva Gomes, E. (2019). "Blockchain: Technology as a Tool for Tax information Exchange or an instrument Threatening the Taxpayer's Privacy?" at 14. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3540277. Accessed 19 July 2019.

[993] Bossa, G. & de Paiva Gomes, E. (2019). "Blockchain: Technology as a Tool for Tax information Exchange or an instrument Threatening the Taxpayer's Privacy?" at 14. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3540277. Accessed 19 July 2019.

[994] Bossa, G. & de Paiva Gomes, E. (2019). "Blockchain: Technology as a Tool for Tax information Exchange or an instrument Threatening the Taxpayer's Privacy?" at 15. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3540277. Accessed 19 July 2019.

[995] Act 28 of 2011.

[996] Section 3(3)(a)(i) of the TAA.

[997] Section 3(3)(b) of the TAA.

From a VAT perspective, the storage and transmission of a digital invoice on a blockchain by a foreign supplier triggers an exchange of taxpayer information.[998] Azam and Mazur argue that a digital invoice can facilitate the exchange of information between tax authorities.[999] In doing so, the administration of VAT and VAT compliance is enhanced enabling tax authorities to collect more data. The data collected can further assist tax authorities in combating VAT fraud while improving revenue collection in the process.[1000]

3.4.13 Building trust between tax authorities and taxpayers

EOI was introduced to combat tax evasion.[1001] The frequent coordination and cooperation between different tax authorities often highlights the lack of trust between taxpayers and tax authorities. It is generally accepted that tax authorities do not trust taxpayers and taxpayers do not trust tax authorities.[1002] The adoption of blockchain can help create trust between taxpayers and tax authorities.[1003] Blockchain's immutable feature can assist tax authorities in performing audits on tax related transactions. The authorities and taxpayers can trust the integrity of information stored on blockchain.[1004] A smart contract can be programmed to establish each taxpayer's

[998] Azam, R. & Mazur, O. (2019). "Cloudy with a chance of taxation" *Florida Tax Review* 22(2): 555.

[999] Azam, R. & Mazur, O. (2019). "Cloudy with a chance of taxation" *Florida Tax Review* 22(2): 555.

[1000] Azam, R. & Mazur, O. (2019). "Cloudy with a chance of taxation" *Florida Tax Review* 22(2): 555.

[1001] Kim, R., C. (2021). "Blockchain Initiatives for Tax Administration" *University of Utah College of Law Research Paper No 427* at 52 – 53. Available at https://ssrn.com/abstract=3798136. Accessed 26 June 2021.

[1002] Sim, S., Owens, J., Petruzzi, R., Tavares, R., J., S., & Migai, C. (2017). "Blockchain, Transfer Pricing, Customs Valuations, and Indirect Taxes: Transforming the Global Tax Environment" *Tax and Accounting Center* at 2. Available at https://www.wu.ac.at/fileadmin/wu/d/i/taxlaw/institute/WU_Global_Tax_Policy_Center/Tax_Technology/BNA_WU_Blockchain_article_June17_final_online_version.pdf. Accessed 1 July 2021.

[1003] Mazur, O. (2021). "Can Blockchain Revolutionize Tax Administration?" SMU Dedman School of Law Legal Studies Research Paper No. 510 at 18 – 19. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3841785. Accessed 23 June 2021.

[1004] Mazur, O. (2021). "Can Blockchain Revolutionize Tax Administration?" SMU Dedman School of Law Legal Studies Research Paper No. 510 at 19. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3841785. Accessed 23 June 2021.

tax liability and remit the necessary amount of tax in real time to the relevant tax authority.[1005]

The need for trust is also significant in the context of EOI where tax authorities across multiple jurisdictions share information but may not necessarily trust each other.[1006] In this context, the lack of trust can be attributed to the absence of a trusted central administrator capable of verifying the authenticity of the information that is exchanged between tax authorities.[1007] To build trust in this environment, a trusted central authority in a consortium blockchain verifies the taxpayer information before relaying that information in real-time to the authorised tax authorities on blockchain.[1008]

3.4.14 Reducing VAT avoidance

It is important to consider whether blockchain can reduce VAT avoidance. Tax avoidance occurs when a taxpayer postpones, reduces, or eliminates their tax liability.[1009] As I have mentioned,[1010] VAT is not payable on imported services where the value of a supply does not exceed R100 per invoice. It is possible for a supplier of electronic services to separate a supply in order to reduce their VAT liability. I make use of an example:

[1005] See Mazur, O. (2021). "Can Blockchain Revolutionize Tax Administration?" SMU Dedman School of Law Legal Studies Research Paper No. 510 at 19. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3841785. Accessed 23 June 2021.

[1006] Kim, R., C. (2021). "Blockchain Initiatives for Tax Administration" *University of Utah College of Law Research Paper No 427* at 5 – 6. Available at https://ssrn.com/abstract=3798136. Accessed 26 June 2021.

[1007] Kim, R., C. (2021). "Blockchain Initiatives for Tax Administration" *University of Utah College of Law Research Paper No 427* at 5 – 6. Available at https://ssrn.com/abstract=3798136. Accessed 26 June 2021.

[1008] See Kim, R., C. (2021). "Blockchain Initiatives for Tax Administration" *University of Utah College of Law Research Paper No 427* at 6. Available at https://ssrn.com/abstract=3798136. Accessed 26 June 2021.

[1009] Croome, B. (ed) *et al* (2013). *Tax Law: an introduction* (Juta & Company (Pty) Ltd, Cape Town) at 22.

[1010] Paragraph 3.3.4 above.

Example 4

Y, an online supplier of digital goods, receives an order from a customer for the purchase of six e-books for a total price of R600. Y issues six separate invoices of R100 and ships six e-books to the customer.

In the example above, it is clear that Y avoids VAT liability by splitting the supply into six separate invoices. This strategy decreases revenue collection for the *fiscus*. In my view, this VAT avoidance scheme can be reduced by using DICE on blockchain.[1011] Using the example above, Y sends the original invoice to the tax authority in the destination country (SARS). SARS authenticates the invoice and saves a copy. The invoice contains information relating to the supply. SARS can contact the consumer to ascertain if the order on the supply is correct. If the order is incorrect, SARS re-sends the invoice to Y for rectification. Once rectified, Y re-sends the invoice to SARS for authentication. If the particulars of the order are correct, SARS signs the invoice with the public key and sends it to Y. Y sends a copy of the signed invoice to the consumer. The consumer ensures that the contents of the invoice are correct. At this point, the consumer can also determine whether Y correctly captured information pertaining to the supply. The consumer signs the invoice and sends it to SARS. SARS re-verifies and stores a copy. SARS signs the invoice and sends it to Y. Y remits VAT to SARS using a smart contract. The tax payment is instantaneous, and all transactions are recorded on blockchain. It is difficult for Y to commit VAT avoidance.

3.4.15 Blockchain and proxy issues

It is important to consider whether blockchain can resolve the issues associated with the use of proxies by foreign suppliers of electronic services.[1012] In the main, blockchain is a type of distributed ledger that records transactions. There are features of blockchain that can aid foreign suppliers to ascertain the location of a consumer. An *oracle*[1013] can be used to determine the place of consumption of the digital goods. The

[1011] See paragraph 3.3.6 above.
[1012] See paragraph 3.2 above.
[1013] See discussion at paragraph 2.8 above.

reason for this is that an *oracle* can verify the authenticity and validity of data.[1014] With an oracle, a foreign supplier can deduce whether the information such as the address and bank details are accurate. If a software oracle is used, it enables the data to be verified from online databases to ensure authenticity. Alternatively, a human *oracle* (preferably a tax official) can verify the data after it has been presented to them by the foreign supplier. Using an *oracle* can ensure that foreign suppliers comply with the provisions of the VAT Act with minimal effort. It should be noted that the degree of compliance is closely linked to the data retrieved by the *oracle*. If the information supplied by an *oracle* is inadequate or incorrect, then compliance will also be low or inadequate because the data cannot be verified. In turn, a foreign supplier cannot determine the identity of the consumer nor the place of consumption.

3.5 Challenges and risks associated with the adoption of blockchain for the collection of VAT

3.5.1 Costs of implementing blockchain

Before adopting blockchain, a tax authority must perform a cost analysis.[1015] In order for a tax authority to make an informed decision regarding the adoption of a particular technology for the administration of tax, it must factor i) the current costs of tax administration, ii) the costs associated with administering a particular tax, and iii) the anticipated costs of investing in a new form of tax administration.[1016] From a tax authority perspective, funds and resources must be allocated to train and hire skilled personnel that will aid blockchain based tax administration. The initial costs of

[1014] Mammadzada, K. *et al* (2020). “Blockchain Oracles: A framework for blockchain-based applications” at 3. Available at https://www.researchgate.net/publication/344079826_Blockchain_Oracles_A_Framework_for_Blockchain-Based_Applications/link/5f53cef992851c250b967e95/download?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19. Accessed 16 June 2024; see also Post, D. & Cipollini, C. (2022). “Fundamental elements of a blockchain-based tax system – when to use blockchain for tax?” *World Tax Journal* 14(4): 532.

[1015] Mazur, O. (2021). “Can Blockchain Revolutionize Tax Administration?” SMU Dedman School of Law Legal Studies Research Paper No. 510 at 40. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3841785. Accessed 23 June 2021; Azam, R. & Mazur, O. (2019). “Cloudy with a chance of taxation” *Florida Tax Review* 22(2): 563.

[1016] Bird, M., R., and Zolt M., E. (2008). “Technology and taxation in developing countries: from hand to mouse” *National Tax Journal* 61(4) Part 2 at 797.

blockchain adoption can include the hiring of i) academics, ii) legal consultants, iii) programmers, iv) software developers, v) quality assurers, and vi) designers.[1017] Generally, the costs of adopting blockchain is determined by various factors. For example, it is important to consider the type of blockchain used, and the features of blockchain app.[1018] Other considerations include i) maintenance costs,[1019] ii) costs relating to upgrades, iii) infrastructure, iv) storage space, v) network speed, vi) encryption, vii) costs relating to smart contracts, and viii) costs of integrating blockchain with the existing system.[1020] It must be noted that the abovementioned list of possible costs incurred is not exhaustive. This is because blockchain technology is a technology that is still developing, and it may take several years before the technology reaches its full potential. As a result, new technical developments on blockchain technology may arise in the future. The possibility of new developments points to the likelihood of additional future expenses which may not have been considered when doing the initial costs analysis.

According to some private corporations, it can cost anywhere between $500 000 to ten million dollars to **develop** a blockchain.[1021] That is equivalent to anything between R8 500 000 to R170 000 000.[1022] These costs do not include maintenance, testing, and other related expenses. It should be noted that the total costs of blockchain implementation can vary from country to country. It will be interesting to see whether SARS has the budget and resources to adopt blockchain for the administration of VAT.

[1017] See Takyar, A. "How to determine the cost of blockchain implementation?". Available at https://www.leewayhertz.com/cost-of-blockchain-implementation/ . Accessed 16 April 2021.

[1018] Takyar, A. "How to determine the cost of blockchain implementation?". Available at https://www.leewayhertz.com/cost-of-blockchain-implementation/ . Accessed 16 April 2021.

[1019] As with all technological innovations, blockchain requires updates. Software updates are necessary for the upkeep of the blockchain system. Software updates can also enhance the security system of the blockchain.

[1020] Andhov, A. (2020). "Corporations on blockchain: Opportunities & challenges" *Cornell International Law Journal* 53(1): 15; Takyar, A. "How to determine the cost of blockchain implementation?". Available at https://www.leewayhertz.com/cost-of-blockchain-implementation/ . Accessed 16 April 2021; Mazur, O. (2021). "Can Blockchain Revolutionize Tax Administration?" SMU Dedman School of Law Legal Studies Research Paper No. 510 at 40. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3841785. Accessed 23 June 2021.

[1021] Andhov, A. (2020). "Corporations on blockchain: Opportunities & challenges" *Cornell International Law Journal* 53(1): 15.

[1022] This is based on the conversation rate between the US dollar and the South African Rand on 24 December 2022 at 08:50 Central African Time (CAT). At that time, $1 = R17.01.

It is also worth considering the costs of blockchain implementation on taxpayers.[1023] In my view, SARS must bear the costs, whether initial or subsequent, for using blockchain to administer VAT. This view is supported by Muller.[1024] Muller correctly states that tax authorities must make investments and bear the costs of running blockchain system.[1025] This is in line with the principle of VAT neutrality. Put simply, foreign suppliers should not bear the burden of VAT administration.[1026] While it is extremely difficult to ascertain the actual total costs of blockchain adoption, it is my view that suppliers must not incur costs associated with blockchain technology. Blockchain operates on a decentralised network of computers. It is sufficient for a supplier to merely possess a node with the specific PC requirements and a reliable Internet connection to join the network. It may also be necessary for the supplier to obtain the necessary network configuration to access blockchain network in the taxing jurisdiction. Once inside the network, the supplier can merely remit the VAT by making use of a smart contract or VATCoins/TVACoins.

3.5.2 Human resources

For blockchain to be adopted efficiently for the administration of VAT, human resources will be required. Before blockchain is functional, it is imperative that tax officials understand blockchain and its various components at a basic level.[1027] With time, blockchain's operation must be understood at an advanced level. Failure to understand blockchain technology and its systems could lead to delays in adoption and fundamental errors can arise in its application.[1028] Owens and De Jong argue that

[1023] Azam, R. & Mazur, O. (2019). "Cloudy with a chance of taxation" *Florida Tax Review* 22(2): 563.

[1024] See Muller, R. (2020). "Proposal for an Automated Real-Time VAT Collection Mechanism in B2C E-Commerce Using Blockchain Technology" *International VAT Monitor* 31(3): 138.

[1025] Muller, R. (2020). "Proposal for an Automated Real-Time VAT Collection Mechanism in B2C E-Commerce Using Blockchain Technology" *International VAT Monitor* 31(3): 138.

[1026] See See OECD (2017). *Mechanisms for the effective collection of VAT/GST* at 11. https://www.oecd.org/tax/tax-policy/mechanisms-for-the-effective-collection-of-VAT-GST.pdf. Accessed 29 March 2019.

[1027] Setyowati, M., S. *et al* (2020). "Blockchain Technology Application for Value-Added Tax Systems" *Journal of Open Innovation: Technology, Market and Complexity* 6(156): 19; Mazur, O. (2021). "Can Blockchain Revolutionize Tax Administration?" SMU Dedman School of Law Legal Studies Research Paper No. 510 at 39. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3841785. Accessed 23 June 2021; Owens, J. & De Jong, J. (2017). "Taxation on the Blockchain: Opportunities and Challenges" *Tax Notes International* 87(6): 601.

[1028] See Setyowati, M., S. *et al* (2020). "Blockchain Technology Application for Value-Added Tax Systems" *Journal of Open Innovation: Technology, Market and Complexity* 6(156): 19; Deloitte generally, tax officials are not trained in the fields of coding/programming, IT, and cryptography. The effect is that these functions may be outsourced to private parties who have the required technical expertise to design platforms such as smart contracts.[1029] I do not agree entirely with this statement. In my view, the issue is not whether tax officials are trained but rather, whether there is enough capacity and resources to train tax officials. While it is factual that tax authorities may not necessarily be trained in coding and programming, it does not necessarily follow that tax authorities cannot be trained in these specialised fields. In my view, it is not economically viable to outsource coding and programming to third parties merely due to a lack of training/knowledge. Instead, it is more beneficial for third parties to train tax officials in specialised fields. Once trained, tax officials can possess the technical expertise to fix programming errors that can arise or re-write source code if necessary.[1030] Alternatively, it is also more economical and beneficial to hire experts that possess the necessary expertise as tax officials on a permanent basis. But Prewet *et al* correctly point out that it can be difficult to retain highly skilled and knowledgeable employees in the field of blockchain technology because such personnel are likely to be in high demand and may call for significant reimbursement.[1031] Retaining trained tax officials is beneficial in the long run because such officials can be subjected to non-disclosure agreements, precluding them from disclosing any confidential taxpayer information.[1032] Due to the sensitive nature of taxpayer information, it does not make sense for tax officials to expose taxpayer information or even create an environment where taxpayer information can be accessed by unauthorised third parties.

(2016). "Blockchain Enigma. Paradox. Opportunity" at 10. Available at https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-blockchain-full-report.pdf. Accessed 13 June 2021; see also Mazur, O. (2021). "Can Blockchain Revolutionize Tax Administration?" SMU Dedman School of Law Legal Studies Research Paper No. 510 at 39. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3841785. Accessed 23 June 2021.

[1029] Owens, J. & De Jong, J. (2017). "Taxation on the Blockchain: Opportunities and Challenges" *Tax Notes International* 87(6): 607.

[1030] Owens and De Jong argue that if private parties program code for use in tax administration, tax officials will be unable to comprehend and verify the code for any accuracy and completeness. Contextually, this could result in the inefficient and inaccurate implementation and application of blockchain for tax purposes. See Owens, J. & De Jong, J. (2017). "Taxation on the Blockchain: Opportunities and Challenges" *Tax Notes International* 87(6): 607.

[1031] Prewet K., W, Prescott G., L, Phillips K. (2020) "Blockchain adoption is inevitable— Barriers and risks remain" *Journal of Corporate Accounting & Finance* 31: 24. Available at https://doi.org/10.1002/jcaf.22415. Accessed 5 May 2021.

[1032] Section 69(1) of the Tax Administration Act compels a current or former SARS official to preserve the secrecy of taxpayer information and precludes such a person from disclosing taxpayer information to a person who is not a SARS official.

3.5.3 IT systems and infrastructure

In addition to the training and hiring of skilled personnel, the adoption of blockchain for tax administration requires a significant overhaul in IT systems and infrastructure. Blockchain is a complex system that runs on a sophisticated and decentralised network. As a result, it is necessary for tax authorities to develop a secure network infrastructure that can accommodate blockchain system.[1033] It is possible that the deployment of a complex system like blockchain technology can cause resistance and challenges to the existing tax administration model.[1034] In my view, this challenge can be heightened by factors such as the lack of blockchain regulation, public perceptions, misinformation about blockchain, and hesitancy by tax administrators. This can be resolved by, for example, training and educating tax officials about the application and deployment of blockchain.

There is a risk that the adoption and integration of blockchain technology in tax administration can cause complications and challenges to the existing IT systems.[1035] If blockchain is integrated too hastily without the necessary assessments and checks, it is possible that the technology can become inadequate at organisational level.[1036] As correctly pointed out by Prewet *et al* the integration of blockchain technology into existing IT systems can be cumbersome and expensive. Additionally, there are currently no applicable standards for the integration of blockchain interfaces with modern IT systems.[1037] It is likely that current IT systems will have to be overhauled altogether to make it compatible with blockchain technology.

[1033] Setyowati, M., S. *et al* (2020). "Blockchain Technology Application for Value-Added Tax Systems" *Journal of Open Innovation: Technology, Market and Complexity* 6(156): 20.

[1034] Bird, M., R., and Zolt M., E. (2008). "Technology and taxation in developing countries: from hand to mouse" *National Tax Journal* 61(4) Part 2 at 796.

[1035] Prewet K., W, Prescott G., L, Phillips K. (2020) "Blockchain adoption is inevitable— Barriers and risks remain" *Journal of Corporate Accounting & Finance* 31: 22. Available at https://doi.org/10.1002/jcaf.22415. Accessed 5 May 2021.

[1036] Caron, F. (2017). "Blockchain: Identifying Risk on the Road to Distributed Ledgers". Available at https://www.isaca.org/resources/isaca-journal/issues/2017/volume-5/blockchain-identifying-risk-on-the-road-to-distributed-ledgers. Accessed 8 May 2021.

[1037] Prewet K., W, Prescott G., L, Phillips K. (2020) "Blockchain adoption is inevitable— Barriers and risks remain" *Journal of Corporate Accounting & Finance* 31: 22. Available at https://doi.org/10.1002/jcaf.22415. Accessed 5 May 2021.

3.5.4 Political will

Fundamental changes in the public sector often requires government backing. Government backing, in the form of political will,[1038] is an important factor in deciding whether technology such as blockchain can be adopted for tax administration and tax compliance.[1039] Generally, if political will is the driving force behind the implementation of a new concept, change tends to happen much quicker as opposed to when political will is lacking.[1040] It should be noted that political will is not a static phenomenon and is therefore subject to change depending on certain circumstances and events.[1041] For example, let us assume that a political regime decides to adopt a policy framework for the adoption of blockchain in the administration of VAT. Notably, the implementation can be delayed if resources, infrastructure, expertise, good governance, and a functioning judicial system is lacking. If a regime's mandate is not completed before a new regime comes into power, challenges may ensue. A new regime may have reservations about allocating a budget for blockchain in the administration of taxes. Budget deficits can lead to cost cutting measures, resulting in the delay or cancellation of blockchain's adoption. Thus, government spending is crucial for blockchain's adoption. As I have mentioned, a project like blockchain requires skilled personnel. The training of staff is critical because the rate of success at which a program can be modernised is dependent on the training and skills of the officials who operate that

[1038] According to Brinkerhoff, 'political will' can be defined as "the commitment of actors to undertake actions to achieve a set of objectives and to sustain the costs of those actions over time." See Brinkerhoff, D. W. (2000). "Assessing political will for anti-corruption efforts: an analytic framework" *Public Administration and Development* 20(3): 242.

[1039] Bird, M., R., and Zolt M., E. (2008). "Technology and taxation in developing countries: from hand to mouse" *National Tax Journal* 61(4) Part 2 at 796. According to Bird, "experience around the world demonstrates that the single most important ingredient for effective tax administration is clear recognition of its importance at high political levels and the willingness to support good administrative practices, even if it is politically difficult to do so". See Bird, R. (2010). "Smart Tax Administration" *Economic Premise No 36* at 2. Available at https://openknowledge.worldbank.org/server/api/core/bitstreams/f509fac1-24b5-52a1-a904-fd93f6080fd3/content. Accessed 9 October 2023.

[1040] Bird, M., R., and Zolt M., E. (2008). "Technology and taxation in developing countries: from hand to mouse" *National Tax Journal* 61(4) Part 2 at 797.

[1041] Brinkerhoff, D., W. (2000). "Assessing political will for anti-corruption efforts: an analytic framework" *Public Administration and Development* 20(3): 243.

technology.[1042] It is important to have political will and a stable government regime offering an opportunity for the successful implementation of policy reform.[1043]

3.5.5 Risks associated with smart contracts

As discussed above,[1044] the remittance of VAT to a tax authority can take place using a smart contract. This suggests that a smart contract is an important tool in the administration of VAT. As discussed above,[1045] a smart contract is a program that executes predetermined instructions. Vague instructions can cause the smart contract code to be poorly developed which, in turn, can lead to unintended consequences for suppliers and tax authorities.[1046] The efficacy of smart contracts can only be as good as the team behind its existence; the software coders, and the persons giving the instructions. Errors in the smart contract can undermine the security of the network which increases the chances of hacking.[1047] If hacked, a smart contract code can be manipulated and used by criminals for illegal activities.[1048] It is for these reasons that a smart contract should be painstakingly designed, meticulously tested, and audited before deployment.[1049] Due to the fact that blockchain is a new technology, it is not inconceivable for errors to occur when blockchain is operational.[1050] Crucially, it is

[1042] Bird, M., R., and Zolt M., E. (2008). “Technology and taxation in developing countries: from hand to mouse” *National Tax Journal* 61(4) Part 2 at 795.

[1043] Brinkerhoff, D., W. (2000). “Assessing political will for anti-corruption efforts: an analytic framework” *Public Administration and Development* 20(3): 244.

[1044] See paragraph 3.3.3 above.

[1045] See Chapter 2, paragraph 2.8 above.

[1046] Prewet K., W, Prescott G., L, Phillips K. (2020) “Blockchain adoption is inevitable— Barriers and risks remain” *Journal of Corporate Accounting & Finance* 31: 25 – 26. Available at https://doi.org/10.1002/jcaf.22415. Accessed 5 May 2021.

[1047] Prewet K., W, Prescott G., L, Phillips K. (2020) “Blockchain adoption is inevitable— Barriers and risks remain” *Journal of Corporate Accounting & Finance* 31: 25 – 26. Available at https://doi.org/10.1002/jcaf.22415. Accessed 5 May 2021; Werbach, K. (2018). *The Blockchain and the New Architecture of Trust* Massachusetts Institute of Technology Press (US) at 124; Temte, M., N. (2019). “Blockchain challenges traditional contract law: Just how are smart contracts” *Wyoming Law Review* 19(1): 109 – 110.

[1048] Prewet K., W, Prescott G., L, Phillips K. (2020) “Blockchain adoption is inevitable— Barriers and risks remain” *Journal of Corporate Accounting & Finance* 31: 25 – 26. Available at https://doi.org/10.1002/jcaf.22415. Accessed 5 May 2021; Temte, M., N. (2019). “Blockchain challenges traditional contract law: Just how are smart contracts” *Wyoming Law Review* 19(1): 109 – 110.

[1049] Prewet K., W, Prescott G., L, Phillips K. (2020) “Blockchain adoption is inevitable— Barriers and risks remain” *Journal of Corporate Accounting & Finance* 31: 26. Available at https://doi.org/10.1002/jcaf.22415. Accessed 5 May 2021.

[1050] Werbach, K. (2018). *The Blockchain and the New Architecture of Trust* Massachusetts Institute of Technology Press (US) at 124 – 125.

important for software coders to develop and test response procedures before any errors occur.[1051]

3.5.6 Lack of universal blockchain regulation

Currently, there is no specific legislation that regulates blockchain technology in South Africa. The lack of regulatory framework is not limited to South Africa since there is currently no universal agreement on the regulation of blockchain internationally.[1052] The adoption of blockchain technology for VAT collection requires a regulatory framework at a national and international scale.[1053] At face value, attempts to regulate blockchain can seem difficult due to the decentralised and multijurisdictional application of blockchain. While is it likely that countries will regulate blockchain at different stages in the future, this should not detract countries from adopting international standards for blockchain regulation.[1054] As Finck correctly points out, it is difficult to have adequate standards for blockchain regulation without international cooperation. Finck further adds that if international regulation is lacking, national laws

[1051] Prewet K., W, Prescott G., L, Phillips K. (2020) "Blockchain adoption is inevitable— Barriers and risks remain" *Journal of Corporate Accounting & Finance* 31: 26. Available at https://doi.org/10.1002/jcaf.22415. Accessed 5 May 2021.

[1052] Owens, J. & De Jong, J. (2017). "Taxation on the Blockchain: Opportunities and Challenges" *Tax Notes International* 87(6): 612; Mazur, O. (2021). "Can Blockchain Revolutionize Tax Administration?" SMU Dedman School of Law Legal Studies Research Paper No. 510 at 36. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3841785. Accessed 23 June 2021.

[1053] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 58 – 59.

[1054] For example, Malta recently presented three Bills in parliament on blockchain and cryptocurrencies. *The Virtual Financial Assets Act* lays out a framework for Initial Coin Offerings (ICO) and regulations relating to the provision of services in virtual currencies. The *Technology Arrangements and Services Act* registers technology service providers and regulates designated innovative technology arrangements. The *Malta Digital Innovation Authority Act* establishes the Malta Digital Innovation Authority. Its function is to support the development and implementation of guiding principles and to promote principles for the development of technological innovations like blockchain. See Parliament of Malta https://parlament.mt/13th-leg/bills/bill-no-044-virtual-financial-assets-bill/; https://www.parlament.mt/en/13th-leg/bills/bill-no-043-innovative-technology-arrangements-and-services-bill/; https://parlament.mt/13th-leg/bills/bill-no-045-malta-digital-innovation-authority-bill/ respectively. Accessed 16 October 2023. The EU is currently looking at EU rules for blockchain to avoid legal and regulatory fragmentation. For example, the Markets in Crypto-Assets Regulation (MiCA) supports innovation while protecting consumers and the integrity of crypto-currency exchanges. See European Commission (2022). *Legal and regulatory framework for blockchain*. Available at https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-blockchain. Accessed 16 October 2023.

and rules can be fragmented making cooperation difficult.[1055] It is thus important for countries to harmonise laws and rules regarding the regulation of blockchain technology.

It is also important for the relevant authorities to adopt a balanced approach when attempting to regulate blockchain.[1056] This is because blockchain, like all technology, has the inherent capability to change without prior notice. The widespread adoption of blockchain can precipitate changes in the application of blockchain technology.[1057] Keeping pace with the necessary changes in blockchain technology is a task that legislators must contend with. For example, it may be necessary for legislators to factor the activities that take place on blockchain to mitigate risks that may arise, and to ensure compliance with the relevant laws.[1058] It stands to reason that a strict approach in the regulation of blockchain technology can inhibit its growth and development.[1059] If governments enact laws that are too strict, then the development of blockchain can be impeded. This can further make the adoption of blockchain rare and expensive.[1060] The restrictive approach towards blockchain regulation can also precipitate the illegal use of blockchain leading to an increase in illegal activities.

A pertinent question that must be posed is whether the adoption of a blockchain regulatory framework can keep pace with the constant developments in blockchain technology. According to the OECD, blockchain technology's complexity is one of the reasons why governments struggle to keep pace with regulation.[1061] For example, the

[1055] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 60.

[1056] See De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 57.

[1057] See Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 110 – 111.

[1058] Deloitte (2016). "Blockchain Enigma. Paradox. Opportunity" at 10. Available at https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-blockchain-full-report.pdf. Accessed 13 June 2021; BSI (2017). "Distributed Ledger Technologies/Blockchain: Challenges, opportunities and the prospects for standards" at 9. Available at https://www.bsigroup.com/LocalFiles/zh-tw/InfoSec-newsletter/No201706/download/BSI_Blockchain_DLT_Web.pdf. Accessed 13 June 2021.

[1059] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 174 – 175.

[1060] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 57.

[1061] OECD (2021). *Case Studies on the Regulatory Challenges Raised by Innovation and the Regulatory Responses* OECD Publishing, Paris at 68. Available at https://doi.org/10.1787/8fa190b5-en. Accessed 18 October 2023.

OECD highlights that a smart contracts "create countless avenues for new transaction structures and business models that could be difficult to understand, monitor, and where appropriate, regulate."[1062] Another challenge to blockchain regulation is the fact that by nature, blockchain and its components are borderless and not rooted to a specific jurisdiction.[1063] The different role players like code developers, miners, and validators can be subject to different regulatory regiments further making it difficult for a single authority to take responsibility.[1064] Moreover, DLT smart contract regulation could miss the mark completely because existing framework could be redundant or unclear.[1065] Simply put, the existing legal framework was not designed for blockchain and DLT technologies.[1066]

The method of regulation can often determine the pace at which changes can be made to a regulatory framework. For example, sandboxing[1067] can bring innovations such as blockchain speedily to the market.[1068] In a sandbox, regulators test a specific technology in a controlled environment to determine the benefits and risks of that technology. It also enables authorities to observe and learn from the technology while also encouraging innovation by providing legal certainty.[1069] One of the issues with sandboxing is that it is confined to a single jurisdiction, which is problematic where the technology must be offered internationally.[1070] Another popular regulatory solution is

[1062] OECD (2021). *Case Studies on the Regulatory Challenges Raised by Innovation and the Regulatory Responses* OECD Publishing, Paris at 68. Available at https://doi.org/10.1787/8fa190b5-en. Accessed 18 October 2023.

[1063] OECD (2021). *Case Studies on the Regulatory Challenges Raised by Innovation and the Regulatory Responses* OECD Publishing, Paris at 68. Available at https://doi.org/10.1787/8fa190b5-en. Accessed 18 October 2023.

[1064] OECD (2021). *Case Studies on the Regulatory Challenges Raised by Innovation and the Regulatory Responses* OECD Publishing, Paris at 68. Available at https://doi.org/10.1787/8fa190b5-en. Accessed 18 October 2023.

[1065] OECD (2021). *Case Studies on the Regulatory Challenges Raised by Innovation and the Regulatory Responses* OECD Publishing, Paris at 69. Available at https://doi.org/10.1787/8fa190b5-en. Accessed 18 October 2023.

[1066] OECD (2021). *Case Studies on the Regulatory Challenges Raised by Innovation and the Regulatory Responses* OECD Publishing, Paris at 69. Available at https://doi.org/10.1787/8fa190b5-en. Accessed 18 October 2023.

[1067] According to Finck, a regulatory sandbox is a "set of rules that allows innovators to test their product or business model in an environment that temporarily exempts them from following some or all legal requirements in place." See Finck, M. (2018). "Blockchains: Regulating the Unknown" *German Law Journal* 19(4): 677.

[1068] Finck, M. (2018). "Blockchains: Regulating the Unknown" *German Law Journal* 19(4): 677; see also OECD (2021). *Case Studies on the Regulatory Challenges Raised by Innovation and the Regulatory Responses* OECD Publishing, Paris at 73. Available at https://doi.org/10.1787/8fa190b5-en. Accessed 18 October 2023.

[1069] Finck, M. (2018). "Blockchains: Regulating the Unknown" *German Law Journal* 19(4): 679.

[1070] Finck, M. (2018). "Blockchains: Regulating the Unknown" *German Law Journal* 19(4): 679.

the so called "wait and see" approach. In this scenario, governments chose to observe how the technology evolves without necessarily acting.[1071] Here, governments let the technology develop before issuing guidelines.[1072] Finck correctly points out that the "wait and see" approach is not necessarily passive because authorities continue to apply existing rules while assembling information and acquiring knowledge from stakeholders and experts, while also considering developments in other countries.[1073] Governments often issue guidance to the public after extensive observation of a technology and its various facets. Governments can then decide to issue informal guidance on how the existing rules and regulations will apply to the new technology.[1074] The problem with this approach is that it often very lengthy because the relevant authorities take time to consider how the technology works before acting. Some countries have opted to enact legislation on blockchain and DLT.[1075] While enacting laws brings legal certainty, it has long term effects in the sense that legislative amendment will be carried out whenever new advancements in technology materialise.[1076]

[1071] OECD (2021). *Case Studies on the Regulatory Challenges Raised by Innovation and the Regulatory Responses* OECD Publishing, Paris at 71. Available at https://doi.org/10.1787/8fa190b5-en. Accessed 18 October 2023; Finck, M. (2018). "Blockchains: Regulating the Unknown" *German Law Journal* 19(4): 675.

[1072] Finck, M. (2018). "Blockchains: Regulating the Unknown" *German Law Journal* 19(4): 675.

[1073] Finck, M. (2018). "Blockchains: Regulating the Unknown" *German Law Journal* 19(4): 675.

[1074] Finck, M. (2018). "Blockchains: Regulating the Unknown" *German Law Journal* 19(4): 676.

[1075] See for example *Article 8 ter of Law Decree No. 135 of 14 December 2018* implemented by the Italian authorities. In terms of Article 8, a smart contract is defined as: "[any] computer program that operates on technologies based on distributed registers and whose execution automatically binds two or more parts on the basis of predefined effects." DLT is defined as: "distributed technologies and information protocols that use a shared, distributed, replicable, accessible register simultaneously, architecturally decentralized on bases cryptographic documents, such as to allow registration, validation, the updating and storage of data in both clear and further protected by cryptography that can be verified by each participant, not alterable and not modifiable." [English translation]. English version available at Olyniwun Ajayi LP (2019). *Examining the Italian legal framework on distributed ledger technology and smart contracts* at 1. Available at https://www.olaniwunajayi.net/blog/wp-content/uploads/2019/03/Examining-the-Italian-Legal-Framework-on-Distributed-Ledger-Technology-and-Smart-Contracts.pdf. Accessed 18 October 2023. Italian version can be accessed at *Gazzetta Ufficiale* (2019). https://www.gazzettaufficiale.it/atto/serie_generale/caricaArticolo?art.versione=1&art.idGruppo=0&art.flagTipoArticolo=0&art.codiceRedazionale=19A00934&art.idArticolo=8&art.idSottoArticolo=3&art.idSottoArticolo1=10&art.dataPubblicazioneGazzetta=2019-02-12&art.progressivo=0. Accessed 18 October 2023.

[1076] Finck, M. (2018). "Blockchains: Regulating the Unknown" *German Law Journal* 19(4): 679.

The EU is currently partaking in a blockchain regulatory sandbox for the regulation of blockchain and other DLT.[1077] The purpose of the sandbox is to establish a "pan-European framework for regulatory dialogues to increase legal certainty for innovative blockchain technology solutions."[1078] The sandbox also aims to encourage regulators and innovators for private and public sector use cases.[1079] According to the European Commission, the dialogue will help identify and communicate best practices for the EU blockchain community.[1080]

It is generally accepted that it is costly and time consuming to promulgate rules and laws.[1081] Lawmakers conduct consultation processes and factor different possible scenarios before enacting legislation.[1082] But challenges arise when changes must be made to legislation due to the rapid developments in technology. Generally, legislative amendments are lengthy and time consuming. During the amendment process, taxpayers can get around the apparent gap in the law by performing practices that lawmakers may not have envisaged.[1083] An alternative approach is to consider standards. Standards can be updated effortlessly due to frequent changes in practice.[1084] Tax authorities must take the initiative and communicate with taxpayers whenever new standards are adopted. Tax authorities are best placed to perform this task because they interact with taxpayers on a frequent basis. Tax authorities can

[1077] European Commission (2024). *European blockchain regulatory sandbox for distributed ledger technologies*. Available at https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Sandbox+Project. Accessed 16 June 2024.

[1078] European Commission (2024). *European blockchain regulatory sandbox for distributed ledger technologies*. Available at https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Sandbox+Project. Accessed 16 June 2024.

[1079] European Commission (2024). *European blockchain regulatory sandbox for distributed ledger technologies*. Available at https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Sandbox+Project. Accessed 16 June 2024.

[1080] European Commission (2024). *European blockchain regulatory sandbox for distributed ledger technologies*. Available at https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Sandbox+Project. Accessed 16 June 2024.

[1081] Bal, A. (2019). "Developing a Regulatory Framework for the Taxation of Virtual Currencies" *Intertax* 47(2): 226.

[1082] Bal, A. (2019). "Developing a Regulatory Framework for the Taxation of Virtual Currencies" *Intertax* 47(2): 226.

[1083] Bal, A. (2019). "Developing a Regulatory Framework for the Taxation of Virtual Currencies" *Intertax* 47(2): 226.

[1084] Bal, A. (2019). "Developing a Regulatory Framework for the Taxation of Virtual Currencies" *Intertax* 47(2): 226.

issue rules, guidelines, and tax policies faster than lawmakers since tax authorities do not necessarily conduct the legislative procedure.[1085]

Blockchain regulation is important because it creates legal certainty.[1086] It can also encourage taxpayers and other participants to accept the mainstream adoption of blockchain technology.[1087] With legal certainty, tax authorities can easily enforce their respective tax laws in so far as blockchain use is concerned. For example, SARS can enforce penalties and interest on taxpayers that do not comply with the provisions of the VAT Act. Thus, the use of blockchain can empower SARS to monitor taxpayers' behaviour and compliance across multiple jurisdictions. The application of blockchain on cross-border transactions can raise questions regarding SARS' extraterritorial powers.[1088] Van Zyl correctly points out that the application of SARS' extraterritorial powers cannot be enforced without bilateral agreements between South Africa and the corresponding jurisdiction where enforcement must occur.[1089]

In my view, it is necessary to make changes to the VAT Act and the Tax Administration Act to fully benefit from blockchain technology. For example, the Tax Administration Act must be amended to enable SARS to enter into agreements with foreign suppliers of digital goods. The agreements can prescribe blockchain standards that SARS and the foreign suppliers can use to administer VAT on blockchain. This process also requires the governments of the tax authority and the government of the suppliers to enter into bilateral agreements on the use of blockchain to collect cross-border VAT on the supply of digital goods.

[1085] Bal, A. (2019). "Developing a Regulatory Framework for the Taxation of Virtual Currencies" *Intertax* 47(2): 227.

[1086] Mazur, O. (2021). "Can Blockchain Revolutionize Tax Administration?" SMU Dedman School of Law Legal Studies Research Paper No. 510 at 37. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3841785. Accessed 23 June 2021.

[1087] Owens, J. & De Jong, J. (2017). "Taxation on the Blockchain: Opportunities and Challenges" *Tax Notes International* 87(6): 611; Mazur, O. (2021). "Can Blockchain Revolutionize Tax Administration?" SMU Dedman School of Law Legal Studies Research Paper No. 510 at 37. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3841785. Accessed 23 June 2021.

[1088] See Van Zyl, S. P. (2013). *The collection of Value Added Tax on online cross-border trade in Digital Goods*. Unpublished LLD thesis (UNISA) at 357 – 358.

[1089] Van Zyl, S. P. (2013). *The collection of Value Added Tax on online cross-border trade in Digital Goods*. Unpublished LLD thesis (UNISA) at 357 – 358; see also Moosa, F. (2020) "Does the Bill of Rights Apply Extraterritorially for Tax Administration Purposes?" *Stellenbosch Law Review* 31(1): 45.

3.5.7 Taxpayer information

The collection of VAT on the cross-border supply of digital goods on blockchain raises potential concerns regarding the privacy of taxpayer information. Although blockchain is transparent in nature, it does not necessarily follow that taxpayer information will be displayed or revealed on blockchain. As has been discussed above,[1090] the collection of VAT on blockchain does not require taxpayer information to be stored in plain text format. For example, the use of government issued TVACoins does not require the storage of any taxpayer information on blockchain. A request by a supplier or consumer for the acquisition of TVACoins can, for example, only be issued with positive identification. For consumers, an identity number or passport number may be sufficient while a VAT registration number will suffice for suppliers. These particulars can be stored on a tax authorities' database outside blockchain. A similar approach can be followed where VAT remittance is effected by means of a smart contract. Here, a tax authority requests and verifies a taxpayer's identity before access is granted on a network. When a taxpayer makes a payment on blockchain, their identities can be recorded on blockchain with their public keys.[1091] It is possible for blockchain and smart contracts to effect tax payments without revealing the nature of the exchange.[1092]

SARS relies on third-parties to collect taxes.[1093] For example, if a taxpayer owes a tax debt to SARS, SARS can authorise a bank to hold money or a salary and pay that money over in satisfaction of a taxpayer's outstanding tax debt.[1094] In practice, SARS divulges taxpayer information to the bank when a notice is issued in terms of section 179 of the TAA. In doing so, SARS breaches its own secrecy provisions contained in the TAA.[1095] The reason for this is because section 179 of the TAA contains particulars regarding a taxpayer, which constitute taxpayer information. To comply with this request, banks can provide a taxpayer's financial statements to SARS. This, it can be

[1090] Paragraphs 3.3.4, 3.3.5, 3.3.6, and 3.3.7.
[1091] Delmotte, C. (2022). "The Promises and Pitfalls of a Blockchain Driven Tax System" at 38. Available at https://ssrn.com/abstract=4187919. Accessed 6 October 2022.
[1092] Delmotte, C. (2022). "The Promises and Pitfalls of a Blockchain Driven Tax System" at 38. Available at https://ssrn.com/abstract=4187919. Accessed 6 October 2022.
[1093] See section 26 of the TAA.
[1094] Section 179 of the TAA.
[1095] See section 69 of the TAA.

argued, breaches a customer's right to privacy in terms of section 14 of the Constitution.[1096] It can happen that a customer has no say or cannot provide consent regarding the disclosure of their financial statements. Moreover, it is unclear how the debt is paid to SARS or how the financial statements are transmitted to SARS. To remedy this issue, I propose that SARS transmits the section 179 notice on a blockchain using a smart contract. The request, made on a private blockchain, enhances privacy because only authorised parties have access to the network. Since the request and the subsequent transmission of data to SARS is made on a private blockchain, privacy concerns are addressed. Blockchain also ensures that SARS always maintains the privacy and confidentiality of taxpayer information.

The storage of taxpayer information on blockchain can be cryptographically secured, ensuring the privacy of taxpayer data. Thus, concerns relating to the potential access of taxpayer information by unauthorised users is nullified. Only the tax authority has access to a taxpayer's information. Initially, a tax authority's request for taxpayer information from the onset is necessary simply because a taxpayer may not be anonymous when remitting taxes.[1097] An anonymous taxpayer can easily undermine the tax administration process. It is possible to store taxpayer data off-chain. Off-chain storage ensures that data is stored outside blockchain. Post and Cipollini correctly point out that if tax data is stored off-chain, audits are performed in a similar manner to tax audits conducted today.[1098] In other words, the same issues and challenges associated with performing audits on traditional databases persist. In my view, anonymising[1099] tax data should be adopted whenever tax data is stored on-chain. This view is also supported by Mazur.[1100]

[1096] The Constitution of the Republic of South Africa, 1996.

[1097] Ainsworth, R., T., Alwohaibi, M., & Cheetham, M. (2016). "VATCOIN: The GCC's Cryptotaxcurrency" at 5. Available at https://www.law.upenn.edu/live/files/5955-gcc-vatcoin.pdf. Accessed 9 April 2021.

[1098] Post, D & Cipollini, C. (2023). "Fundamental Elements of a Blockchain-Based Tax System: Governance, Legal and Technology Aspects" *World Tax Journal* 15(3): 28. [unpublished version].

[1099] See discussion at paragraph 4.8.5 below.

[1100] Mazur, O. (2022). "Can blockchain revolutionize tax administration?" *Penn State Law Review* 127(1): 156.

3.5.8 Broader application of blockchain

One of the major concerns associated with the broader application of blockchain in cross-border transactions is proficiency. For example, the broader application of VATCoins in B2B transactions raises concerns around workability.[1101] In the context of VATCoins, do the respective jurisdictions have sufficient computing capacity to collect VATCoins from all cross-border B2B transactions within an economic zone such as the EU? Does the computing capacity allow for the collection of data from an economic zone such as the EU?[1102] The questions posed by Ainsworth *et al*[1103] are relevant because they highlight the need for a blockchain system to be scalable.[1104] In other words, it is important to determine the speed at which a blockchain can record vast amounts of transactions. This is particularly important in the context of VAT collection where e-commerce transactions take place frequently and in high volumes.[1105] Additionally, blockchain should be capable of handling cross-border

[1101] Ainsworth, R. T., Alwohaibi, M., Cheetham, M., & Tirand, C., V. (2018). "A VATCoin Solution to MTIC Fraud: Past Efforts, Present Technology and the EU's 2017 Proposal" *Boston University School of Law, Law and Economics Research Paper No. 18-08* at 27 – 28. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3151394. Accessed 24 May 2021.

[1102] Ainsworth, R. T., Alwohaibi, M., Cheetham, M., & Tirand, C., V. (2018). "A VATCoin Solution to MTIC Fraud: Past Efforts, Present Technology and the EU's 2017 Proposal" *Boston University School of Law, Law and Economics Research Paper No. 18-08* at 28. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3151394. Accessed 24 May 2021.

[1103] Ainsworth, Alwohaibi, Cheetham and Tirand.

[1104] According to Prewett, Prescott and Phillips, scalability in the context of blockchain refers to the "ability of a blockchain's computation process to be used in a wide range of capabilities and to accomplish these objectives in a reasonable time period." See Prewet K., W, Prescott G., L, Phillips K. (2020) "Blockchain adoption is inevitable— Barriers and risks remain" *Journal of Corporate Accounting & Finance* 31: 21 – 22. Available at https://doi.org/10.1002/jcaf.22415. Accessed 5 May 2021; see also discussion on scalability at paragraph 2.10.2 above; De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 56.

[1105] Blocks are batches of transaction data. The amount of data contained in a block together with the chain's block generation speed determines the number of transactions per second (TPS) that a network can handle. Thus, the TPS is tied to the size of each block. One way to do this is by increasing the size of the blocks. Increasing the size of the blocks means more transactions can be stored in the block. The downside to this is that node operators need to download new block once they are generated. Block sizes range from 1 MB, 4MB, and 32 MB on the Bitcoin Blockchain. Naturally, if blockchain were to be implemented at a global scale the sizes of the blocks can go up to a gigabyte of data. This can pose a challenge to node operators especially where the persons or entities running the nodes cannot afford the hardware or Internet connections capable of handling this change. There are projects like ILCOIN that use a protocol known as RIFT. According to the developers of ILCOIN, the protocol enables them to create a block up to 5 GB and process 100 000 TPS. For a full discussion on this see Edwood, F. (2020). "Block size and scalability, explained." Available at https://cointelegraph.com/explained/block-size-and-scalability-explained#:~:text=behind%20the%20scenes.-,What%20are%20the%20arguments%20for%20and%20against%20increasing%20block%20size,will%20lead%20to%20greater%20centralization. Accessed 24 August 2023. It should be transactions while the tax authority in the consumption jurisdiction must be capable of recording and verifying the transactions within a reasonable time.[1106] Thus, it can be said that the mainstream adoption of blockchain is contingent on the technology's ability to process high volumes of transactions expeditiously.[1107] Merkx notes that AI can help tax authorities verify large amounts of data recorded on blockchain.[1108] For example, a tax authority can use AI to conduct an audit. If a taxpayer wants to ascertain whether a supplier is compliant or has paid the right amount of VAT, machine learning algorithms can facilitate this process. With machine learning, the tax authority would be to analyse the content of each invoice to see if the supplier is VAT compliant.[1109]

Bal correctly states that a blockchain-based VAT can yield more benefits if it is used for domestic and cross-border trade.[1110] The collection of VAT on blockchain must be developed and managed by more than one jurisdiction.[1111] Furthermore, Bal notes that the corresponding jurisdictions must agree on issues such as technology standards, service level agreements, the decision-making procedures, audits, and dispute

noted that different protocols have different block size limits. For example, Bitcoin Cash has a limit of 32 MB, Litecoin has a current limit of 1 MB, and Ethereum does not have a block size but a gas limit. Currently, a block size in Ethereum has a size of 15 million gas but this can go up to 30 million gas depending on the network demands. See Ethereum.org (2023) *Blocks*. Available at https://ethereum.org/en/developers/docs/blocks/#:~:text=Each%20block%20has%20a%20target,(2x%20target%20block%20size). Accessed 24 August 2023. See also Bitstamp Learn (2022). *What is block size?* Available at https://www.bitstamp.net/learn/crypto-101/what-is-block-size/#:~:text=The%20size%20of%20a%20block,as%20the%20block%20size%20limit. Accessed 24 August 2023. A Bitcoin block can store over 2000 transactions while blocks on Ethereum can handle an unlimited number of transactions. See also Bitstamp Learn (2022). *What is block size?* Available at https://www.bitstamp.net/learn/crypto-101/what-is-block-size/#:~:text=The%20size%20of%20a%20block,as%20the%20block%20size%20limit. Accessed 24 August 2023.

[1106] Tax authorities should ensure that they have the necessary infrastructure and personnel to record, verify and audit transactions on the blockchain. The failure to do this can result in delays or inefficiencies in the use of blockchain for VAT collection.

[1107] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 56.

[1108] Merkx, M. (2019). "VAT and Blockchain: Challenges and Opportunities Ahead" *EC Tax Review* 28(2): 87.

[1109] Zambrano, R. *Using New Technologies to Improve Existing VAT/GST Systems* in Owens, J., & Risse, R. (eds) (2021). *Tax Law and Digitalization: The New Frontier for Government and Business: Principles, Use Cases and Outlook* Kluwer Law International at 100.

[1110] Bal, A. (2023). *Tax management through blockchain – will this be possible?* Available at https://www.forbes.com/sites/aleksandrabal/2023/02/09/tax-management-through-blockchainwill-this-ever-be-possible/. Accessed 20 June 2024.

[1111] Bal, A. (2023). *Tax management through blockchain – will this be possible?* Available at https://www.forbes.com/sites/aleksandrabal/2023/02/09/tax-management-through-blockchainwill-this-ever-be-possible/. Accessed 20 June 2024.

resolution mechanisms.[1112] Bal's view re-emphasises the importance of international co-operation if blockchain-based VAT collection is to succeed.

As more transactions get recorded on blockchain, the bigger blockchain becomes. It also stands to reason that the quicker transactions get recorded, the quicker it takes for a blockchain to increase in size.[1113] A blockchain's scalability also highlights an important factor that potential adopters of blockchain technology must consider; storage capabilities.[1114] It is important to have sufficient storage space to cater for blockchain's inevitable increase in size. Contextually, the remittance of VAT and subsequent validation by tax authorities creates a record on blockchain. Those records are replicated across all the nodes.[1115] Due to the extended need for storage, it is imperative for tax authorities to formulate a long-term sustainable strategy and determine the associated costs of adopting blockchain technology.[1116]

3.5.9 Cash vs card payments

It is possible for the adoption of blockchain to create market distortions and other unintended consequences. For instance, the acceptance of cash as a payment method can be seen as differentiation if other businesses only accept debit or credit card as payment methods.[1117] For example, local suppliers that only accept cash as a payment method cannot remit VAT effectively and speedily compared to foreign suppliers that could benefit from the efficient use blockchain technology. In the latter

[1112] Bal, A. (2023). *Tax management through blockchain – will this be possible?* Available at https://www.forbes.com/sites/aleksandrabal/2023/02/09/tax-management-through-blockchainwill-this-ever-be-possible/. Accessed 20 June 2024.

[1113] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 56.

[1114] See also Prewet K., W, Prescott G., L, Phillips K. (2020) "Blockchain adoption is inevitable— Barriers and risks remain" *Journal of Corporate Accounting & Finance* 31: 23. Available at https://doi.org/10.1002/jcaf.22415. Accessed 5 May 2021; De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 56.

[1115] Prewet K., W, Prescott G., L, Phillips K. (2020) "Blockchain adoption is inevitable— Barriers and risks remain" *Journal of Corporate Accounting & Finance* 31: 25. Available at https://doi.org/10.1002/jcaf.22415. Accessed 5 May 2021.

[1116] Prewet K., W, Prescott G., L, Phillips K. (2020) "Blockchain adoption is inevitable— Barriers and risks remain" *Journal of Corporate Accounting & Finance* 31: 25. Available at https://doi.org/10.1002/jcaf.22415. Accessed 5 May 2021.

[1117] Merkx, M. (2019). "VAT and Blockchain: Challenges and Opportunities Ahead" *EC Tax Review* 28(2): 88.

case, VAT remittance is executed instantaneously via a smart contract.[1118] This can lead to differentiation between local suppliers and foreign suppliers.[1119] The differentiation stems from the fact that local suppliers do not make use of smart contracts while their international counterparts use smart contracts (or VATCoins and TVACoins) to remit VAT, particularly where both supply the same goods or services.[1120]

In my view, the differentiation can be resolved by introducing blockchain technology as a VAT collection model at local and international level. The adoption of blockchain technology at a local and international scale can balance the e-commerce playing field. In my view, this is in line with the principle of VAT neutrality.

3.5.10 Need for international cooperation and blockchain standards

The cross-border use of blockchain for the collection of VAT requires international cooperation. Cooperation between countries, suppliers, and tax authorities is crucial. Even if a country unilaterally adopts blockchain to collect VAT, the success of that adoption is contingent on the cooperation and willingness of suppliers situated in multiple jurisdictions. The absence of international cooperation may render the cross-border application of blockchain ineffective.

The need for international cooperation goes hand in hand with the need for countries to regulate blockchain and adopt blockchain standards. The lack of blockchain regulation in the suppliers' jurisdiction could negatively impact the adoption of blockchain in the taxing jurisdiction. The lack of regulation can cause uncertainty and scepticism regarding blockchain technology's acceptance in the international community. To mitigate the risks associated with a lack of mainstream blockchain regulation, it may be necessary for governments to enter into bilateral agreements or

[1118] Merkx, M. (2019). "VAT and Blockchain: Challenges and Opportunities Ahead" *EC Tax Review* 28(2): 88.

[1119] See Van Zyl, S. P. (2013). *The collection of Value Added Tax on online cross-border trade in Digital Goods*. Unpublished LLD thesis (UNISA) at 357.

[1120] Merkx, M. (2019). "VAT and Blockchain: Challenges and Opportunities Ahead" *EC Tax Review* 28(2): 88.

Double Tax Agreements (DTA).[1121] The ratification of bilateral agreements is necessary to ensure that governments have a common understanding of the adoption of blockchain for the collection of VAT on the supply of cross-border goods and services. The agreement between countries can also identify and adopt rules and common standards regarding the use of blockchain for the collection of VAT.

The International Standards Organisation[1122] (ISO) has developed several standards on blockchain technology.[1123] For example, the ISO has developed standards on blockchain and distributed ledger technologies and use cases.[1124] This, along with other standards under development, can go a long way into aiding government sectors, financial institutions, and other entities in the mainstream adoption of blockchain. Kim correctly points out that the adoption of blockchain standards in tax administration is essential because a tax blockchain must connect with other sectors such as financial and other regulatory networks for it to be successful.[1125] Moreover, the United States and the EU are currently developing standards through the standards development organisations (SDOs).[1126] The SDOs is "an organisation focused on developing, publishing, or disseminating technical standards to meet the needs of an industry or field."[1127]

[1121] According to SARS, a Double Tax Agreement (DTA) is an agreement entered into between two tax administrations of two countries for the purposes of eliminating double taxation. See https://www.sars.gov.za/legal-counsel/international-treaties-agreements/double-taxation-agreements-protocols/. Accessed 14 June 2021. For example, SARS can enter into bilateral agreements with jurisdictions of foreign major e-commerce suppliers to South Africa. Companies such as Uber, Airbnb, Spotify and Amazon provide services to South African residents. SARS can then enter into bilateral agreements with the jurisdictions where the companies originate from to secure blockchain technology as a VAT collection model.

[1122] The International Standards Organisation is an independent non-governmental international organisation with a current membership of 165. South Africa is a member of the ISO. The objective of the ISO is to "bring experts together to share knowledge and develop voluntary, consensus based, market relevant International Standards that support innovation and provide solutions to global challenges." Available at https://www.iso.org/about-us.html. Accessed 15 July 2021.

[1123] See https://www.iso.org/search.html?PROD_isoorg_en%5Bquery%5D=blockchain&PROD_isoorg_en%5Bmenu%5D%5Bfacet%5D=standard. Accessed 16 June 2024.

[1124] See "ISO/DTR 3242 Blockchain and distributed ledger technologies – use cases." Available at https://www.iso.org/standard/79543.html. Accessed 15 July 2021.

[1125] Kim, Y. (2022). "Blockchain initiatives for tax administration" *University of California Los Angeles Law Review* 69(1): 307.

[1126] Kim, Y. (2022). "Blockchain initiatives for tax administration" *University of California Los Angeles Law Review* 69(1): 305.

[1127] See Standards Coordinating Body. "Organisations Developing Standards". Available at https://www.standardscoordinatingbody.org/sdos. Accessed 29 December 2022.

It is important to have harmonised standards[1128] when adopting a technology such as blockchain because of the issues around interoperability.[1129] In other words, if countries adopt a unilateral approach in coding blockchain, it may make interoperability[1130] extremely difficult.[1131] This can have unintended consequences for tax authorities and businesses. To illustrate this, I make use of an example.

Example 5

> X is a supplier of goods and services. X is a VAT vendor situated in the UK. X supplies services to C, a consumer in South Africa. X accounts for and remits VAT to SARS using a smart contract. There is no bilateral agreement between South Africa and the UK regarding the use and adoption of blockchain technology for VAT collection.

Although X remits VAT to SARS, the process can easily be hampered if the UK and South Africa have different standards regarding the application of blockchain. Put simply, blockchain code in South Africa can be substantially different to blockchain code in the UK. The result is that the code used by the supplier and the tax authority varies significantly, leading to incompatibility issues between X's smart contract and blockchain in South Africa. This can lead to no taxation on the part of the supplier

[1128] Kim correctly states that: "there are strong needs for the standardisation of blockchain technology to improve interoperability, adaptability, and capability of integration. Blockchain may grow exponentially with standardisation because standardisation will eliminate some of the hurdles that may be caused by different blockchain designs that prevent the broad adoption of blockchain." See Kim, Y. (2022). "Blockchain initiatives for tax administration" *University of California Los Angeles Law Review* 69(1): 305.

[1129] See Prewet K., W, Prescott G., L, Phillips K. (2020) "Blockchain adoption is inevitable— Barriers and risks remain" *Journal of Corporate Accounting & Finance* 31: 22. Available at https://doi.org/10.1002/jcaf.22415. Accessed 5 May 2021; Kim, Y. (2022). "Blockchain initiatives for tax administration" *University of California Los Angeles Law Review* 69(1): 305.

[1130] Kerber and Schweltzer define interoperability as "the ability of a system, product or service to communicate and function with other (technically different) systems, products or services." See Kerber, W., & Schweitzer, H. (2017). "Interoperability in the digital economy" *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 8(1): 40; see also Tasca, P. & Piselli, R., *The Blockchain Paradox* in Hacker, P., Lianos, L., Dimitropoulos, G., Eich, S., (eds) (2019) *Regulating Blockchain: Techno-social and Legal challenges* Oxford University Press (UK) at 35. Belu defines interoperability as "the ability to easily distribute information and perform transactions between different blockchain systems." See Belu, G. M. (2020). "Blockchain Technology and Customs Procedures" *The Romanic Economic Journal* Year XXIII issue 78: at 23.

[1131] Mazur mentions two ways in which interoperability can be achieved. The first method is to use an external third party. The second method is to make use of other blockchains to attest and exchange information with other blockchain enabled devices. See Mazur, O. (2021). "Can Blockchain Revolutionize Tax Administration?" SMU Dedman School of Law Legal Studies Research Paper No. 510 at 38. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3841785. Accessed 23 June 2021.

because the smart contract used by the supplier may be programmed in a language that is not compatible with blockchain code in South Africa.

Prewett *et al* correctly point out that due to a lack of standardisation, the participants in a blockchain can be precluded from communicating and collaborating effectively.[1132] The widespread adoption of blockchain by various sectors can further complicate matters. For instance, blockchain users in the health sector may develop their own blockchains. That blockchain may not necessarily be consistent with blockchain standards used by tax authorities.[1133] The multiple uses of blockchain technology by different sectors can also lead to fragmentation.[1134] Mazur correctly argues that standardisation is crucial in attaining interoperability and data exchange among different blockchain users.[1135] This view is supported by Belu who argues that standards are necessary because there is no single blockchain network, but a multitude of private or hybrid blockchains.[1136] Belu further argues that developing standards can give the market confidence and internationally agreed ways of working for greater interoperability.[1137]

Adopting harmonised blockchain standards can help in the following manner:

i) Using common standards can play an important part in ensuring interoperability between multiple blockchains and doing so can reduce the risk of fragmentation;

[1132] Prewet K., W, Prescott G., L, Phillips K. (2020) “Blockchain adoption is inevitable— Barriers and risks remain” *Journal of Corporate Accounting & Finance* 31: 22 – 23. Available at https://doi.org/10.1002/jcaf.22415. Accessed 5 May 2021.

[1133] Deloitte (2016). “Blockchain Enigma. Paradox. Opportunity” at 10. Available at https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-blockchain-full-report.pdf. Accessed 13 June 2021.

[1134] BSI (2017). “Distributed Ledger Technologies/Blockchain: Challenges, opportunities and the prospects for standards” at 7 – 9. Available at https://www.bsigroup.com/LocalFiles/zh-tw/InfoSec-newsletter/No201706/download/BSI_Blockchain_DLT_Web.pdf. Accessed 13 June 2021.

[1135] Mazur, O. (2021). “Can Blockchain Revolutionize Tax Administration?” SMU Dedman School of Law Legal Studies Research Paper No. 510 at 39. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3841785. Accessed 23 June 2021.

[1136] Belu, G. M. (2020). “Blockchain Technology and Customs Procedures” *The Romanic Economic Journal* Year XXIII issue 78: at 23.

[1137] Belu, G. M. (2020). “Blockchain Technology and Customs Procedures” *The Romanic Economic Journal* Year XXIII issue 78: at 23.

ii) Common standards can address security and privacy concerns relating to data governance;

iii) Adopting common standards can create agreements on the use of consistent terminology and vocabulary, improving the understanding of the technology in the process.[1138]

There is a view that it may be counterproductive to adopt standards relating to the technical aspects of blockchain technology.[1139] Currently, there are no specific universally accepted standards on the format of blockchain;[1140] there no standards pertaining to the way data is configured on blockchain; there are no standards on the size of blocks nor are there any standards on the communication protocols.[1141] Blockchain's immaturity has a significant impact on the way the standards will be framed and adopted.[1142] As a result, it is possible for blockchain standards to change constantly as new technical aspects emerge because of the mainstream use of blockchain.[1143]

[1138] BSI (2017). "Distributed Ledger Technologies/Blockchain: Challenges, opportunities and the prospects for standards" at 16 – 23. Available at https://www.bsigroup.com/LocalFiles/zh-tw/InfoSec-newsletter/No201706/download/BSI_Blockchain_DLT_Web.pdf. Accessed 13 June 2021; Prewet K., W, Prescott G., L, Phillips K. (2020) "Blockchain adoption is inevitable—Barriers and risks remain" *Journal of Corporate Accounting & Finance* 31: 22 – 23. Available at https://doi.org/10.1002/jcaf.22415. Accessed 5 May 2021.

[1139] BSI (2017). "Distributed Ledger Technologies/Blockchain: Challenges, opportunities and the prospects for standards" at 19. Available at https://www.bsigroup.com/LocalFiles/zh-tw/InfoSec-newsletter/No201706/download/BSI_Blockchain_DLT_Web.pdf. Accessed 13 June 2021.

[1140] See Prewet K., W, Prescott G., L, Phillips K. (2020) "Blockchain adoption is inevitable— Barriers and risks remain" *Journal of Corporate Accounting & Finance* 31: 23. Available at https://doi.org/10.1002/jcaf.22415. Accessed 5 May 2021.

[1141] BSI (2017). "Distributed Ledger Technologies/Blockchain: Challenges, opportunities and the prospects for standards" at 19. Available at https://www.bsigroup.com/LocalFiles/zh-tw/InfoSec-newsletter/No201706/download/BSI_Blockchain_DLT_Web.pdf. Accessed 13 June 2021.

[1142] BSI (2017). "Distributed Ledger Technologies/Blockchain: Challenges, opportunities and the prospects for standards" at 19. Available at https://www.bsigroup.com/LocalFiles/zh-tw/InfoSec-newsletter/No201706/download/BSI_Blockchain_DLT_Web.pdf. Accessed 13 June 2021.

[1143] BSI (2017). "Distributed Ledger Technologies/Blockchain: Challenges, opportunities and the prospects for standards" at 20. Available at https://www.bsigroup.com/LocalFiles/zh-tw/InfoSec-newsletter/No201706/download/BSI_Blockchain_DLT_Web.pdf. Accessed 13 June 2021.

3.5.11 Blockchain security

It is important to secure blockchain network. The success of a blockchain hinges on whether adequate security measures are put in place. If blockchain's network is constantly breached by unauthorised personnel or entities, participants may be reluctant to use that network due to fears of data loss. The reluctance to use a blockchain network can also create mistrust in blockchain network. The challenge can be compounded if there are no measures in place to redress the loss of data.

The security of a blockchain can be increased by making use of a private permissioned blockchain.[1144] Private blockchains only grant access to participants whose identity is known to blockchain administrator.[1145] While the use of a private blockchain slows down transactions, in the South African context a private blockchain has enhanced security features to protect the privacy of taxpayers. When deploying a private blockchain, it is important to ensure that there is adequate infrastructure in place to establish a secure network.[1146] Blockchain administrators must consider the potential risks that may arise due to blockchain use. Once identified, the risks can be managed by implementing a security model that caters for blockchain and its intended purposes.[1147] In my view, a blockchain's security can also be enhanced by restricting the type and format of data stored on blockchain. As mentioned above,[1148] data stored on a blockchain can be encrypted.

Smart contracts play a crucial role in the collection of VAT. For this reason, it is important that blockchain administrators safeguard the use and application of smart contracts. This statement cannot be overstated for the simple reason that participants across the world will be making use of smart contracts to remit VAT to the relevant

[1144] See IBM. "What is Blockchain Security?" Available at https://www.ibm.com/topics/blockchain-security. Accessed 17 June 2021.

[1145] As already mentioned, the private blockchain is conducive for collecting VAT due to the restrictions imposed by the tax authority. Access is restricted to vetted and trusted parties, encryption of tax data can be implemented, zero-knowledge proof can also be adopted, and the type of data stored on the blockchain can be limited. These processes enhance the security of a private blockchain. See also discussion in Chapter 4.

[1146] IBM. "What is Blockchain Security?" Available at https://www.ibm.com/topics/blockchain-security. Accessed 17 June 2021.

[1147] IBM. "What is Blockchain Security?" Available at https://www.ibm.com/topics/blockchain-security. Accessed 17 June 2021.

[1148] See paragraph 3.3.3 above.

authorities. Since blockchain administrators can code blockchain, it follows that blockchain administrators must programme the smart contracts. In my view, the participants (taxpayers) should not be placed in a position where they must code smart contracts. This will pose an unnecessary burden on the taxpayers, and it can reduce the willingness of voluntary uptake. It remains the responsibility of blockchain administrators (tax authorities) to ensure that smart contracts are checked on a regular basis to warrant optimum operational levels. Additionally, the burden of coding smart contract must rest with a tax authority.

Smart contracts can be secured by writing a secure code.[1149] The security of the code can be influenced by the programmer and the programming practices. It can be difficult to hack a smart contract if the standard of the programming is high.[1150] Once coded, the smart contract must be tested before use. This is done to secure the smart contract.[1151] Lastly, it may be necessary for blockchain administrators to insure the smart contract code against potential failures.[1152]

3.5.12 Blockchain governance

One of the most important considerations for the adoption of blockchain are challenges surrounding blockchain governance. The considerations help determine matters such as control of blockchain, the rules used to make changes to blockchain code, and the decision-making process of blockchain.[1153] Blockchain governance processes are

[1149] G DATA Blog (2020). "How secure are smart contracts?". Available at https://www.gdatasoftware.com/blog/2020/12/36570-how-secure-are-smart-contracts. Accessed 17 June 2021.

[1150] G DATA Blog (2020). "How secure are smart contracts?". Available at https://www.gdatasoftware.com/blog/2020/12/36570-how-secure-are-smart-contracts. Accessed 17 June 2021.

[1151] G DATA Blog (2020). "How secure are smart contracts?". Available at https://www.gdatasoftware.com/blog/2020/12/36570-how-secure-are-smart-contracts. Accessed 17 June 2021.

[1152] G DATA Blog (2020). "How secure are smart contracts?". Available at https://www.gdatasoftware.com/blog/2020/12/36570-how-secure-are-smart-contracts. Accessed 17 June 2021.

[1153] Kianieff, M. (2019) *Blockchain Technology and the Law Opportunities and Risks* Routledge Publishing (UK) at 99; Bacon, J., Millard, C., & Singh, J. (2018). "Blockchain Demystified: A technical and Legal Introduction to Distributed and Centralised Ledgers" *Richmond Journal of Law & Technology* 25(1): 33 – 34; Mazur, O. (2021). "Can Blockchain Revolutionize Tax Administration?" SMU Dedman School of Law Legal Studies Research Paper No. 510 at 37 – 38. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3841785. Accessed 23 important because it enables blockchain system to react real-work events and become sophisticated as time goes by.[1154] It is very difficult for blockchain system to improve or to adapt to world events without governance processes.[1155] Finck distinguishes between endogenous and exogenous factors that influence blockchain's protocol.[1156] Exogenous factors are external factors such as changes in the law and social norms. Endogenous factors include upgrades to the software protocol or to change the characteristics of the protocol.[1157]

There are two types of blockchain governance processes. First, on-chain governance relates to the "rules encoded directly into the underlying infrastructure of blockchain systems."[1158] Here, all the rules regarding the decision-making process and procedures are coded into the consensus protocol.[1159] If a decision has been made on blockchain, the protocol adapts the change automatically.[1160] Second, off-chain governance relates to "all other types of rules that might affect the operation or future development of a blockchain system."[1161] The rules and procedures are not

June 2021; Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 183.

[1154] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 184.

[1155] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 184.

[1156] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 184 – 185.

[1157] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 184; see also De Filippi, P. & McMullen, G. (2018). "Governance of blockchain systems: Governance of and by distributed infrastructure" *Blockchain Research Institute and COALIA* at 18 – 20. Available at https://hal.science/hal-02046787/document. Accessed 15 October 2023.

[1158] De Filippi, P. & McMullen, G. (2018). "Governance of blockchain systems: Governance of and by distributed infrastructure" *Blockchain Research Institute and COALIA* at 4. Available at https://hal.science/hal-02046787/document. Accessed 15 October 2023.

[1159] Post, D & Cipollini, C. (2023). "Fundamental Elements of a Blockchain-Based Tax System: Governance, Legal and Technology Aspects" *World Tax Journal* 15(3): 5. [unpublished version]; see also Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 192.

[1160] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 192; Post, D & Cipollini, C. (2023). "Fundamental Elements of a Blockchain-Based Tax System: Governance, Legal and Technology Aspects" *World Tax Journal* 15(3): 5. [unpublished version].

[1161] De Filippi, P. & McMullen, G. (2018). "Governance of blockchain systems: Governance of and by distributed infrastructure" *Blockchain Research Institute and COALIA* at 4. Available at https://hal.science/hal-02046787/document. Accessed 15 October 2023.

automatically enforced during off-chain governance. This feature enables blockchain system to adapt to external changes and circumstances more quickly.[1162]

Generally, a blockchain's governance differs from one platform to another.[1163] Put differently, the type of blockchain and the reason for its adoption have a bearing on blockchain's governance. For instance, the Bitcoin protocol relies on the consensus mechanism (*proof-of-work*) where nodes decide which new blocks should be added to blockchain. The decision as to which new blocks should be added is determined by rules contained in the Bitcoin's source code.[1164] In the context of Bitcoin, the users, nodes, miners, and the developers determine the general technical improvements to the protocol including how *soft* and *hard forks* should be effected.[1165] The implementation of the consensus mechanism on the Bitcoin blockchain helps to validate the accuracy of the data stored on blockchain.[1166]

According to Kim, it is necessary to adopt a consensus mechanism for the administration of taxes where a central authority is lacking; in situations where the participants do not fully trust each other; or where tax information is shared between parties.[1167] In my view, it may be necessary to adopt a consensus mechanism where a central administrator validates the transactions on blockchain. For example, it is necessary to have a consensus mechanism when VAT is administered on blockchain. The tax authority validates the accuracy of the transactions against the information provided on a digital invoice. The tax authority remains in control of blockchain, and

[1162] Post, D & Cipollini, C. (2023). "Fundamental Elements of a Blockchain-Based Tax System: Governance, Legal and Technology Aspects" *World Tax Journal* 15(3): 6. [unpublished version]; De Filippi, P. & McMullen, G. (2018). "Governance of blockchain systems: Governance of and by distributed infrastructure" *Blockchain Research Institute and COALIA* at 20 – 21. Available at https://hal.science/hal-02046787/document. Accessed 15 October 2023.

[1163] Bacon, J., Millard, C., & Singh, J. (2018). "Blockchain Demystified: A technical and Legal Introduction to Distributed and Centralised Ledgers" *Richmond Journal of Law & Technology* 25(1): 34.

[1164] Kianieff, M. (2019) *Blockchain Technology and the Law Opportunities and Risks* Routledge Publishing (UK) at 100.

[1165] Bacon, J., Millard, C., & Singh, J. (2018). "Blockchain Demystified: A technical and Legal Introduction to Distributed and Centralised Ledgers" *Richmond Journal of Law & Technology* 25(1): 34.

[1166] Mazur, O. (2021). "Can Blockchain Revolutionize Tax Administration?" SMU Dedman School of Law Legal Studies Research Paper No. 510 at 37. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3841785. Accessed 23 June 2021.

[1167] Kim, R., C. (2021). "Blockchain Initiatives for Tax Administration" *University of Utah College of Law Research Paper No 427* at 5. Available at https://ssrn.com/abstract=3798136. Accessed 26 June 2021.

all governance related issues remain the sole function of the tax authority. In other words, blockchain is custom made for the collection of VAT on the cross-border supply of digital goods and services. Bug fixes, rectification of errors, and any updates to blockchain must be done by the tax authority where the latter is the designer and proprietor of blockchain. If, however, the tax authority only has a licence to use blockchain infrastructure, bug fixes would be reported to the proprietor. This process can take time and result in delays during the VAT administration processes. It should be noted that if participants become aware of or identify errors or bugs when using smart contracts, those must be communicated to the tax authorities immediately. The speedy notification can enable tax authorities to perform the necessary updates to ensure that the bugs are fixed timeously.

3.5.13 The loss of private keys

It is important to consider the effects of the potential theft or loss of a private key. A private key[1168] is an important part of the VAT collection process on blockchain. As I stated earlier,[1169] a VAT vendor can sign a digital invoice with their private key. In doing so, the VAT vendor authenticates the data on the invoice. It stands to reason that without a private key, a VAT vendor cannot sign a digital invoice, making their compliance burden difficult. It can also be stated that if the VAT vendor does not sign the digital invoice, the integrity of the data on the invoice can be questioned. This can cause delays in VAT remittance and the VAT administration process. The theft or loss of a VAT vendor's private key can bring these challenges to the fore. It is possible for a person with unauthorised access to a private key to access information, or any digital asset secured by a private key.[1170] To contextualise this, a VAT vendor who loses their private key can lose data and can be excluded from remitting VAT to SARS. For these reasons, it is important to have a private key management system.[1171] A private key management system can prevent the theft or loss of private keys. In this system, an

[1168] See discussions at paragraphs and 2.3.3.1 and 2.5.6 above.

[1169] See Paragraph 3.3.3 above.

[1170] Prewet K., W, Prescott G., L, Phillips K. (2020) "Blockchain adoption is inevitable— Barriers and risks remain" *Journal of Corporate Accounting & Finance* 31: 27. Available at https://doi.org/10.1002/jcaf.22415. Accessed 5 May 2021.

[1171] Prewet K., W, Prescott G., L, Phillips K. (2020) "Blockchain adoption is inevitable— Barriers and risks remain" *Journal of Corporate Accounting & Finance* 31: 27. Available at https://doi.org/10.1002/jcaf.22415. Accessed 5 May 2021.

intermediary can be tasked with managing the private keys to minimise the risks of theft or loss.[1172] From a South African perspective, a separate division at SARS can be tasked with the management of private keys. This can further reduce a VAT vendor's compliance burden when remitting VAT on a blockchain to SARS.

3.6 Conclusion

This chapter demonstrates how VAT can be collected on blockchain. The chapter has determined that suppliers can use smart contracts to remit VAT in real-time. To assist tax authorities, a digital invoice signed electronically by a supplier lays the foundation for an efficient audit. The use of government issued cryptocurrencies like VATCoins/TVACoins can also facilitate VAT collection. With the use of VATCoins/TVACoins, a supplier does not hold any VAT in fiat money. Instead, there is an exchange of government issued cryptocurrencies between consumers, suppliers, and tax authorities in real-time. Only governments are allowed to issue these cryptocurrencies. The benefit of using government issued cryptocurrencies is that VAT fraud is reduced. The use of DICE in conjunction with blockchain and government issued cryptocurrencies shows great promise. Regional communities like the Southern African Development Community (SADC) can greatly benefit from this model.

This chapter also highlights how blockchain can make the administration of taxes seamless and efficient. For example, suppliers do not incur any transaction costs because VAT remittance is done instantaneously and without the presence of a financial intermediary. The compliance burden incurred by suppliers is reduced due to the speed and ease at which VAT collection and remittance takes place. The use of blockchain can reduce tax fraud, reduce the administrative burden on tax authorities, and improve trade. Blockchain can enhance international cooperation in tax administration. Moreover, the automatic nature of VAT payments can significantly

[1172] Prewet K., W, Prescott G., L, Phillips K. (2020) "Blockchain adoption is inevitable— Barriers and risks remain" *Journal of Corporate Accounting & Finance* 31: 27. Available at https://doi.org/10.1002/jcaf.22415. Accessed 5 May 2021.

increase tax compliance which can lead to higher revenue for governments.[1173] Higher government revenue can reduce the VAT gap.[1174]

Despite its potential in the administration of taxes, the adoption of blockchain faces several challenges. The costs of blockchain adoption are extremely high. It is difficult to put a fixed price from the outset because blockchain has yet to go mainstream. The constant changes and advancement in technology can also affect the price of blockchain adoption. Ultimately, blockchain associated costs depend on its intended use and the amount of participants present on the network. The lack of; i) blockchain standards, ii) blockchain regulation, iii) skilled personnel, and iv) IT systems and infrastructure pose hurdles to blockchain adoption. The security of blockchain network and political will are factors that must be present from the onset since it could determine the success of blockchain adoption. Since blockchain, as a VAT collection tool has not been tested in South Africa, I do not advocate for nor against the application of the technology for South Africa. Consequently, the legal implications of the use of blockchain as a VAT collection tool are discussed.

In the next chapter, I discuss the impact of blockchain on a person's right to privacy with specific reference to data privacy.

[1173] Delmotte, C. (2022). "The Promises and Pitfalls of a Blockchain Driven Tax System" at 15. Available at https://ssrn.com/abstract=4187919. Accessed 6 October 2022.

[1174] Delmotte, C. (2022). "The Promises and Pitfalls of a Blockchain Driven Tax System" at 15. Available at https://ssrn.com/abstract=4187919. Accessed 6 October 2022.

CHAPTER 4: DATA PRIVACY AND BLOCKCHAIN

4.1 Introduction

In Chapter 3, I consider how VAT can be collected on blockchain. Blockchain has features that are conducive for the collection of VAT. Blockchain's transparent nature enables tax authorities to verify taxpayers' transactions. A tax authority can audit a taxpayer's returns to ensure that the VAT returns are accurate. The transparent audit functionality can encourage tax compliance among taxpayers. Blockchain automates tax calculations and remittance, reducing the administrative burden in the process.[1175] Errors during and after the submission of returns can be identified and rectified. The speed at which VAT is remitted and the ease at which taxpayers can rectify errors significantly reduces the compliance burden incurred by taxpayers. Chapter 3 also pinpoints how VAT fraud can be reduced on blockchain. The use of VATCoins on blockchain can provide tax authorities with a mechanism to decrease VAT fraud. VATCoins are issued by tax authorities, and they provide a transparent method to track VAT payments.[1176]

In this chapter, I explore the impact of blockchain on data privacy. The collection of VAT, or any other tax for that matter, on a decentralised digital platform has the potential to encroach a taxpayer's right to data privacy. In this discussion, I consider two important points. First, it is important to understand what data privacy is, to set the scene for the rest of the chapter. Second, I explore the measures that can be deployed on blockchain to protect data privacy. In the context of VAT collection, information stored on blockchain constitutes tax information which must be protected. I focus on blockchain mechanics that can be used to protect taxpayers' data.

[1175] Bal, A. (2018). "Does the Tax Sector Need Blockchain?" *White Paper IBFD* at 4.
[1176] Alexander, G. (2022). "Blocking the Gap: The Potential for Blockchain Technology to secure VAT Compliance" *EC Tax Review* 31(3): 153.

4.2 What is privacy?

Before modern times, the question of 'privacy' revolved around the legal limitations placed on others to encroach a person's private space.[1177] While it is true that the law afforded protection to a person's property and their right to life, the same could not have been said about a person's right to privacy. In 1890, Warren and Brandeis submit that a person's privacy was worth protecting. They also argued that the invasion of a person's privacy by newspaper companies and the press required protection. Furthermore, the advancement of civilization led to people's withdrawal to a private abode where they would be free from public scrutiny. They termed this right, the 'right to be left alone'.[1178] Godkin coined the definition of privacy slightly differently. Godkin defined privacy as:

> "The right to decide how much knowledge of [a person's] personal thought and feeling, and how much knowledge, therefore, of his tastes, and habits, of his own private doings and affairs, and those of his family living under his roof, the public at large shall have, is as much one of his natural rights…"[1179]

While privacy in a person's abode was recognised, the right to privacy outside one's natural abode once venturing into the public domain was a contentious issue. Can a person exercise their right to privacy when they venture into the public domain? Does the law afford protection to a person who wanders into the public?[1180] The answer to these questions was in the negative because the moment a person enters the public domain, they 'renounced' their right to privacy.[1181] This was primarily because a person was not able to control who has access to their information. When in public, it is difficult to influence what others see about a person.[1182] Information about a person becomes readily available to the public and the law cannot be used to compel people to be oblivious to information about others.[1183] More pertinently, it is difficult to 'unknow'

[1177] Lessig, L. (2006). *Code: Version 2.0* Basic Books (US) at 201.

[1178] Warren, S., D., & Brandeis, L., D., (1890). "The right to privacy" 4 *Harvard Law Review* 193 – 220.

[1179] Godkin, E., L., (1890). "The Rights of the Citizen, IV—To His Own Reputation" *Scribner's Magazine* vol 8 issue 1 at 65.

[1180] Lessig, L. (2006). *Code: Version 2.0* Basic Books (US) at 202.

[1181] Lessig, L. (2006). *Code: Version 2.0* Basic Books (US) at 202.

[1182] Lessig, L. (2006). *Code: Version 2.0* Basic Books (US) at 202.

[1183] See Lessig, L. (2006). *Code: Version 2.0* Basic Books (US) at 202.

a person or information about a person once it becomes publicly available. Holvast differentiates between territorial privacy and bodily privacy.[1184] Territorial privacy deals with how a person relates to other people. A person can control access to his domestic environment.[1185] Bodily privacy deals with controlling who touches one's body.[1186] Another feature of privacy is a person's ability to exchange facts about themselves, someone, or an event. This information can be shared through various means (a conversation, mobile phone, or the Internet) or on social media platforms like *Instagram*. When a person engages with these various forms of media, their personal information[1187] is collected. For example, a person joining *Facebook* for the first time is often required to input their name, surname, date of birth and country of residence. This type of information is collected, processed, and stored on *Facebook*. This is an example of informational privacy.[1188]

4.2.1 Why is privacy important?

4.2.1.1 Autonomy

Generally, all natural persons covet independence and the need to be free from the control of other natural persons.[1189] The notion of autonomy emanates from every human being's desire to be unique. The uniqueness espouses human dignity and individuality.[1190] Each individual has an 'inner circle'. There are several 'inner circles' that each person has. The relationship a person has with other people determines the type of information that will be divulged. The closer the proximity of the relationship

[1184] Holvast, J., "*History of Privacy"* in De Leeuw, K., & Bergstra, J., (eds) (2007) "*The History of Information Security: A Comprehensive Handbook"* (Elsevier) at 741.

[1185] Holvast, J., "*History of Privacy"* in De Leeuw, K., & Bergstra, J., (eds) (2007) "*The History of Information Security: A Comprehensive Handbook"* (Elsevier) at 741.

[1186] Holvast, J., "*History of Privacy"* in De Leeuw, K., & Bergstra, J., (eds) (2007) "*The History of Information Security: A Comprehensive Handbook"* (Elsevier) at 741.

[1187] See definition in paragraph 4.4 below.

[1188] Holvast, J., "*History of Privacy"* in De Leeuw, K., & Bergstra, J., (eds) (2007) "*The History of Information Security: A Comprehensive Handbook"* (Elsevier) at 741; Volokh defines information privacy as "the right to control other people's communication of personally identifiable information about you." See Volokh, E. (1999). "Freedom of speech and information privacy: The troubling implications of a right to stop people from speaking about you" *Stanford Law Review* 50(5): 1050 – 1051.

[1189] Westin, A., F., (1966) "Science, Privacy, and Freedom: Issues and Proposals for the 1970's. Part I--The Current Impact of Surveillance on Privacy" *Columbia Law Review* 66(6): 1022.

[1190] Westin, A., F., (1966) "Science, Privacy, and Freedom: Issues and Proposals for the 1970's. Part I--The Current Impact of Surveillance on Privacy" *Columbia Law Review* 66(6): 1022.

between individuals, the more likely it is that ‘secrets’ will be shared. Conversely, the further the proximity of relations between individuals, the less likely that ‘secrets’ will be divulged.[1191] As one moves further away from their ‘inner circle’, the revelation of secrets diminishes and the conversations with others outside the circle is much more controlled.[1192]

It is possible for a person’s autonomy to be threatened.[1193] Generally, a person’s privacy is infringed when one loses control over data containing facts about themselves.[1194] Contextually, a person’s autonomy is threatened once another person breaks into the inner circle and retrieves sensitive information belonging to that person.[1195] This infringement not only causes psychological hurt but it puts one directly below the control and potentially influence of the holder of that sensitive information.[1196] Therefore, it is important for privacy to safeguard one’s autonomy to allow a person to make life choices and to develop his or her sense of individuality.[1197]

4.2.1.2 Limited communication

An individual’s interaction with other people is often limited to the confinement of suburban environments. This is partly because it is not possible to have personal interaction with every person encountered in public.[1198] For any credible exchange to take place between two people, both parties must be comfortable with their surroundings. An individual is more likely to share sensitive information with people

[1191] Westin, A., F., (1966) “Science, Privacy, and Freedom: Issues and Proposals for the 1970's. Part I--The Current Impact of Surveillance on Privacy” *Columbia Law Review* 66(6): 1022 – 1023.

[1192] Westin, A., F., (1966) “Science, Privacy, and Freedom: Issues and Proposals for the 1970's. Part I--The Current Impact of Surveillance on Privacy” *Columbia Law Review* 66(6): 1023.

[1193] See Westin, A., F., (1966) “Science, Privacy, and Freedom: Issues and Proposals for the 1970's. Part I--The Current Impact of Surveillance on Privacy” *Columbia Law Review* 66(6): 1023.

[1194] Lessig, L. (2006). *Code: Version 2.0* Basic Books (US) at 200.

[1195] Westin, A., F., (1966) “Science, Privacy, and Freedom: Issues and Proposals for the 1970's. Part I--The Current Impact of Surveillance on Privacy” *Columbia Law Review* 66(6): 1023.

[1196] Westin, A., F., (1966) “Science, Privacy, and Freedom: Issues and Proposals for the 1970's. Part I--The Current Impact of Surveillance on Privacy” *Columbia Law Review* 66(6): 1023.

[1197] Westin, A., F., (1966) “Science, Privacy, and Freedom: Issues and Proposals for the 1970's. Part I--The Current Impact of Surveillance on Privacy” *Columbia Law Review* 66(6): 1023.

[1198] Westin, A., F., (1966) “Science, Privacy, and Freedom: Issues and Proposals for the 1970's. Part I--The Current Impact of Surveillance on Privacy” *Columbia Law Review* 66(6): 1028.

they are close to. These include colleagues, friends, and family. At the core of any interaction is the ability or inability to trust people close to them.[1199]

4.2.1.3 Privacy as an emotional release mechanism

Individuals incur various degrees of tension throughout their livelihoods. The strains and pressures often emanate from relationships, encounters at work, peers, friends, and social interactions. The demands of society affect a person's mental and physical health.[1200] At times, it becomes necessary for individuals to release themselves emotionally from the pressures that society gives.[1201] With privacy, an individual can maintain some sense of 'normality' by taking time off to unwind, vent and break free from the emotional pressures of life. Privacy allows individuals to freely express their emotions without any public judgment. The private emotional relief is necessary to prevent individuals from acquiring any psychological and mental distress.[1202]

4.2.1.4 Self-evaluation and decision making

Each individual responds to life's challenges in a unique way. At times, it is necessary to coordinate experiences into routines to fully understand them. Individuals do this to make decisions and to achieve uniqueness.[1203] A busy life negatively impacts a person's ability to manage the constant flow of information that they are exposed to. To decipher and process all the information, an individual needs time and privacy to reflect and make appropriate decisions.[1204]

[1199] Westin, A., F., (1966) "Science, Privacy, and Freedom: Issues and Proposals for the 1970's. Part I--The Current Impact of Surveillance on Privacy" *Columbia Law Review* 66(6): 1028; Holvast, J., "*History of Privacy"* in De Leeuw, K., & Bergstra, J., (eds) (2007) "*The History of Information Security: A Comprehensive Handbook"* (Elsevier) at 741.

[1200] Westin, A., F., (1966) "Science, Privacy, and Freedom: Issues and Proposals for the 1970's. Part I--The Current Impact of Surveillance on Privacy" *Columbia Law Review* 66(6): 1024 – 1026.

[1201] Westin, A., F., (1966) "Science, Privacy, and Freedom: Issues and Proposals for the 1970's. Part I--The Current Impact of Surveillance on Privacy" *Columbia Law Review* 66(6): 1025.

[1202] Westin, A., F., (1966) "Science, Privacy, and Freedom: Issues and Proposals for the 1970's. Part I--The Current Impact of Surveillance on Privacy" *Columbia Law Review* 66(6): 1024 – 1026.

[1203] Westin, A., F., (1966) "Science, Privacy, and Freedom: Issues and Proposals for the 1970's. Part I--The Current Impact of Surveillance on Privacy" *Columbia Law Review* 66(6): 1026.

[1204] Westin, A., F., (1966) "Science, Privacy, and Freedom: Issues and Proposals for the 1970's. Part I--The Current Impact of Surveillance on Privacy" *Columbia Law Review* 66(6): 1026 – 1027.

4.3 Data privacy and the information society

We live in revolutionary times where people's information is easily searched on search engines like *Google* or found on websites like *Wikipedia, Facebook, Instagram,* and *LinkedIn*. Often, people elect to display information about themselves on these media platforms to communicate with people around the world. On other occasions, the disclosure of a person's information is incidental rather than voluntary. For example, when a person shops online, their personal information is stored and retrieved by the corporations that run e-commerce websites. Similarly, Internet browsers and websites use cookies[1205] to track a person's Internet activities, interests, and searches. As people continue to interact on the Internet, they leave traces of information about themselves when they shop online, when filing tax returns, when sharing pictures and when they interact with family and friends.[1206] It is possible for individuals to reveal their personal information without knowing.[1207] Today, it is almost impossible to conduct an activity or perform a function without revealing one's personal information.[1208] This trend is likely to continue as technological and digital advancements continue to form part of people's lives. Moreover, the advent of the fourth industrial revolution (4IR)[1209] is expected to proliferate significant changes in the manner we relate, work, and interact with people.

The increased use of digital technology has coincided with increased online activity. Individuals transact on multiple platforms, creating online digital footprints in the process. These digital footprints are captured and stored on computer networks

[1205] A cookie is a text file containing code that is stored on a person's computer when that person accesses a website. Apart from collecting a person's website surfing history, they can be used to store a person's passwords and identify users. See Solove, D., J. (2001). "Privacy and power: Computer databases and metaphors for information privacy" *Stanford Law review* 53(6): 1411.

[1206] Mai., J. E. (2016). "Big data privacy: The datafication of personal information" *The Information Society* 32(3): 192 – 193. Available at https://doi.org/10.1080/01972243.2016.1153010. Accessed 5 July 2020; see also Solove, D., J. (2008). *Understanding Privacy* Harvard University Press at 5.

[1207] Mai., J. E. (2016). "Big data privacy: The datafication of personal information" *The Information Society* 32(3): 192 – 193. Available at https://doi.org/10.1080/01972243.2016.1153010. Accessed 5 July 2020.

[1208] Mai., J. E. (2016). "Big data privacy: The datafication of personal information" *The Information Society* 32(3): 193. Available at https://doi.org/10.1080/01972243.2016.1153010. Accessed 5 July 2020.

[1209] The 4IR is technological revolution synonymous with emerging technologies such as the Internet of Things (IoT), robots, 3D printing, biotechnology and quantum computing. See Schwab, K., (2016). *The Fourth Industrial Revolution* Crown Publishing at 5.

around the world.[1210] The digital footprints or personal identifying information (PII)[1211] consist of personal information collected in what Solove refers to as 'digital dossiers'.[1212] According to Solove, a 'digital dossier' "is a collection of detailed data about an individual."[1213] It is possible to reconstruct bits of information belonging to an individual in a process called aggregation.[1214] The effect is that aggregation recreates a person's identity.

Another challenge posed by increased use in digital technology is the storage of data on computer databases owned by corporations. This data or 'Big data' is reconstructed and analysed to form predictive behavioural patterns about individuals.[1215] Once a person's preferences and 'likes' are identified, the corporations proceed to sell products to these persons.[1216] A corporation can decide to sell people's personal information to other corporations without their knowledge or consent.[1217]

[1210] Solove, D. J., (2004). *The digital person: technology and privacy in the information age* New York University Press at 1.

[1211] See Ciocchetti, C. A. (2007). "E-commerce and information privacy: Privacy policies as personal information protectors" *American Business Law Journal* 44(1): 56. Any data that is intrinsically linked to the identity of a person is personal identifying information. Examples include a person's ID number, gender, sex, credit card details, bank account, name. Ciocchetti refers to personal identifying information as pieces of personal information that represents a mere pixel of their life but when pieced together, they present a rather detailed picture of a person's identity.

[1212] Solove, D. J., (2004). *The digital person: technology and privacy in the information age* New York University Press at 1.

[1213] Solove, D. J., (2004). *The digital person: technology and privacy in the information age* New York University Press at 1.

[1214] Solove, D. J., (2004). *The digital person: technology and privacy in the information age* New York University Press at 44 – 47; See Ciocchetti, C. A. (2007). "E-commerce and information privacy: Privacy policies as personal information protectors" *American Business Law Journal* 44(1): 56; Solove, D. J. (2006). "Taxonomy of privacy" *University of Pennsylvania Law Review* 154(3): 477-564; Solove, D., J. (2008). *Understanding Privacy* Harvard University Press at 33 – 189. According to Solove, the challenge that aggregation poses to privacy is that entities use technology to analyse personal information and formulate identities about individuals. While it may be useful for companies who want to sell the correct products to individuals, it may also be used to unfairly deny persons opportunities such as obtaining finance for a motor vehicle or applying for credit. Decisions like these are often based on person's financial reputation as a single factor in denying him or her credit and therefore severely impacting their lives.

[1215] Solove, D. J., (2004). *The digital person: technology and privacy in the information age* New York University Press at 1; see also Mai., J. E. (2016). "Big data privacy: The datafication of personal information" *The Information Society* 32(3): 192 – 199. Available at https://doi.org/10.1080/01972243.2016.1153010. Accessed 5 July 2020; Wheeler, T. (2019). *From Gutenberg to Google: The History of our Future* Brookings Institution Press at 185 – 187.

[1216] Wheeler, T. (2019). *From Gutenberg to Google: The History of our Future* Brookings Institution Press at 189.

[1217] Mai., J. E. (2016). "Big data privacy: The datafication of personal information" *The Information Society* 32(3): 192 – 199. Available at https://doi.org/10.1080/01972243.2016.1153010. Accessed 5 July 2020.

4.4 What is personal information?

The term 'personal information' has no universally accepted definition.[1218] Countries adopt different interpretations based on their respective legislative frameworks. The lack of uniformity also translates to distinct legal consequences pertaining to the collection and processing of personal information.[1219] According to Murphy, personal information is "any data about an individual that is identifiable to that individual."[1220] The EU data protection directive (DPD) has a similar definition.[1221] It should be noted that the EU DPD uses 'personal data' as opposed to 'personal information'.[1222] Article 2(a) of the EU DPD defines personal data as:

> "Any information relating to an identified or identifiable natural person ('data subject')".[1223]

The definition of personal information is broad. It incapsulates all information that is associated with a person.[1224] It is possible for information that may not necessarily be deemed as 'private', to be considered worthy of protection because it constitutes personal information.[1225] For example, a person who is in possession of another person's physical address may be deemed to have collected personal information.[1226]

[1218] The term 'personal data' is often used as synonym. As a result, these terms are used interchangeably in this thesis.

[1219] Spiekermann, S. *et al* (2015). "The challenges of personal data markets and privacy." Available https://link.springer.com/article/10.1007/s12525-015-0191-0. Accessed 18 July 2020.

[1220] Murphy, R. S. (1996). "Property rights in personal information: An economic defense of privacy" *Georgetown Law Journal* 84: 2383; see also Solove, D., J. (2008). *Understanding Privacy* Harvard University Press at 25; Jens-Erik, M., (2016). "Big data privacy: The datafication of personal information" *The Information Society* 32(3): 195. Available at https://doi.org/10.1080/01972243.2016.1153010. Accessed 5 July 2020.

[1221] See EU directive 95/46/EC of the European Parliament and the Council of 24 October 1995.

[1222] The difference has more to do with interpretation. This is because data is unprocessed information while information is processed data.

[1223] Article 2(a) of the EU directive 95/46/EC of the European Parliament and the Council of 24 October 1995.

[1224] Mai., J. E. (2016). "Big data privacy: The datafication of personal information" *The Information Society* 32(3): 195. Available at https://doi.org/10.1080/01972243.2016.1153010. Accessed 5 July 2020.

[1225] See Mai., J. E. (2016). "Big data privacy: The datafication of personal information" *The Information Society* 32(3): 195. Available at https://doi.org/10.1080/01972243.2016.1153010. Accessed 5 July 2020. Murphy gives a person's income, credit record, genetic code and eye colour as examples of personal information. See Murphy, R. S. (1996). "Property rights in personal information: An economic defense of privacy" *Georgetown Law Journal* 84: 2383.

[1226] See Mai., J. E. (2016). "Big data privacy: The datafication of personal information" *The Information Society* 32(3): 195. Available at https://doi.org/10.1080/01972243.2016.1153010. Accessed 5 July 2020.

A quick *Google* search about a professional tennis player can lead someone to a *Wikipedia* page containing personal information about the tennis.[1227] If a narrow interpretation is followed, only information that is distinctive to an individual constitutes personal information. Examples include an identity (ID) number, a person's name, or blood type.[1228]

A closer look at the definition of personal data suggests that there should be a link between the person and their data. If the information cannot readily identify the person, it is likely that such information does not constitute personal data. It is possible to link data to a person through a process called identification. According to Solove, identification is the process of "connecting information to individuals".[1229] With identification, a person is unable to remain anonymous.[1230] For example, a person can voluntarily reveal personal information about themselves when conducting online transactions. The information can be used in future to identify the same person that made the transaction.

4.5 The uses of personal information

4.5.1 Public use of personal information

Public bodies generally collect personal information for purposes of governance.[1231] In order for a government to provide basic services to its people, it requires information about its citizens. Often, the degree of service delivery is subject to the production of

[1227] This brings an important issue relating to collection of personal information. It cannot be said that obtaining common knowledge about famous persons from a public constitutes an invasion of privacy because the nature and scope of the famous' person's profession necessitates availing personal information about oneself. Even if a journalist conducts an interview with that famous person and learns new information previously not known to the public, the collection of information may not necessarily infringe that person's privacy.

[1228] See Mai., J. E. (2016). "Big data privacy: The datafication of personal information" *The Information Society* 32(3): 195. Available at https://doi.org/10.1080/01972243.2016.1153010. Accessed 5 July 2020.

[1229] Solove, D., J. (2008). *Understanding Privacy* Harvard University Press at 122.

[1230] Solove, D., J. (2008). *Understanding Privacy* Harvard University Press at 125.

[1231] Grayson, B. (2006). "Personal Information in Government Records: Protecting the Public Interest in Privacy" *Saint Louis University Public Law Review* 25(1): 63. Available at: https://scholarship.law.slu.edu/plr/vol25/iss1/6. Accessed 15 July 2020; see also Solove, D. J. (2002). "Access and aggregation: Public records, privacy and the constitution" *Minnesota Law Review* 86(6): 1137 – 1218.

accurate information provided by an individual.[1232] For this reason, government agencies retain personal information relating to its citizens.[1233] Personal information kept by the government includes information such as a person's weight, height, nationality, residence, location, property, and family life.[1234] The retention of personal information does not end there. If a person wants to conduct business with the government,[1235] or import goods to their country,[1236] that person is often required to furnish additional information such bank details, a telephone number, and a physical address.[1237] On other occasions, personal information may be required by the government for purposes of law enforcement.[1238] In order to combat serious crimes such as child pornography, drug trafficking, fraud, and cybercrime, personal information may be required by law enforcement agencies.[1239] The aftermath of the

[1232] For example, the South African Birth and Death Registration Act 51 of 1992 (BDR Act) states that the Director General of the Department of Home Affairs is the custodian of all records pertaining to all births and deaths in South Africa. Similarly, the birth of a child born in South Africa must be duly registered in terms of the BDR Act. The registration of a child's birth is contingent of the provision of personal information relating to the child's parents. Such information includes biometrics and the name of child's parents. Failure to provide adequate information may lead to the delay in the registration of a child's birth. If a child's birth is not registered with the State, that child may grow up without an identity document precluding the latter from accessing basic education, health and later in life tertiary education, access to housing, inability to access credit, loans and so on.

[1233] Grayson, B. (2006). "Personal Information in Government Records: Protecting the Public Interest in Privacy" *Saint Louis University Public Law Review* 25(1): 63. Available at: https://scholarship.law.slu.edu/plr/vol25/iss1/6. Accessed 15 July 2020.

[1234] Solove, D. J. (2002). "Access and aggregation: Public records, privacy and the constitution" *Minnesota Law Review* 86(6): 1139.

[1235] Grayson, B. (2006). "Personal Information in Government Records: Protecting the Public Interest in Privacy" *Saint Louis University Public Law Review* 25(1): 64. Available at: https://scholarship.law.slu.edu/plr/vol25/iss1/6. Accessed 15 July 2020.

[1236] SARS requires individuals importing goods into South Africa to obtain an importers code. In terms of the Regulations, a person may not import more than 3 items or products to the combined value of R50 000 in a full calendar year unless they have an importers code. What this means in simple terms is that a person cannot buy (import) more than 3 goods from outside South Africa. To obtain additional goods, such a person must register as an importer in the Republic. In addition to providing SARS with their ID, physical address, telephone number and bank statements, that person may have to register a company just to obtain physical goods from outside the Republic. See sections 59A and 120 of the Customs and Excise Act 91 of 1964 read with Government Gazette No. 36433 of 10 May 2013.

[1237] According to Volmink, it may be safer to avoid doing business with the government due to the inherent risks such as a lack of indemnity and the inability of government s to honour contractual obligations. See Volmink, P. (2020). *"Is it safe to do business with government?"* Available at https://www.news24.com/fin24/opinion/opinion-is-it-safe-to-do-business-with-government-20200127. Accessed 15 June 2020.

[1238] Solove, D. J., (2004). *The digital person: technology and privacy in the information age* New York University Press at 5; Abdulrauf, L., A., (2015). *The Legal Protection of Data Privacy in Nigeria: Lessons from Canada and South Africa* Unpublished LLD thesis (University of Pretoria) at 34.

[1239] Solove, D. J., (2004). *The digital person: technology and privacy in the information age* New York University Press at 5.

September 11 terrorist attacks has incentivised governments' resolve to collect personal information. The data collected assists the government in putting preventative and security measures against possible terrorist attacks.[1240]

Recently, the COVID-19 pandemic has led to the collection of personal information by governments. In April 2020, the South African government partnered with *Vodacom* to collect personal data during the global COVID-19 pandemic.[1241] Mobile phones containing pre-installed applications (Apps) were distributed to South African healthcare workers. During screening for COVID-19 symptoms, the healthcare workers input real-time patient data, including a patient's geolocation, for purposes of tracking and tracing.[1242]

The Internet revolution has facilitated the integration of technological advancements into the public sector. The provision of conventional services to citizens occurs over the counter at government offices.[1243] Often, service delivery is delayed or made inefficient by government workers. This can result in long queues for access to basic services. On other occasions, people are left frustrated by government officials especially when they are informed that the system collapses due to technical issues.[1244] These challenges are often caused by the centralised nature of government infrastructure. The implementation of an e-government system can reduce government inefficiencies and promote efficient service delivery by increasing access

[1240] Solove, D. J., (2004). *The digital person: technology and privacy in the information age* New York University Press at 5. See also Abdulrauf, L., A., (2015). *The Legal Protection of Data Privacy in Nigeria: Lessons from Canada and South Africa* Unpublished LLD thesis (University of Pretoria) at 35.

[1241] See https://www.youtube.com/watch?v=7p3DhOn3Kp4. Accessed 12 November 2023.

[1242] See https://www.youtube.com/watch?v=7p3DhOn3Kp4. Accessed 12 November 2023. According to the OECD, telecommunication companies make use of what is known as call data records (CDRs). These enable "data produced by telecommunication service providers on telephone calls or other telecommunications transactions, which provide valuable insights into population movements. As network operators serve substantial portions of the population across entire nations, the movements of millions of people at fine spatial and temporal scales can be measured in near real-time. The resulting information and trends are invaluable for governments seeking to track the COVID-19 outbreak, warn vulnerable communities, and understand the impact of policies such as social distancing and confinement." See https://www.oecd.org/coronavirus/policy-responses/tracking-and-tracing-covid-protecting-privacy-and-data-while-using-apps-and-biometrics-8f394636/. Accessed 15 July 2020.

[1243] Basu, S. (2004). "E-government and developing countries: an overview" *International Review of Law, Computers & Technology* 18(1): 112. Available at https://doi.org/10.1080/13600860410001674779. Accessed 15 July 2020.

[1244] A popular phrase used by government officials is that they system is 'offline'.

to better government services, reducing administrative costs, improving accountability, and promoting transparency.[1245] With the implementation of e-government and information communication technology (ICT) services,[1246] government's interconnectedness can facilitate the dissemination of personal information between government agencies.[1247] There are instances where personal information can be collected by government agencies. Technological advancements can facilitate electronic transactions between government agencies and citizens. The frequency of these transactions makes it possible for governments to establish customer trends to identify where services should be improved.[1248]

4.5.2 Private use of personal information

In contrast to the public sector, the private sector's use of personal information hinges primarily on marketing and money.[1249] The use of personal data by private actors is not a new phenomenon. In fact, the use of personal information for private use started before the dawn of the Internet.[1250] Conventional marketing was predominantly orchestrated by word of mouth or by shopkeepers visiting their customers to sell their products.[1251] The advent of the Internet has coincided with the increased distribution

[1245] Basu, S. (2004). "E-government and developing countries: an overview" *International Review of Law, Computers & Technology* 18(1): 109 – 111. Available at https://doi.org/10.1080/13600860410001674779. Accessed 15 July 2020.

[1246] In as much as the use of ICT services may be widespread in developed countries, the opposite is also accurate for developing countries. A lack of trust in the government, political stability or instability, government structure, demand, and economic structure are some of the factors Basu mentions as key factors in the establishment of an e-government. Additionally, factors like political will or the lack thereof, budget deficits, inequality, corruption, crime, social issues and a lack of proper regulatory framework have a significant bearing on the implementation of an e-government system in developing countries. Even if such a system where to be implemented, there is a presupposition that most citizens will have access to this system. This is not entirely accurate especially where most citizens do not have access to basic services such as healthcare and education. The creation of an e-government in system will necessitate improved public education on the use of ICT services, better IT infrastructure, trust in government and effective regulatory mechanisms that ensure the protection of data privacy for citizens.

[1247] Basu, S. (2004). "E-government and developing countries: an overview" *International Review of Law, Computers & Technology* 18(1): 123. Available at https://doi.org/10.1080/13600860410001674779. Accessed 15 July 2020.

[1248] Basu, S. (2004). "E-government and developing countries: an overview" *International Review of Law, Computers & Technology* 18(1): 124. Available at https://doi.org/10.1080/13600860410001674779. Accessed 15 July 2020.

[1249] Solove, D. J., (2004). *The digital person: technology and privacy in the information age* New York University Press at 16.

[1250] Rubin, P., H. & Thomas, M., L. (2002). *Privacy and the Commercial use personal information* Springer (New York) at xii.

[1251] Solove, D. J., (2004). *The digital person: technology and privacy in the information age* New York University Press at 16.

of personal information. The effect is that increased information has been made available online. Advertising companies use the Internet as a market hub to obtain customer information. By observing customer activities online, advertising companies can predict consumer behaviour and choices before conveying the necessary advertisements.[1252]

To access a financial product or purchase financial services, financial institutions require people to prove their identity.[1253] Recently, there has been a trend by banks to operate online and provide online digital services.[1254] Irrespective of how a financial institution operates, financial institutions have the propensity to collect and share personal information to third parties. Personal information such as credit score, income, physical address, and spending habits are all known to a person's bank. While this information may not necessarily be of value to banks *per se*, it is valuable to other private actors like advertising companies. Selling personal information to these companies generates money for banks.[1255]

Credit bureaus provide credit reporting services to people. Credit reporting has become an important service for credit lenders.[1256] The provision of credit to individuals can be beneficial to governments and to the economy because it promotes financial inclusion, particularly in developing countries.[1257] Conducting a credit risk assessment is a rigorous process that includes verifying employment history, identifying a person, and detecting fraud.[1258] In the US, credit bureaus play a huge

[1252] Rubin, P., H. & Thomas, M., L. (2002). *Privacy and the Commercial use personal information* Springer (New York) at xii.

[1253] This is a requirement established in terms of section 21 of the Financial Intelligence Centre Act 38 of 2001.

[1254] In South Africa, TymeBank became South Africa's first digital online bank. See https://thepaypers.com/expert-opinion/tymebank-the-first-digital-only-bank-in-south-africa--780573. Accessed 17 July 2020.

[1255] See Thompson, A. (2019). "Banks and financial apps in South Africa are sharing your personal information - here's how to stop them" *Business Insider SA.* Available at https://www.businessinsider.co.za/banking-apps-share-your-information-2019-11. Accessed 17 July 2020.

[1256] Rubin, P., H. & Thomas, M., L. (2002). *Privacy and the Commercial use personal information* Springer (New York) at 12.

[1257] See https://compuscan.co.za/2020/02/17/how-a-credit-bureau-affects-financial-inclusion/. Accessed 17 July 2020. According to Rubin and Thomas, the provision of credit to any individual is contingent on the availability of personal information. See Rubin, P., H. & Thomas, M., L. (2002). *Privacy and the Commercial use personal information* Springer (New York) at 11.

[1258] See Christl, W., (2017). "How Companies use personal data against people: Automated disadvantage, personalized persuasion, and the societal ramifications of the commercial use of part in people's lives due to credit bureau's extended coverage. A bureau's centralised nature enables it to store vast amounts of personal data. Often, these credit bureaus obtain personal data from insurance companies, banks, lenders, credit card companies and telecommunication companies.[1259]

4.6 Concerns relating to data privacy

4.6.1 Surveillance

The surveillance of personal data is not new. In fact, surveillance has traditionally taken place physically.[1260] The traditional forms of surveillance included placing guards at the top of observation towers while sophisticated forms include the use of microphones and cameras.[1261] Technology has enhanced surveillance to greater heights. With technology at the forefront, private corporations and other actors have found new ways to conduct surveillance on people. For example, surveillance can take place through directed means like observation on closed-circuit television (CCTV); through automation on mobile telecommunications platforms; or when done voluntarily by people giving their information on social media platforms.[1262]

personal information" *working paper by Cracked Labs* at 11. Available at https://crackedlabs.org/dl/CrackedLabs_Christl_DataAgainstPeople.pdf. Accessed 16 July 2020.

[1259] Rubin, P., H. & Thomas, M., L. (2002). *Privacy and the Commercial use personal information* Springer (New York) at 12; See Christl, W., (2017). "How Companies use personal data against people: Automated disadvantage, personalized persuasion, and the societal ramifications of the commercial use of personal information" *working paper by Cracked Labs* at 11. Available at https://crackedlabs.org/dl/CrackedLabs_Christl_DataAgainstPeople.pdf. Accessed 16 July 2020; see also Christl, W. (2017). "Corporate Surveillance in Everyday Life." Report by Cracked Labs June 2017. Available at: http://crackedlabs.org/en/corporate-surveillance. Accessed 18 July 2020.

[1260] See Clarke, R., (1994). "The Digital Persona and its Application to Data Surveillance." Available at http://www.rogerclarke.com/DV/DigPersona.html#DV. Accessed 5 August 2020.

[1261] See Clarke, R., (1994). "The Digital Persona and its Application to Data Surveillance." Available at http://www.rogerclarke.com/DV/DigPersona.html#DV. Accessed 5 August 2020.

[1262] Lyon, D. (2014). "Surveillance, Snowden, and Big Data: Capacities, consequences, critique" *Big Data and Society* at 5. Available at https://journals.sagepub.com/doi/pdf/10.1177/2053951714541861. Accessed 5 August 2020.

Data surveillance[1263] is a new way of monitoring and surveillance using technological methods.[1264] Data surveillance can be extended to incorporate data collection.[1265] Solove opines that surveillance is intrusive of people's privacy because observation by other natural persons facilitates judgments that have the propensity to influence a person's life.[1266] While it is true that personal information can be made public, the sharing of information that one considers 'secret' leads to a more severe form of privacy encroachment.[1267]

The intrusive nature of surveillance highlights the need to balance between a person's right to privacy and the need for a country to protect its citizens.[1268] For example, information obtained in a public domain can be useful to crime combating agencies for the prevention of a crime. Countries and government agencies can exceed the bounds of surveillance for reasons unknown to the public. Government's justification for surveillance is often couched in the notion that 'citizens must be protected'. For example, in 2013, *Edward Snowden* disclosed documents to media outlets that purported to show massive widespread surveillance orchestrated by the Federal Bureau of Investigation (FBI) and the National Security Agency (NSA).[1269] The surveillance was made possible because these security agencies had direct access to servers belonging to telecommunications and social media companies.[1270]

[1263] Clarke defines 'data surveillance' as the "systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons." Clarke goes on to define two types of data surveillance. Firstly, personal surveillance occurs when an identifiable person is monitored for a specific purpose. Secondly, mass surveillance where a large group of identified persons are monitored to identify persons of interest to an organisation. See Clarke, R., (1994). "The Digital Persona and its Application to Data Surveillance." Available at http://www.rogerclarke.com/DV/DigPersona.html#DV. Accessed 5 August 2020.

[1264] Solove, D. J., (2004). *The digital person: technology and privacy in the information age* New York University Press at 32 – 33.

[1265] Solove, D. J., (2004). *The digital person: technology and privacy in the information age* New York University Press at 33.

[1266] Solove, D. J., (2004). *The digital person: technology and privacy in the information age* New York University Press at 34.

[1267] Solove, D. J., (2004). *The digital person: technology and privacy in the information age* New York University Press at 16. For this reason, and in as much surveillance is intrusive it may reveal important information about an individual. The information collected by security agencies can help with the prevention of crimes like terrorism.

[1268] See Abdulrauf, L., A., (2015). *The Legal Protection of Data Privacy in Nigeria: Lessons from Canada and South Africa* Unpublished LLD thesis (University of Pretoria) at 44.

[1269] Lyon, D. (2014). "Surveillance, Snowden, and Big Data: Capacities, consequences, critique" *Big Data and Society* at 2. Available at https://journals.sagepub.com/doi/pdf/10.1177/2053951714541861. Accessed 5 August 2020.

[1270] Lyon, D. (2014). "Surveillance, Snowden, and Big Data: Capacities, consequences, critique" *Big Data and Society* at 2. Available at https://journals.sagepub.com/doi/pdf/10.1177/2053951714541861. Accessed 5 August 2020.

4.6.2 Identity theft

The proliferation of Internet use has resulted in the electronic collection of data. Consequently, the appropriation of financial and identity theft has become prevalent.[1271] The anonymous nature of the Internet has enabled attackers to pry and steal people's identities.[1272] The appropriation of information often takes place when an individual conducts e-commerce transaction, surfs the web, banks online or visits gaming websites.[1273]

In the past, fraudsters retrieved a person's information by going through their garbage to obtain discarded documents like phone bills or bank statements.[1274] Other methods include stealing people's wallets, breaking into residential homes in order to retrieve personal information, and bribing employees at government facilities to access private records that contain personal information.[1275] Extreme measures include perpetrators posing as bank officials in order to retrieve personal information from unsuspecting

[1271] Milne, G., *et al* (2004). "Consumers' Protection of Online Privacy and Identity" *The Journal of Consumer Affairs* 38(2): 217.

[1272] Cassim, F. (2015). "Protecting Personal Information in the era of Identity Theft: Just How Safe is our Personal Information from identity thieves?" *Potchefstroom Electronic Law Journal* 18(2): 69.

[1273] Milne, G., *et al* (2004). "Consumers' Protection of Online Privacy and Identity" *The Journal of Consumer Affairs* 38(2): 217; Cassim, F. (2015). "Protecting Personal Information in the era of Identity Theft: Just How Safe is our Personal Information from identity thieves?" *Potchefstroom Electronic Law Journal* 18(2): 71; Aïmeur, E., & Schőnfeld, D. (2011). "The ultimate invasion of privacy: Identity theft" *2011 Ninth Annual International Conference on Privacy, Security and Trust* at 1. Available at https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5971959&casa_token=U2s7CN1Sa1QAAAAA:wAzrdGlSn_pY2T4FCAlp80-uUeu4xz_IXH9TXQJtyqwqSpTSRlkFef5taOkf5Lgchq5wB50k7ZfM&tag=1. Accessed 5 August 2020.

[1274] Aïmeur, E., & Schőnfeld, D. (2011). "The ultimate invasion of privacy: Identity theft" *2011 Ninth Annual International Conference on Privacy, Security and Trust* at 5. Available at https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5971959&casa_token=U2s7CN1Sa1QAAAAA:wAzrdGlSn_pY2T4FCAlp80-uUeu4xz_IXH9TXQJtyqwqSpTSRlkFef5taOkf5Lgchq5wB50k7ZfM&tag=1. Accessed 5 August 2020; Newman, G., R. (2004). *Identity Theft* US Department of Justice at 12. Available at https://secure.goozmo.com/user_files/19180.pdf. Accessed 15 August 2020; Perl, M. W. (2003). "It's not always about the money: Why the state identity theft laws fail to adequately address criminal record identity theft" *Journal of Criminal Law & Criminology* 94(1): 173; Federal Trade Commission (2003). "ID Theft: When Bad Things Happen to your Good Name" at 3. Available at http://www.iwar.org.uk/ecoespionage/resources/id-theft/idtheft.pdf. Accessed 15 August 2020.

[1275] Newman, G., R. (2004). *Identity Theft* US Department of Justice at 12. Available at https://secure.goozmo.com/user_files/19180.pdf. Accessed 15 August 2020.

victims.[1276] With technological advancements, new online methods of identity theft have come to the fore. It is now possible to steal personal information through techniques such as typo squatting,[1277] phishing,[1278] keyloggers,[1279] spamming,[1280] pharming,[1281] sniffing,[1282] and screen logging.[1283]

[1276] Aïmeur, E., & Schőnfeld, D. (2011). "The ultimate invasion of privacy: Identity theft" *2011 Ninth Annual International Conference on Privacy, Security and Trust* at 5. Available at https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5971959&casa_token=U2s7CN1Sa1QAAAAA:wAzrdGlSn_pY2T4FCAlp80-uUeu4xz_IXH9TXQJtyqwqSpTSRlkFef5taOkf5Lgchq5wB50k7ZfM&tag=1. Accessed 5 August 2020; Perl, M. W. (2003). "It's not always about the money: Why the state identity theft laws fail to adequately address criminal record identity theft" *Journal of Criminal Law & Criminology* 94(1): 173; Federal Trade Commission (2003). "ID Theft: When Bad Things Happen to your Good Name" at 3. Available at http://www.iwar.org.uk/ecoespionage/resources/id-theft/idtheft.pdf. Accessed 15 August 2020.

[1277] Moore and Eldeman define typosquatting as the "intentionally registering misspellings of popular websites in anticipation that users mistype those domains and reach squatters' sites." See Moore, T. & Edelman, B., (2010). "Measuring the Perpetrators and Funders of Typosquatting" 14th International Conference on Financial Cryptography and Data Security at 1. Available at https://www.benedelman.org/typosquatting/typosquatting.pdf. Accessed 15 August 2020.

[1278] According to Sullins, phishing is "a form of online identity theft that uses fraudulent e-mails to trick recipients into divulging personal financial information on fraudulent imitation websites." See Sullins, L. L. (2006). "Phishing for solution: Domestic and international approaches to decreasing online identity theft" *Emory International Law Review* 20(1): 397 – 398. See also Cassim, F. (2015). "Protecting Personal Information in the era of Identity Theft: Just How Safe is our Personal Information from identity thieves?" *Potchefstroom Electronic Law Journal* 18(2): 74.

[1279] According to Emigh, keyloggers "are programs that install themselves either into a web browser or as a device driver and monitor data being input and send relevant data to a phishing server." See Emigh, A. (2006). "The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond" *Journal of Digital Forensic Practice* 1(3): 248.

[1280] Generally, a spam consists of unsolicited e-mails targeted towards a specific person or group of persons.

[1281] Pharming is a process whereby an attacker changes an actual website's gateway, interfering with the domain name in order to obtain all information. See Emigh, A. (2006). "The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond" *Journal of Digital Forensic Practice* 1(3): 250; Aïmeur, E., & Schőnfeld, D. (2011). "The ultimate invasion of privacy: Identity theft" *2011 Ninth Annual International Conference on Privacy, Security and Trust* at 5. Available at https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5971959&casa_token=U2s7CN1Sa1QAAAAA:wAzrdGlSn_pY2T4FCAlp80-uUeu4xz_IXH9TXQJtyqwqSpTSRlkFef5taOkf5Lgchq5wB50k7ZfM&tag=1. Accessed 5 August 2020.

[1282] Sniffing is technique that enables an attacker to interrupt communication on a network. See Aïmeur, E., & Schőnfeld, D. (2011). "The ultimate invasion of privacy: Identity theft" *2011 Ninth Annual International Conference on Privacy, Security and Trust* at 5. Available at https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5971959&casa_token=U2s7CN1Sa1QAAAAA:wAzrdGlSn_pY2T4FCAlp80-uUeu4xz_IXH9TXQJtyqwqSpTSRlkFef5taOkf5Lgchq5wB50k7ZfM&tag=1. Accessed 5 August 2020; see also Potnuru, M., (2012). "Limits of the Federal Wiretap Act's Ability to Protect Against Wi-Fi Sniffing" *Michigan Law Review* 111(1): 89 – 117.

[1283] A screenlogger is a form of crimeware "that take snapshots of the user interface regularly, or when a connection to a secured web site starts." See Aïmeur, E., & Schőnfeld, D. (2011). "The ultimate invasion of privacy: Identity theft" *2011 Ninth Annual International Conference on Privacy, Security and Trust* at 5. Available at https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5971959&casa_token=U2s7CN1Sa1QAAAAA:wAzrdGlSn_pY2T4FCAlp80-

One other prominent method of appropriating personal information is through malware[1284] infections.[1285]

Identity theft occurs when a person's personal identifying information is used to commit theft or fraud.[1286] The attacker collects an individual's identifying information from government records, company databases, e-mails, discarded items and hacking social media platforms.[1287] All these sources contain vital information that can easily be accessed by attackers. For example, *Sony Pictures Entertainment* was hacked in 2014 by a group of hackers who stole personal and confidential information belonging

uUeu4xz_IXH9TXQJtyqwqSpTSRlkFef5taOkf5Lgchq5wB50k7ZfM&tag=1. Accessed 5 August 2020. See also Emigh, A. (2006). "The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond" *Journal of Digital Forensic Practice* 1(3): 245 – 260.

[1284] A malware is an "unwanted software that running on a user's computer that performs malicious actions." See See also Emigh, A. (2006). "The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond" *Journal of Digital Forensic Practice* 1(3): 246.

[1285] Aïmeur, E., & Schőnfeld, D. (2011). "The ultimate invasion of privacy: Identity theft" *2011 Ninth Annual International Conference on Privacy, Security and Trust* at 5 - 6. Available at https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5971959&casa_token=U2s7CN1Sa1QAAAAA:wAzrdGlSn_pY2T4FCAlp80-uUeu4xz_IXH9TXQJtyqwqSpTSRlkFef5taOkf5Lgchq5wB50k7ZfM&tag=1. Accessed 5 August 2020.

[1286] Aïmeur, E., & Schőnfeld, D. (2011). "The ultimate invasion of privacy: Identity theft" *2011 Ninth Annual International Conference on Privacy, Security and Trust* at 1 - 2. Available at https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5971959&casa_token=U2s7CN1Sa1QAAAAA:wAzrdGlSn_pY2T4FCAlp80-uUeu4xz_IXH9TXQJtyqwqSpTSRlkFef5taOkf5Lgchq5wB50k7ZfM&tag=1. Accessed 5 August 2020; Solove, D. J. (2002). "Identity theft, privacy, and the architecture of vulnerability" *Hastings Law Journal* 54(4): 1243; Cassim, F. (2015). "Protecting Personal Information in the era of Identity Theft: Just How Safe is our Personal Information from identity thieves?" *Potchefstroom Electronic Law Journal* 18(2): 69 – 74. The OECD defines 'identity theft' as "when a party acquires, transfers, possesses, or uses personal information of a natural or legal person in an unauthorised manner, with the intent to commit, or in connection with, fraud or other crimes." See OECD (2008). "Scoping Paper on Online Identity Theft" at 3. Available at http://www.oecd.org/internet/consumer/40644196.pdf. Accessed 6 August 2020. The United States General Accounting Office (GAO) defines 'identity theft' as the "stealing of another person's personal identifying information— such as Social Security number (SSN), date of birth, and mother's maiden name—and then using the information to fraudulently establish credit, run up debt, or take over existing financial accounts." See GAO (2002). "Identity Theft: Greater Awareness and Use of Existing Data Are Needed" at 1. Available at https://www.gao.gov/assets/240/234959.pdf. Accessed 6 August 2020; Perl, M. W. (2003). "It's not always about the money: Why the state identity theft laws fail to adequately address criminal record identity theft" *Journal of Criminal Law & Criminology* 94(1): 173.

[1287] Solove, D. J. (2002). "Identity theft, privacy, and the architecture of vulnerability" *Hastings Law Journal* 54(4): 1244; Aïmeur, E., & Schőnfeld, D. (2011). "The ultimate invasion of privacy: Identity theft" *2011 Ninth Annual International Conference on Privacy, Security and Trust* at 2 - 3. Available at https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5971959&casa_token=U2s7CN1Sa1QAAAAA:wAzrdGlSn_pY2T4FCAlp80-uUeu4xz_IXH9TXQJtyqwqSpTSRlkFef5taOkf5Lgchq5wB50k7ZfM&tag=1. Accessed 5 August 2020.

to *Sony Pictures* employees.[1288] The motive for the hack and subsequent theft was unknown but it appears as if the hack was conducted in order to prevent the release of a movie that portrayed an assassination plot against the then North Korean leader.[1289] A person's identity can also be stolen in order to commit a criminal act or to use a victim's identity in order to obtain medical treatment.[1290]

The impact posed by identity theft is not limited to economic loss but also extends to psychological harm.[1291] This is due to the constant demand for victims to fix the damage caused by attackers. When a person's identity is stolen, it takes years for the victim to recover their identity.[1292] This is partly because an attacker taints a victim's identity by accumulating inaccurate information such as criminal offences or bad debt on the victim's identity.[1293]

4.6.3 Data mining

Data mining is the process of "analysing data in order to discover previously unknown relationships among the variables contained in a database."[1294] Put differently, the

[1288] See https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/. Accessed 6 August 2020.

[1289] See https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/. Accessed 6 August 2020.

[1290] Aïmeur, E., & Schőnfeld, D. (2011). "The ultimate invasion of privacy: Identity theft" *2011 Ninth Annual International Conference on Privacy, Security and Trust* at 2. Available at https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5971959&casa_token=U2s7CN1Sa1QAAAAA:wAzrdGlSn_pY2T4FCAlp80-uUeu4xz_IXH9TXQJtyqwqSpTSRlkFef5taOkf5Lgchq5wB50k7ZfM&tag=1. Accessed 5 August 2020.

[1291] Solove, D. J. (2002). "Identity theft, privacy, and the architecture of vulnerability" *Hastings Law Journal* 54(4): 1244; Cassim, F. (2015). "Protecting Personal Information in the era of Identity Theft: Just How Safe is our Personal Information from identity thieves?" *Potchefstroom Electronic Law Journal* 18(2): 75; Lynch, J. (2005). "Identity theft in cyberspace: Crime control methods and their effectiveness in combating phishing attacks" *Berkeley Technology Law Journal* 20(1): 263 – 264.

[1292] Solove, D. J. (2002). "Identity theft, privacy, and the architecture of vulnerability" *Hastings Law Journal* 54(4): 1244; Cassim, F. (2015). "Protecting Personal Information in the era of Identity Theft: Just How Safe is our Personal Information from identity thieves?" *Potchefstroom Electronic Law Journal* 18(2): 75; Lynch, J. (2005). "Identity theft in cyberspace: Crime control methods and their effectiveness in combating phishing attacks" *Berkeley Technology Law Journal* 20(1): 264.

[1293] Solove, D. J. (2002). "Identity theft, privacy, and the architecture of vulnerability" *Hastings Law Journal* 54(4): 1244.

[1294] Winn, J., & Wrathall, J. R. (2000). "Who owns the customer the emerging law of commercial transactions in electronic customer data" *Business Lawyer* (ABA) 56(1): 235; Kianieff, M. (2019) *Blockchain Technology and the Law Opportunities and Risks* Routledge Publishing (UK) at 158; Himma, K., E., & Tavani, H., T., (eds) (2008). *The Handbook of Information and Computer* data retrieved by any entity or corporation can be used to ascertain links and details about an individual that would otherwise be unknown. For example, an e-commerce business can analyse a customer's previous purchases on its website and conclude that the customer is probably a student. The business can use a customer's order history to make that inference.[1295] According to Winn and Wrathall, data mining can also reveal the "chronological sequence of events; facilitate the classification of data according to newly recognized patterns such as customer profiles; allow clustering of data into groups not previously known and forecast based on newly discovered patterns that aid prediction."[1296]

It is easier to conduct data mining[1297] if a business has large storage facilities. The storage facilities consist of consolidated databases that are generally used for processing information intended for marketing and sales.[1298] Businesses use the warehouses as central archives where all important data is stored and collected.[1299] The data is often collected from numerous sources such as marketing and finance,[1300] to online transactions. The data is then carefully chosen and categorised into data warehouses to be accessed at a later stage by analytical applications.[1301]

Data warehousing is beneficial because it enables entities to store vast amounts of data without relying on innovative technological advancements. Emphasis is placed

Ethics Wiley publishing at 153; Kianieff, M. (2012) "The Evolution of Consumer Privacy Law: How Privacy by Design Can Benefit from Insights in Commercial Law and Standardization" *Canadian Journal of Law and Technology* 10(1): 3.

[1295] Winn, J., & Wrathall, J. R. (2000). "Who owns the customer the emerging law of commercial transactions in electronic customer data" *Business Lawyer* (ABA) 56(1): 235.

[1296] Winn, J., & Wrathall, J. R. (2000). "Who owns the customer the emerging law of commercial transactions in electronic customer data" *Business Lawyer* (ABA) 56(1): 235

[1297] According to Tavani, data mining entails combining statistical analysis, data visualization, pattern recognition, artificial intelligence and knowledge acquisition from expert systems. See Tavani, H., T., (1999). "Informational privacy, data mining, and the Internet" *Ethics and Information Technology* at 137.

[1298] Tavani, H., T., (1999). "Informational privacy, data mining, and the Internet" *Ethics and Information Technology* at 142.

[1299] Kianieff, M. (2012) "The Evolution of Consumer Privacy Law: How Privacy by Design Can Benefit from Insights in Commercial Law and Standardization" *Canadian Journal of Law and Technology* 10(1): 3; Winn, J., & Wrathall, J. R. (2000). "Who owns the customer the emerging law of commercial transactions in electronic customer data" *Business Lawyer* (ABA) 56(1): 235.

[1300] See Gupta, V., R. (1997). "Whitepaper: Introduction to Data Warehousing" http://www.sserve.com/dwintro.asp. Accessed 22 August 2020.

[1301] Winn, J., & Wrathall, J. R. (2000). "Who owns the customer the emerging law of commercial transactions in electronic customer data" *Business Lawyer* (ABA) 56(1): 235.

on storing data on a standard computer.[1302] However, difficulties arise when private entities and governments collect personal information without people's knowledge.[1303] The collection of data is often done to establish consumer spending habits and to conduct unwanted marketing.[1304] This is made possible because corporations use mechanisms that can predict human behaviour.[1305] The data collected is given to third parties in exchange for money.[1306] Governments can use data mining techniques to identify criminal intent from the analysis of data collected from various sources. This enhances government's chances of preventing alleged perpetrators before a crime takes place.[1307]

4.6.4 Data profiling

Data profiling is the compilation of information dossiers about individuals to determine their interests by making a correlation with other profiles and data.[1308] Data profiling is mainly used to forecast consumer behaviour.[1309] Due to its predictive analysis components, data profiling is used to target individuals for marketing purposes. Individuals often get inundated with unsolicited e-mails and adverts from marketing companies.[1310] Data profiling is not exclusive to e-commerce companies. Telecommunication companies, supermarkets and even banks collate information regarding consumer purchases.[1311] With sensitive information at their disposal, companies easily target specific individuals by using adverts or promotions without the

[1302] Kianieff, M. (2019) *Blockchain Technology and the Law Opportunities and Risks* Routledge Publishing (UK) at 158.

[1303] Tavani, H., T., (1999). "Informational privacy, data mining, and the Internet" *Ethics and Information Technology* at 138.

[1304] Kianieff, M. (2019) *Blockchain Technology and the Law Opportunities and Risks* Routledge Publishing (UK) at 158.

[1305] Solove, D., J. (2008). *Understanding Privacy* Harvard University Press at 191.

[1306] Kianieff, M. (2019) *Blockchain Technology and the Law Opportunities and Risks* Routledge Publishing (UK) at 158.

[1307] Solove, D., J. (2008). *Understanding Privacy* Harvard University Press at 192.

[1308] Ziegeldorf, J. H., Morchon, O., G., & K., Wehrle (2013). "Privacy in the Internet of Things: Threats and challenges" *Security and Communications Network* at 2735.

[1309] McClurg, A., J., (2003). "A thousand words are worth a Picture: A Privacy tort response to consumer data profiling" *Northwestern University Law Review* 98(1): 66.

[1310] Ziegeldorf, J. H., Morchon, O., G., & K., Wehrle (2013). "Privacy in the Internet of Things: Threats and challenges" *Security and Communications Network* at 2735.

[1311] McClurg, A., J., (2003). "A thousand words are worth a Picture: A Privacy tort response to consumer data profiling" *Northwestern University Law Review* 98(1): 66 – 67.

latter's prior consent. Not only does this technique result in gratuitous adverts and e-mails, but it can also lead to price discrimination.[1312]

4.6.5 Datafication

During the last decade, there has been a rise in social media usage. Sites like *Facebook*, *Instagram,* and *X*[1313] have popularised online social interactions. People's behaviour on network sites has changed to the extent that it is now possible to determine a person's interests. This can be seen from the way a person interacts with social events and other people. For example, the sharing of intimate moments and experiences with a certain group of people suggests that the group is intimately related to the sender.

Social media companies began to 'codify' or 'datafy'[1314] people's social activities by collecting and monitoring behaviour on social media platforms, apps, tablets, and mobile phones.[1315] Previously, it was difficult to quantify a person's interests, information searches, emotional responses, "likes" and even friends.[1316] This became possible through a process called datafication. Datafication is the process of collecting and transforming social interactions and behaviours into quantifiable data.[1317] The data is then processed, tracked, and analysed for various uses. Governments use this data to track human behaviour while corporations use the data to predict human

[1312] See Stepanek, M. (2000) "Weblining." Available at https://www.bloomberg.com/news/articles/2000-04-02/weblining. Accessed 7 September 2020; Odlysko, A. (2003) *"Privacy, Economics, and Price Discrimination on the Internet"*. Available at https://dl.acm.org/doi/pdf/10.1145/948005.948051. Accessed 12 December 2022.

[1313] Previously 'Twitter'.

[1314] See Mai, J., E. (2016). "Big Data privacy: The datafication of personal information" *The information society* 32(3): 193.

[1315] Van Dijk, J. (2014). "Datafication, dataism and dataveillance: Big Data between paradigm and ideology" *Surveillance and Society* 12(2): 198; Meijas, U., A. & Couldry, N. (2019). "Datafication" *Internet Policy Review* 8(4): 1 – 3.

[1316] Van Dijk, J. (2014). "Datafication, dataism and dataveillance: Big Data between paradigm and ideology" *Surveillance and Society* 12(2): 198.

[1317] Mai, J., E. (2016). "Big Data privacy: The datafication of personal information" *The information society* 32(3): 193; Van Dijk, J. (2014). "Datafication, dataism and dataveillance: Big Data between paradigm and ideology" *Surveillance and Society* 12(2): 198; Meijas, U., A. & Couldry, N. (2019). "Datafication" *Internet Policy Review* 8(4): 1 – 10.

behaviour.[1318] Often, corporations and other entities earn money by selling products to the users or by selling the collected data to third parties.[1319]

4.6.6 The Internet

The Internet has become a hub for the collection of personal information.[1320] Recently, there has been a trend by government agencies to release and place public records on the Internet.[1321] This is a risky move because the release of public records on the Internet has the propensity to avail personal identifiable information to identity thieves. This can lead to legal action against the government agencies responsible for the publication. An affected party must show that, on a balance of probability, they suffered financial loss because the publication of personal information led to the theft of their data. There is an implied legal duty on government agencies to safeguard a person's personal data.[1322]

According to Solove,[1323] there are two ways in which a personal information can be collected over the Internet. First, where personal information is directly collected from an individual. This takes place when a person gains access to a website and proceeds to input their personal information. Personal information can be collected by an e-commerce business whenever a person transacts online. It then becomes easier for an e-commerce business to keep track of an individual's transactional data.[1324]

[1318] Meijas, U., A. & Couldry, N. (2019). "Datafication" *Internet Policy Review* 8(4): 1 – 10; Van Dijk, J. (2014). "Datafication, dataism and dataveillance: Big Data between paradigm and ideology" *Surveillance and Society* 12(2): 198.

[1319] Meijas, U., A. & Couldry, N. (2019). "Datafication" *Internet Policy Review* 8(4): 3.

[1320] Solove, D., J. (2001). "Privacy and power: Computer databases and metaphors for information privacy" *Stanford Law review* 53(6): 1409.

[1321] Solove, D., J. (2001). "Privacy and power: Computer databases and metaphors for information privacy" *Stanford Law review* 53(6): 1409. For example, there has been a trend in releasing information relating to individuals considered to have 2 separate identity numbers on the Internet. This trend by the government exposes individuals to potential risks such as identity theft. Often, these notices contain personal identifiable information like a person's name, surname, date of birth and even residential address. The release of such personal information on the Internet is unclear. See www.gov.za/sites/default/files/gcis_document/201409/36742gen808ab.pdf. Accessed 8 September 2020.

[1322] See section 19 of the Protection of Personal Information Act 4 of 2013.

[1323] Solove, D., J. (2001). "Privacy and power: Computer databases and metaphors for information privacy" *Stanford Law review* 53(6): 1393 – 1462.

[1324] Solove, D., J. (2001). "Privacy and power: Computer databases and metaphors for information privacy" *Stanford Law review* 53(6): 1411.

Second, Internet users are susceptible to what is referred to as “clickstream data”.[1325] Whenever a person surfs the web, information is collected and recorded on the website.[1326] That information is then processed by the website to determine the amount of times it has received online visitors.[1327] To enhance the chances of obtaining more information from Internet users, websites place cookies on a user’s PC to retrieve information. When a user returns to that website at a later stage, the website recognises the user. This process enables websites to identify users.[1328]

Identification is not limited to the presence of cookies on personal computers. There are various indicators that can be used to identify natural persons. These indicators, or identifiers, can be used as identifying information to reveal a person’s identity.[1329] If the information can adequately identify an individual without the aid of an external source, then that information is a direct identifier. Examples of direct identifiers include a person’s signature and name.[1330] If the information does not adequately identify an individual but when combined with other information, leads to the discovery of a person’s identity, then that information is an indirect identifier.[1331] Examples of indirect identifiers include a person’s occupation and their marital status.[1332] The process of identification is often necessary to identify natural persons. For example, in order for a person to access financial services, some form of identification is required. A person can present a government issued identity document or use their biometric information

[1325] Solove, D., J. (2001). “Privacy and power: Computer databases and metaphors for information privacy” *Stanford Law review* 53(6): 1411.

[1326] According to Solove, information collected includes a user’s Internet Service Provider (ISP), time spent on the webpage and the type of computer and software used to access that website. See Solove, D., J. (2001). “Privacy and power: Computer databases and metaphors for information privacy” *Stanford Law review* 53(6): 1411.

[1327] Solove, D., J. (2001). “Privacy and power: Computer databases and metaphors for information privacy” *Stanford Law review* 53(6): 1411.

[1328] Solove, D. J., (2004). *The digital person: technology and privacy in the information age* New York University Press at 24; Solove, D., J. (2001). “Privacy and power: Computer databases and metaphors for information privacy” *Stanford Law review* 53(6): 1411.

[1329] See Finnish Social Science Data Archive. “Anonymisation and Personal Data”. Available at https://www.fsd.tuni.fi/aineistonhallinta/en/anonymisation-and-identifiers.html. Accessed 9 September 2020.

[1330] See Finnish Social Science Data Archive. “Anonymisation and Personal Data”. Available at https://www.fsd.tuni.fi/aineistonhallinta/en/anonymisation-and-identifiers.html. Accessed 9 September 2020.

[1331] See Finnish Social Science Data Archive. “Anonymisation and Personal Data”. Available at https://www.fsd.tuni.fi/aineistonhallinta/en/anonymisation-and-identifiers.html. Accessed 9 September 2020.

[1332] See Finnish Social Science Data Archive. “Anonymisation and Personal Data”. Available at https://www.fsd.tuni.fi/aineistonhallinta/en/anonymisation-and-identifiers.html. Accessed 9 September 2020.

to prove their identity. In extreme circumstances, identification has been used by governments to subdue their critiques and, at times, it has also been used to control the movement of people.[1333]

4.7 Blockchain and data privacy

The discussion above has demonstrated that governments and corporate entities collect, store, process, and to a certain extent, control personal information. These institutions process data primarily for profit making and to expand their position of power.[1334] It has also been shown that centralised models of operations enable governments and corporate entities to use databases for assembling personal information.[1335]

Blockchain has the potential to bring change. Blockchain offers the possibility of a decentralised model of handling data, which gives individuals data sovereignty and control over their personal data.[1336] Decentralised data handling allows individuals to share their personal data with trusted entities.[1337] However, Finck cautions that blockchains do not necessarily provide privacy guarantees so it is necessary to combine data sovereignty with additional mechanisms.[1338] Security safeguards can be implemented to ensure that blockchains do not reveal data stored on them.[1339] Despite

[1333] See Solove, D., J. (2008). *Understanding Privacy* Harvard University Press at 125.

[1334] Finck, M. (2018). "Blockchain and Data Protection in the European Union" *Max Planck Institute for Innovation and Competition Research Paper No. 18-01* at 7. Available at https://cybersecurity.master.di.unimi.it/articoli/blockchain%20gdpr.pdf. Accessed at 21 September 2020.

[1335] Finck, M. (2018). "Blockchain and Data Protection in the European Union" *Max Planck Institute for Innovation and Competition Research Paper No. 18-01* at 7. Available at https://cybersecurity.master.di.unimi.it/articoli/blockchain%20gdpr.pdf. Accessed at 21 September 2020.

[1336] Finck, M. (2018). "Blockchain and Data Protection in the European Union" *Max Planck Institute for Innovation and Competition Research Paper No. 18-01* at 7. Available at https://cybersecurity.master.di.unimi.it/articoli/blockchain%20gdpr.pdf. Accessed 21 September 2020.

[1337] Finck, M. (2018). "Blockchain and Data Protection in the European Union" *Max Planck Institute for Innovation and Competition Research Paper No. 18-01* at 7. Available at https://cybersecurity.master.di.unimi.it/articoli/blockchain%20gdpr.pdf. Accessed 21 September 2020.

[1338] Finck, M. (2018). "Blockchain and Data Protection in the European Union" *Max Planck Institute for Innovation and Competition Research Paper No. 18-01* at 8. Available at https://cybersecurity.master.di.unimi.it/articoli/blockchain%20gdpr.pdf. Accessed 21 September 2020.

[1339] Finck, M. (2018). "Blockchain and Data Protection in the European Union" *Max Planck Institute for Innovation and Competition Research Paper No. 18-01* at 8. Available at these risks, blockchain's recordkeeping capabilities can potentially make intermediaries redundant. If that happens, blockchain can decentralise the collection, storage, and processing of data.[1340]

As mentioned above,[1341] one of the attributes of using a blockchain is the prospect of engaging in pseudonymous transactions. For example, a participant can determine the number of bitcoins transferred to another participant by analysing the latter's public key. However, a participant may not necessarily have the tools to identify the recipient of bitcoins due to a lack of identifying information.[1342] Identification can only be achieved if the participant possesses personal identifying information.[1343] The key to determine the impact of blockchain on a person's privacy is whether third parties can easily ascertain the identity of participants and the nature of the transactions on blockchain. Another factor to consider is whether the transactions reveal the identity of a participant on blockchain.

To address these issues, it is important to recognise the relevant role players (participants) on a blockchain. Thereafter, I discuss the types of transactions that can take place on a blockchain.

4.7.1 Types of participants on blockchain

4.7.1.1 Miners

Miners play an important role in the creation of blockchains. Miners generate new blocks that can be added to existing blocks. To achieve this, miners use a consensus protocol to assemble transactions into a new block before they are added to a

https://cybersecurity.master.di.unimi.it/articoli/blockchain%20gdpr.pdf. Accessed 21 September 2020.

[1340] Finck, M. (2018). "Blockchain and Data Protection in the European Union" *Max Planck Institute for Innovation and Competition Research Paper No. 18-01* at 6. Available at https://cybersecurity.master.di.unimi.it/articoli/blockchain%20gdpr.pdf. Accessed 21 September 2020.

[1341] Paragraph 2.5.6 in Chapter 2 above.

[1342] Kianieff, M. (2019) *Blockchain Technology and the Law Opportunities and Risks* Routledge Publishing (UK) at 151.

[1343] Kianieff, M. (2019) *Blockchain Technology and the Law Opportunities and Risks* Routledge Publishing (UK) at 151.

blockchain network.[1344] According to Artzt *et al*, miners validate transactions which have previously been submitted by other participants.[1345] Miners do not determine the type of data that must be recorded on a blockchain.[1346] For this reason, it cannot be said that miners determine the purposes and means of processing of personal data.[1347]

4.7.1.2 Participants

Blockchain participants are the most well-known users of blockchains. According to the *Commission Nationale de l'informatique et de Libértes* (CNIL), a participant can be a person who has been given the rights to make entries on blockchain or makes a transaction for which they request validation.[1348] It is clear from the description that a participant can determine the type of transactions recorded on a blockchain. Generally, and depending on the setup of blockchain, a central administrator grants access to the participants and determines the rules regarding the type of data recorded on blockchain. For example, a network of hospitals can create a private blockchain to share confidential medical records. For this reason, a central administrator can grant access to health care practitioners only. Their role can be restricted to the input of healthcare data on blockchain.

[1344] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 20.

[1345] Artzt, M., (ed) Determann, L., Long, W., *Blockchain and Data Privacy* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 203.

[1346] Artzt, M., (ed) Determann, L., Long, W., *Blockchain and Data Privacy* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 203.

[1347] Artzt, M., (ed) Determann, L., Long, W., *Blockchain and Data Privacy* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 203.

[1348] Commission Nationale de l'informatique et de Libértes (2018). *"Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data"*. Available at https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data. Accessed 20 September 2020.

4.7.1.3 An accessor

An accessor is a person that has the right to access a copy of a blockchain.[1349] The CNIL does not necessarily give examples of 'accessors' for purposes of blockchain. From the definition, it can be argued that a central administrator qualifies as an accessor. This is because a central administrator performs a governance role on blockchain. In the context of blockchain, governance refers to "the processes, rules, and procedures relied on to maintain the protocol."[1350] If a central administrator can modify blockchain protocol, determine the rules or decide the type of data stored on blockchain, then it can be said that the central administrator performs a governance role. A central administrator can retain a copy of blockchain.

It is important to consider whether a node qualifies as an 'accessor'. A node is a computer that stores a copy of a blockchain. A node is used by miners for validating new blocks.[1351] However, any other participant can use a node to validate transactions. Regardless of the type of blockchain that is used, a natural person or juristic person can directly access blockchain provided they have a node.[1352] However, possessing a node does not necessarily guarantee certain rights to the participant. This is because an administrator can determine who has access to a blockchain. A person who hacks and gains entry into a private blockchain cannot be considered an accessor because they have not been given the rights to access a copy of blockchain. In a public blockchain, the rights can be allocated to all the participants because a public blockchain is accessible to everyone. It can be concluded that the status of an accessor is determined by the way access to a blockchain has been granted.

[1349] Commission Nationale de l'informatique et de Libértes (2018). *"Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data"*. Available at https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data. Accessed 20 September 2020.

[1350] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 183.

[1351] Artzt, M., (ed) Determann, L., Long, W., *Blockchain and Data Privacy* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 203.

[1352] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 14.

Notably, there are different rights that can be made available on a blockchain. Access rights are rights given to access blockchain network and to read data on the ledger.[1353] Users given access rights only view what happens on a blockchain but do not take part in the development of the network and the writing of new data.[1354] Typically, entities or persons with access rights have limited roles such as monitoring and auditing.[1355]

4.7.1.4 Validators

A validator is a blockchain participant that is responsible for validating transactions and maintaining security on blockchain network.[1356] Validators confirm new transactions before they are added to blockchain. The validators use the network's rules to ensure that blockchain transactions are valid.[1357] It should be noted that each blockchain has its own rules regarding the number of transactions that can be stored in each block.[1358] Validators also add blocks to blockchain using the *proof-of-stake* consensus mechanism.[1359]

4.7.2 Data transactions on blockchain

Data on a blockchain is stored inside a block. Any type of data, including personal information, can be stored on a blockchain.[1360] This means that financial transactions

[1353] Post, D & Cipollini, C. (2023). "Fundamental Elements of a Blockchain-Based Tax System: Governance, Legal and Technology Aspects" *World Tax Journal* 15(3): 3. [unpublished version].

[1354] Post, D & Cipollini, C. (2023). "Fundamental Elements of a Blockchain-Based Tax System: Governance, Legal and Technology Aspects" *World Tax Journal* 15(3): 3. [unpublished version].

[1355] Post, D & Cipollini, C. (2023). "Fundamental Elements of a Blockchain-Based Tax System: Governance, Legal and Technology Aspects" *World Tax Journal* 15(3): 3. [unpublished version].

[1356] Orenes-Lerma, L. (2023). *What is a blockchain validator?* Available at https://www.ledger.com/academy/what-is-a-blockchain-validator. Accessed 7 October 2023.

[1357] Orenes-Lerma, L. (2023). *What is a blockchain validator?* Available at https://www.ledger.com/academy/what-is-a-blockchain-validator. Accessed 7 October 2023.

[1358] Phemex (2021). *Who are the blockchain validators: network users powering the blockchain functionality*. Available at https://phemex.com/academy/blockchain-validator-process. Accessed 7 October 2023.

[1359] Orenes-Lerma, L. (2023). *What is a blockchain validator?* Available at https://www.ledger.com/academy/what-is-a-blockchain-validator. Accessed 7 October 2023.

[1360] Blockchain Bundesverband (2018). "*Blockchain, Data protection and GDPR*" at 4. Available at https://www.bundesblock.de/wp-content/uploads/2019/01/GDPR_Position_Paper_v1.0.pdf. Accessed 21 September 2020.

and documents can be recorded on a blockchain.[1361] It is possible to store data as "digital art", as a document or even as plain text.[1362] Since data can be stored in these formats, it is important to implement security safeguards on blockchain. One of these security measures is private and public key encryption. Without access to the correct cryptographic key, no person can uncover the original data.[1363] If a person possesses another person's private key, then the holder of the private key can decrypt the data and obtain its original content. In a blockchain, a public key is akin to a person's identity or address. Hence, a transaction cannot take place without a public key. Although a public key consists of numbers and letters, it is a digital representation of a natural person. A public key is also encrypted to hide a person's identity.[1364] Consequently, a public key is considered data in so far as it can be attributed to a natural person. If additional information or identifiers are combined with a public key, a person's identity can be revealed.[1365]

A hash function can also be implemented to safeguard data on a blockchain.[1366] Once data in a block has accumulated to a certain magnitude, it is "chained" to another block

[1361] Blockchain Bundesverband (2018). "*Blockchain, Data protection and GDPR*" at 4. Available at https://www.bundesblock.de/wp-content/uploads/2019/01/GDPR_Position_Paper_v1.0.pdf. Accessed 21 September 2020.

[1362] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 90; see also Finck, M. (2018). "Blockchain and Data Protection in the European Union" *Max Planck Institute for Innovation and Competition Research Paper No. 18-01* at 4. Available at https://cybersecurity.master.di.unimi.it/articoli/blockchain%20gdpr.pdf. Accessed 21 September 2020.

[1363] Finck, M. (2018). "Blockchain and Data Protection in the European Union" *Max Planck Institute for Innovation and Competition Research Paper No. 18-01* at 4. Available at https://cybersecurity.master.di.unimi.it/articoli/blockchain%20gdpr.pdf. Accessed 21 September 2020.

[1364] Artzt, M., (ed) Determann, L., Long, W., *Blockchain and Data Privacy* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 195; Finck, M. (2018). "Blockchain and Data Protection in the European Union" *Max Planck Institute for Innovation and Competition Research Paper No. 18-01* at 4. Available at https://cybersecurity.master.di.unimi.it/articoli/blockchain%20gdpr.pdf. Accessed 21 September 2020.

[1365] According to Article 4(1) of the General Data Protection Regulation (GDPR), 'personal data' is defined as: "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." See also Finck, M. (2018). "Blockchain and Data Protection in the European Union" *Max Planck Institute for Innovation and Competition Research Paper No. 18-01*. Available at https://cybersecurity.master.di.unimi.it/articoli/blockchain%20gdpr.pdf. Accessed at 21 September 2020.

[1366] A brief description of a hash function was discussed at paragraph 2.5.6 in Chapter 2 above.

through a process called hashing.[1367] Computer algorithms optimise blocks of data to ensure that it reaches a certain length. Each block has a unique hash and a hash from a previous block that enables the new block to link to the previous block. This mechanism ensures that the data is stored in a sequential manner, making it difficult for any person to alter previous blocks.[1368] According to blockchain *Bundesverband*,[1369] storing hashed data on a blockchain is important because hashing conceals plain text data. Second, it ensures that data is validated. And last, data can be stored on larger blocks as opposed to using the entire block for storage.[1370]

Blockchain provides a mechanism that enables users to verify the occurrence of a transaction without the need to disclose the identity of blockchain users. There is a mechanism, known as *zero-knowledge-proof* algorithm, that enables a user in possession of data to display that data without revealing its contents.[1371] The *zero-knowledge proof* is currently used on, amongst others, the *Monero* and *Zcash* blockchain networks. These public blockchains use advanced cryptographic

[1367] Finck, M. (2018). "Blockchain and Data Protection in the European Union" *Max Planck Institute for Innovation and Competition Research Paper No. 18-01* at 4. Available at https://cybersecurity.master.di.unimi.it/articoli/blockchain%20gdpr.pdf. Accessed at 21 September 2020.

[1368] Finck, M. (2018). "Blockchain and Data Protection in the European Union" *Max Planck Institute for Innovation and Competition Research Paper No. 18-01* at 4. Available at https://cybersecurity.master.di.unimi.it/articoli/blockchain%20gdpr.pdf. Accessed at 21 September 2020; Artzt, M., (ed) Determann, L., Long, W., *Blockchain and Data Privacy* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 197.

[1369] Blockchain Bundesverband is community-based organization in Germany that seeks to educate decision makers in politics and large corporations about the importance of blockchain adoption in society. See https://bundesblock.de/about-us/. Accessed 21 September 2020.

[1370] Blockchain Bundesverband (2018). "*Blockchain, Data protection and GDPR*" at 4. Available at https://www.bundesblock.de/wp-content/uploads/2019/01/GDPR_Position_Paper_v1.0.pdf. Accessed 21 September 2020.

[1371] Werbach, K. (2018). *The Blockchain and the New Architecture of Trust* Massachusetts Institute of Technology Press (US) at 107; Artzt, M., (ed) Determann, L., Long, W., *Blockchain and Data Privacy* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 239; Blockchain Bundesverband (2018). "*Blockchain, Data protection and GDPR*" at 5. Available at https://www.bundesblock.de/wp-content/uploads/2019/01/GDPR_Position_Paper_v1.0.pdf. Accessed 21 September 2020; Finck, M. (2018). "Blockchain and Data Protection in the European Union" *Max Planck Institute for Innovation and Competition Research Paper No. 18-01* at 15. Available at https://cybersecurity.master.di.unimi.it/articoli/blockchain%20gdpr.pdf. Accessed at 21 September 2020; De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 39 & 67. For an extensive discussion see Ben-Sasson, E., *et al* (2014). "Zerocash: Decentralized Anonymous Payments from Bitcoin" *IEEE Symposium on Security and Privacy* at 459 – 474.

techniques to conceal the identity of the receiver and sender during any transaction.[1372] For example, a person can send bitcoins to another person on blockchain. The algorithm merely shows that bitcoins have been spent from the sender's wallet.[1373]

4.7.3 How blockchain affects data privacy

4.7.3.1 Data irreversibility

Data placed on blockchain is irreversible irrespective of who stores the data. Since blockchain architecture was primarily designed for recordkeeping,[1374] its immutable capabilities make it difficult to make changes to the data. Changes can only be made if the participatory nodes work together to recalibrate the blocks.[1375] Additionally, once data has been stored on blockchain it cannot be erased. This feature causes friction with certain legislative provisions that require deletion of personal information where it is no longer needed.[1376] Data irreversibility has benefits in so far as record management is concerned.[1377] For instance, a juristic person may be required to keep records and documentation for an extended period. Compliance is made easier if blockchain is used to store data.

[1372] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 67; Artzt, M., (ed) Determann, L., Long, W., *Blockchain and Data Privacy* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 239; Ben-Sasson, E., *et al* (2014). "Zerocash: Decentralized Anonymous Payments from Bitcoin" *IEEE Symposium on Security and Privacy* at 459 – 474.

[1373] Blockchain Bundesverband (2018). "*Blockchain, Data protection and GDPR*" at 5. Available at https://www.bundesblock.de/wp-content/uploads/2019/01/GDPR_Position_Paper_v1.0.pdf. Accessed 21 September 2020.

[1374] Finck, M. (2018). "Blockchain and Data Protection in the European Union" *Max Planck Institute for Innovation and Competition Research Paper No. 18-01* at 6. Available at https://cybersecurity.master.di.unimi.it/articoli/blockchain%20gdpr.pdf. Accessed at 21 September 2020.

[1375] Roberta, F. (2017). *Blockchain and individuals' control over personal data in European data protection law* Masters thesis (Tilburg University) at 30.

[1376] Chang, H., (2017). "Blockchain: Disrupting data protection?" Privacy Law and Business International Report University of Hong Kong Faculty of Law Research Paper No. 2017/041 at 2. Available at SSRN: https://ssrn.com/abstract=3093166. Accessed 22 September 2020. For example, in terms of section 14(4) of the POPI Act, a responsible party must delete any record of personal information as soon as possible and after the responsible is no longer required to retain that information. A full discussion follows in Chapter 6 below.

[1377] Chang, H., (2017). "Blockchain: Disrupting data protection?" Privacy Law and Business International Report University of Hong Kong Faculty of Law Research Paper No. 2017/041 at 2. Available at SSRN: https://ssrn.com/abstract=3093166. Accessed 22 September 2020.

4.7.3.2 Data transparency

In a public blockchain, all data stored can be observed and accessed by all the participants on that network. A participant has access to all the records from the inception of blockchain.[1378] Privacy issues arise on a public blockchain where personal information is stored. It is difficult for private information to be protected and kept confidential due to the open nature of a public blockchain.[1379] Also, it is also difficult to establish the identities of all the users on a public blockchain. On a private blockchain, the users are preselected and trusted beforehand. A private blockchain is designed in such a way that a central authority determines the type of data stored on a blockchain. The closed network makes it conducive for the transmission of sensitive data to trusted participants. Since the user's identity is known, it is much easier to hold the participants accountable.

4.7.3.3 Pseudonymous identity

Pseudonymity is made possible by using a public key. Pseudonymity protects a participant's identity.[1380] Pseudonymisation refers to the use of an identifier as a way to conceal a person's identity.[1381] It should be recognised that pseudonymisation has certain drawbacks. It is possible to identify a user on blockchain if supplementary information or metadata is used.[1382] This is because blockchain transactions consist

[1378] Werbach, K. (2018). *The Blockchain and the New Architecture of Trust* Massachusetts Institute of Technology Press (US) at 105.

[1379] Chang, H., (2017). "Blockchain: Disrupting data protection?" Privacy Law and Business International Report University of Hong Kong Faculty of Law Research Paper No. 2017/041 at 2. Available at SSRN: https://ssrn.com/abstract=3093166. Accessed 22 September 2020.

[1380] Roberta, F. (2017). *Blockchain and individuals' control over personal data in European data protection law* Masters thesis (Tilburg University) at 30.

[1381] Garfinkel, L., S. (2015). "De-Identification of Personal Information" *National Institute of Standards and Technology* at 2. Available at https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf. Accessed 22 September 2020; De Filippi, P. (2016). "The interplay between decentralization and privacy: the case of blockchain technologies" *Journal of Peer Production Alternative Internets* at 11. Article 4(5) of the GDPR defines 'pseudonymisation' as: "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."

[1382] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 29; Roberta, F. (2017). *Blockchain and individuals' control over personal data in European data protection law* Master's thesis (Tilburg University) at 30.

of metadata which includes the transaction itself and the address of the recipient.[1383] For example, when two natural persons exchange bitcoins (object of the transaction) their addresses (both private and public key) consist of metadata.[1384] This metadata, when combined with digital signatures and IP addresses, can be used to reveal the identities of parties on blockchain system.[1385] Re-identification[1386] poses a threat to privacy because a natural person may be identified by linking information that was previously de-identified[1387] with other datasets.[1388]

4.8 Mechanisms deployed to mitigate privacy concerns on blockchain

4.8.1 Restricting the type of data stored on blockchain

To mitigate privacy concerns, it is possible to limit the type of data stored and recorded on blockchain. Practically, this can be achieved by excluding any personal information on blockchain.[1389] Shah *et al* submit that the broad definitions of personal data across various countries makes it difficult for data stored on a blockchain to avoid falling in

[1383] Bacon, J., *et al* (2017). "Blockchain Demystified" *Queen Mary University of London, School of Law Legal Studies Research Paper No. 268/2017* at 40. Available https://papers.ssrn.com/sol3/papers.cfm?Abstract_id=3091218. Accessed 5 January 2020.

[1384] Bacon, J., *et al* (2017). "Blockchain Demystified" *Queen Mary University of London, School of Law Legal Studies Research Paper No. 268/2017* at 40. Available https://papers.ssrn.com/sol3/papers.cfm?Abstract_id=3091218. Accessed 5 January 2020.

[1385] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 29; Bacon, J., *et al* (2017). "Blockchain Demystified" *Queen Mary University of London, School of Law Legal Studies Research Paper No. 268/2017* at 40. Available https://papers.ssrn.com/sol3/papers.cfm?Abstract_id=3091218. Accessed 5 January 2020. That is why it is possible to identify users of Bitcoin.

[1386] "Re-identification" is the process of identifying a person by from data that was previously de-identified. See Garfinkel, L., S. (2015). "De-Identification of Personal Information" *National Institute of Standards and Technology* at 9. Available at https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf. Accessed 22 September 2020.

[1387] "Deidentification" is the process of modifying personal information to change its use making it impractical to identify the natural person. See Mohammed J., K., (2018). "*Big Data Deidentification, Reidentification and Anonymization*" ISACA Journal. Available at https://www.isaca.org/resources/isaca-journal/issues/2018/volume-1/big-data-deidentification-reidentification-and-anonymization. Accessed 24 June 2020. For an alternative definition, see Garfinkel, L., S. (2015). "De-Identification of Personal Information" *National Institute of Standards and Technology* at 2. Available at https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf. Accessed 22 September 2020.

[1388] Garfinkel, L., S. (2015). "De-Identification of Personal Information" *National Institute of Standards and Technology* at 12. Available at https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf. Accessed 22 September 2020.

[1389] Shah, P. *et al* (2019). "Blockchain Technology: Data Privacy Issues and Potential Mitigation Strategies" *Thomson Reuters Practical Law* at 7. https://www.davispolk.com/files/blockchain_technology_data_privacy_issues_and_potential_mitigation_strategies_w-021-8235.pdf. Accessed 17 June 2020.

the scope of personal data as defined in data protection laws.[1390] Due to the varying legal aspects relating to the interpretation of 'personal data', legal remedies provided for in data protection laws can differ. Aspects relating to pseudonymity and anonymity will likely also differ from one country to another particularly if countries use private public key encryption on blockchain system.[1391]

The following concessions can be made to boost privacy on a blockchain. Personal data can be stored off-chain.[1392] Instead of storing personal data on a blockchain, personal data may be stored on an external database, on a server or through a third party.[1393] A hash can be used to link off-chain personal data to transactions on blockchain.[1394] Personal information can be recorded and encrypted on an external

[1390] Shah, P. *et al* (2019). "Blockchain Technology: Data Privacy Issues and Potential Mitigation Strategies" *Thomson Reuters Practical Law* at 7. https://www.davispolk.com/files/blockchain_technology_data_privacy_issues_and_potential_mitigation_strategies_w-021-8235.pdf. Accessed 17 June 2020.

[1391] Shah, P. *et al* (2019). "Blockchain Technology: Data Privacy Issues and Potential Mitigation Strategies" *Thomson Reuters Practical Law* at 7. https://www.davispolk.com/files/blockchain_technology_data_privacy_issues_and_potential_mitigation_strategies_w-021-8235.pdf. Accessed 17 June 2020.

[1392] Shah, P. *et al* (2019). "Blockchain Technology: Data Privacy Issues and Potential Mitigation Strategies" *Thomson Reuters Practical Law* at 7. https://www.davispolk.com/files/blockchain_technology_data_privacy_issues_and_potential_mitigation_strategies_w-021-8235.pdf. Accessed 17 June 2020; Jiménez-Gómez & Sofia, B. (2020). "Risks of Blockchain for data protection: A European Approach" *Santa Clara High Technology Law Journal* 36(3): 333 – 335; Berberich, M. & Steiner, M. (2016). "Blockchain technology and the GDPR - how to reconcile privacy and distributed ledgers" *European Data Protection Law Review* 2(3): 422-426; Finck, M. (2018). "Blockchain and Data Protection in the European Union" *Max Planck Institute for Innovation and Competition Research Paper No. 18-01* at 11. Available at https://cybersecurity.master.di.unimi.it/articoli/blockchain%20gdpr.pdf. Accessed 21 September 2020.

[1393] Eberhardt, J. & Tai, S. (2017). "On or off the Blockchain? Insights on off-chaining Computation and Data" *Information Systems Engineering* at 2. Available at http://www.ise.tu-berlin.de/fileadmin/fg308/publications/2017/2017-eberhardt-tai-offchaining-patterns.pdf. Accessed 22 September 2020; Shah, P. *et al* (2019). "Blockchain Technology: Data Privacy Issues and Potential Mitigation Strategies" *Thomson Reuters Practical Law* at 7. https://www.davispolk.com/files/blockchain_technology_data_privacy_issues_and_potential_mitigation_strategies_w-021-8235.pdf. Accessed 17 June 2020; Jiménez-Gómez & Sofia, B. (2020). "Risks of Blockchain for data protection: A European Approach" *Santa Clara High Technology Law Journal* 36(3): 333 – 335.

[1394] Jiménez-Gómez & Sofia, B. (2020). "Risks of Blockchain for data protection: A European Approach" *Santa Clara High Technology Law Journal* 36(3): 334; Berberich, M. & Steiner, M. (2016). "Blockchain technology and the GDPR - how to reconcile privacy and distributed ledgers" *European Data Protection Law Review* 2(3): 422-426; Finck, M. (2018). "Blockchain and Data Protection in the European Union" *Max Planck Institute for Innovation and Competition Research Paper No. 18-01* at 11. Available at https://cybersecurity.master.di.unimi.it/articoli/blockchain%20gdpr.pdf. Accessed 21 September 2020.

database instead of a blockchain.[1395] It is advantageous to store personal data off-chain because it limits the possibility of data manipulation by unauthorised agents[1396] and it reduces costs associated with storage on blockchain.[1397]

Another strategy that can be adopted is to store data on a single node.[1398] The addition of data on new blocks can be stopped but only after the verification process is complete.[1399] This way, the other nodes on the system access the 'primary' node every time verification must take place. In doing so, privacy is maintained because only a single node stores personal data, which promotes confidentiality in the process. This process is also beneficial because it limits storage capacity to a single node, which saves energy in the process.[1400]

4.8.2 Private permissioned blockchain architecture

As I have mentioned, a private blockchain increases the chances of preserving privacy. Fewer known participants can reduce the chances of unauthorised access to personal data. Fewer known participants can also reduce the stringent consensus operations which can safeguard privacy.[1401] A central administrator can implement steps to safeguard data on a private blockchain. First, a central administrator

[1395] Finck, M. (2018). "Blockchain and Data Protection in the European Union" *Max Planck Institute for Innovation and Competition Research Paper No. 18-01* at 11. Available at https://cybersecurity.master.di.unimi.it/articoli/blockchain%20gdpr.pdf. Accessed 21 September 2020.

[1396] Shah, P. *et al* (2019). "Blockchain Technology: Data Privacy Issues and Potential Mitigation Strategies" *Thomson Reuters Practical Law* at 7. https://www.davispolk.com/files/blockchain_technology_data_privacy_issues_and_potential_mitigation_strategies_w-021-8235.pdf. Accessed 17 June 2020.

[1397] Finck, M. (2018). "Blockchain and Data Protection in the European Union" *Max Planck Institute for Innovation and Competition Research Paper No. 18-01* at 12. Available at https://cybersecurity.master.di.unimi.it/articoli/blockchain%20gdpr.pdf. Accessed 21 September 2020.

[1398] Moerel, L., (2019). "Blockchain & Data Protection…and Why They Are Not on a Collision Course" *European Preview of Private Law* 26(6): 847.

[1399] Moerel, L., (2019). "Blockchain & Data Protection…and Why They Are Not on a Collision Course" *European Preview of Private Law* 26(6): 847.

[1400] Moerel, L., (2019). "Blockchain & Data Protection…and Why They Are Not on a Collision Course" *European Preview of Private Law* 26(6): 847.

[1401] Shah, P. *et al* (2019). "Blockchain Technology: Data Privacy Issues and Potential Mitigation Strategies" *Thomson Reuters Practical Law* at 7. https://www.davispolk.com/files/blockchain_technology_data_privacy_issues_and_potential_mitigation_strategies_w-021-8235.pdf. Accessed 17 June 2020.

authorises a select number of vetted and approved participants.[1402] Authorised participants can be compelled to follow strict consensus practices for data privacy.[1403] Last, a central administrator can take technical measures to reduce and regulate the amount of personal data that participants process.[1404] Since a central authority vets participants, there is a greater degree of accountability and opportunity to assign various roles to participants. For instance, a central authority can determine which participants on blockchain can process data.[1405] This manner of governance enables central authorities to oversee the cross-border flow of data.[1406]

4.8.3 Enhanced data encryption techniques

Hash functions and encryption are the conventional techniques used to make data secure on a blockchain.[1407] If data is encrypted (with a private key), a person with the appropriate (public) key can decrypt the data potentially revealing personal data.[1408] Thus data encryption is effective if the keys are in the right hands. If an unauthorised person has access to the keys, personal data can fall in the wrong hands.[1409] The use of hash functions enhances security. A hash operates in a way that the same input

[1402] Shah, P. *et al* (2019). "Blockchain Technology: Data Privacy Issues and Potential Mitigation Strategies" *Thomson Reuters Practical Law* at 7. https://www.davispolk.com/files/blockchain_technology_data_privacy_issues_and_potential_mitigation_strategies_w-021-8235.pdf. Accessed 17 June 2020.

[1403] Shah, P. *et al* (2019). "Blockchain Technology: Data Privacy Issues and Potential Mitigation Strategies" *Thomson Reuters Practical Law* at 7. https://www.davispolk.com/files/blockchain_technology_data_privacy_issues_and_potential_mitigation_strategies_w-021-8235.pdf. Accessed 17 June 2020.

[1404] Shah, P. *et al* (2019). "Blockchain Technology: Data Privacy Issues and Potential Mitigation Strategies" *Thomson Reuters Practical Law* at 7. https://www.davispolk.com/files/blockchain_technology_data_privacy_issues_and_potential_mitigation_strategies_w-021-8235.pdf. Accessed 17 June 2020.

[1405] Shah, P. *et al* (2019). "Blockchain Technology: Data Privacy Issues and Potential Mitigation Strategies" *Thomson Reuters Practical Law* at 7. https://www.davispolk.com/files/blockchain_technology_data_privacy_issues_and_potential_mitigation_strategies_w-021-8235.pdf. Accessed 17 June 2020.

[1406] Shah, P. *et al* (2019). "Blockchain Technology: Data Privacy Issues and Potential Mitigation Strategies" *Thomson Reuters Practical Law* at 7. https://www.davispolk.com/files/blockchain_technology_data_privacy_issues_and_potential_mitigation_strategies_w-021-8235.pdf. Accessed 17 June 2020.

[1407] Jiménez-Gómez, S., B. (2020). "Risks of Blockchain for data protection: A European Approach" *Santa Clara High Technology Law Journal* 36(3): 335.

[1408] Jiménez-Gómez, S., B. (2020). "Risks of Blockchain for data protection: A European Approach" *Santa Clara High Technology Law Journal* 36(3): 335.

[1409] See Werbach, K. (2018). *The Blockchain and the New Architecture of Trust* Massachusetts Institute of Technology Press (US) at 40.

yields the same output.[1410] However, a computer can decrypt a hash by linking sets of data to determine if the output is similar to the previously known output.[1411] *Zero-knowledge-proof* can be considered as an alternative enhanced method of encryption. The reason for this is simple. *Zero-knowledge-proof* allows a person or entity to verify transactions without accessing a user's public key. Even consensus can be reached by all the nodes on the network without verifying if the precise hash was used on a new block. This process simplifies the consensus mechanism. Privacy is preserved because personal data is not shared.[1412]

Buterin suggests cryptographically secure obfuscation as a mechanism to further improve privacy.[1413] This is achieved by making use of encryption to hide transactions so that transactions are 'unseen' to everyone. To do this, a program is turned into what Buterin refers to as a 'black box' without necessarily changing its functionality. It becomes impossible to establish how the program functions.[1414] A challenge admitted by Buterin is that it is 'mathematically impossible' to have complete black box obfuscation.[1415]

[1410] Jiménez-Gómez, S., B. (2020). "Risks of Blockchain for data protection: A European Approach" *Santa Clara High Technology Law Journal* 36(3): 335.

[1411] Jiménez-Gómez, S., B. (2020). "Risks of Blockchain for data protection: A European Approach" *Santa Clara High Technology Law Journal* 36(3): 335.

[1412] Moerel, L., (2019). "Blockchain & Data Protection…and Why They Are Not on a Collision Course" *European Preview of Private Law* 26(6): 848.

[1413] Buterin, V. (2015). "Privacy on the Blockchain". Available at https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/. Accessed 24 September 2020.

[1414] Buterin, V. (2015). "Privacy on the Blockchain". Available at https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/. Accessed 24 September 2020.

[1415] Buterin, V. (2015). "Privacy on the Blockchain". Available at https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/. Accessed 24 September 2020; see also Finck, M. (2018). "Blockchain and Data Protection in the European Union" *Max Planck Institute for Innovation and Competition Research Paper No. 18-01* at 11. Available at https://cybersecurity.master.di.unimi.it/articoli/blockchain%20gdpr.pdf. Accessed 21 September 2020.

4.8.4 Editable blockchain

In 2017, *Accenture*[1416] was awarded a patent for the creation of an editable blockchain.[1417] According to *Accenture*, the prototype can enable blockchain to be edited to resolve human errors, accommodate legal and regulatory requirements, and address other issues while preserving cryptographic features.[1418] It appears that the prototype blockchain will be used in limited sectors like banking, insurance, and capital markets.[1419] The prototype is designed for permissioned blockchain and not for permissionless blockchains.[1420]

An editable blockchain could significantly improve privacy related issues in different ways. With an editable blockchain, a central authority can make changes to an existing blockchain by deleting or editing blocks that contain sensitive data.[1421] To do this, a 'chameleon' hash function re-establishes complementary algorithms via a person's private keys.[1422] As a result, it is not necessary to use a *hard fork* to implement changes on the original blocks since no change actually takes place on the original

[1416] Accenture "is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations." See Accenture (2016). "Accenture Debuts Prototype of 'Editable' Blockchain for Enterprise and Permissioned Systems". Available at https://newsroom.accenture.com/news/accenture-debuts-prototype-of-editable-blockchain-for-enterprise-and-permissioned-systems.htm. Accessed 13 August 2023.

[1417] Higgins, S. (2017). "Accenture awarded patent for 'editable blockchain' tech". Available at https://www.coindesk.com/markets/2017/09/28/accenture-awarded-patent-for-editable-blockchain-tech/. Accessed 13 August 2023.

[1418] Accenture (2016). "Accenture Debuts Prototype of 'Editable' Blockchain for Enterprise and Permissioned Systems". Available at https://newsroom.accenture.com/news/accenture-debuts-prototype-of-editable-blockchain-for-enterprise-and-permissioned-systems.htm. Accessed 13 August 2023.

[1419] Accenture (2016). "Accenture Debuts Prototype of 'Editable' Blockchain for Enterprise and Permissioned Systems". Available at https://newsroom.accenture.com/news/accenture-debuts-prototype-of-editable-blockchain-for-enterprise-and-permissioned-systems.htm. Accessed 13 August 2023.

[1420] Accenture (2016). "Accenture Debuts Prototype of 'Editable' Blockchain for Enterprise and Permissioned Systems". Available at https://newsroom.accenture.com/news/accenture-debuts-prototype-of-editable-blockchain-for-enterprise-and-permissioned-systems.htm. Accessed 13 August 2023.

[1421] See Accenture. (2016). "*Editing the Uneditable Blockchain: Why distributed ledger technology must adapt to an imperfect world"* Accenture at 7. Available at https://www.accenture.com/_acnmedia/pdf-33/accenture-editing-uneditable-blockchain.pdf. Accessed 30 June 2020.

[1422] Accenture (2016). "*Editing the Uneditable Blockchain: Why distributed ledger technology must adapt to an imperfect world"* Accenture at 7. Available at https://www.accenture.com/_acnmedia/pdf-33/accenture-editing-uneditable-blockchain.pdf. Accessed 30 June 2020.

blockchain.[1423] Normally, any changes to a blockchain requires breaking the hash that connects the blocks together. But with a chameleon hash, changes can be made to a block by replacing it without interrupting the hash linked chain.[1424]

The flexible approach that an editable blockchain brings further enhances privacy by erasing any personal data to comply with privacy and data protection laws.[1425] Blockchain's immutable feature means that any human programming error can potentially stay on blockchain system for as long as it is in existence. However, where human error is so severe that it negatively compromises the confidentiality or secrecy of personal data, an editable blockchain allows a central authority to single-handedly rectify the human error.[1426] The rectification of human error enables users of blockchain to comply with data protection laws.[1427]

4.8.5 Anonymisation techniques

Anonymisation is a technique that permanently removes information linked to a natural person making that natural person unidentifiable.[1428] In order for anonymisation to

[1423] Accenture (2016). "*Editing the Uneditable Blockchain: Why distributed ledger technology must adapt to an imperfect world*" Accenture at 7. Available at https://www.accenture.com/_acnmedia/pdf-33/accenture-editing-uneditable-blockchain.pdf. Accessed 30 June 2020.

[1424] Accenture (2016). "*Editing the Uneditable Blockchain: Why distributed ledger technology must adapt to an imperfect world*" Accenture at 7. Available at https://www.accenture.com/_acnmedia/pdf-33/accenture-editing-uneditable-blockchain.pdf. Accessed 30 June 2020.

[1425] Accenture (2016). "*Editing the Uneditable Blockchain: Why distributed ledger technology must adapt to an imperfect world*" Accenture at 7. Available at https://www.accenture.com/_acnmedia/pdf-33/accenture-editing-uneditable-blockchain.pdf. Accessed 30 June 2020.

[1426] See Accenture (2016). "*Editing the Uneditable Blockchain: Why distributed ledger technology must adapt to an imperfect world*" Accenture at 3. Available at https://www.accenture.com/_acnmedia/pdf-33/accenture-editing-uneditable-blockchain.pdf. Accessed 30 June 2020; Moerel, L., (2019). "Blockchain & Data Protection…and Why They Are Not on a Collision Course" *European Preview of Private Law* 26(6): 849.

[1427] For example, section 14 of the POPI Act requires a responsible party to delete a record of personal information as soon as possible and when the responsible party is no longer authorised to store that information.

[1428] Data Protection Working Party (2014). "Opinion 05/2014 on Anonymisation Techniques" *Article 29 Data Protection Working Party EU* at 2 – 11. Available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. Accessed 22 September 2020; See Mohammed J., K., (2018). "*Big Data Deidentification, Reidentification and Anonymization*" ISACA Journal. Available at https://www.isaca.org/resources/isaca-journal/issues/2018/volume-1/big-data-deidentification-reidentification-and-anonymization. Accessed 24 June 2020; De Filippi, P. (2016). "The interplay between decentralization and privacy: the case of blockchain technologies" *Journal of Peer Production Alternative Internets* occur, a natural person's data must be processed by a central authority. Thereafter techniques are used to prevent a natural person from identification in the future. The process is irreversible, meaning that once anonymisation has taken place, it is no longer possible to identify a natural person.[1429] In order for anonymisation to work efficiently, the context in which it is used must be clearly set out and defined. Also, the reason for implementing anonymisation must be ascertained from the beginning.[1430]

~~**Student name**~~	**Graduation Year (Generalization)**	**Grade Average (Noise Addition: +/- Random Value A to F)**
~~**John Doe**~~	~~1996~~ 1990s	~~B~~ B+
~~**Jane Doe**~~	~~1989~~ 1980s	~~C~~ C-
~~**John Smith**~~	~~2003~~ 2000	~~A~~ A-

Figure 11[1431]

There are two techniques that are used to anonymise personal data. Randomisation is a technique that eliminates the association between the data and the natural person.[1432] 'Noise addition' is a form of randomisation that adjusts a natural person's

at 11; Directive 95/46/EC does not address anonymization directly. It states: "Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; whereas codes of conduct within the meaning of Article 27 may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible."

[1429] Data Protection Working Party (2014). "Opinion 05/2014 on Anonymisation Techniques" *Article 29 Data Protection Working Party EU* at 2 – 11. Available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. Accessed 22 September 2020

[1430] Data Protection Working Party (2014). "Opinion 05/2014 on Anonymisation Techniques" *Article 29 Data Protection Working Party EU* at 3. Available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. Accessed 22 September 2020.

[1431] **Figure 11** illustrates how anonymisation takes place. Adopted from Mohammed J., K., (2018). "*Big Data Deidentification, Reidentification and Anonymization*" ISACA Journal. Available at https://www.isaca.org/resources/isaca-journal/issues/2018/volume-1/big-data-deidentification-reidentification-and-anonymization. Accessed 24 June 2020.

[1432] Data Protection Working Party (2014). "Opinion 05/2014 on Anonymisation Techniques" *Article 29 Data Protection Working Party EU* at 12. Available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. Accessed 22 attributes (data) by either adding or removing certain elements in the data. This process makes accurate data inaccurate. For example, a person's date of birth is originally recorded on a database as '2 March 1983'. But through anonymisation, the data can be recorded as '25 September 1996'. Noise addition makes it difficult for a third party to identify a specific individual.[1433] It should be noted that the *Working Party* recommends that noise addition be combined with quasi-identifiers and the erasure of attributes to render this technique more effective.[1434] 'Permutation' is another randomisation technique that rearranges the attributes (data) from one natural person with that of another natural person.[1435]

A second technique to consider in the anonymisation process is Generalisation. Generalisation involves weakening the attributes (data) of a natural person by altering the classification or order of data.[1436] For example, generalisation can transform data

September 2020; Mohammed J., K., (2018). "*Big Data Deidentification, Reidentification and Anonymization*" ISACA Journal. Available at https://www.isaca.org/resources/isaca-journal/issues/2018/volume-1/big-data-deidentification-reidentification-and-anonymization. Accessed 24 June 2020.

[1433] Data Protection Working Party (2014). "Opinion 05/2014 on Anonymisation Techniques" *Article 29 Data Protection Working Party EU* at 12. Available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. Accessed 22 September 2020; see also Mohammed J., K., (2018). "*Big Data Deidentification, Reidentification and Anonymization*" ISACA Journal. Available at https://www.isaca.org/resources/isaca-journal/issues/2018/volume-1/big-data-deidentification-reidentification-and-anonymization. Accessed 24 June 2020; see Finck, M. (2018). "Blockchain and Data Protection in the European Union" *Max Planck Institute for Innovation and Competition Research Paper No. 18-01* at 15. Available at https://cybersecurity.master.di.unimi.it/articoli/blockchain%20gdpr.pdf. Accessed at 21 September 2020.

[1434] Data Protection Working Party (2014). "Opinion 05/2014 on Anonymisation Techniques" *Article 29 Data Protection Working Party EU* at 12. Available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. Accessed 22 September 2020; see also Finck, M. (2018). "Blockchain and Data Protection in the European Union" *Max Planck Institute for Innovation and Competition Research Paper No. 18-01* at 15 - 16. Available at https://cybersecurity.master.di.unimi.it/articoli/blockchain%20gdpr.pdf. Accessed 21 September 2020.

[1435] Data Protection Working Party (2014). "Opinion 05/2014 on Anonymisation Techniques" *Article 29 Data Protection Working Party EU* at 13. Available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. Accessed 22 September 2020; see also Mohammed J., K., (2018). "*Big Data Deidentification, Reidentification and Anonymization*" ISACA Journal. Available at https://www.isaca.org/resources/isaca-journal/issues/2018/volume-1/big-data-deidentification-reidentification-and-anonymization. Accessed 24 June 2020

[1436] Data Protection Working Party (2014). "Opinion 05/2014 on Anonymisation Techniques" *Article 29 Data Protection Working Party EU* at 16. Available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. Accessed 22 September 2020.

that records a person ordinarily working in New York to a person working in the US.[1437] 'K-anonymity' and 'aggregation' are generalisation techniques that make it difficult to identify a natural person by associating that person with other people.[1438]

4.8.6 Blockchain identity management

Everyone has an identity.[1439] Conventional identification cards and documents are issued by governments. To prove one's identity, a person must reproduce an identity document. This suggests that a centralised government has the authority to issue documents that prove a person's identity.[1440] Blockchain has the potential to create an online identity system that gives natural persons control of their own personal data and allowing individuals to share that data with whomever they wish.[1441] For example, *Accenture* and *Microsoft* created a project on the Ethereum blockchain that enables

[1437] Data Protection Working Party (2014). "Opinion 05/2014 on Anonymisation Techniques" *Article 29 Data Protection Working Party EU* at 16. Available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. Accessed 22 September 2020.

[1438] Data Protection Working Party (2014). "Opinion 05/2014 on Anonymisation Techniques" *Article 29 Data Protection Working Party EU* at 13. Available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. Accessed 22 September 2020.

[1439] In South Africa, the government issues Identity Document or Smart ID cards to citizens and permanent residents who are over the age of 16. These documents prove a person's identity and must be produced at the request of an 'authorised officer'. See sections 15 and 17 of the Identification Act 68 of 1997.

[1440] Moerel, L., (2019). "Blockchain & Data Protection…and Why They Are Not on a Collision Course" *European Preview of Private Law* 26(6): 850.

[1441] Finck, M. (2018). "Blockchain and Data Protection in the European Union" *Max Planck Institute for Innovation and Competition Research Paper No. 18-01* at 7 - 8. Available at https://cybersecurity.master.di.unimi.it/articoli/blockchain%20gdpr.pdf. Accessed at 21 September 2020; see also Blockchainhub Berlin (2017). "Identity as a Bottleneck for Blockchain". Available at https://blockchainhub.net/blog/blog/decentralized-identity-blockchain/. Accessed 24 September 2020; Mainelli, M. (2017). "Blockchain could help us Reclaim control of Our personal Data". Available at https://hbr.org/2017/10/smart-ledgers-can-help-us-reclaim-control-of-our-personal-data. Accessed 24 September 2020. Mainelli mentions that DLTs can also help us manage our personal to the point that we could even sell this information to whomever we want; see also Tobin, A., & Reed, D. (2016). "The Inevitable Rise of Self-Sovereign Identity" *Sovrin Foundation* at 9 – 13. Available at https://sovrin.org/wp-content/uploads/2017/06/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf. Accessed 24 September 2020; see also Accenture (2017). "Accenture, Microsoft create Blockchain Solution to support ID2020." Available at https://newsroom.accenture.com/news/accenture-microsoft-create-blockchain-solution-to-support-id2020.htm. Accessed 24 September 2020; De Filippi refers to this as 'data sovereignty' saying that individuals should have the power to share information outside the influence of governments and corporations. See De Filippi, P. (2016). "The interplay between decentralization and privacy: the case of blockchain technologies" *Journal of Peer Production Alternative Internets* at 4.

individuals to store their personal information off-chain.[1442] A person's biometrics is made available to the government only when the individual grants access. This enables an individual to prove his or her identity by availing their personal identifying information for a limited period and only when required to do so.[1443] Identity management is beneficial because no other corporation or institution will have access to that information.[1444]

4.9 The secrecy provision in the TAA

In this section, I briefly discuss the secrecy provision in the Tax Administration Act 28 of 2011 (TAA). In South Africa, a SARS official is required to preserve the secrecy of taxpayer information[1445] and that official cannot disclose the information to a person who is not a SARS official.[1446] Despite this provision, there are instances where taxpayer information can be disclosed.[1447] For example, an official can disclose

[1442] Accenture (2017). "Accenture, Microsoft create Blockchain Solution to support ID2020." Available at https://newsroom.accenture.com/news/accenture-microsoft-create-blockchain-solution-to-support-id2020.htm. Accessed 24 September 2020.

[1443] Accenture (2017). "Accenture, Microsoft create Blockchain Solution to support ID2020." Available at https://newsroom.accenture.com/news/accenture-microsoft-create-blockchain-solution-to-support-id2020.htm. Accessed 24 September 2020; Moerel, L., (2019). "Blockchain & Data Protection…and Why They Are Not on a Collision Course" *European Preview of Private Law* 26(6): 850.

[1444] Moerel, L., (2019). "Blockchain & Data Protection…and Why They Are Not on a Collision Course" *European Preview of Private Law* 26(6): 850 – 851; Tobin, A., & Reed, D. (2016). "The Inevitable Rise of Self-Sovereign Identity" *Sovrin Foundation* at 3. Available at https://sovrin.org/wp-content/uploads/2017/06/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf. Accessed 24 September 2020.

[1445] The definition has been given at paragraph 3.3.3, footnote 573.

[1446] Section 69(1) of the TAA.

[1447] Section 69(2) of the TAA reads: "Subsection (1) does not prohibit the disclosure of taxpayer information by a person who is a current or former SARS official – (a) in the course of performance of duties under a tax Act or customs and excise legislation, such as - (i) to the South African Police Service or the National Prosecuting Authority, if the information relates to, and constitutes material information for the proving of, a tax offence; (ii) as a witness in civil or criminal proceedings under a tax Act; or (iii) the taxpayer information necessary to enable a person to provide such information as may be required by SARS from that person; (b) under any other Act which expressly provides for the disclosure of the information despite the provisions in this Chapter; (c) by order of a High Court; or (d) if the information is public information. (3) An application to the High Court for the order referred to in subsection (2)(c) requires prior notice to SARS of at least 15 business days unless the court, based on urgency, allows a shorter period. (4) SARS may oppose the application on the basis that the disclosure may seriously prejudice the taxpayer concerned or impair a civil or criminal tax investigation by SARS. (5) The court may not grant the order unless satisfied that the following circumstances apply: (a) the information cannot be obtained elsewhere; (b) the primary mechanisms for procuring evidence under an Act or rule of court will yield or yielded no or disappointing results; (c) the information is central to the case; and (d) the information does not constitute biometric information. (6) Subsection (1) does not prohibit the disclosure of information - (a) to the taxpayer; or (b) with the written consent of the taxpayer, to another person. (7) Biometric taxpayer information if the information is public information.[1448] The purpose of the secrecy provision is to protect a taxpayer's right to privacy.[1449] During the VAT collection process, information relating to the supply can be collected by SARS. For example, a digital invoice can inform SARS that a customer purchased a digital book when a supply is made. If a blockchain is used for VAT collection, SARS collects the appropriate amount of VAT and information pertaining to the supply. This information constitutes taxpayer information which falls under the secrecy provision of the TAA. An official may not divulge such information unless special circumstances exist.[1450] Let us assume that the supply reveals information that relates to the commission of a crime. If that is the case, can a SARS official disclose such information to law enforcement agencies? In my view, it is unlikely that SARS will divulge such information out of its own accord to law enforcement agencies. It can also be argued that such information would have been picked up by SARS on blockchain because of blockchain's immutable and transparent nature. It should be noted that the TAA secrecy provision also prevents public access of taxpayer information on a blockchain. For this reason, taxpayer information transmitted on a blockchain must be protected using strong encryption techniques like *zero-knowledge proof* or by fully anonymising taxpayer information.

It should be noted that information contained in the transaction mentioned above also constitutes confidential information. The definition of SARS confidential information in the TAA is broad.[1451] My focus is on three provisions of section 68 of the TAA. First,

information of a taxpayer may not be disclosed by SARS except under the circumstances described in subsection (2)(a)(i). (8) The Commissioner may, despite the provisions of this section, disclose - (a) the name and taxpayer reference number of a taxpayer; (b) a list of - (i) pension funds, pension preservation funds, provident funds, provident preservation funds and retirement annuity funds as defined in section 1(1) of the Income Tax Act; and (ii) public benefit organisations approved for the purposes of sections 18A and 30 of the Income Tax Act; (c) the name and tax practitioner registration number of a registered tax practitioner; and (d) taxpayer information in an anonymised form."

[1448] Section 68(2)(d) of the TAA.

[1449] See discussion at paragraph 6.2 below.

[1450] See footnote 1447.

[1451] Section 68(1) of the TAA defines 'SARS confidential information' as: "information relevant to the administration of a tax Act that is - (a) personal information about a current or former SARS official, whether deceased or not; (b) information subject to legal professional privilege vested in SARS; (c) information that was supplied in confidence by a third party to SARS the disclosure of which could reasonably be expected to prejudice the future supply of similar information, or information from the same source; (d) information related to investigations and prosecutions described in section 39 of the Promotion of Access to Information Act; (e) information related to the operations of SARS, including an opinion, advice, report, recommendation or an account

SARS confidential information includes information relevant to the administration of a tax Act that is a computer program.[1452] I already defined a computer program above.[1453] In my view, a blockchain constitutes a computer program. Blockchain consists of sequential blocks that contain information. In the VAT collection context, those blocks contain data. The data consists of transaction data, digital invoices, and identities of taxpayers. As already discussed, this information constitutes taxpayer information. In my view, and since a blockchain constitutes a computer program, it is not in the public interest for **anyone**[1454] to access a blockchain because blockchain contains a multiplicity of transactions that constitute taxpayer information. Moreover, deciphering blockchain can reveal information relating to other taxpayers. Blockchain ledger stores all the transactions, and a copy thereof cannot be obtained by third parties because it can reveal information that was not originally intended to be revealed. Once it becomes public, the ledger can reveal all the transactions that have been recorded on blockchain since its inception. This can breach taxpayer's privacy, undermine the tax administration process, and it can erode trust. For these reasons, I do not believe that a SARS official should disclose SARS confidential information if SARS uses blockchain (computer program) for administering taxes.[1455] Second,

of a consultation, discussion or deliberation that has occurred, if - (i) the information was given, obtained or prepared by or for SARS for the purpose of assisting to formulate a policy or take a decision in the exercise of a power or performance of a duty conferred or imposed by law; and (ii) the disclosure of the information could reasonably be expected to frustrate the deliberative process in SARS or between SARS and other organs of state by - (aa) inhibiting the candid communication of an opinion, advice, report or recommendation or conduct of a consultation, discussion or deliberation; or (bb) frustrating the success of a policy or contemplated policy by the premature disclosure thereof; (f) information about research being or to be carried out by or on behalf of SARS, the disclosure of which would be likely to prejudice the outcome of the research; (g) information, the disclosure of which could reasonably be expected to prejudice the economic interests or financial welfare of the Republic or the ability of the government to manage the economy of the Republic effectively in the best interests of the Republic, including a contemplated change or decision to change a tax or a duty, levy, penalty, interest and similar moneys imposed under a tax Act or the Customs and Excise Act; (h) information supplied in confidence by or on behalf of another state or an international organisation to SARS; (i) a computer program, as defined in section 1(1) of the Copyright Act, 1978 (Act No. 98 of 1978), owned by SARS; (j) information relating to the security of SARS buildings, property, structures or systems; and (k) information relating to the verification or audit selection procedure or method used by SARS, the disclosure of which could reasonably be expected to jeopardise the effectiveness thereof."

[1452] Section 68(1)(i) of the TAA.

[1453] Paragraph 3.3.1, footnote 625.

[1454] My own emphasis.

[1455] Section 68(3) of the TAA gives scenarios when a SARS official may disclose SARS confidential information. These include "(a) the information is public information; (b) authorised by the Commissioner; (c) disclosure is authorised under any other Act which expressly provides for the disclosure of the information despite the provisions in this Chapter; (d) access has been

SARS confidential information includes information supplied in confidence by or on behalf of another state or international organisation.[1456] If SARS uses blockchain to exchange tax information with another tax authority, information supplied by a foreign tax authority is sent to SARS in confidence and such information constitutes SARS confidential information. For the same reasons mentioned above, I do not believe that a blockchain ledger containing such information should be made available to anyone other than SARS due to blockchain's features. The information supplied by the foreign tax authority on blockchain should not be disclosed under any circumstances. Last, SARS confidential information includes information relating to the verification or audit method used by SARS.[1457] A blockchain used for tax administration allows SARS to conduct verification and audits on taxpayers and taxpayer transactions. In my view, disclosing a blockchain can reasonably jeopardise the effectiveness of the tax administration process.[1458] It is not in anyone's interests to access this verification and audit method (a blockchain). In my view, the provisions in the TAA do not adequately protect taxpayers if SARS uses blockchain to administer taxes. As a result, the TAA should be amended to exclude the application of sections 68(3) and 69 of the TAA on SARS and SARS officials when taxes are administered on blockchain.

In *Arena Holdings (Pty) Limited t/a Financial Mail v SARS and others*,[1459] the Constitutional Court had to determine whether section 35(1)[1460] and section 46[1461] of Promotion of Access to Information Act (PAI Act)[1462] and the secrecy provisions in the

granted for the disclosure of the information in terms of the Promotion of Access to Information Act; or (e) required by order of a High Court."

[1456] Section 68(1)(h) of the TAA.

[1457] Section 68(1)(k) of the TAA.

[1458] Section 68(1)(k) of the TAA.

[1459] (CCT 365/21) [2023] ZACC 13; 2023 (8) BCLR 905 (CC); 2023 (5) SA 319.

[1460] Section 35 reads: "(1) Subject to subsection (2), the information officer of the South African Revenue Service, referred to in section 2(3), must refuse a request for access to a record of that Service if it contains information which was obtained or is held by that Service for the purposes of enforcing legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act, 1997(Act No. 34 of 1997). (2) A record may not be refused in terms of subsection (1) insofar as it consists of information about the requester or the person on whose behalf the request is made."

[1461] Section 46 reads: "Despite any other provision of this Chapter, the information officer of a public body must grant a request for access to a record of the body contemplated in section 34(1), 36(1), 37(1)(a), or (b), 38(a) or (b), 39(1)(a) or (b), 40, 41(1)(a) or (b), 42(1) or (3), 43(1) or (2), 44(1) or (2) or 45 if: (a) the disclosure of the record would reveal evidence of – (i) a substantial contravention of, or failure to comply with, the law; or (ii) an imminent and serious public safety or environmental risk; and (b) the public interest in the disclosure of the record clearly outweighs the harm contemplated in the provision in question."

[1462] Act 2 of 2000.

TAA were unconstitutional to the extent that it precluded access to tax information if the request was in the public's interest (public-interest override).[1463] The applicants, a media company, argued that these provisions prevented the media from obtaining tax information from SARS and reporting tax information which they believed contained information that purported to show evidence of corruption.[1464] The applicants also argued that this limitation was unconstitutional to the extent that it limited the right to access information in terms of section 32(1) of the Constitution and the right to freedom of expression in section 16 of the Constitution.[1465] The minority judgment[1466] held that the limitation was justifiable because the provisions of the TAA provided for a balance between access to taxpayer information and preserving taxpayer secrecy. Also, the Court held the disclosure of taxpayer information would pose a challenge to the privacy interests of individuals and this could be detrimental to the reputations and societal standings if taxpayers.[1467] The majority judgment[1468] found that it was difficult to defend the prohibition in section 35(1) of the PAI Act because various exceptions to confidentiality exist within the TAA.[1469] The majority of the judges also found that the argument that absolute confidentiality is necessary to ensure tax compliance could not be sustained because there are certain exceptions to this rule in the TAA.[1470] The Court held that taxpayers generally comply with tax obligations because the law requires them to do so in order to avoid criminal sanctions.[1471]

I briefly discuss the *Arena* judgment because it highlights SARS's obligation to keep taxpayer information secret. In other words, taxpayers expect SARS to keep information about their financial and personal lives confidential.[1472] Also, the case underscores the fact that SARS is party to multiple international agreements.[1473] In terms of these agreements, taxpayer information is shared with other entities subject

[1463] At paragraph [17].
[1464] At paragraph [17].
[1465] At paragraph [18].
[1466] At paragraph [1] – [122].
[1467] At paragraph [112] – [114].
[1468] At paragraph [123] – [205].
[1469] At paragraph [177].
[1470] At paragraph [178].
[1471] At paragraph [184].
[1472] At paragraph [56].
[1473] The USA Foreign Account Tax Compliance Act (FATCA) Intergovernmental Agreement, Bilateral Tax Information Exchange Agreements (TIEAs), the Convention on Mutual Administrative Assistance in Tax Matters, and several Bilateral Double Taxation Agreements and Protocols. See paragraph [91].

to the necessary confidentiality clauses.[1474] This ensures that tax information is disseminated in confidence, which coincides with SARS obligations under international law.[1475] For these reasons, I maintain that a private blockchain assists SARS to perform its functions while preserving the confidentiality of taxpayer information. A public blockchain is not suitable under these circumstances because it allows anyone with a node to access the network and to retrieve taxpayer information.

4.10 Conclusion

This chapter demonstrates that blockchain affects data privacy. Be that as it may, blockchain's characteristics are also conducive for techniques that assist to maintain data privacy. While no single privacy enhancing technique is without issues, a combination of techniques can prove crucial in the promotion of privacy in a decentralised ledger.

The secrecy provisions in the TAA do not adequately protect taxpayer information if SARS administers taxes on blockchain. I believe that the TAA must be amended to exclude the application of certain provisions when taxes are administered on a blockchain.

In the next chapter, I discuss how the legislative framework in the EU protects data processed on a blockchain.

[1474] At paragraph [91].
[1475] At paragraph [94].

CHAPTER 5: THE PROTECTION OF PERSONAL INFORMATION ON BLOCKCHAIN – THE EU

5.1 Introduction

In the previous chapter, I discussed the relationship between privacy and blockchain. Chapter three explored the role that governments and private corporations play when processing personal information. It was established that governments use personal information primarily for the provision of services to citizens. The collection of personal information at public level is 'passive' in the sense that a country merely accesses personal information from government records to provide services to the public. Private entities collect and process personal information actively to generate revenue. The uses of personal information on a public and private scale have been enhanced by the Internet and other technologies. However, Internet use has also highlighted concerns associated with the collection and processing of personal information. Issues such as identity theft, surveillance, data mining, and data profiling have gained prominence.

Blockchain's immutability, public nature, and transparency have heightened these issues. While blockchain can complicate issues around privacy, its infrastructure has capabilities that can protect data privacy. The implementation of a single privacy enhancing technique on blockchain may not be sufficient. A combination of data privacy techniques can be effective in the protection of data privacy.

In this chapter, I explore the data protection provisions in the EU's GDPR. The processing of personal information on a decentralised blockchain has the potential to raise tensions with the provisions of the GDPR. This study also explores the impact that the GDPR has on blockchain applications.

5.2 Data protection

5.2.1 What is data protection?

From the outset, it must be noted that the terms ‘data privacy’ and ‘data protection’ are synonyms. North America and Canada use the term ‘data privacy’ while ‘data protection’ is mostly used in Europe.[1476] For purposes of this study, I shall use the term ‘data protection’.

The term ‘data protection’ has been described as a ‘misnomer’ because protection is not necessarily afforded to data[1477] *per se* but rather to the processing of data[1478] belonging to an individual.[1479] In other words, data protection principles aim to protect the rights of individuals whenever their personal information is processed by public and private entities.[1480] Despite the apparent ‘misnomer’, data protection has been widely defined. For instance, Roos defines data protection as “the legal protection of a person with regard to the processing of data concerning himself or herself by another person or institution.”[1481] Bennett structures the definition of data protection slightly differently. According to Bennett, data protection constitutes “policies designed to

[1476] See Abdulrauf, L. (2014). “Do we need to bother about protecting our personal data: Reflections on neglecting data protection in Nigeria” *Yonsei Law Journal* 5(2): 169; Makulilo, A., B. (2012). “Privacy and data protection in Africa: a state of the art” *International Data Privacy Law* 2(3): 164.

[1477] It is important to note that ‘personal data’ and ‘personal information’ are synonyms. Roos defines ‘data’ as the “unstructured facts or raw material that needs to be processed and organized to produce information.” Ross defines ‘information’ as “data that are organized, structured and meaningful to the recipient.” See Roos, A. (2007). “Data protection: Explaining the international backdrop and evaluating the current South African position” *South African Law Journal* 124(2): 401 at footnote 4.

[1478] Article 2(b) of the EU directive 95/46/EC of the European Parliament and the Council of 24 October 1995 defines ‘data processing’ as: “any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.”

[1479] Tamò-Larrieux, A., (2018). *Designing for Privacy and its Legal Framework: Data Protection by Design and Default for the Internet of Things* Springer at 76; see also Schwartz, P., (1992). “Data Processing and Government Administration: The Failure of the American Legal Response to the Computer” *Hastings Law Journal* 43(5): 1374.

[1480] Tamò-Larrieux, A., (2018). *Designing for Privacy and its Legal Framework: Data Protection by Design and Default for the Internet of Things* Springer at 76.

[1481] Roos, A. (2006). “Core principles of data protection law” *Comparative and International Law Journal of Southern Africa* 39(1): 104.

regulate the collection, storage, use and transmittal of personal information."[1482] Honduis defines data protection as "the body of law which secures every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms and in particular his right of privacy with regard to automatic processing of personal data relating to him."[1483]

The role of data protection is clear. First, data protection seeks to ensure that the processing of personal information of natural persons is done lawfully by individuals and other actors.[1484] The processing of personal information includes storage, collection, and dissemination. Second, data protection legalises all stages in the processing of data.[1485] Last, data protection seeks to protect individuals from the unlawful use, storage, collection, and dissemination of their personal information.[1486]

It is generally accepted that data protection laws apply to information that can be used to identify natural persons.[1487] For this reason, any information that cannot identify a natural person is not considered personal information. According to Abdulrauf, data protection laws do not apply to: (i) any information that is processed for public interest, (ii) any information processed for personal activity, (iii) any information processed for journalistic and artistic purposes, and (iv) de-identified data.[1488]

[1482] Bennett, C., J. (1992). *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* Cornell University Press at 13; see also Roos, A. (2003). *The law of data (privacy) protection: a comparative and theoretical study* (unpublished LLD thesis Unisa 2003) at 16.

[1483] Honduis, F., W. (1983). "A Decade of International Data Protection" *Netherlands International Law Review* 30(2): 103; see also Roos, A. (2003). *The law of data (privacy) protection: a comparative and theoretical study* (unpublished LLD thesis Unisa (2003) at 16.

[1484] Abdulrauf, L. (2014). "Do we need to bother about protecting our personal data: Reflections on neglecting data protection in Nigeria" *Yonsei Law Journal* 5(2): 170; Bygrave, L., A. (2014). *Data Privacy Law: An International Perspective* Oxford University Press (UK) at 1.

[1485] Abdulrauf, L. (2014). "Do we need to bother about protecting our personal data: Reflections on neglecting data protection in Nigeria" *Yonsei Law Journal* 5(2): 171.

[1486] Abdulrauf, L. (2014). "Do we need to bother about protecting our personal data: Reflections on neglecting data protection in Nigeria" *Yonsei Law Journal* 5(2): 170; De Hert, P., & Gutwirth, S., *Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action* in S. Gutwirth *et al* (eds) (2009). *Reinventing Data Protection?* Springer at 4.

[1487] Bygrave, L., A. (2014). *Data Privacy Law: An International Perspective* Oxford University Press (UK) at 1.

[1488] Abdulrauf, L. (2014). "Do we need to bother about protecting our personal data: Reflections on neglecting data protection in Nigeria" *Yonsei Law Journal* 5(2): 171.

5.2.2 A brief overview of data protection

The proliferation of computers in the 1950s signalled a new era that initiated the spread of information on a global scale. In fact, the use of computers was influential in the collection, processing, and dissemination of information at speeds never previously encountered.[1489] The introduction of computers and technology also aided the expansion of multinational companies.[1490] In order for multinational companies to render better services, it was necessary to achieve product uniformity and identity. This could only be achieved if multinational companies accessed markets that were previously inaccessible.[1491] The advent of computers and technology facilitated the transfer of information through computer networks. Different users across the globe were able to access information on these networks. Financial information and employment records became readily accessible to companies.[1492]

The growth of technology and information dissemination led to the recognition of two important opposing factors in the international arena. These were the protection of an individual's privacy and the promotion of the free flow of information among states.[1493] Protecting an individual's privacy requires preserving a certain degree of confidentiality. The preservation of privacy requires a reduction in the flow of personal information. An extensive approach to the restriction of the flow information, particularly on the international scale, could lead to a limitation of the free flow of information.[1494] In view of the above, it is important to note that a discussion on data protection is not restricted to provisions that seek to protect an individual's personal

[1489] Roos, A. (2007). "Data protection: Explaining the international backdrop and evaluating the current South African position" *South African Law Journal* 124(2): 401.

[1490] Lloyd, J., I. (2011). *Information Technology Law* 6th edition Oxford University Press (New York) at 23.

[1491] Lloyd, J., I. (2011). *Information Technology Law* 6th edition Oxford University Press (New York) at 23.

[1492] Roos, A. (2007). "Data protection: Explaining the international backdrop and evaluating the current South African position" *South African Law Journal* 124(2): 401.

[1493] Beling, C., T. (1983). "Transborder Data Flows: International Privacy Protection and the Free Flow of Information" *Boston College International and Comparative Law Review* 6(2): 594; Lloyd, J., I. (2011). *Information Technology Law* 6th edition Oxford University Press (New York) at 23.

[1494] Beling, C., T. (1983). "Transborder Data Flows: International Privacy Protection and the Free Flow of Information" *Boston College International and Comparative Law Review* 6(2): 594.

information but also a discussion on the promotion of commerce[1495] on an international scale.[1496]

5.2.3 The development of data protection law

5.2.3.1 Overview

In order to address the disparity between the protection of an individual's privacy and the free flow of information, it became necessary to harmonise data protection laws.[1497] It was established that a lack of harmonisation in data protection laws placed an unnecessary burden on multinational companies due to the different regulatory compliance measures in various countries where data was stored, collected or transferred.[1498] Additionally, the lack of regulation surrounding the automated processing of personal information required redress from lawmakers.[1499]

International organisations accepted that there was a need to regulate the cross-border transfer of information due to its increased importance in the global economy.[1500] What follows is a discussion of the most significant organisations that implemented measures to protect personal information.

[1495] This is particularly accurate in the context of e-commerce where goods and services are exchanged. That exchange cannot take place without the recipient providing personal information to the seller. It is trite that commerce boosts economies of states.

[1496] For this reason, Beling states when implementing data protection measures into national laws certain factors need to be considered. The first is whether there are any provisions that enable the transborder transfer of data. Second, whether the provisions are legally binding between states. Third, the extent and application of any enforcement mechanisms. And last, the nature of data subjects covered by data protection. See Beling, C., T. (1983). "Transborder Data Flows: International Privacy Protection and the Free Flow of Information" *Boston College International and Comparative Law Review* 6(2): 594 – 595.

[1497] It is widely accepted that the German State of Hese was enacted the first data protection law in 1970. Thereafter, Sweden enacted the Swedish Data Protection Act in 1973. See Roos., A. (2007). "Data protection: Explaining the international backdrop and evaluating the current South African position" *South African Law Journal* 124(2): 402 footnote 12; Lloyd, J., I. (2011). *Information Technology Law* 6th edition Oxford University Press (New York) at 22.

[1498] Lloyd, J., I. (2011). *Information Technology Law* 6th edition Oxford University Press (New York) at 23.

[1499] Roos., A. (2007). "Data protection: Explaining the international backdrop and evaluating the current South African position" *South African Law Journal* 124(2): 402.

[1500] Roos., A. (2007). "Data protection: Explaining the international backdrop and evaluating the current South African position" *South African Law Journal* 124(2): 403.

5.2.3.2 The United Nations

Privacy protection measures were introduced after the events of the Second World War (WWII) when fascist groups relied on personal information to attack and cause carnage to people.[1501] These incidents that took place in central Europe led to the resolution and approval of the Universal Declaration of Human Rights (UDHR) on 10 December 1948.[1502] The UDHR is essentially a Declaration that aims to proclaim first generation rights consisting of political and civil rights and second generation rights that consists of cultural, social and economic rights.[1503] Although the UDHR has been widely adopted, the Declaration is not a legal binding document.[1504]

The Declaration contains thirty articles.[1505] The rights entrenched in the Declaration do not specifically address data protection. For example, Article 9 of the Declaration mentions the right of an individual not to be arrested arbitrarily. Article 15 of the Declaration enforces everyone's right to nationality including the right not to have such nationality deprived arbitrarily.[1506] The Article that is of significance to this study is Article 12 of the Declaration. Article 12 reads "no one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against the

[1501] Makulilo, A., B. (2012). *Protection of Personal Data in sub-Saharan Africa* published *Dr Jur* thesis (Universität Bremen) at 107; According to Lloyd, the Nazis and the Communist regime in East Germany misused individual's personal information. Consequently, data protection legislation was introduced to curb private and public entities from processing personal information. See Lloyd, J., I. (2011). *Information Technology Law* 6th edition Oxford University Press (New York) at 22; Abdulrauf, L., A., (2015). *The Legal Protection of Data Privacy in Nigeria: Lessons from Canada and South Africa* Unpublished LLD thesis (University of Pretoria) at 49.

[1502] UN General Assembly Resolution 217A (III) A/RES/3/217A 10 December 1948; Dugard, J. (2011). *International Law: A South African Perspective* Juta & Co Ltd (Cape Town) at 325.

[1503] Dugard, J. (2011). *International Law: A South African Perspective* Juta & Co Ltd (Cape Town) at 325.

[1504] Dugard, J. (2011). *International Law: A South African Perspective* Juta & Co Ltd (Cape Town) at 325; Makulilo, A., B. (2012). *Protection of Personal Data in sub-Saharan Africa* published *Dr Jur* thesis (Universität Bremen) at 108.

[1505] UN General Assembly (1948). *The Universal Declaration of Human Rights*. Available at https://www.ohchr.org/en/udhr/documents/udhr_translations/eng.pdf . Accessed 18 February 2021.

[1506] Articles 9 and 15 of the UDHR. See UN General Assembly (1948). *The Universal Declaration of Human Rights*. Available at https://www.ohchr.org/en/udhr/documents/udhr_translations/eng.pdf . Accessed 18 February 2021.

interference or attacks."[1507] A key component of Article 12 is the protection of an individual's privacy and the prohibition of any interference. Makulilo argues that there is a limitation on an individual's right to privacy in the Declaration.[1508] The limitation arises from Article 29(2) of the Declaration which states that "in the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in democratic society."[1509] Makulilo argues further that it is necessary to limit an individual's rights to balance the other rights provided in the Declaration.[1510]

Another important instrument that played a significant role in the development of data protection is the International Covenant on Civil and Political Rights (ICCPR). The ICCPR is a human rights treaty that affirms an individual's right to self-determination.[1511] Article 17(1) of the ICCPR states that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence or to attacks upon his honour and reputation."[1512] Article 17(2) states "everyone has the right to the protection of the law against such interference or attacks."[1513] Although the treaty's main focus is on civil and political rights,[1514] it is said that the right to privacy

[1507] See UN General Assembly Resolution 217A (III) A/RES/3/217A 10 December 1948; Makulilo, A., B. (2012). *Protection of Personal Data in sub-Saharan Africa* published *Dr Jur* thesis (Universität Bremen) at 108.

[1508] Makulilo, A., B. (2012). *Protection of Personal Data in sub-Saharan Africa* published *Dr Jur* thesis (Universität Bremen) at 109.

[1509] Article 29(2) of the UDHR. See UN General Assembly (1948). *The Universal Declaration of Human Rights*. Available at https://www.ohchr.org/en/udhr/documents/udhr_translations/eng.pdf . Accessed 18 February 2021; see also Makulilo, A., B. (2012). *Protection of Personal Data in sub-Saharan Africa* published *Dr Jur* thesis (Universität Bremen) at 108 – 109.

[1510] Makulilo, A., B. (2012). *Protection of Personal Data in sub-Saharan Africa* published *Dr Jur* thesis (Universität Bremen) at 109.

[1511] Dugard, J. (2011). *International Law: A South African Perspective* Juta & Co Ltd (Cape Town) at 327.

[1512] UN General Assembly International Covenant on Civil and Political Rights adopted on 19 December 1966. Available at https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf. Accessed 10 December 2020.

[1513] UN General Assembly International Covenant on Civil and Political Rights adopted on 19 December 1966. Available at https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf. Accessed 10 December 2020.

[1514] Makulilo, A., B. (2012). *Protection of Personal Data in sub-Saharan Africa* published *Dr Jur* thesis (Universität Bremen) at 109.

established the foundation that eventually led to the formulation of data protection principles.[1515]

In 1968, the United Nations (UN) adopted a resolution to implement data privacy mechanisms. The resolution took place in Tehran at the International Conference on Human Rights convened by the UN General Assembly 20 years after the UDHR.[1516] According to the plenary meeting held on 19 December 1968, the UN General Assembly sought to examine the challenges posed to human rights by science and technology. While the General Assembly acknowledged the role that scientific discoveries and technological advancements played in the development of society and the economy, concerns were raised about the impact that these advancements affected the rights and freedoms of individuals.[1517] One of the developments that came out of the conference was the 1976 publication of a report advising countries to sanction data privacy legislation covering computerized personal data systems in the private and public sectors.[1518]

Subsequent to the 1968 resolution, the UN adopted *Guidelines for the Regulation of Computerized Personal Data Files* (the 1990 UN Guidelines) in 1990.[1519] The 1990 UN Guidelines established ‘minimum guarantees’ for implementation in national legislation that seek to protect personal information.[1520] The 1990 UN Guidelines apply to personal information stored on computer files by public and private entities.[1521] Additionally, the guidelines also apply to personal information kept or processed by

[1515] Bygrave, L. A. (1998). “Data protection pursuant to the right to privacy in human rights treaties” *International Journal of Law and Information Technology* 6(3): 248.

[1516] Hondius, F., W. (1980). “Data Law in Europe” *Stanford Journal of International Law* (16): 90; Roos, A. (2003). *The law of data (privacy) protection: a comparative and theoretical study* (unpublished LLD thesis Unisa 2003) at 151 footnote 1.

[1517] See UN General Assembly Resolution on Human Rights and Scientific and Technological Developments 2450 of 19 December 1968.

[1518] Bygrave, L., A. (2014). *Data Privacy Law: An International Perspective* Oxford University Press (UK) at 51; Yilma, K., M. (2019) “The United Nations data privacy system and its limits” *International Review of Law, Computers & Technology* 33(2): 224-248.

[1519] See UN General Assembly Guidelines for the Regulation of Computerized Personal Data Files A/RES/45/95 of 14 December 1990.

[1520] See UN General Assembly Guidelines for the Regulation of Computerized Personal Data Files A/RES/45/95 of 14 December 1990; Bygrave, L., A. (2014). *Data Privacy Law: An International Perspective* Oxford University Press (UK) at 51 – 52; Lloyd, J., I. (2011). *Information Technology Law* 6th edition Oxford University Press (New York) at 28 – 29.

[1521] See UN General Assembly Guidelines for the Regulation of Computerized Personal Data Files A/RES/45/95 of 14 December 1990; Bygrave, L., A. (2014). *Data Privacy Law: An International Perspective* Oxford University Press (UK) at 51 – 52.

international governmental organizations and the manual processing of files by legal entities.[1522]

5.2.3.3 The OECD guidelines

The OECD begun work on data protection rules in 1969 when experts were tasked to explore how aspects such as digital transformation and cross border data flows affected privacy.[1523] The OECD published the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (the OECD Guidelines) on 23 September 1980.[1524] The OECD Guidelines consist of eight principles designed to cover the electronic and manual processing of personal information by the private and public sector.[1525] Although the OECD Guidelines are not binding on countries,[1526] they set the standard for data protection framework in national laws.[1527]

According to the OECD, the primary reason for the adoption of the guidelines was the increased transmission of data across national borders which originated from the spread and establishment of automatic data processing.[1528] The lack of harmonisation in national laws had a significant impact on the flow of personal information across countries. The rapid growth of technology and computers contributed to the increased flow of personal information. The OECD observed that any curtailment of the free flow

[1522] See UN General Assembly Guidelines for the Regulation of Computerized Personal Data Files A/RES/45/95 of 14 December 1990; see also Lloyd, J., I. (2011). *Information Technology Law* 6th edition Oxford University Press (New York) at 28 – 29.

[1523] Lloyd, J., I. (2011). *Information Technology Law* 6th edition Oxford University Press (New York) at 27.

[1524] OECD (1980). *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Available at http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Accessed 10 December 2020.

[1525] OECD (1980). *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Available at http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Accessed 10 December 2020; Bygrave, L., A. (2014). *Data Privacy Law: An International Perspective* Oxford University Press (UK) at 43.

[1526] Makulilo, A., B. (2012). *Protection of Personal Data in sub-Saharan Africa* published *Dr Jur* thesis (Universität Bremen) at 133; Roos, A. (2003). *The law of data (privacy) protection: a comparative and theoretical study* (unpublished LLD thesis Unisa 2003) at 155.

[1527] Abdulrauf, L., A., (2015). *The Legal Protection of Data Privacy in Nigeria: Lessons from Canada and South Africa* Unpublished LLD thesis (University of Pretoria) at 54.

[1528] OECD (1980). Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Available at http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Accessed 10 December 2020.

of personal information was a hindrance on key sectors of the economy such as insurance and banking.[1529] The OECD sought to remove any barriers that limited the transborder flow of personal information.[1530] According to Abdulrauf, this demonstrated the OECD's commercial interest in maintaining the cross-border flow of personal information.[1531]

The OECD updated its guidelines in 2013 because of growing advancements in technology.[1532] The new guidelines focus primarily on "the practical implementation of privacy protection through an approach grounded in risk management and the need for greater efforts to address the global dimension of privacy through improved interoperability."[1533] The OECD identifies concepts that can be used as aids for privacy protection. At national level, strategic coordination may be required at all levels of government.[1534] Second, it is important to look at management programmes that organisations can use to implement privacy protection.[1535] And last, a notification system can be introduced to notify a central authority and to natural persons if security breaches occur.[1536]

[1529] OECD (1980). Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Available at http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Accessed 10 December 2020.

[1530] Abdulrauf, L., A., (2015). *The Legal Protection of Data Privacy in Nigeria: Lessons from Canada and South Africa* Unpublished LLD thesis (University of Pretoria) at 53.

[1531] Abdulrauf, L., A., (2015). *The Legal Protection of Data Privacy in Nigeria: Lessons from Canada and South Africa* Unpublished LLD thesis (University of Pretoria) at 53.

[1532] See Abdulrauf, L., A., (2015). *The Legal Protection of Data Privacy in Nigeria: Lessons from Canada and South Africa* Unpublished LLD thesis (University of Pretoria) at 53.

[1533] OECD (2013). *The OECD Privacy Framework* at 4. Available at http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. Accessed 12 December 2020; Abdulrauf, L., A., (2015). *The Legal Protection of Data Privacy in Nigeria: Lessons from Canada and South Africa* Unpublished LLD thesis (University of Pretoria) at 53; Bygrave, L., A. (2014). *Data Privacy Law: An International Perspective* Oxford University Press (UK) at 44.

[1534] OECD (2013). *The OECD Privacy Framework* at 4. Available at http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. Accessed 12 December 2020.

[1535] OECD (2013). *The OECD Privacy Framework* at 4. Available at http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. Accessed 12 December 2020.

[1536] OECD (2013). *The OECD Privacy Framework* at 4. Available at http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. Accessed 12 December 2020.

5.2.3.4 The Council of Europe

The Council of Europe[1537] (CoE) is a regional international organisation that seeks to protect human rights and enforce the rule of law.[1538] According to Bygrave, the CoE is the first organisation that has drafted a multilateral treaty that specifically deals with data protection.[1539] The treaty adopted by the CoE, known as the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*,[1540] was approved on 28 January 1981.[1541] The adoption came as a result of recommendations and resolutions by the Council's Parliamentary Assembly in the 1970s. The Council's Parliamentary Assembly sought to examine the impact that science and technology had on human rights infringement.[1542]

The Council Committee Members established that the processing of personal information by computer technology presented new challenges that were not adequately addressed by the European Convention of Human Rights[1543] (ECHR),

[1537] The CoE was founded in 1949 by Sir Winston Churchill, Konrad Adenauer, Robert Schuman, Paul-Henri Spaak, Alcide de Gasperi and Ernst Bevin. The organisation currently has 47 member states. These include Albania, Andorra, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Monaco, Montenegro, Netherlands, North Macedonia, Norway, Poland, Portugal, Republic of Moldova, Romania, Russian Federation, San Marino, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey, Ukraine and the United Kingdom. The CoE's headquarters is situated in Strasbourg, France. Available at https://www.coe.int/en/web/about-us/who-we-are. Accessed 13 December 2020.

[1538] Hondius, F., W. (1980). "Data Law in Europe" *Stanford Journal of International Law* (16): 91.

[1539] See Bygrave, L., A. (2014). *Data Privacy Law: An International Perspective* Oxford University Press (UK) at 31.

[1540] Available at https://rm.coe.int/1680078b37. Accessed 13 December 2020.

[1541] See CoE (1981). *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. Available at https://rm.coe.int/1680078b37. Accessed 13 December 2020; Bygrave, L., A. (2014). *Data Privacy Law: An International Perspective* Oxford University Press (UK) at 31 – 32, Abdulrauf, L., A., (2015). *The Legal Protection of Data Privacy in Nigeria: Lessons from Canada and South Africa* Unpublished LLD thesis (University of Pretoria) at 55.

[1542] Hondius, F., W. (1980). "Data Law in Europe" *Stanford Journal of International Law* (16): 91; Makulilo, A., B. (2012). *Protection of Personal Data in sub-Saharan Africa* published *Dr Jur* thesis (Universität Bremen) at 145 – 156; Bygrave, L., A. (2014). *Data Privacy Law: An International Perspective* Oxford University Press (UK) at 31 – 43; Abdulrauf, L., A., (2015). *The Legal Protection of Data Privacy in Nigeria: Lessons from Canada and South Africa* Unpublished LLD thesis (University of Pretoria) at 54 – 58.

[1543] The European Convention of Human Rights is a convention that was established in Rome on 4 November 1950 by the CoE. Available at https://www.echr.coe.int/documents/convention_eng.pdf. Accessed 13 December 2020.

which applied the automated processing of personal information.[1544] The ECHR was perceived to be restrictive because it only applied to public bodies and natural persons. Second, the ECHR had two articles, namely the right to respect for private and family life (Article 8) and the right to freedom of expression (Article 10), which on face value appeared to be inconsistent with each other.[1545] Third, challenges emanating from the manipulation of computer use was not covered by the ECHR.[1546] Last, it was found that member countries did not have adequate measures in their respective national laws to protect personal information.[1547]

Based on the findings, the Council Committee members recommended the adoption of additional Resolutions. Resolution No 22 of 1973[1548] and Resolution No 29 of 1974[1549] were implemented to facilitate the enactment of principles on the protection of individuals' privacy rights.[1550] The protection was afforded against what the CoE referred to as "data banks"[1551] in the private and public sectors. The implementation

[1544] Hondius, F., W. (1980). "Data Law in Europe" *Stanford Journal of International Law* (16): 92; Makulilo, A., B. (2012). *Protection of Personal Data in sub-Saharan Africa* published *Dr Jur* thesis (Universität Bremen) at 145 – 156; Bygrave, L., A. (2014). *Data Privacy Law: An International Perspective* Oxford University Press (UK) at 31 – 43; Abdulrauf, L., A., (2015). *The Legal Protection of Data Privacy in Nigeria: Lessons from Canada and South Africa* Unpublished LLD thesis (University of Pretoria) at 54 – 58; Bygrave, L., A. (2014). *Data Privacy Law: An International Perspective* Oxford University Press (UK) at 35.

[1545] Hondius, F., W. (1980). "Data Law in Europe" *Stanford Journal of International Law* (16): 92; Makulilo, A., B. (2012). *Protection of Personal Data in sub-Saharan Africa* published *Dr Jur* thesis (Universität Bremen) at 145 – 156.

[1546] Hondius, F., W. (1980). "Data Law in Europe" *Stanford Journal of International Law* (16): 92; Makulilo, A., B. (2012). *Protection of Personal Data in sub-Saharan Africa* published *Dr Jur* thesis (Universität Bremen) at 145 – 156.

[1547] Bygrave, L., A. (2014). *Data Privacy Law: An International Perspective* Oxford University Press (UK) at 34.

[1548] CoE (1973). *Resolution on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector*. Available at https://rm.coe.int/1680502830. Accessed 14 December 2020.

[1549] CoE (1974). *Resolution on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector*. Available at https://rm.coe.int/16804d1c51. Accessed 14 December 2020.

[1550] See Hondius, F., W. (1980). "Data Law in Europe" *Stanford Journal of International Law* (16): 92.

[1551] According to Honduis, 'data banks' are "concentrations of data banks." See Hondius, F., W. (1980). "Data Law in Europe" *Stanford Journal of International Law* (16): 102. The CoE uses a slightly different term and definition. According to the CoE, 'electronic data banks' refers to "any electronic data processing system which is used to handle such information." In this context, the 'information' that CoE is referring to is personal information. See CoE (1973). *Resolution on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector*. Available at https://rm.coe.int/1680502830. Accessed 14 December 2020 and CoE (1974). *Resolution on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector*. Available at https://rm.coe.int/16804d1c51. Accessed 14 December 2020. Honduis states that the CoE has since abandoned the term 'electronic data bank' due to the of these Resolutions resulted in the harmonisation of data protection laws in member countries. The harmonisation consolidated the data protection measures with the aim of preserving the free flow of data in European Countries.[1552]

Interestingly, the Convention is legally binding on member countries.[1553] Although it does not specifically prescribe enforceable rights in courts of law, member countries are obligated to absorb the relevant principles in their national laws.[1554] Due to its influence, the Convention resulted in the assumption of the EU Directive 95/46/EC.[1555]

5.2.3.5 The EU Data Protective Directive

The EU Data Protection Directive 95/46/EC (DPD) is the most crucial and noteworthy directive on data protection.[1556] Concerned with the impact that computer technology had on the protection of human rights, the European Parliament (EP) urged EU member countries to implement, ratify and sign a Directive on data privacy.[1557]

Work commenced in 1981 after the European Commission discovered inconsistent application of data protection laws among member countries. The European Commission sought to remove elements in national privacy laws that impeded the attainment of the internal market and growth in the computer industry.[1558] The lack of uniformity among member countries highlighted the limitations of the CoE Convention

apparent constraints the term had on the storage of personal information. The distinction between the private and public sectors has also been removed.

[1552] Bygrave, L., A. (2014). *Data Privacy Law: An International Perspective* Oxford University Press (UK) at 34.

[1553] Makulilo, A., B. (2012). *Protection of Personal Data in sub-Saharan Africa* published *Dr Jur* thesis (Universität Bremen) at 147; Abdulrauf, L., A., (2015). *The Legal Protection of Data Privacy in Nigeria: Lessons from Canada and South Africa* Unpublished LLD thesis (University of Pretoria) at 57.

[1554] Makulilo, A., B. (2012). *Protection of Personal Data in sub-Saharan Africa* published *Dr Jur* thesis (Universität Bremen) at 147.

[1555] Makulilo, A., B. (2012). *Protection of Personal Data in sub-Saharan Africa* published *Dr Jur* thesis (Universität Bremen) at 147.

[1556] Bygrave, L., A. (2014). *Data Privacy Law: An International Perspective* Oxford University Press (UK) at 53; Abdulrauf, L., A., (2015). *The Legal Protection of Data Privacy in Nigeria: Lessons from Canada and South Africa* Unpublished LLD thesis (University of Pretoria) at 60; Birnhack, M., D. (2008). “The EU Data Protection Directive: An engine of a global regime” *Computer Law & Security Review* 24(6): 512.

[1557] Bygrave, L., A. (2014). *Data Privacy Law: An International Perspective* Oxford University Press (UK) at 54.

[1558] Bygrave, L., A. (2014). *Data Privacy Law: An International Perspective* Oxford University Press (UK) at 55.

and the OECD Guidelines in motivating member countries to sanction a comprehensive data protection regime.[1559]

In 1990, the Commission released the initial framework Directive on data protection.[1560] Subsequent to its adoption, the Directive received much disapproval from privacy advocates and businesses. After several discussions, a second amended Directive was issued in 1992 but was similarly disapproved.[1561] Three years after the initial framework was adopted, the EP ratified the *Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data* (the DPD) on 24 October 1995.[1562] The DPD is primarily based on the UN Guidelines, the CoE Convention, and the OECD Guidelines.[1563]

5.3 The General Data Protection Regulation

5.3.1 Overview

The EP adopted the General Data protection Regulation (the GDPR) on 27 April 2016.[1564] Although the GDPR was approved in 2016, it only came into effect on 25 May 2018.[1565] The GDPR's status is akin to legislation. EU member countries cannot unilaterally amend the provisions of the GDPR. Therefore, the GDPR operates as

[1559] Bygrave, L., A. (2014). *Data Privacy Law: An International Perspective* Oxford University Press (UK) at 55.

[1560] Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data COM(90) 314 final – SYN 287; see also Bygrave, L., A. (2014). *Data Privacy Law: An International Perspective* Oxford University Press (UK) at 56; Abdulrauf, L., A., (2015). *The Legal Protection of Data Privacy in Nigeria: Lessons from Canada and South Africa* Unpublished LLD thesis (University of Pretoria) at 61.

[1561] Bygrave, L., A. (2014). *Data Privacy Law: An International Perspective* Oxford University Press (UK) at 56; Abdulrauf, L., A., (2015). *The Legal Protection of Data Privacy in Nigeria: Lessons from Canada and South Africa* Unpublished LLD thesis (University of Pretoria) at 61.

[1562] Abdulrauf, L., A., (2015). *The Legal Protection of Data Privacy in Nigeria: Lessons from Canada and South Africa* Unpublished LLD thesis (University of Pretoria) at 61.

[1563] Birnhack, M., D., (2008). "The EU Data Protection Directive: An engine of a global regime" *Computer Law & Security Report* (24): 511.

[1564] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. Accessed 24 December 2020.

[1565] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. Accessed 24 December 2020. Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 88.

umbrella law that supersedes any national law that addresses the protection of personal information.[1566]

The GDPR repealed the EU DPD 95/46/EC with effect from 25 May 2018.[1567] According to Bygrave, the reform was primarily due to the persistent inconsistencies in data protection rules across EU states. Furthermore, the application of the EU DPD across online platforms proved to be problematic.[1568] It was necessary to make changes to address the inefficiencies of the DPD and improve the protection of personal data.[1569] To achieve this, data protection rules required consistent application through enforcement mechanisms that seek to create trust and enable the digital economy to expand.[1570]

Although the GDPR applies to EU citizens in member countries, the GDPR's application is far-reaching and extends to any entity that provides services in the EU.[1571] The GDPR's extensive application reinforces the EU's aim of protecting the rights and freedoms of EU citizens.[1572] It is important to point out that the GDPR affords protection to natural persons only and does not apply to the processing of information belonging to legal persons.[1573]

[1566] IT Governance Privacy Team (2017). *EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide* (2nd edition) IT Governance Publishing (UK) at 14.

[1567] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. Accessed 24 December 2020.

[1568] Bygrave, L., A. (2014). *Data Privacy Law: An International Perspective* Oxford University Press (UK) at 71.

[1569] Bygrave, L., A. (2014). *Data Privacy Law: An International Perspective* Oxford University Press (UK) at 71.

[1570] Recital 7 of the GDPR. Available at https://gdpr-info.eu/recitals/no-7/. Accessed 27 December 2020; Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 91 – 92.

[1571] IT Governance Privacy Team (2017). *EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide* (2nd edition) IT Governance Publishing (UK) at 11.

[1572] IT Governance Privacy Team (2017). *EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide* (2nd edition) IT Governance Publishing (UK) at 12.

[1573] Recital 14 of the GDPR. Available at https://gdpr-info.eu/recitals/no-14/. Accessed 22 February 2020.

5.3.2 Objectives of the GDPR

The GDPR recognises data protection as a fundamental right. This means that natural persons have the right to have their personal information protected.[1574] The second objective of the GDPR is to promote the free movement of personal information within the EU. The flow of personal information must not be hindered by the rules and provisions pertaining to the protection of personal information belonging to natural persons.[1575]

5.3.3 Applicability of the GDPR

5.3.3.1 Material scope of GDPR

The application of the GDPR is largely determined by whether personal information has been processed. According to Article 2(1), the GDPR applies to the manual and automatic processing of personal information that forms part of a filing system or that is intended to form part of a filing system.[1576]

The term 'processing' is broadly defined in the GDPR and includes the automatic and manual collection, storage, use or destruction of personal information.[1577] Further, 'personal data' is defined as:

> "Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number,

[1574] Article 1 of the GDPR. Available at https://gdpr-info.eu/art-1-gdpr/. Accessed 27 December 2020.

[1575] Article 1 of the GDPR. Available at https://gdpr-info.eu/art-1-gdpr/. Accessed 27 December 2020.

[1576] Article 2(1) of the GDPR. Available at https://gdpr-info.eu/art-1-gdpr/. Accessed 27 December 2020.

[1577] Article 4(2) of the GDPR. Available at https://gdpr-info.eu/art-4-gdpr/. Accessed 4 January 2021. 'Processing' is defined as ""Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."

> location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person."[1578]

General data is excluded from the definition of personal data. Only data that can be used to identify a natural person is considered personal data. The identification of a natural person can occur directly or indirectly. Whether a natural person is identified is a question of fact. A simple likelihood of identification, regardless of how trivial the identifier may be, will likely make that data personal for GDPR purposes.[1579] If identification occurs by linking different sets of data, those sets of data constitute personal data.[1580] Currently, the GDPR does not indicate the party responsible for identifying natural persons. Voigt and Von dem Bussche opine that any entity in possession of information can identify a natural person.[1581]

5.3.3.2 Territorial scope of the GDPR

It is important to consider the territorial application of the GDPR. According to Article 3(1), the GDPR applies to the processing of personal data in the EU by a controller or a processor.[1582] The controller or processor must be conducting activities through an

[1578] Article 4 of the GDPR. Available at https://gdpr-info.eu/art-4-gdpr/. Accessed 4 January 2021.

[1579] Voigt, P., & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide* Springer International Publishing at 12.

[1580] Voigt, P., & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide* Springer International Publishing at 12.

[1581] Voigt, P., & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide* Springer International Publishing at 12; see also Ramsey, S. (2018). *The General Data Protection Regulation vs The Blockchain – A legal study on the compatibility between blockchain technology and the GDPR* Thesis in Law and Informatics (Stockholm University) at 29 – 30.

[1582] A controller is defined as: "The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law." See Article 4(7) of the GDPR. Available at https://gdpr-info.eu/art-4-gdpr/. Accessed 5 January 2021.

establishment in the EU.[1583] It is irrelevant whether the processing of personal data takes place in the EU as long as that personal data belongs to an EU citizen.[1584]

The GDPR applies to the processing of personal data by a non-resident controller provided that the controller supplies goods and services to a data subject in the EU.[1585] The GDPR also covers any behavioural surveillance of EU citizens within the EU by controllers.[1586] The extent to which the GDPR may be applied to an individual's behaviour depends on the definition of 'monitoring'. Due to the extensive protection afforded to EU citizens, it is said that the GDPR's territorial scope has a broad application.[1587]

5.4 Blockchain and the GDPR

5.4.1 Overview

The application of the GDPR on a decentralised platform like blockchain raises several concerns. The GDPR legislative framework was originally intended for the processing of personal data by centralised identifiable institutions.[1588] Data controllers and processors' inability to enforce the rights of data subjects on blockchain has also

[1583] For GDPR purposes, an establishment is "the effective and real exercise of activity through stable arrangements. The legal form of the arrangement, whether through a branch or subsidiary with a legal personality is not the determining factor in that respect." See Recital 22 of the GDPR. Available at https://gdpr-info.eu/recitals/no-22/. Accessed 23 February 2021; See also Duarte, D., G. (2019). "An Introduction to Blockchain Technology from a Legal Perspective and Its Tensions With the GDPR" *Cyberlaw Journal of the Cyberlaw Research Centre of the University of Lisbon School of Law 2019* at 27 – 28. Available at SSRN: https://ssrn.com/abstract=3545331. Accessed 5 February 2021.

[1584] See Article 3(1) of the GDPR. Available at https://gdpr-info.eu/art-3-gdpr/. Accessed 5 January 2021.

[1585] Article 3(2) of the GDPR. Available at https://gdpr-info.eu/art-3-gdpr/. Accessed 5 January 2021.

[1586] Article 3(2) of the GDPR. Available at https://gdpr-info.eu/art-3-gdpr/. Accessed 5 January 2021.

[1587] See also Duarte, D., G. (2019). "An Introduction to Blockchain Technology from a Legal Perspective and Its Tensions With the GDPR" *Cyberlaw Journal of the Cyberlaw Research Centre of the University of Lisbon School of Law 2019* at 27. Available at SSRN: https://ssrn.com/abstract=3545331. Accessed 5 February 2021.

[1588] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 88; Duarte, D., G. (2019). "An Introduction to Blockchain Technology from a Legal Perspective and Its Tensions With the GDPR" *Cyberlaw Journal of the Cyberlaw Research Centre of the University of Lisbon School of Law 2019* at 27. Available at SSRN: https://ssrn.com/abstract=3545331. Accessed 5 February 2021.

raised concerns.[1589] Finck argues that there is a likelihood that the GDPR's application could make the operation of a blockchain network unlawful.[1590]

This section analyses the relationship between the relevant rules of the GDPR and the application of blockchain technology.

5.4.2 Blockchain and the territorial scope of the GDPR

In order to ascertain whether the GDPR applies to a transaction on blockchain, it is important to establish the identity of the controller. The controller's identity has a bearing on the relevant applicable jurisdiction.[1591] A public blockchain is decentralised in nature and has the capability of extending to various jurisdictions around the world. The public blockchain's extensive application creates challenges for the protection of personal information and the enforcement of data subject rights.[1592]

Private blockchains provide opportunities for the consistent application of the provisions of the GDPR. A private blockchain can enable data subjects to enforce their rights on blockchain. For example, if a data controller in the EU processes personal data on a private blockchain, the GDPR will apply to that transaction.[1593] If a data controller is not located in the EU but processes personal information where Member State law[1594] applies by virtue of public international law, then the GDPR applies to that transaction.[1595]

[1589] Duarte, D., G. (2019). "An Introduction to Blockchain Technology from a Legal Perspective and Its Tensions With the GDPR" *Cyberlaw Journal of the Cyberlaw Research Centre of the University of Lisbon School of Law 2019* at 27. Available at SSRN: https://ssrn.com/abstract=3545331. Accessed 5 February 2021.

[1590] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 88.

[1591] Miller, A. (2019). *Data protection on blockchain in the context of the General Data Protection Regulation* Master's thesis (University of Tartu) at 36.

[1592] Miller, A. (2019). *Data protection on blockchain in the context of the General Data Protection Regulation* Master's thesis (University of Tartu) at 36.

[1593] See Berberich, M., & Steiner, M. (2016). "Blockchain technology and the GDPR how to reconcile privacy and distributed ledgers" *European Data Protection Law Review* 2(3): 423.

[1594] Member State Law is the law of a particular country in the EU. The law includes legislation, judicial decisions and the Constitution of that state. See https://e-justice.europa.eu/content_member_state_law-6-en.do. Accessed 3 February 2021.

[1595] Article 3(3) of the GDPR. Available at https://gdpr-info.eu/art-3-gdpr/. Accessed 8 March 2021.

5.4.3 The processing of data on blockchain

It is important to determine whether personal data is processed on that blockchain. As mentioned above,[1596] the GDPR applies to the electronic and manual processing of personal data for filling or storing purposes. If we consider the definition of 'processing' under the GDPR, any form of storage, collection, use or dissemination of information constitute 'processing' for purposes of the GDPR. The definition of 'processing' is broad enough to include the handling of personal data. Blockchains were primarily intended to be used for storage purposes.[1597] Consequently, any data stored and recorded on a blockchain leads to the conclusion that the GDPR applies to that blockchain network.[1598] It must be borne in mind that the GDPR applies to private, hybrid (consortium), and public blockchains irrespective of its location in the EU provided that blockchain processes EU citizens' personal data.[1599]

Artzt *et al* point out correctly that if updates are made to a blockchain to ensure that the relevant participants on the network access the most up-to-date version of the database, such an update may constitute 'data processing' for GDPR purposes.[1600] The reason for this is straightforward. If an update alters the way personal data on a blockchain is stored or structured, then the update is consistent with the definition of the 'processing' under the GDPR. Similarly, the performance of a *soft fork*[1601] on a blockchain may constitute 'data processing' for GDPR purposes. When a *soft fork* is performed, an updated version of blockchain software becomes available to the

[1596] See paragraph 5.3.3 above.

[1597] See Finck, M. (2018). "Blockchains and data protection in the European Union" *European Data Protection Law Review* 4(1): 19.

[1598] Artzt, M., (ed) Determann, L., Long, W., *Blockchain and Data Privacy* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 198 – 199.

[1599] Duarte, D., G. (2019). "An Introduction to Blockchain Technology from a Legal Perspective and Its Tensions With the GDPR" *Cyberlaw Journal of the Cyberlaw Research Centre of the University of Lisbon School of Law 2019* at 28. Available at SSRN: https://ssrn.com/abstract=3545331. Accessed 5 February 2021.

[1600] Artzt, M., (ed) Determann, L., Long, W., *Blockchain and Data Privacy* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 199.

[1601] See paragraph 2.5.2 above.

relevant nodes.[1602] Like standard software updates, conducting a *soft fork* alters a blockchain.

5.4.4 Personal data on a blockchain

It is important to consider whether data stored on a blockchain qualifies as 'personal data' for purposes of the GDPR. This is significant because if data stored on a blockchain does not comply with the definition of 'personal data', then the GDPR may not apply to that blockchain transaction.[1603] As discussed above,[1604] the definition of 'personal data' under the GDPR is sufficiently broad to include data that can be combined with other data (for instance metadata) to identify a natural person. As already discussed above,[1605] it is possible to identify a natural person on a blockchain network by combining that person's IP address and their public key.[1606]

The process of 'masking' a natural person's personal data is provided for in the GDPR. The process, known as pseudonymisation, is a security feature used by processors or data controllers to meet their data protection obligations.[1607] Data controllers and processors may use other security measures together with pseudonymisation to protect a natural person's personal data.[1608]

[1602] Van der Laan, J. *Understanding Blockchain* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 40.

[1603] See Artzt, M., (ed) Determann, L., Long, W., *Blockchain and Data Privacy* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 194; Duarte, D., G. (2019). "An Introduction to Blockchain Technology from a Legal Perspective and Its Tensions With the GDPR" *Cyberlaw Journal of the Cyberlaw Research Centre of the University of Lisbon School of Law 2019* at 29 – 30. Available at SSRN: https://ssrn.com/abstract=3545331. Accessed 5 February 2021.

[1604] See paragraph 5.3.3.1 above.

[1605] Paragraph 4.8.3.3 above.

[1606] Bacon, J., Millard, C., & Singh, J. (2018). "Blockchain Demystified: A technical and Legal Introduction to Distributed and Centralised Ledgers" *Richmond Journal of Law & Technology* 25(1): 62; Duarte, D., G. (2019). "An Introduction to Blockchain Technology from a Legal Perspective and Its Tensions With the GDPR" *Cyberlaw Journal of the Cyberlaw Research Centre of the University of Lisbon School of Law 2019* at 32. Available at SSRN: https://ssrn.com/abstract=3545331. Accessed 5 February 2021.

[1607] Recital 28 of the GDPR. Available at https://gdpr-info.eu/recitals/no-28/. Accessed 24 February 2021; see also Duarte, D., G. (2019). "An Introduction to Blockchain Technology from a Legal Perspective and Its Tensions With the GDPR" *Cyberlaw Journal of the Cyberlaw Research Centre of the University of Lisbon School of Law 2019* at 30 – 31. Available at SSRN: https://ssrn.com/abstract=3545331. Accessed 5 February 2021.

[1608] Recital 28 of the GDPR. Available at https://gdpr-info.eu/recitals/no-28/. Accessed 24 February 2021.

There are three distinct ways of storing data on a blockchain.[1609] First, if data is stored as plain text, that data will be consistent with the definition of personal data under the GDPR.[1610] Data in plain text may contain identifiers that can be linked to a natural person.[1611] It is possible for natural persons to be identified by combining online identifiers such as IP addresses and Apps.[1612] Second, it is possible for encrypted data to be considered 'personal data' for GDPR purposes.[1613] Encryption can pseudonymise data.[1614] A third party will be unable to directly identify a person whose data has been encrypted by a public key.[1615] Although the public and private key pseudonymises data, it does not preclude a public key from acting as an identifier.[1616] There is a possibility that a public key may be combined with other identifiers in order to identify a natural person.[1617] The test that is used to determine whether a natural person can be identified is an objective one.[1618] Objective factors include the amount of time spent to identify the natural person, the costs incurred by the entity seeking to identify the person and the technology available at the disposal of the entity at the time

[1609] Finck, M. (2018). "Blockchains and data protection in the European Union" *European Data Protection Law Review* 4(1): 22.

[1610] Finck, M. (2018). "Blockchains and data protection in the European Union" *European Data Protection Law Review* 4(1): 22.

[1611] See Article 4(1) of the GDPR. Available at https://gdpr-info.eu/art-4-gdpr/. Accessed 4 January 2021.

[1612] Recital 30 of the GDPR. Available at https://gdpr-info.eu/recitals/no-30/. Accessed 7 January 2021.

[1613] Bacon, J., Millard, C., & Singh, J. (2018). "Blockchain Demystified: A technical and Legal Introduction to Distributed and Centralised Ledgers" *Richmond Journal of Law & Technology* 25(1): 62.

[1614] De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* Harvard University Press (US) at 38 – 39; Kianieff, M. (2019) *Blockchain Technology and the Law Opportunities and Risks* Routledge Publishing (UK) at 160; Finck, M. (2018). "Blockchains and data protection in the European Union" *European Data Protection Law Review* 4(1): 22.

[1615] Artzt, M., (ed) Determann, L., Long, W., *Blockchain and Data Privacy* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 195; Finck, M. (2018). "Blockchains and data protection in the European Union" *European Data Protection Law Review* 4(1): 22.

[1616] Artzt, M., (ed) Determann, L., Long, W., *Blockchain and Data Privacy* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 195; Recital 30 of the GDPR. Available at https://gdpr-info.eu/recitals/no-30/. Accessed 7 January 2021.

[1617] Bacon, J., Millard, C., & Singh, J. (2018). "Blockchain Demystified: A technical and Legal Introduction to Distributed and Centralised Ledgers" *Richmond Journal of Law & Technology* 25(1): 62; Artzt, M., (ed) Determann, L., Long, W., *Blockchain and Data Privacy* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 195 – 197.

[1618] Recital 26 of the GDPR. Available at https://gdpr-info.eu/recitals/no-26/. Accessed 7 January 2021; Artzt, M., (ed) Determann, L., Long, W., *Blockchain and Data Privacy* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 195 – 197.

of the processing.[1619] Due to the perceived tenuous safeguards offered by public keys in relation to the protection of data, there is a view that public keys should be viewed as a security feature.[1620] Third, transaction data may constitute personal data for GDPR purposes.[1621] Transaction data is data that is hashed by making use of specific algorithms.[1622] Using a hash function, large amounts of data can be converted into smaller unique characters. The unique characters form a digital signature or a hash output.[1623] A key feature of a hash function is the inability for hashed data to be reverse engineered.[1624] This feature has been the subject of much debate among scholars and authors.[1625]

[1619] Recital 26 of the GDPR. Available at https://gdpr-info.eu/recitals/no-26/. Accessed 7 January 2021; Artzt, M., (ed) Determann, L., Long, W., *Blockchain and Data Privacy* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 195 – 197.

[1620] Data Protection Working Party (2014). "Opinion 05/2014 on Anonymisation Techniques" *Article 29 Data Protection Working Party EU* at 3. Available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. Accessed 22 September 2020; Kianieff poses an important question in this regard. Kianieff asks whether the use of pseudonymisation techniques like encryption potentially weaken blockchains' ability to protection personal information. Kianieff lists recent instances where pseudonymisation failed to protect personal information. See Kianieff, M. (2019) *Blockchain Technology and the Law Opportunities and Risks* Routledge Publishing (UK) at 161 – 165.

[1621] Finck, M. (2018). "Blockchains and data protection in the European Union" *European Data Protection Law Review* 4(1): 22; Duarte, D., G. (2019). "An Introduction to Blockchain Technology from a Legal Perspective and Its Tensions With the GDPR" *Cyberlaw Journal of the Cyberlaw Research Centre of the University of Lisbon School of Law 2019* at 32. Available at SSRN: https://ssrn.com/abstract=3545331. Accessed 5 February 2021.

[1622] Artzt, M., (ed) Determann, L., Long, W., *Blockchain and Data Privacy* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 197.

[1623] Van der Laan, J. *Understanding Blockchain* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 11 – 12; Mirchandani, A. (2019). "The GDPR-Blockchain Paradox: Exempting Permissioned Blockchains from the GDPR" Fordham Intellectual Property Media & Entertainment Law Journal 29(4): 1209; Bacon, J., Millard, C., & Singh, J. (2018). "Blockchain Demystified: A technical and Legal Introduction to Distributed and Centralised Ledgers" *Richmond Journal of Law & Technology* 25(1): 9.

[1624] This means that once data has been hashed, it is extremely difficult for that data to return to its original state. See Mirchandani, A. (2019). "The GDPR-Blockchain Paradox: Exempting Permissioned Blockchains from the GDPR" Fordham Intellectual Property Media & Entertainment Law Journal 29(4): 1225; Van der Laan, J. *Understanding Blockchain* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 14 – 15; Finck, M. (2018). "Blockchains and data protection in the European Union" *European Data Protection Law Review* 4(1): 22; Duarte, D., G. (2019). "An Introduction to Blockchain Technology from a Legal Perspective and Its Tensions With the GDPR" *Cyberlaw Journal of the Cyberlaw Research Centre of the University of Lisbon School of Law 2019* at 33. Available at SSRN: https://ssrn.com/abstract=3545331. Accessed 5 February 2021.

[1625] There is overwhelming support for hashed data to be considered as personal data. See Mirchandani, A. (2019). "The GDPR-Blockchain Paradox: Exempting Permissioned Blockchains from the GDPR" *Fordham Intellectual Property Media & Entertainment Law Journal* 29(4): 1225; Artzt, M., (ed) Determann, L., Long, W., *Blockchain and Data Privacy* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and*

The crux of the argument stems from the classification of hashed data as an anonymisation technique. If hashed data is considered as an anonymisation technique, it is excluded from the definition of 'personal data' for GDPR purposes. Recital 26 of the GDPR makes it clear that pseudonymised data constitutes personal data if it is combined with additional information to identify a natural person. Recital 26 also makes it clear that anonymised data does not constitute 'personal data'. Therefore, if a natural person can be identified by combining hashed data and other data, then the combination of data can constitute 'personal data' for GDPR purposes. However, if hashed data can no longer identify a natural person (anonymised data) or if hashed data has become anonymised to the point where a natural person is no longer identifiable, then that hashed data constitutes non-personal data which renders the application of GDPR inoperable.[1626]

5.4.5 The controller

A 'controller' or 'data controller' is a legal or natural person that is responsible for establishing the objectives and means of processing personal data.[1627] Put simply, the controller is a legal person who is responsible for ensuring that processed data complies with the GDPR regulations.[1628] It is difficult for a data subject to enforce his or her rights on a blockchain without the presence of a controller. For this reason, a

resolving the legal challenges of blockchain technology Kluwer Law International at 198; Finck, M. (2018). "Blockchains and data protection in the European Union" *European Data Protection Law Review* 4(1): 22.

[1626] See Recital 26 of the GDPR. Available at https://gdpr-info.eu/recitals/no-26/. Accessed 7 January 2021; Artzt, M., (ed) Determann, L., Long, W., *Blockchain and Data Privacy* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 195 – 198; Mirchandani, A. (2019). "The GDPR-Blockchain Paradox: Exempting Permissioned Blockchains from the GDPR" *Fordham Intellectual Property Media & Entertainment Law Journal* 29(4): 1224 – 1226; Finck, M. (2018). "Blockchains and data protection in the European Union" *European Data Protection Law Review* 4(1): 22 – 23; Finck, M., & Pallas, F. (2020). "They who must not be identified – distinguishing personal from non-personal data under the GDPR" *International Data Privacy Law Journal* 10(1): 11 – 36.

[1627] Article 4(7) of the GDPR. Available at https://gdpr-info.eu/art-4-gdpr/. Accessed 4 January 2021.

[1628] Bacon, J., Millard, C., & Singh, J. (2018). "Blockchain Demystified: A technical and Legal Introduction to Distributed and Centralised Ledgers" *Richmond Journal of Law & Technology* 25(1): 63; Duarte, D., G. (2019). "An Introduction to Blockchain Technology from a Legal Perspective and Its Tensions With the GDPR" *Cyberlaw Journal of the Cyberlaw Research Centre of the University of Lisbon School of Law 2019* at 34. Available at SSRN: https://ssrn.com/abstract=3545331. Accessed 5 February 2021.

controller is ultimately accountable to a data subject.[1629] A controller can determine what happens to an individual's personal information.[1630] A controller's role includes putting appropriate technical measures to show that the processing of data is done in compliance with the GDPR Regulations.[1631]

A controller must be distinguished from a data processor. The distinction enables data subjects to enforce their fundamental right to data protection.[1632] A data processor is a legal or natural person that is responsible for processing personal data on behalf of a controller.[1633] The definition of data processor presupposes a contractual agreement or mandate between a controller and a data processor.[1634] The contractual relationship

[1629] Jimenez-Gomez, B. (2020). "Risks of blockchain for data protection: European approach" *Santa Clara High Technology Law Journal* 36(3): 311; Duarte, D., G. (2019). "An Introduction to Blockchain Technology from a Legal Perspective and Its Tensions With the GDPR" *Cyberlaw Journal of the Cyberlaw Research Centre of the University of Lisbon School of Law 2019* at 34. Available at SSRN: https://ssrn.com/abstract=3545331. Accessed 5 February 2021.

[1630] Mirchandani, A. (2019). "The GDPR-Blockchain Paradox: Exempting Permissioned Blockchains from the GDPR" *Fordham Intellectual Property Media & Entertainment Law Journal* 29(4): 1220 at footnote 120; Jimenez-Gomez, B. (2020). "Risks of blockchain for data protection: European approach" *Santa Clara High Technology Law Journal* 36(3): 311.

[1631] Article 24(1) of the GDPR. Available at https://gdpr-info.eu/art-24-gdpr/. Accessed 13 January 2021.

[1632] Jimenez-Gomez, B. (2020). "Risks of blockchain for data protection: European approach" *Santa Clara High Technology Law Journal* 36(3): 311.

[1633] Article 4(8) of the GDPR. Available at https://gdpr-info.eu/art-4-gdpr/. Accessed 4 January 2021.

[1634] This view is supported by Articles 28(3) and (9) of the GDPR. Available at https://gdpr-info.eu/art-28-gdpr/. Accessed 14 January 2021. Article 28(3) reads: "Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor: (a) process the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State Law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits such information on important grounds of public interest; (b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality; (c) takes all measures required t pursuant to Article 32; (d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor; (e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III; (f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor; (g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data; (h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

between a controller and data processor assumes a hierarchical style of data processing under the GDPR.[1635] This also implies that a data processor may not process data without the authority or consent of the data controller. Any conduct or processing of data by the data processor could result in civil liabilities where no instruction or authority is obtained from the data controller.

5.4.5.1 Data controllers on public blockchains

The identification of a data controller in a public decentralised blockchain is difficult. There is no central authority that operates a public blockchain. Instead, the public blockchain consists of users (nodes) that interact with each other.[1636] The situation is compounded by the fact that public blockchains are devoid of any hierarchical structure making any identification arduous and impractical.[1637] From a European perspective, the lack of a data controller removes any potential data protection enforcement measures that a data subject possesses.[1638] Furthermore, there are certain obligations that must be conducted by a controller.[1639] For example, Article 25(1) of the GDPR states that a "controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects."[1640] The peremptory provision clearly imposes a duty on a controller to give

With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions." Article 28(9) reads: "The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form."

[1635] Erbguth, J. (2019). "Five ways to GDPR-compliant use of blockchains" *European Data Protection Law Review* 5(3): 431.

[1636] Finck, M. (2018). "Blockchains and data protection in the European Union" *European Data Protection Law Review* 4(1): 26.

[1637] Jimenez-Gomez, B. (2020). "Risks of blockchain for data protection: European approach" *Santa Clara High Technology Law Journal* 36(3): 311.

[1638] See Jimenez-Gomez, B. (2020). "Risks of blockchain for data protection: European approach" *Santa Clara High Technology Law Journal* 36(3): 311.

[1639] Erbguth, J. (2019). "Five ways to GDPR-compliant use of blockchains" *European Data Protection Law Review* 5(3): 432.

[1640] See Article 25 of the GDPR. Available at https://gdpr-info.eu/art-25-gdpr/. Accessed 14 January 2021.

effect to the protection of data by design and default.[1641] However, obligations such as these cannot be adhered to without establishing a data controller's identity.

5.4.5.2 Can nodes be considered data controllers?

Pursuant to the discussion above, it is necessary to consider alternative data controllers. As already discussed,[1642] nodes are computers that store copies of a blockchain.[1643] Although any person can own a node and access a public blockchain, it does not necessarily follow that all nodes can be controllers.[1644] According to Bacon *et al*, in order for a node to be considered a controller, a node must show that it has the "purposes and means" of processing personal data.[1645] Consider the following example:

Example 6

FI is a financial institution. FI makes use of a blockchain based technology to prevent identity fraud. To achieve this and to promote know-your-customer (KYC) protocols, FI implements a system where clients make use of their fingerprints for identification purposes. Client information is then stored on a private network blockchain. The network can be accessed by other financial institutions.[1646]

In the example above, the purpose of processing personal data is to prevent identity theft.[1647] The financial institution tries to prevent identity fraud by storing personal data

[1641] See Article 25 of the GDPR. Available at https://gdpr-info.eu/art-25-gdpr/. Accessed 14 January 2021.

[1642] See paragraph 2.5 above.

[1643] Finck, M. (2018). "Blockchains and data protection in the European Union" *European Data Protection Law Review* 4(1): 19; Artzt, M., (ed) Determann, L., Long, W., *Blockchain and Data Privacy* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 205.

[1644] This view is supported by Finck. See Finck, M. (2018). "Blockchains and data protection in the European Union" *European Data Protection Law Review* 4(1): 26.

[1645] Bacon, J., Millard, C., & Singh, J. (2018). "Blockchain Demystified: A technical and Legal Introduction to Distributed and Centralised Ledgers" *Richmond Journal of Law & Technology* 25(1): 64.

[1646] Higginson, M. *et al* (2019). "*Blockchain and retail banking: Making the connection*." Available at https://www.mckinsey.com/industries/financial-services/our-insights/blockchain-and-retail-banking-making-the-connection#. Accessed 16 January 2021.

[1647] For this reason, it is argued that the financial institution is processing data for its own purposes. That is, to prevent fraud.

on a blockchain-based system. The nodes and miners merely process the data on behalf of the financial institution. The role of the nodes and miners on that blockchain is secondary to the role of the financial institution. The nodes and miners are processors of personal data.[1648] The role of the financial institution is primary in that it decides how and why the data should be processed.[1649]

5.4.5.3 Data controllers on private blockchains

It is easier to determine a data controller on a private blockchain due to the closed nature of blockchain network. Here, a central authority is responsible for maintaining the private blockchain. The central authority can also determine whether personal data can be processed. It can also determine the type of data processed and how that data will be processed.[1650] The central authority is responsible for ensuring that any other node on the network complies with the rules of the GDPR. A data subject is better placed to enforce their rights in terms of the GDPR if a central authority can be easily identified.

5.4.6 The transfer of data to third-party countries

The GDPR makes provision for the transfer of personal information to third-party countries outside the EU. The cross-border transfer of personal information is necessary for the development of international cooperation and international trade.[1651] The transfer of information to a third-party country can only be done if the provisions relating to the transfer of information the GDPR are complied with.[1652] In terms of the GDPR, personal information may be transferred to a third-party country or to an

[1648] Kianieff, M. (2019) *Blockchain Technology and the Law Opportunities and Risks* Routledge Publishing (UK) at 174.

[1649] Jimenez-Gomez, B. (2020). "Risks of blockchain for data protection: European approach" *Santa Clara High Technology Law Journal* 36(3): 311.

[1650] Duarte, D., G. (2019). "An Introduction to Blockchain Technology from a Legal Perspective and Its Tensions With the GDPR" *Cyberlaw Journal of the Cyberlaw Research Centre of the University of Lisbon School of Law 2019* at 38. Available at SSRN: https://ssrn.com/abstract=3545331. Accessed 5 February 2021.

[1651] Recital 101 of the GDPR. Available at https://gdpr-info.eu/recitals/no-101/. Accessed 4 February 2021. See also Miller, A. (2019). *Data protection on blockchain in the context of the General Data Protection Regulation* Master's thesis (University of Tartu) at 39.

[1652] Recital 101 of the GDPR. Available at https://gdpr-info.eu/recitals/no-101/. Accessed 4 February 2021. See also Miller, A. (2019). *Data protection on blockchain in the context of the General Data Protection Regulation* Master's thesis (University of Tartu) at 39.

international organisation if the Commission is satisfied that the third-party country or international organisation has adequate levels of protection.[1653] When determining the adequacy of the level of protection, the Commission must consider elements mentioned in Article 45(2) of the GDPR.[1654] Once the Commission is satisfied that the adequacy levels are available in the third-party country, the transfer of personal information will not require further authorisation.[1655]

Blockchain's decentralised nature clearly challenges the Commission's ability to determine adequacy levels in third-party countries. The Commission's ability is impeded by blockchain's simplified and seamless transfer of personal information across multiple jurisdictions without any control measures. Public blockchains are particularly problematic because nodes can be located anywhere around the world resulting in the seamless cross-border transfer of data.[1656] From a privacy perspective, this can create a platform for data breaches resulting in the loss of sensitive data. While the transfer of personal information to third-party countries can aide the GDPR's

[1653] Article 45(1) of the GDPR. Available at https://gdpr-info.eu/art-45-gdpr/. Accessed 4 February 2021.

[1654] These include: "(a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred; (b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and (c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data." See Article 45(2) of the GDPR. Available at https://gdpr-info.eu/art-45-gdpr/. Accessed 4 February 2021.

[1655] Article 45(1) of the GDPR. Available at https://gdpr-info.eu/art-45-gdpr/. Accessed 4 February 2021; see also Duarte, D., G. (2019). "An Introduction to Blockchain Technology From a Legal Perspective and Its Tensions With the GDPR" *Cyberlaw Journal of the Cyberlaw Research Centre of the University of Lisbon School of Law 2019* at 44 – 47. Available at SSRN: https://ssrn.com/abstract=3545331. Accessed 5 February 2021.

[1656] Finck, M. (2018). "Blockchains and data protection in the European Union" *European Data Protection Law Review* 4(1): 27 – 28.

intention to promote international trade, it must be done with the appropriate safeguards.[1657]

However, it is possible for a data controller or processor to transfer personal information to third-party country without the relevant adequacy measures.[1658] A data controller or a processor that transfers personal information to a third country must ensure "that enforceable data subject rights and effective legal remedies for data subjects are available."[1659] It is clear from the wording of Article 46(1) of the GDPR that the onus rests on the data controller or the processor to ensure that the recipient third-party country has data protection measures. Where a third country lacks data protection mechanisms, a data controller must implement appropriate safeguards. These include making use of binding corporate rules, adopting contractual clauses authorised by a supervisory authority or inserting standard data protection clauses by the Commission.[1660] According to Recital 108, the safeguards should ensure compliance with the data protection measures and ensure that the rights of data subjects are enforced.[1661]

It is also difficult for a data controller to enforce the GDPR safeguards in a public blockchain because nodes are not easily identifiable. And if nodes cannot be identified, the jurisdiction of the node cannot be established. Additionally, it is possible for any person around the world to download a copy of blockchain and access any personal information that may be stored on that blockchain.[1662]

[1657] Article 46 of the GDPR. Available at https://gdpr-info.eu/art-46-gdpr/. Accessed 4 February 2021.

[1658] Article 46(1) of the GDPR. Available at https://gdpr-info.eu/art-46-gdpr/. Accessed 4 February 2021.

[1659] Article 46(1) of the GDPR. Available at https://gdpr-info.eu/art-46-gdpr/. Accessed 4 February 2021.

[1660] Recital 108 of the GDPR. Available at https://gdpr-info.eu/recitals/no-108/. Accessed 5 February 2021. See also Duarte, D., G. (2019). "An Introduction to Blockchain Technology from a Legal Perspective and Its Tensions With the GDPR" *Cyberlaw Journal of the Cyberlaw Research Centre of the University of Lisbon School of Law 2019* at 44 – 47. Available at SSRN: https://ssrn.com/abstract=3545331. Accessed 5 February 2021.

[1661] Recital 108 of the GDPR. Available at https://gdpr-info.eu/recitals/no-108/. Accessed 5 February 2021.

[1662] Miller, A. (2019). *Data protection on blockchain in the context of the General Data Protection Regulation* Master's thesis (University of Tartu) at 41.

Transferring personal information on a private blockchain does not provide similar challenges. In a private blockchain, a central authority is familiar with all the participants on a blockchain network. As a result, it is easier for the central authority to determine the location of the other participants and thereafter ensure that safeguards are present in the jurisdiction where personal information is transferred.

The GDPR makes provision for the transfer of data in the absence of adequacy decision or appropriate safeguards.[1663] A natural person (data subject) may consent[1664] to the transfer of his or her personal information to a third-party country. The consent is subject to a natural person being made aware of possible risks[1665] that may ensue as a result of data transfer.[1666] It is not clear from the wording of the provisions in the GDPR how such consent must be obtained from a data subject.[1667] On a public blockchain, it is unclear how consent can be obtained.[1668] It is submitted that even if consent were to be obtained, the transparent nature of a public blockchain makes it difficult to control who receives the data. Consent on a private blockchain can be controlled by establishing the location and identity of the recipient of the personal information.[1669]

[1663] Article 49(1) of the GDPR. Available at https://gdpr-info.eu/art-49-gdpr/. Accessed 5 February 2021.

[1664] Consent is defined in Article 4(11) of the GDPR as: "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her." Available at https://gdpr-info.eu/art-4-gdpr/. Accessed 5 February 2021.

[1665] Such risks may include the fact that the data controller or processor is making use of a blockchain in order to transfer the data to a third country. Despite the potential risks involved in using blockchains, the responsibility remains on the data controller or processor to ensure that the blockchain has security measures in place to prevent unauthorized access.

[1666] Article 49(1)(a) of the GDPR. Available at https://gdpr-info.eu/art-49-gdpr/. Accessed 5 February 2021. See also Finck, M. (2018). "Blockchains and data protection in the European Union" *European Data Protection Law Review* 4(1): 28.

[1667] Under normal circumstances, it is preferable to obtain written consent from a data subject. This is to ensure legal certainty and limit liability for data controllers or processors.

[1668] Finck, M. (2018). "Blockchains and data protection in the European Union" *European Data Protection Law Review* 4(1): 28.

[1669] See Finck, M. (2018). "Blockchains and data protection in the European Union" *European Data Protection Law Review* 4(1): 28.

5.4.7 The rights of data subjects under the GDPR

The GDPR makes provision for data subjects to enforce their rights when their personal information is processed.[1670] These rights, including the right to erasure and the right to rectification, are on face value in conflict with blockchain technology. As has been discussed, it is difficult to erase or rectify data on a blockchain. For this reason, the enforcement of the rights of data subjects on a blockchain becomes impractical.[1671] Artzt *et al* correctly point out that any attempt to erase or rectify data on blockchain can be detrimental to the participants' trust in blockchain.[1672]

5.4.7.1 The right to be forgotten

The right to be forgotten[1673] was implemented by the European Parliament for the first time in 1995.[1674] Article 12(b) of the Directive required the "rectification, erasure or blocking of data that did not comply with the provisions of the Directive due to incomplete or inaccurate nature of the data."[1675] The purpose of this provision was to aide EU citizens to remove their personal information from Internet silos.[1676]

[1670] Articles 15 – 22 of the GDPR; Artzt, M., (ed) Determann, L., Long, W., *Blockchain and Data Privacy* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 226; Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 103.

[1671] Artzt, M., (ed) Determann, L., Long, W., *Blockchain and Data Privacy* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 226 – 277; Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 103 – 104.

[1672] Artzt, M., (ed) Determann, L., Long, W., *Blockchain and Data Privacy* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 227.

[1673] According to Rosen, the right to be forgotten originated from French law (*le droit à l'oubli*). This right enabled a convicted criminal to oppose any publication relating to his time spent in jail. See Rosen, J. (2012). "The Right to Be Forgotten" *Stanford Law Review Online* 64: 88.

[1674] Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. See also Gabison, G., (2016). "Policy Considerations for the Blockchain Technology Public and Private Applications" *SMU Science and Technology Law Review* 19(3): 331.

[1675] Article 12(b) of the 1995 Directive.

[1676] Gabison, G., (2016). "Policy Considerations for the Blockchain Technology Public and Private Applications" *SMU Science and Technology Law Review* 19(3): 331; Rosen, J. (2012). "The Right to Be Forgotten" *Stanford Law Review Online* 64: 88 – 92.

The right to be forgotten is currently entrenched in article 17 of the GDPR. This right to be forgotten requires a data controller to erase a natural person's personal information without any delay.[1677] It also requires the data controller to erase personal information under certain circumstances. For example, if a natural person's personal information is processed unlawfully, the data controller must erase such personal information.[1678]

A data controller who discloses personal information to the public must take reasonable steps to inform other data controllers processing personal information that the data subject has requested erasure of any links to or copy of that personal information.[1679] The right to be forgotten does not apply (i) where the processing of personal information is necessary to exercise the right to freedom of expression and information; (ii) for the establishment, exercise or defence of legal claims; (iii) for reasons of public interest in the area of public health; (iv) for compliance with a legal obligation which requires processing by Union or Member State Law; and (v) where the controller is subject or for achieving purposes in the public interest, scientific or historical research purposes.[1680]

Although the right to be forgotten seeks to protect the rights of data subjects, its application can be problematic. First, the term 'erasure' is not defined in the GDPR. The result is that the term 'erasure' is susceptible to different interpretations.[1681] For

[1677] Article 17(1) of the GDPR. Available at https://gdpr-info.eu/art-17-gdpr/. Accessed 9 February 2021.

[1678] Article 17(1)(d) of the GDPR. Available at https://gdpr-info.eu/art-17-gdpr/. Accessed 9 February 2021. In terms of Article 17(1), personal information must be erased by a data controller where "(a) the personal information are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2) and where there is no other legal ground for the processing; (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing or the data subject objects to the processing pursuant to Article 21(2); (e) the personal information have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; (f) the personal information have been collected in relation to the offer of information society services referred to in Article 8(1)."

[1679] Article 17(2) of the GDPR. Available at https://gdpr-info.eu/art-17-gdpr/. Accessed 9 February 2021. See also Recital 66 of the GDPR. Available at https://gdpr-info.eu/recitals/no-66/. Accessed 9 February 2021.

[1680] Article 17(3)(a) to (e) of the GDPR. Available at https://gdpr-info.eu/art-17-gdpr/. Accessed 9 February 2021.

[1681] See Finck, M. (2018). "Blockchains and data protection in the European Union" *European Data Protection Law Review* 4(1): 31; Artzt, M., (ed) Determann, L., Long, W., *Blockchain and Data Privacy* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to* example, the Article 29 Data Protection Working Party released an opinion on Cloud Computing in 2012.[1682] For purposes of Could Computing, Data Protection Working Party mentions that 'erasure' occurs when storage media is destroyed or when personal information is deleted through overwriting.[1683] According to Artzt *et al*, it is possible that the term 'erasure' may not necessarily mean to delete personal information.[1684] It is submitted that the term 'erasure' should be considered in the light of the manner and the infrastructure in which the personal information is stored.[1685] Contextually, if a natural person instructs a data controller to delete his or her personal information stored on a blockchain, such 'erasure' can, for example, be effected when a private key is deleted or destroyed.[1686]

The second factor that makes the application of the right to be forgotten difficult to apply is blockchain's append only and immutable features. These features make it difficult to erase any data stored on a blockchain.[1687] A controller in a private or public blockchain will be unable to comply with Article 17 of the GDPR because the deletion of personal information stored on a blockchain is not possible. However, Duarte points

understanding and resolving the legal challenges of blockchain technology Kluwer Law International at 229; Duarte, D., G. (2019). "An Introduction to Blockchain Technology from a Legal Perspective and Its Tensions With the GDPR" *Cyberlaw Journal of the Cyberlaw Research Centre of the University of Lisbon School of Law 2019* at 43 – 44. Available at SSRN: https://ssrn.com/abstract=3545331. Accessed 5 February 2021.

[1682] Article 29 Data Protection Working Party Opinion 05/2012 on Cloud Computing (WP 196). Available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf. Accessed 9 February 2021.

[1683] Article 29 Data Protection Working Party Opinion 05/2012 on Cloud Computing (WP 196) at 12. Available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf. Accessed 9 February 2021; see also Artzt, M., (ed) Determann, L., Long, W., *Blockchain and Data Privacy* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 229 – 230.

[1684] Artzt, M., (ed) Determann, L., Long, W., *Blockchain and Data Privacy* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 229.

[1685] See Finck, M. (2018). "Blockchains and data protection in the European Union" *European Data Protection Law Review* 4(1): 31.

[1686] Artzt, M., (ed) Determann, L., Long, W., *Blockchain and Data Privacy* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 230 – 233; Commission Nationale de l'informatique et de Libértes (2018). *"Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data"* at 8. Available at https://www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf. Accessed 20 September 2020.

[1687] Duarte, D., G. (2019). "An Introduction to Blockchain Technology From a Legal Perspective and Its Tensions With the GDPR" *Cyberlaw Journal of the Cyberlaw Research Centre of the University of Lisbon School of Law 2019* at 43. Available at SSRN: https://ssrn.com/abstract=3545331. Accessed 5 February 2021.

out that a controller in a private blockchain can comply with the right to erasure if the provisions of Article 17(2) of the GDPR are applied.[1688]

5.4.7.2 The right to rectification

Article 16 of the GDPR confers the right to request data controllers to rectify any inaccurate personal information that concerns him or her without any delay.[1689] The right to rectification includes a data subject's right to have incomplete personal information rectified by a data controller.[1690] Once a data subject has requested the deletion or erasure of his or her personal information, the data controller must notify all the recipients to whom the personal information has been disclosed, of such rectification or erasure.[1691]

It is difficult to conduct any rectification on a blockchain. Blockchain's append only feature means that nodes cannot change the data stored on a block.[1692] Once data is stored on a blockchain, it is almost impossible to change that data.[1693] Further, a data controller cannot rectify any incomplete personal information belonging to a data subject.[1694] In a public blockchain, a node can only alter its own copy of blockchain. Most of the nodes on blockchain network use the original version of blockchain. Even if a node was to make changes to the original version of blockchain, it must co-operate with all the nodes on the network to create a hard fork. Co-operation is only possible

[1688] Duarte, D., G. (2019). "An Introduction to Blockchain Technology From a Legal Perspective and Its Tensions With the GDPR" *Cyberlaw Journal of the Cyberlaw Research Centre of the University of Lisbon School of Law 2019* at 44. Available at SSRN: https://ssrn.com/abstract=3545331. Accessed 5 February 2021.

[1689] Article 16 of the GDPR. Available at https://gdpr-info.eu/art-16-gdpr/. Accessed 11 February 2021.

[1690] Article 16 of the GDPR. Available at https://gdpr-info.eu/art-16-gdpr/. Accessed 11 February 2021.

[1691] Article 19(1) of the GDPR. Available at https://gdpr-info.eu/art-19-gdpr/ . Accessed 11 February 2021.

[1692] Finck, M. (2018). "Blockchains and data protection in the European Union" *European Data Protection Law Review* 4(1): 29.

[1693] Duarte, D., G. (2019). "An Introduction to Blockchain Technology From a Legal Perspective and Its Tensions With the GDPR" *Cyberlaw Journal of the Cyberlaw Research Centre of the University of Lisbon School of Law 2019* at 42. Available at SSRN: https://ssrn.com/abstract=3545331. Accessed 5 February 2021.

[1694] Duarte, D., G. (2019). "An Introduction to Blockchain Technology From a Legal Perspective and Its Tensions With the GDPR" *Cyberlaw Journal of the Cyberlaw Research Centre of the University of Lisbon School of Law 2019* at 42. Available at SSRN: https://ssrn.com/abstract=3545331. Accessed 5 February 2021.

if a node can successfully identify all the nodes on the network. For these reasons, Duarte correctly argues that it is possible for rectification to occur in a private blockchain where changes have a better chance of being implemented due to the presence of a central authority.[1695]

5.4.7.3 The right of access by a data subject

Data subjects have the right to obtain confirmation from a data controller that their personal information is being processed.[1696] Where a data controller has processed personal information belonging to a natural person, the latter has the right to access the reasons why processing has taken place. It is also possible for a data subject to access information regarding the length of time for which his or her personal information will be stored. A data subject can access information regarding the existence of automated decision-making including profiling and the categories of personal information concerned.[1697]

Where a data subject's personal information has been transferred to a third-party country, a data controller must inform a data subject of any appropriate safeguards undertaken in relation to that transfer.[1698] A data subject reserves the right to request a copy of any personal information that has undergone processing. However, a data subject's right to obtain a copy of his or her personal information must not adversely affect the rights and freedoms of others.[1699]

It is difficult for a data controller to be familiar with the type of data that is stored on a public blockchain since that data is either hashed or encrypted.[1700] Moreover, a data

[1695] Duarte, D., G. (2019). "An Introduction to Blockchain Technology From a Legal Perspective and Its Tensions With the GDPR" *Cyberlaw Journal of the Cyberlaw Research Centre of the University of Lisbon School of Law 2019* at 42. Available at SSRN: https://ssrn.com/abstract=3545331. Accessed 5 February 2021.

[1696] Article 15(1) of the GDPR. Available at https://gdpr-info.eu/art-15-gdpr/. Accessed 12 February 2021.

[1697] Article 15(1) of the GDPR. Available at https://gdpr-info.eu/art-15-gdpr/. Accessed 12 February 2021.

[1698] Article 15(2) of the GDPR. Available at https://gdpr-info.eu/art-15-gdpr/. Accessed 12 February 2021.

[1699] Article 15(3) read with Article 15(4) of the GDPR. Available at https://gdpr-info.eu/art-15-gdpr/. Accessed 12 February 2021.

[1700] Finck, M. (2018). "Blockchains and data protection in the European Union" *European Data Protection Law Review* 4(1): 29; see also Duarte, D., G. (2019). "An Introduction to Blockchain controller cannot determine who is processing a data subject's personal information due to the inability to identify the users on a public blockchain. Finck opines that even if a data subject were to contact a node, it would be difficult for that node to ascertain whether or not a data subject's personal information has been processed on blockchain.[1701] It is also challenging for a data subject to obtain a copy of his or her personal information on blockchain because such information has been cryptographically pseudonymised[1702] and a node can only provide their respective local copy of blockchain to a data subject. That copy may not necessarily be the exact copy used by other users to process data on blockchain network.[1703]

In a private blockchain, a central authority (data controller) knows the identity of the nodes on the network. On a closed network, a data controller can manage a data subject's personal information. The data controller can determine the type of data processed, how to process that data and who to share that data with. In doing so, the data controller is better placed to account for and implement the rights of data subjects.[1704]

5.5 Methods to make blockchain GDPR compliant

The discussion above has demonstrated the tension between the application of blockchain and the EU GDPR. Some of the identified tensions include the ability to enforce the rights of data subjects, the identification of controllers and the transfer of

Technology from a Legal Perspective and Its Tensions With the GDPR" *Cyberlaw Journal of the Cyberlaw Research Centre of the University of Lisbon School of Law 2019* at 41. Available at SSRN: https://ssrn.com/abstract=3545331. Accessed 5 February 2021.

[1701] Finck, M. (2018). "Blockchains and data protection in the European Union" *European Data Protection Law Review* 4(1): 29; see also Duarte, D., G. (2019). "An Introduction to Blockchain Technology from a Legal Perspective and Its Tensions With the GDPR" *Cyberlaw Journal of the Cyberlaw Research Centre of the University of Lisbon School of Law 2019* at 44 – 47. Available at SSRN: https://ssrn.com/abstract=3545331. Accessed 5 February 2021.

[1702] Finck, M. (2018). "Blockchains and data protection in the European Union" *European Data Protection Law Review* 4(1): 29.

[1703] Duarte, D., G. (2019). "An Introduction to Blockchain Technology from a Legal Perspective and Its Tensions With the GDPR" *Cyberlaw Journal of the Cyberlaw Research Centre of the University of Lisbon School of Law 2019* at 41 – 42. Available at SSRN: https://ssrn.com/abstract=3545331. Accessed 5 February 2021.

[1704] Duarte, D., G. (2019). "An Introduction to Blockchain Technology from a Legal Perspective and Its Tensions With the GDPR" *Cyberlaw Journal of the Cyberlaw Research Centre of the University of Lisbon School of Law 2019* at 42. Available at SSRN: https://ssrn.com/abstract=3545331. Accessed 5 February 2021.

personal data to third countries.[1705] As Duarte correctly points out, the GDPR assumes that there is a single central authority that can either be identified as a processor or data controller.[1706] Despite these challenges, Erbguth identifies five ways that can be used to make blockchains compliant with the GDPR.[1707]

5.5.1 Avoid storing personal data on a blockchain

As discussed above,[1708] the GDPR applies to the processing of personal data of EU citizens. It stands to reason that storing information other than personal data will not render any of the provisions of the GDPR relevant.[1709] For instance, data on the impact of global warming and its effect on the rise of sea levels may be stored on a blockchain.

5.5.2 Off-chain storage of personal data

It has been mentioned that data may be stored off-chain.[1710] The storage of personal data outside a blockchain has benefits. Privacy is maintained because personal data is not privy to nodes that would have had access had the data been stored on blockchain. Storing data off-chain limits access to selected authorized users only. Another advantage is that once personal data is stored off-chain, it is easier to detect data breaches. If data is tampered with or changed, detecting such activities becomes simpler compared to detection a blockchain.[1711] The storage of personal data off-chain

[1705] Duarte, D., G. (2019). "An Introduction to Blockchain Technology from a Legal Perspective and Its Tensions With the GDPR" *Cyberlaw Journal of the Cyberlaw Research Centre of the University of Lisbon School of Law 2019* at 47. Available at SSRN: https://ssrn.com/abstract=3545331. Accessed 5 February 2021.

[1706] Duarte, D., G. (2019). "An Introduction to Blockchain Technology from a Legal Perspective and Its Tensions With the GDPR" *Cyberlaw Journal of the Cyberlaw Research Centre of the University of Lisbon School of Law 2019* at 47. Available at SSRN: https://ssrn.com/abstract=3545331. Accessed 5 February 2021; see also Giordano, M., T. *Blockchain and the GDPR: New Challenges for Privacy and Security* in Cappiello, B., & Carullo, G., (eds) (2020). *Blockchain, Law and Governance* Springer at 276.

[1707] Erbguth, J. (2019). "Five ways to GDPR-compliant use of blockchains" *European Data Protection Law Review* 5(3): 432 – 433.

[1708] See paragraph 4.3.3 above.

[1709] Erbguth, J. (2019). "Five ways to GDPR-compliant use of blockchains" *European Data Protection Law Review* 5(3): 433.

[1710] See paragraph 3.8 above.

[1711] Duarte, D., G. (2019). "An Introduction to Blockchain Technology from a Legal Perspective and Its Tensions With the GDPR" *Cyberlaw Journal of the Cyberlaw Research Centre of the University of Lisbon School of Law 2019* at 51. Available at SSRN: https://ssrn.com/abstract=3545331. Accessed 5 February 2021.

also enables data subjects to enforce their rights.[1712] If personal data is stored off-chain, data controllers are better placed to comply with the provisions of the GDPR.[1713]

5.5.3 Legal justification

An argument can be made to allow for the permanent justification of the storage of personal data on a blockchain.[1714] In other words, even though the application of a blockchain may contravene the provisions of the GDPR, legal justification may be sought to render blockchain operable. What is considered 'just' can depend on the circumstances of each case. For example, where it can be shown that the use of blockchain and its features would be in the best interest of the public then a legal justification can be made.

5.5.4 Build forgettable blockchains

Immutability is one of the unique features of a blockchain. If need be, a blockchain can be designed without the immutable feature provided that the immutable feature is not specifically required.[1715] Without immutability, a conventional distributed database may be used to store personal data.[1716] Compliance with the GDPR is made possible when data subjects are able to enforce their rights.

5.5.5 Users put their data on public blockchains

When a user sends bitcoins to another user on the Bitcoin network, he or she does this by generating a transaction that contains the recipient's public key. The sender

[1712] Duarte, D., G. (2019). "An Introduction to Blockchain Technology from a Legal Perspective and Its Tensions With the GDPR" *Cyberlaw Journal of the Cyberlaw Research Centre of the University of Lisbon School of Law 2019* at 51. Available at SSRN: https://ssrn.com/abstract=3545331. Accessed 5 February 2021.

[1713] Duarte, D., G. (2019). "An Introduction to Blockchain Technology from a Legal Perspective and Its Tensions With the GDPR" *Cyberlaw Journal of the Cyberlaw Research Centre of the University of Lisbon School of Law 2019* at 51. Available at SSRN: https://ssrn.com/abstract=3545331. Accessed 5 February 2021.

[1714] See Erbguth, J. (2019). "Five ways to GDPR-compliant use of blockchains" *European Data Protection Law Review* 5(3): 433.

[1715] Erbguth, J. (2019). "Five ways to GDPR-compliant use of blockchains" *European Data Protection Law Review* 5(3): 433.

[1716] Erbguth, J. (2019). "Five ways to GDPR-compliant use of blockchains" *European Data Protection Law Review* 5(3): 433.

then codes the transaction with their private key.[1717] In situations like these, Erbguth argues that users should be considered data controllers.[1718] He argues further that an organisation may provide certificates for users to sign and send to a public blockchain.[1719]

It has already been mentioned[1720] that public and private keys are considered personal data for GDPR purposes. Based on Erbguth's viewpoint, it can be argued that each time a user sends bitcoins to other users, the sender processes their own personal data. In doing so, users cannot hold an organisation or central authority responsible for processing their personal data. Users are then expected to comply with the relevant provisions of the GDPR.

5.6 Conclusion

The protection of a natural person's personal data is considered one of the most important rights in the EU. The GDPR was implemented to give natural persons control of their own personal data while maintaining the cross-border flow of information. The GDPR seeks to empower natural persons by giving them remedies that can be enforced against data controllers and processors. Data controllers and processors act as custodians of personal data.

The use of blockchain technology poses threats to the protection of personal data. One of the challenges emanating from the use of blockchains is the identification of data controllers. In terms of the GDPR, it is the data controllers' responsibility to ensure that the rights of the data subjects are enforced. Additionally, data subjects have the right to hold data controllers and processors accountable for the processing of their personal data. However, it has been found that establishing the identity of processors and data controllers on public blockchains is difficult.

[1717] Brito, J. *et al* (2015). *The Law of Bitcoin* iUniverse publishing (US) at 8.

[1718] Erbguth, J. (2019). "Five ways to GDPR-compliant use of blockchains" *European Data Protection Law Review* 5(3): 433.

[1719] Erbguth, J. (2019). "Five ways to GDPR-compliant use of blockchains" *European Data Protection Law Review* 5(3): 433.

[1720] Paragraph 5.4.4 above.

The rights of data subjects envisaged under the GDPR cannot easily be enforced due to blockchain's characteristics. For example, the GDPR requires data subject's personal data to be forgotten. In the context of blockchain, the right to be forgotten is akin to deleting personal data. As has been discussed, deleting information on a blockchain is not possible. In terms of the GDPR, data subjects also have the right to rectification. This right includes changing or editing personal data that is no longer accurate. It is difficult to effect changes to data stored on a blockchain to blockchain's immutable nature.

Despite the difficulties highlighted by the application of blockchain in the EU, there are measures that can be implemented to make blockchain compliant with the GDPR. Erbguth identifies five methods that can be used to make blockchain compliant with the GDPR. Like in the previous chapter, storing personal data off-chain is a feature that can make blockchain users compliant with the GDPR. Additional methods such as not storing personal data on any blockchain; having a legal justification; having users put their own personal data on a public blockchain and building forgettable blockchains are seen to be compliant with the GDPR.

In the next chapter, I discuss how the provisions of the POPI Act can protect personal information in South Africa.

CHAPTER 6: THE PROTECTION OF PERSONAL INFORMATION ON BLOCKCHAIN – SOUTH AFRICA

6.1 Introduction

Blockchain primarily functions as a recordkeeping ledger capable of storing data. The collection of VAT from the supply of digital goods on blockchain raises important questions around taxpayer privacy and taxpayer confidentiality.[1721] While using blockchain for the collection of VAT may be beneficial to tax authorities and taxpayers, the benefits should not come at the cost of eroding taxpayer privacy and confidentiality. If a taxpayer's right to privacy and confidentiality is eroded, it is likely that taxpayers lose trust in the tax administration process. A lack of trust can lead to low tax compliance. Low tax compliance can negatively impact revenue collection. Low revenue collection can lead to little or low levels of public expenditure across all spheres of government. Decreased levels in government spending can reduce economic growth. People's perception of blockchain can be negatively impacted if blockchain use cases are seen as non-compliant with data privacy laws. If government and businesses do not trust blockchain, blockchain cannot grow and develop.

To remedy this domino effect, it is important to address the privacy considerations associated with the collection and administration of VAT on blockchain. In this chapter, I consider how the provisions of the Protection of Personal Information (POPI) Act 4 of 2013 can be applied to blockchain technology. The chapter begins by discussing the relevant provisions of the POPI Act. Thereafter, blockchain's application for the VAT administrative process is considered to ascertain whether it conforms to the provisions of the POPI Act.

[1721] There's a difference between privacy and confidentiality. Debelva and Mosquera define privacy as "the right to keep one's affairs secret" while confidentiality refers to "information disclosed to a person or entity should not be disclosed to an unrelated third party whether intentionally or by accident." See Debelva, F. & Mosquera, I. (2017). "Privacy and Confidentiality in Exchange of Information Procedures: Some Uncertainties, Many Issues but Few Solutions" *Intertax* 45(5): 363.

6.2 The Protection of Personal Information Act

South Africa promulgated its first data protection legislation in 2013. The POPI Act gives effect to the Constitutional right to privacy entrenched in section 14 of the Constitution.[1722] The right to privacy includes the right to protection against the unlawful collection, retention, dissemination, and use of personal information.[1723] The POPI Act, while taking cognisant of the constitutional values of democracy and openness, seeks to promote economic growth and social progress by removing impediments to the free flow of information.[1724] The POPI Act regulates the processing of personal information by private and public bodies in a manner that gives effect to the right to privacy. The POPI Act ensures that this regulation is consistent with international standards.[1725]

Initially, section 1, Part A of Chapter 5, section 112, and section 113 of the POPI Act were operational since 11 April 2014.[1726] Sections 2 to 38; and sections 55 to 109; section 111 and section 114(1) to (3) of the POPI Act are effective as of 1 July 2020.[1727]

6.2.1 What is personal information?

Paragraph 4.4 discussed personal information from a global perspective. In this section, I look at what constitutes 'personal information' from a South African perspective. Hence, I do not repeat the discussion and statements made in paragraph 4.4 above.

[1722] Section 14 of the Constitution of the Republic of South Africa, 1998 reads: "everyone has the right to privacy, which includes the right not to have – (a) their person or home searched; (b) their property searched; (c) their possessions seized; or (d) the privacy of their communications infringed."

[1723] The Preamble of the POPI Act.

[1724] The Preamble of the POPI Act.

[1725] The Preamble of the POPI Act.

[1726] See Government Notice 912 in Government Gazette 37067 dated 26 November 2013; Pillay, L. (2014). "The partial commencement of the Protection of Personal Information Act 2013" *Without Prejudice* at 54.

[1727] Janse van Rensburg, R. (2020). "*POPI Act officially in effect*". Available at https://solidariteit.co.za/en/popi-act-officially-in-effect/. Accessed 15 March 2020.

From the onset, it should be noted that 'personal information' has been defined broadly in the POPI Act. The following constitutes 'personal information' for purposes of the POPI Act:

i) "Information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

ii) information relating to the education or the medical, financial, criminal or employment history of the person;

iii) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

iv) the biometric information of the person;

v) the personal opinions, views or preferences of the person;

vi) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

vii) the views or opinions of another individual about the person; and

viii) the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person."[1728]

The definition of 'personal information' above is not exhaustive[1729] and in my view, it is possible to supplement the definition with 'any information that can be closely linked or used to identify a natural person'. In this regard, it is important to consider whether information that is stored, processed, collected, or retrieved on a blockchain constitutes personal information for purposes of the POPI Act. As discussed earlier,[1730] data stored on a blockchain can be hashed or encrypted to promote privacy. However, this process is reversible. In other words, with the appropriate computation power and tools, it is possible to reverse hashed or encrypted data to reveal the original data, hence identifying a data subject. The original data constitutes personal

[1728] Section 1 of the definition of 'personal information' in the POPI Act.
[1729] See the wording of the definition of 'personal information' in the POPI Act.
[1730] See paragraph 4.8.3.

information. For this reason, it is my view that hashed data and encrypted data should constitute 'personal information' for purposes of the POPI Act. This view is consistent with the argument that encrypted data and hashed data can be considered 'personal data' for EU GDPR purposes.[1731]

The POPI Act makes provision for a responsible party to use unique identifiers[1732] to identify data subjects.[1733] However, the POPI Act does not provide a list of unique identifiers. This, in my view, is a shortcoming. A closer look at the definition of 'personal information' in section 1 of the POPI Act reveals that online identifiers constitute 'personal information'.[1734] Online identifiers include a person's IP address, cookie identifiers, and radio frequency identification tags.[1735] Online identifiers can be extended to include advertising IDs, pixel tags, account handles, device fingerprints, and MAC addresses.[1736] Ordinarily, online identifiers and unique identifiers *per se* cannot readily be used to identify a data subject. However, if an online identifier and a unique identifier are combined, then it is possible to identify a data subject with relative ease.[1737] Online identifiers and unique identifiers can also be combined to create a profile of a data subject.[1738]

[1731] See discussion at paragraph 5.4.4 above.

[1732] A unique identifier can have different meaning depending on the discipline and context in which it is used. For example, SARS defines a unique identifier as "a number allocated to each property, local business, trade and/or profession as per the information declared on income tax form". See https://www.sars.gov.za/faq/faq-what-is-a-unique-identifier/. Accessed 21 July 2022. Generally, unique identifiers include a person's ID, name, digital signature, and a passport number. See Martin, A. & Martinovic, I. (2016). "Security and Privacy Impacts of a Unique Personal Identifier" at 1 – 19. Available at https://ora.ox.ac.uk/catalog/uuid:90cf14a1-beb3-4322-b18d-deffe8c7f861/download_file?file_format=application%2Fpdf&safe_filename=workingpaperno4martinmartinovic.pdf. Accessed 21 July 2022.

[1733] Section 1 of the definition of 'unique identifier' in the POPI Act reads: "any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to the responsible party."

[1734] See part (c) of the definition of 'personal information' in the POPI Act.

[1735] See Recital 30 of the EU GDPR.

[1736] See Information Commissioner's Office (ICO). "*What are identifiers and related factors*?" Available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-are-identifiers-and-related-factors/. Accessed 21 July 2022.

[1737] See Recital 30 of the EU GDPR.

[1738] See Recital 30 of the EU GDPR.

6.3 Jurisdictional application of the POPI Act

The POPI Act applies to private and public bodies that process personal information recorded by or for a responsible party by making use of automated[1739] or non-automated means.[1740] It should be noted that the POPI Act applies to non-automated processing if the record forms part of a filing system.[1741] Although not explicitly stated in the POPI Act, 'automated means' can include computers, aircrafts, robots, artificial intelligence, self-driving motor vehicles, or any other system that can be programmed by computer code. This means that a blockchain system falls under the ambit of POPI Act because a blockchain can operate automatically in response to instructions given by its users.[1742] As alluded to above, the manual processing of personal information falls into the ambit of the POPI Act if it is recorded on a filling system. The POPI Act defines a filling system as "any structured set of personal information whether centralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria."[1743] A closer look at the definition of a 'filing system' in the POPI Act suggests that a blockchain can be considered as a 'filling system'. This is because a blockchain can store personal information in a decentralised or dispersed manner capable of access in multiple geographical locations. A 'record' is broadly defined in the POPI Act and includes "any recorded information regardless of form or medium in the possession or under the control of a responsible party, whether or not it was created by a responsible party and regardless of when it came into existence."[1744] It is my view that blockchain is a 'record' for purposes of POPI because

[1739] 'Automated' refers to any equipment capable of operating automatically in response to instructions given for the purpose of processing information. See section 3(4) of the POPI Act. Interestingly, the Electronic Communications and Transactions Act (ECTA) defines 'automated transaction' as: "an electronic transaction conducted or performed, in whole or in part, by means of data messages in which the conduct or data messages of one or both parties are not reviewed by a natural person in the ordinary course of such natural person's business or employment." See the definition of 'automated transaction' in section 1 of the ECTA Act.

[1740] Section 3(1)(a) of the POPI Act. See also Papadopoulos, S. & Snail ka Mtuze, S. (eds) (2022). *Cyberlaw@SA: the law of the internet in South Africa* (4th edition) Van Schaik Publishers at 349.

[1741] Section 3(1)(a) of the POPI Act.

[1742] Section 3(4) of the POPI Act.

[1743] See definition of 'filing system' in section 1 of the POPI Act.

[1744] See definition of 'record' in section 1 of the POPI Act. Examples of a 'record' include: "(i) writing material; (ii) information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored; (iii) label, making or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means; (iv) book, map, plan, graph or drawing; (v) photograph, film, negative, tape, or other device in which one or more visual images are embodied so as to be capable, with or a responsible party can create a blockchain for purposes of storing personal information.

The second important aspect to consider when applying the provisions of the POPI Act to blockchain is whether personal information has been processed by a responsible party. A responsible party is a private or public body or any other person that processes personal information.[1745] The government, a revenue authority, a municipality, a public university, provincial, and national departments are all examples of public bodies. Private bodies include social media companies, medical aid companies, private tertiary institutions, and other multinational companies. The responsible party must be domiciled in South Africa.[1746] The POPI Act does not define 'domicile'. It is unclear why the term 'domicile' was used in the POPI Act. In the South African tax framework, 'residence' is the term often used to determine a person's tax status in the country. The term 'resident' is commonly used in the Income Tax Act 58 of 1962 (the Income Tax Act) to determine a person's tax liability. In my view and for purposes of the POPI Act, a public body is domiciled in South Africa if it originates or is established in South Africa. A private body is domiciled in South Africa if it has a permanent establishment in South Africa. Importantly, the POPI Act also applies to responsible parties not domiciled in South Africa provided that the responsible party makes use of automated or non-automated means in South Africa for purposes other than to forward personal information.[1747] In my view, this provision fails to consider the possibility that a non-domiciled responsible party processes personal information when transmission of personal information actually takes place.[1748] The effect of this provision also raises concerns around the POPI Act's extraterritorial application. To illustrate this, I make use of an example.

without the aid of some other equipment, of being reproduced." See definition of 'record' in section 1 of the POPI Act. See also Papadopoulos, S. & Snail ka Mtuze, S. (eds) (2022). *Cyberlaw@SA: the law of the internet in South Africa* (4th edition) Van Schaik Publishers at 353.

[1745] See definition of 'responsible party' in section 1 of the POPI Act.

[1746] Section 3(1)(b)(i) of the POPI Act.

[1747] Section 3(1)(b)(ii) of the POPI Act.

[1748] 'Processing' means: "any operation or activity or any set of operation, whether or not by automatic means, concerning personal information including (a) the collection, receipt, recording, organization, collation, storage, updating or modification, retrieval, alteration, consultation or use; (b) dissemination by means of transmission, distribution or making available in any other form; or (c) merging, linking, as well as restriction, degradation, erasure or destruction of information." See the definition of 'processing' in section 1 of the POPI Act.

Example 7

TX (situated in a foreign jurisdiction) processes personal information. TX transmits personal information to South Africa by making use of a blockchain. TX joins a private blockchain network located in South Africa. TX transmits the data through a smart contract. TX is domiciled in a country that does not have Data Protection laws. South Africa does not send personal information to TX or to its country of incorporation.

In this example above, the POPI Act does not apply to TX because TX uses automated means located in South Africa to forward personal information. In other words, TX can use the data as it pleases and is under no obligation to implement safety and security measures to ensure that personal information is protected. If an unauthorised party accesses and retrieves data stored by TX, data subjects will be unaware of the data breach because TX has no obligation to report the data breach. Additionally, the data subjects are unable to enforce their right to privacy because TX does not have data protection laws in its country of origin. Additionally, it can also be argued that the POPI Act does not have extraterritorial application. This distinction must be drawn with the EU GDPR. The EU GDPR's application is not limited to the location or jurisdiction of the data controller (responsible party).[1749] In other words, the EU GDPR applies to the processing of personal data by a data controller located in the EU regardless of whether processing takes place in the EU or not.[1750] In my view, the mere fact that a non-domiciled responsible party forwards personal information to South Africa suggests that personal information is either collected or stored at any given time. If one considers that personal information is processed when a party disseminates,

[1749] See Article 3(1) of the EU GDPR.

[1750] See Article 3(1) of the EU GDPR. Article 3(2) of the EU GDPR reads: "This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union." Makulilo argues that the EU GDPR has a worldwide scope. In practical terms, if an African data controller or processor has an 'establishment' in the EU where personal data is processed in the context of the activities of that establishment, then the EU GDPR applies to that African data controller. If an African data controller does not have an 'establishment' in the EU but processes personal data of EU citizens may be subject to the EU GDPR if the processing of data is connected with the offering of goods or services or if the processing relates to the monitoring of EU citizens' behaviour. See Makulilo, A. B. (2017). "The GDPR implications for data protection and privacy protection in Africa" *International Journal for the Data Protection Officer, Privacy Officer and Privacy Counsel* 1(2): 17.

distributes, or makes available in any other form,[1751] then it follows that "forwarding" personal information constitutes "processing" for purposes of the POPI Act. To remedy this defect, it is my view that the POPI Act should be amended to make provision for its application regardless of the location of the responsible party. This is to ensure that the POPI Act applies to a non-domiciled responsible party irrespective of whether that party forwards personal information to South Africa.[1752]

The POPI Act applies to the processing of personal information to the exclusion of any legislation that regulates personal information to the extent that the latter is materially inconsistent to POPI's provisions.[1753] Simply put, the POPI Act is the primary legislation that regulates the processing of personal information in South Africa. Notably, if another legislation provides extensive conditions for the processing of personal information, then the latter framework applies.[1754] It is important to consider the effects of this provision. Again, I make use of an example.

<u>Example 8</u>

Z is a French citizen living and working in South Africa. The French tax authority has reason to believe that Z has not been tax compliant for the past ten years. The French tax authorities request tax information from SARS. The requested information can assist the French tax authorities to ascertain Z's tax liability and compliance. SARS duly obliges and transmits Z's tax information to the French tax authority.

Suppose that Z asks SARS to provide them with the tax information sent to the French tax authority. SARS sends the relevant tax information to Z in a non-readable format (anonymised data). Z does not have any recourse in terms of the POPI Act because

[1751] See part (b) of the definition of 'processing' in the POPI Act.

[1752] According to the Preamble of the POPI Act, POPI Act seeks to regulate the flow of personal information across the borders of South Africa. This suggests that the POPI Act may have been modelled on the data protection regulations in the EU. Additionally, the POPI Act seeks to balance the protection of an individual's personal information while maintaining an interest in the promotion of economic activity. It is difficult for the POPI Act to achieve the objectives set out in the Act if its territorial scope is confined to the borders of South Africa only. The challenge can be remedied by extending the Act's territorial scope to include processing of personal information belonging to South African citizens outside the borders of South Africa.

[1753] Section 3(2)(a) of the POPI Act; See also Papadopoulos, S. & Snail ka Mtuze, S. (eds) (2022). *Cyberlaw@SA: the law of the internet in South Africa* (4th edition) Van Schaik Publishers at 353.

[1754] Section 3(2)(b) of the POPI Act; See also Papadopoulos, S. & Snail ka Mtuze, S. (eds) (2022). *Cyberlaw@SA: the law of the internet in South Africa* (4th edition) Van Schaik Publishers at 353.

as it stands, there is no provision in the POPI Act that enables Z to receive the information in a readable format. However, Z can invoke Article 20 of the EU GDPR.[1755] In terms of Article 20, Z has the right to receive tax information provided by SARS in a structured, commonly used, and machine-readable format.[1756] This right is clearly not afforded in the POPI Act. Because the EU GDPR provides an extensive right not afforded in the POPI Act, it is submitted that the provisions of the GDPR can apply in this scenario. This view is consistent with the POPI Act since the latter Act gives effect to Z's right to constitutional privacy.[1757]

6.4 Exclusions to the scope of the POPI Act

6.4.1 Personal activities

There are certain activities that fall outside of the ambit of the POPI Act. The POPI Act does not apply to the processing of personal information during personal or household activities.[1758] This provision is similar to Article 2(a) of the EU GDPR.[1759]

6.4.2 De-identification

The POPI Act does not apply to personal information that has been de-identified to the extent that it cannot be re-identified.[1760] The POPI Act defines "de-identify" as the deletion of information that identifies a data subject. It also refers to the deletion of

[1755] Article 20 of the EU GDPR reads: "(1) The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where: (a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and (b) the processing is carried out by automated means. (2) In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible. (3) The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. (4) The right referred to in paragraph 1 shall not adversely affect the tights and freedoms of others."

[1756] Article 20(1) of the EU GDPR.

[1757] Section 2(a) of the POPI Act read with section 3(3) of the POPI Act.

[1758] Section 6(1)(a) of the POPI Act.

[1759] Article 2(1)(a) of the EU GDPR reads: "This Regulation does not apply to the processing of personal data in the course of an activity which falls outside the scope of the Union law."

[1760] Section 6(1)(b) of the POPI Act.

information that can be used or manipulated by a reasonably foreseeable method to identify the data subject. Last, de-identification refers to the deletion of information that can be linked by a reasonably foreseeable method to other information that identifies the data subject.[1761] In essence, the POPI Act only applies to identifiable personal information.[1762] Anonymous data is not considered 'personal information' for purposes of the POPI Act. This is because it is difficult to identify a data subject using anonymised data. This means that the processing of anonymous data falls outside the ambit of the POPI Act.[1763] A private or public body is not compelled to comply with the provisions of POPI Act if they process anonymised data. I use another example to illustrate this point.

Example 9

SARS receives a request for tax information from *Bundeszentralamt für Steuern* (German tax authority). The request relates to a German citizen residing in South Africa who is believed to have failed to submit tax returns for the past five years. SARS anonymises the German citizen's tax information before remitting it to *Bundeszentralamt für Steuern* on a private blockchain.

In the example above, SARS has anonymised tax information before its remission to Germany. In doing so, SARS has excluded the applicability of the provisions of the POPI Act. Similarly, and as discussed above,[1764] the EU GDPR does not apply to anonymised data.[1765] This also means that the *Bundeszentralamt für Steuern* is not required to comply with the provisions of the EU GDPR. The reason for this is that anonymised information is incapable of identifying a natural person.[1766] As already discussed above,[1767] ascertaining whether information has been anonymised is a

[1761] See definition of 'de-identify' in section 1 of the POPI Act.

[1762] Papadopoulos, S. & Snail ka Mtuze, S. (eds) (2022). *Cyberlaw@SA: the law of the internet in South Africa* (4th edition) Van Schaik Publishers at 353.

[1763] Papadopoulos, S. & Snail ka Mtuze, S. (eds) (2022). *Cyberlaw@SA: the law of the internet in South Africa* (4th edition) Van Schaik Publishers at 353.

[1764] Paragraph 5.4.4 above.

[1765] Recital 26 of the EU GDPR.

[1766] Recital 26 of the EU GDPR; see also Artzt, M., (ed) Determann, L., Long, W., *Blockchain and Data Privacy* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 196.

[1767] Paragraph 5.4.4 above.

matter of fact. In other words, one should determine the reasonable likelihood of identification.[1768] If SARS uses an anonymisation technique to make it impossible to identify the identity of a taxpayer, then the provisions of the POPI Act fall away because anonymised information does not constitute personal information for POPI Act. Put simply, there is no nexus between the taxpayer and the anonymised data.

It can be argued that since anonymised data does not constitute personal information for purposes of POPI, then it follows that anonymised data does not constitute 'taxpayer information' as defined.[1769] The definition of personal information in the POPI Act is very broad and includes information relating to a person's education, finances, criminal, and employment history.[1770] Although tax information is not expressly mentioned in the definition of personal information, it is my view that taxpayer information constitutes 'personal information' for POPI purposes. The reason for this is clear. Taxpayer information includes information relating to a taxpayer's income and other related personal details and circumstances.[1771] Thus, taxpayer information includes a person's gender, age, ID number, physical address, and e-mail address. This information constitutes 'personal information' in terms of the POPI Act.[1772]

In my view, if taxpayer information is anonymised to the extent that it is impossible for any person to link the anonymised information to a taxpayer, then such anonymised data is not 'taxpayer information' as defined. It is irrational to exclude anonymised data from the provisions of the POPI Act but then treat anonymised data as taxpayer information for purposes of the Tax Administration Act[1773] since taxpayer information is, for all intents and purposes, personal information. SARS has indicated that nothing precludes it from disclosing taxpayer information in anonymised form.[1774] In my view,

[1768] Artzt, M., (ed) Determann, L., Long, W., *Blockchain and Data Privacy* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 196.

[1769] Section 67(1)(b) of the Tax Administration Act defines taxpayer information as: "any information provided by a taxpayer or obtained by SARS in respect of the taxpayer, including biometric information."

[1770] Section 1 of the definition of 'personal information' in the POPI Act.

[1771] Cockfield, A., J. 2010. "Protecting Taxpayer Privacy Rights Under Enhanced Cross-border Tax Information Exchange: Toward A multilateral Taxpayer Bill of Rights" *UBC Law Review* 42(2): 437.

[1772] Section 1 of the definition of 'personal information' in the POPI Act.

[1773] Act 28 of 2011.

[1774] Section 69(8)(d) of the Tax Administration Act. SARS can also disclose taxpayer information in 'anonymous' form to the Statistician-General as may be required for the purpose of carrying out this is significant for two reasons. First, this can be interpreted to mean that SARS does not consider anonymised information as taxpayer information. Second, the disclosure of anonymised information implies that SARS does not believe that such information can be used to identify a taxpayer.

It should be noted that the purpose of anonymisation is not to escape the application of any legislative provisions but rather to ensure that the privacy of natural persons is protected. Anonymising data ensures that information is not linked to a natural identifiable or juristic person.[1775] Additionally, anonymising personal information ensures that a public or private body does not breach the relevant data protection legislation.[1776] For example, the use of anonymised data by SARS on a blockchain removes the requirement to obtain consent from a taxpayer every time their personal information is processed.[1777] As pointed out above, collection of VAT by blockchain poses a risk to taxpayer information. As a result, it is necessary to consider protecting taxpayer information on blockchain. It remains the sole responsibility of tax authorities to ensure that taxpayer information is anonymised.

6.4.3 On behalf of a public body

The provisions of the POPI Act do not apply to public bodies that process personal information in the interest of national security.[1778] If a public body processes personal information for purposes of assisting in the identification of the financing terrorism and other related activities, then this form of processing falls outside the ambit of the POPI Act.[1779] The POPI Act also excludes the processing of personal information in so far as it relates to the prevention and identification of the proceeds of unlawful activities and the combating of money-laundering activities. The exclusion extends to the processing of personal information when investigating offences, prosecuting offenders, the execution of sentences, or security measures to the extent that

the Statistician-General's duties. See section 70(2)(a) of the Tax Administration Act. It should also be noted that currently, the Tax Administration Act does not define the terms 'anonymous' and 'anonymised form'.

[1775] The definition of 'person' in section 1 of the POPI Act includes a juristic person.

[1776] See Groos, D. & van Veen, E. (2020). "Anonymised Data and the Rule of Law" *European Data Protection Law Review* 6(4): 498 – 508.

[1777] See section 11(1)(a) of the POPI Act.

[1778] Section 6(1)(c)(i) of the POPI Act.

[1779] Section 6(1)(c)(i) of the POPI Act.

adequate safeguards have been established in specific legislation for the protection of personal information.[1780]

6.4.4 Cabinet members and the judiciary

The processing of personal information by Cabinet and its committees or the Executive Council of a province is excluded from the provisions of the POPI Act.[1781] The processing of personal information by members of the judiciary who perform judicial functions of a court in the Constitutional Court, Supreme Court of Appeal, the High Court, the Magistrates' Courts, or any other court recognised in terms of an Act of Parliament is specifically excluded.[1782]

6.4.5 Journalistic, literary or artistic purposes

The POPI Act does not apply to the processing of personal information for the purposes of journalistic, literary or artistic expression to the extent that it does not override the public's interest, and the right to privacy with the right to freedom of expression.[1783] When a journalist or a person who performs journalistic function processes personal information and that person is subject to a code of ethics that provides adequate safeguards for the protection of personal information, the code of ethics will apply to the exclusion of the POPI Act.[1784] The following factors indicate whether adequate safeguards have been provided for in the code of ethics: (i) the special importance of the public interest in freedom of expression, (ii) the call to secure the integrity of personal information, (iii) domestic and international standards of professional integrity for journalists, (iv) the nature and ambit of self-regulatory forms of supervision provided by the profession and (v) domestic and international standards balancing the public interest in allowing for the free flow of information to the public

[1780] Section 6(1)(c)(ii) of the POPI Act.
[1781] Section 6(1)(d) of the POPI Act.
[1782] Section 6(1)(e) of the POPI Act read with section 166 of the Constitution of the Republic of South Africa.
[1783] Section 7(1) of the POPI Act; see Papadopoulos, S. & Snail ka Mtuze, S. (eds) (2022). *Cyberlaw@SA: the law of the internet in South Africa* (4th edition) Van Schaik Publishers at 354.
[1784] Section 7(2) of the POPI Act; Papadopoulos, S. & Snail ka Mtuze, S. (eds) (2022). *Cyberlaw@SA: the law of the internet in South Africa* (4th edition) Van Schaik Publishers at 354.

through the media in recognition of the right of the public to be informed and public interest in safeguarding the protection of personal information of data subjects.[1785]

6.4.6 Exemption by the Information Regulator

In terms of section 37 of the POPI Act, the Information Regulator[1786] can grant an exemption to a responsible party to process personal information even if the processing is in breach of a condition for the processing of such information.[1787] For example, the Information Regulator can grant an exemption if it is satisfied that breaching the condition for the processing of personal information is in the public interest and that processing outweighs any interference of a data subject's privacy.[1788] Another scenario where the Information Regulator can grant an exemption is where the processing is substantially beneficial to the data subject or a third party to the extent that it outweighs any interference with the privacy of the data subject or the third party.[1789] For purposes of this section, 'public interest' includes national security, important economic and financial interests of a public body, the prevention, detection and prosecution of offences, historical, statistical or research activity, or the special importance of the interest in freedom of expression.[1790] The Information Regulator can impose reasonable conditions in respect of any exemption granted above.[1791]

Section 38 of the POPI provides for the exemption of the processing of personal information in respect of certain functions. For example, a public body can process personal information in order to discharge a relevant function without granting a data subject the right to object to the processing of personal information.[1792] For purposes of section 38 of the POPI Act, a 'relevant function' is defined as:

[1785] Section 7(3) of the POPI Act; see also Papadopoulos, S. & Snail ka Mtuze, S. (eds) (2022). *Cyberlaw@SA: the law of the internet in South Africa* (4th edition) Van Schaik Publishers at 353.

[1786] The Information Regulator is an independent juristic person that is subject to the Constitution of the Republic of South Africa. The Information Regulator is impartial and performs its functions and exercises its powers without fear, favour, or prejudice. See section 39 of the POPI Act.

[1787] Section 37(1) of the POPI Act.

[1788] Section 37(1)(a) of the POPI Act.

[1789] Section 37(1)(b) of the POPI Act.

[1790] Section 37(2) of the POPI Act.

[1791] Section 37(3) of the POPI Act.

[1792] Section 38(1) read with section 11(3) and (4) of the POPI Act.

"any function— (a) of a public body; or (b) conferred on any person in terms of the law, which is performed with the view to protecting members of the public against— (i) financial loss due to dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons concerned in the provision of banking, insurance, investment or other financial services or in the management of bodies corporate; or (ii) dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons authorised to carry on any profession or other activity."[1793]

A public body is also exempt from collecting personal information directly from the data subject if the public body processes personal information for a relevant function.[1794] Section 38 can also be invoked by a public body to limit further processing in terms of section 15 of the POPI Act.[1795] Lastly, a public body can be exempted from notifying a data subject when collecting personal information as long as that public body performs a relevant function.[1796]

6.5 The rights of data subjects in the POPI Act

A data subject is a person afforded protection in terms of the POPI Act.[1797] The definition of 'person' in the POPI Act includes juristic person meaning companies, partnerships, and other corporate entities irrespective of their location.[1798] Data subjects are afforded certain rights in terms of the POPI Act. For purposes of this section, any reference made to a data subject includes a juristic person.

[1793] Section 38(2) of the POPI Act.

[1794] Section 38(1) read with section 12 of the POPI Act; see also Papadopoulos, S. & Snail ka Mtuze, S. (eds) (2022). *Cyberlaw@SA: the law of the internet in South Africa* (4th edition) Van Schaik Publishers at 355.

[1795] Section 38(1) read with section 15 of the POPI Act.

[1796] Section 38(1) read with section 18 of the POPI Act; see also Papadopoulos, S. & Snail ka Mtuze, S. (eds) (2022). *Cyberlaw@SA: the law of the internet in South Africa* (4th edition) Van Schaik Publishers at 355.

[1797] See the definition of 'data subject in section 1 of the POPI Act.

[1798] See the definition of 'person' read with the definition of 'personal information' in section 1 of the POPI Act.

6.5.1 The right to be notified

A data subject has the right to be notified when their personal information is collected.[1799] The onus rests on the responsible party to ensure that the data subject is notified whenever their personal information has been collected. If the personal information is not directly collected from the data subject, the source of the collection must be made known to the data subject.[1800] Other factors that must be made known to the data subject include: (i) the name and address of the responsible party; (ii) the purpose for which the information is being collected; (iii) whether or not the supply of the information by that data subject is voluntary or mandatory; (iv) the consequences of failure to provide the information; (v) any particular law authorising or requiring the collection of the information.[1801] Interestingly, a responsible party must notify a data subject when the former intends to transfer information to a third country or international organisation.[1802]

A responsible party is not required to notify a data subject that their personal information is being collected if the data subject gives his or her consent.[1803] The POPI Act defines consent as "any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information."[1804] It should be noted that the consent of a data subject is not required when SARS enforces legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act.[1805] In other words, SARS is not required to obtain the consent of the taxpayer prior to sharing tax information with foreign jurisdictions.[1806] This provision can be applied in the context of exchange of information. Exchange of information enables tax authorities to share tax information in order to prevent double taxation and tax evasion. During the exchange process, financial institutions retrieve tax information from taxpayers' financial accounts. Financial institutions share that

[1799] Section 5(a)(i) of the POPI Act.
[1800] Section 18(1)(a) of the POPI Act.
[1801] Section 18(1)(b) – (f).
[1802] Section 18(1)(g).
[1803] Section 18(4)(a).
[1804] Section 1 of the definition of 'consent' in the POPI Act.
[1805] Section 18(4)(c)(ii) of the POPI Act; see also Fritz, C. (2021). "South African Taxpayer's Right to Privacy in Cross-Border Exchange of Tax Information" *Constitutional Court Review* 11(1): 427.
[1806] Section 72(1)(e) of the POPI Act.

information with the relevant domestic tax authorities. In my view, the consent exemption provision mentioned above ensures effective AEOI without delays. The legal requirement to obtain consent from a data subject (taxpayer), which ensures that a data subject is aware of any possible cross-border transfer of their personal information, is not always practicable in every situation. There are a number of reasons why it is unrealistic to always obtain consent from a data subject. For example, a data subject can be uncooperative to the request for consent. It is possible that a data subject may be unavailable at the time a request is made. It is also likely that a taxpayer may not fully understand the reasons of the request for consent. Fritz correctly states that it is unlikely for a taxpayer (data subject) to willingly consent to exchange of information because a taxpayer would have to understand the implication and risks associated with an exchange.[1807]

Fritz and Moller argue that a taxpayer should be informed of an impending exchange of tax information and a taxpayer should be allowed to challenge such a decision.[1808] The basis of their argument stems from a person's right to just administrative action in terms of section 33 of the Constitution.[1809] Moller questions whether SARS makes a 'decision'[1810] for purposes of the Promotion of Administrative Justice Act 3 of 2000 (PAJA) when exchanging personal information with another country. Moller reasons that the AEOI process involves collecting and combining information received from various financial institutions; establishing whether a particular country identified by various indicia has a double tax treaty with South Africa; and transmitting the

[1807] Fritz, C. (2021). "South African Taxpayer's Right to Privacy in Cross-Border Exchange of Tax Information" *Constitutional Court Review* 11(1): 425.

[1808] Fritz, C. (2021). "South African Taxpayer's Right to Privacy in Cross-Border Exchange of Tax Information" *Constitutional Court Review* 11(1): 428; Moller, L. (2016). "*An analysis of the current framework for the exchange of taxpayer information, with special reference to the taxpayer in South Africa's constitutional rights to privacy and just administrative action*" MCom mini dissertation (University of Cape Town) at 45 – 46.

[1809] Section 33 of the Constitution reads: "(1) Everyone has the right to administrative action that is lawful, reasonable and procedurally fair. (2) Everyone whose rights have been adversely affected by administrative action has the right to be given written reasons."

[1810] Section 1 of the definition of 'decision' in PAJA reads: "any decision of an administrative nature made, proposed to be made, or required to be made, as the case may be, under an empowering provision, including a decision relating to – (a) making, suspending, revoking or refusing to make an order, award or determination; (b) giving, suspending, revoking or refusing to give a certificate, direction, approval, consent or permission; (c) issuing, suspending, revoking or refusing to issue a licence, authority or other instrument; (d) imposing a condition or restriction; (e) making a declaration, demand or requirement; (f) retaining, or refusing to deliver up, an article; or (g) doing or refusing to do any other act or thing of an administrative nature, and a reference to a failure to take a decision must be construed accordingly."

processed data to a foreign competent authority.[1811] In the context of AEOI, Moller argues that a SARS officials fails to apply their mind on the substance of information exchange because information is transmitted without first establishing whether such information is foreseeably relevant to the receiving country.[1812] Moller also argues that the decision to share information with other countries constitutes 'administrative action'[1813] because it involves the administration of tax information pursuant to exchange obligations in terms of a tax treaty. Additionally, the administration of the tax treaties enables tax authorities to audit taxpayer compliance with the relevant tax laws of the countries party to the treaty.[1814] This passive administrative process, which includes SARS' failure to vet or subject the relevant data to an evaluative process, amounts to failure to make a decision in terms of PAJA.[1815]

[1811] Moller, L. (2016). "*An analysis of the current framework for the exchange of taxpayer information, with special reference to the taxpayer in South Africa's constitutional rights to privacy and just administrative action*" MCom mini dissertation (University of Cape Town) at 40; OECD (2012). "Automatic Exchange of Information: What it is, How it works, Benefits, What remains to be done" at 9. Available at https://www.oecd.org/ctp/exchange-of-tax-information/automatic-exchange-of-information-report.pdf. Accessed 27 January 2022.

[1812] Moller, L. (2016). "*An analysis of the current framework for the exchange of taxpayer information, with special reference to the taxpayer in South Africa's constitutional rights to privacy and just administrative action*" MCom mini dissertation (University of Cape Town) at 41.

[1813] Section 1 of the definition of 'administrative action' reads: "any decision taken, or any failure to take a decision, by (a) an organ of state, when – (i) exercising a power in terms of the Constitution or a provincial constitution; or (ii) exercising a public power or performing a public function in terms of any legislation; or (b) a natural or juristic person, other than an organ of state, when exercising a public power or performing a public function in terms of an empowering provision, which adversely affects the rights of any person and which has a direct, external legal effect, but does not include - (aa) the executive powers or functions of the National Executive, including the powers or functions referred to in sections 79(1) and (4), 84(2)(a), (b), (c), (d), (f), (g), (h), (i) and (k), 85(2)(b), (c), (d) and (e), 91(2), (3), (4) and (5), 92(3), 93, 97, 98, 99 and 100 of the Constitution; (bb) the executive powers or functions of the Provincial Executive, including the powers or functions referred to in sections 121(1) and (2), 125(2)(d), (e) and (f), 126, 127(2), 132(2), 133(3)(b), 137, 138, 139 and 145(1) of the Constitution; (cc) the executive powers or functions of a municipal council; (dd) the legislative functions of Parliament, a provincial legislature or a municipal council; (ee) the judicial functions of a judicial officer of a court referred to in section 166 of the Constitution or of a Special Tribunal established under section 2 of the Special Investigating Units and Special Tribunals Act, 1996 (Act No. 74 of 1996), and the judicial functions of a traditional leader under customary law or any other law; (ff) a decision to institute or continue a prosecution; (gg) a decision relating to any aspect regarding the nomination, selection or appointment of a judicial officer or any other person, by the Judicial Service Commission in terms of any law; hh) any decision taken, or failure to take a decision, in terms of any provision of the Promotion of Access to Information Act, 2000; or (ii) any decision taken, or failure to take a decision, in terms of section 4(1)."

[1814] Moller, L. (2016). "*An analysis of the current framework for the exchange of taxpayer information, with special reference to the taxpayer in South Africa's constitutional rights to privacy and just administrative action*" MCom mini dissertation (University of Cape Town) at 41.

[1815] Moller, L. (2016). "*An analysis of the current framework for the exchange of taxpayer information, with special reference to the taxpayer in South Africa's constitutional rights to privacy and just administrative action*" MCom mini dissertation (University of Cape Town) at 41 – 42.

Fritz is of the view that the decision by SARS to exchange tax information is an administrative action that must be lawful, reasonable, and procedurally fair as per section 33 of the Constitution.[1816] Fritz argues that since the provisions of PAJA are more favourable to those of POPI in so far as exchange of information is concerned, then the provisions of the latter should prevail.[1817] In particular, the provisions of section 3(2)(b) of PAJA reads:

> "In order to give effect to the right to procedurally fair administrative action, an administrator, subject to subsection (4), must give a person referred to in subsection (1) – (i) adequate notice of the nature and purpose of the proposed administrative action; (ii) a reasonable opportunity to make representations; (iii) a clear statement of the administrative action; (iv) adequate notice of any right of review or internal appeal, where applicable; and (v) adequate notice of the right to request reasons in terms of section 5."[1818]

Fritz argues that it is prudent for SARS to inform taxpayers of an imminent request so that taxpayers can make representations.[1819] This is done to ensure that taxpayer's rights to privacy is protected.[1820] There are certain drawbacks to this view. As acknowledged by Fritz, this process can cause delays in the tax administration process.[1821] Second, there are instances when it is not necessary to inform a taxpayer of an impending request. For example, when SARS is not in possession of the requested information and SARS must make use of its information gathering powers.[1822] Third, section 4(a) of PAJA provides that an administrator can depart from the requirements set out in section 3(2)(b) of PAJA when it is reasonable and just to do so.[1823] In my view, it is not always practicable to notify the taxpayer that a request

[1816] Fritz, C. (2021). "South African Taxpayer's Right to Privacy in Cross-Border Exchange of Tax Information" *Constitutional Court Review* 11(1): 429.

[1817] Fritz, C. (2021). "South African Taxpayer's Right to Privacy in Cross-Border Exchange of Tax Information" *Constitutional Court Review* 11(1): 430; See also section 3(2)(b) of the POPI Act.

[1818] Section 3(2)(b) of PAJA.

[1819] Fritz, C. (2021). "South African Taxpayer's Right to Privacy in Cross-Border Exchange of Tax Information" *Constitutional Court Review* 11(1): 430.

[1820] Fritz, C. (2021). "South African Taxpayer's Right to Privacy in Cross-Border Exchange of Tax Information" *Constitutional Court Review* 11(1): 430.

[1821] Fritz, C. (2021). "South African Taxpayer's Right to Privacy in Cross-Border Exchange of Tax Information" *Constitutional Court Review* 11(1): 430.

[1822] Fritz, C. (2021). "South African Taxpayer's Right to Privacy in Cross-Border Exchange of Tax Information" *Constitutional Court Review* 11(1): 430.

[1823] Fritz, C. (2021). "South African Taxpayer's Right to Privacy in Cross-Border Exchange of Tax Information" *Constitutional Court Review* 11(1): 430; Section 4(a) of PAJA.

for their tax information has been made. It is important to look at each case on its own merits. While it is trite that taxpayers have a right to privacy, the right to privacy *per se* is not an absolute right. Since the right to privacy naturally encompasses the protection of personal information, the right to data protection (personal information) is not an absolute right.[1824] The right to privacy can be limited in terms of section 36 of the Constitution. Additionally, the purpose of the provisions in PAJA is to ensure that administrators follow the correct procedures when taking administrative action. This is to ensure that a person's rights are not adversely affected.[1825] In my view and considering the importance of exchange of information, an administrator (responsible party) can ensure that the transfer of tax information to another jurisdiction is done only if the latter jurisdiction has the necessary safeguards to ensure that the privacy and confidentiality of taxpayer information is protected. A responsible party can employ technical measures such as public-private key infrastructure and anonymisation techniques to ensure that tax information is kept secure each time it is transferred to another jurisdiction. The mere fact that a taxpayer has not been notified each time that their information is transmitted to another jurisdiction does not necessarily mean that the taxpayer's right to privacy and confidentiality has not been observed. The responsible party must ensure that the IT infrastructure used to transmit tax information has the necessary security safeguards.[1826]

[1824] See Fritz, C. (2021). "South African Taxpayer's Right to Privacy in Cross-Border Exchange of Tax Information" *Constitutional Court Review* 11(1): 415 – 416; Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 113; Recital 4 of the EU GDPR reads: "The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity."

[1825] See section 3(1) of PAJA.

[1826] Section 19 of the POPI Act reads: "(1) A responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent— (a) loss of, damage to or unauthorised destruction of personal information; and (b) unlawful access to or processing of personal information. (2) In order to give effect to subsection (1), the responsible party must take reasonable measures to— (a) identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control; (b) establish and maintain appropriate safeguards against the risks identified; (c) regularly verify that the safeguards are effectively implemented; and (d) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards. (3) The responsible party must have due regard to generally accepted information security practices

There is a view that taxpayers should be made aware by financial institutions that information in their possession is subject to FATCA/OECD standards.[1827] This can be achieved by inserting a clause to that effect in a bank-client contractual agreement. By signing the contractual agreement, the client consents to having their tax information shared with other jurisdictions. Existing clients can be made aware of a financial institution's tax reporting obligations.[1828] The rules and procedures relating to a financial institution's obligation for tax reporting purposes should be clear and in writing. The rules must clearly indicate that tax information must be shared with revenue authorities. The revenue authorities can then share this information automatically with another jurisdiction.[1829] The reasons for information exchange must be clearly stated. Clients can be notified that any exchange is subject to the presence of privacy and confidentiality laws in the requesting country. Clients can have the option of accepting or rejecting the contractual terms and conditions associated with exchange of information. If a client rejects the terms and conditions, then a financial institution should not be obligated to provide financial, banking services, or intermediary services to that client. By accepting the terms and conditions, the client automatically consents to having their tax information shared with revenue authorities irrespective of the revenue authority's location. Van Zyl notes that a customer's right to privacy is limited where a customer conducts business transactions which require the bank to make payments on the client's behalf.[1830] Additionally, van Zyl also notes that a customer's right to privacy is not infringed upon where a financial institution transmits information pertaining to a transaction to SARS in terms of a statutory duty.[1831] The reason for this is that every time a customer enters into a transaction

and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations."

[1827] Panayi, C. H. J. I. (2016). "Current trends on automatic exchange of information" *University School of Accountancy Research Paper* at 31. Available at https://accountancy.smu.edu.sg/cet/sites/accountancy.smu.edu.sg.cet/files/Current%20Trends%20on%20Automatic%20Exchange%20of%20Information.pdf. Accessed 15 March 2022; Baker, P. & Pistone, P. (2015). *General Report, The Practical Protection of Taxpayers' Fundamental Rights* (IFA Cahiers 2015 – Volume 100B) at 64.

[1828] For example, see Nedbank's notification to clients at https://www.nedbank.co.za/content/nedbank/desktop/gt/en/personal/tools-and-guidance/bank-anytime-anywhere/FATCA.html. Accessed 15 March 2022.

[1829] For example, see Nedbank's notification to clients at https://www.nedbank.co.za/content/nedbank/desktop/gt/en/personal/tools-and-guidance/bank-anytime-anywhere/FATCA.html. Accessed 15 March 2022.

[1830] Van Zyl, S. P. (2013). *The collection of Value Added Tax on online cross-border trade in Digital Goods*. Unpublished LLD thesis (UNISA) at 339.

[1831] Van Zyl, S. P. (2013). *The collection of Value Added Tax on online cross-border trade in Digital Goods*. Unpublished LLD thesis (UNISA) at 339.

with a bank, they subject themselves to a country's tax laws and, in the process, give consent through their conduct.[1832]

In my view, the process of nullifying consent from the onset of AEOI reduces the administrative burden imposed on revenue authorities. The time spent to identify and contact every taxpayer to provide consent each time a request is made, is reduced. The time spent waiting for a taxpayer to provide their consent is minimised. No costs are incurred by the revenue authorities to identify and contact the taxpayer. If blockchain is adopted, and consent is required, the time taken to give consent is minimised because a smart contract can be sued. The time it takes for SARS to receive the consent is reduced because blockchain provides instantaneous responses/notifications by deploying smart contracts. In turn, this makes the tax administration process smoother and more efficient.

The second point to consider is the issue of access. A responsible party must notify a data subject when their personal information has been accessed by an unauthorised person.[1833] The responsible party is also required to notify the Information Regulator should unauthorised access to a data subject's personal information occur.[1834] Section 22(2) of the POPI Act requires that a data subject be notified of any security breaches as soon as reasonably possible after the discovery of the data breach.[1835] Factors such as the legitimate needs of the law enforcement, measures reasonably necessary to determine the scope of the compromise, and measures taken to restore the integrity of the responsible party's information system must be considered.[1836] A responsible party can delay notification to the data subject if a public body responsible for the prevention, detection or investigation of offences determines that the notification will impede a criminal investigation by the public body concerned.[1837] In my view, this provision could potentially have unintended consequences for SARS and other tax authorities. If a security breach occurs, a responsible party must notify the data subject in writing and communicate to the data subject by emailing them; sending the

[1832] Van Zyl, S. P. (2013). *The collection of Value Added Tax on online cross-border trade in Digital Goods*. Unpublished LLD thesis (UNISA) at 339.
[1833] Section 5(a)(ii) of the POPI Act read with section 22(1)(b) of the POPI Act.
[1834] Section 22(1)(a) of the POPI Act.
[1835] Section 22(2) of the POPI Act.
[1836] Section 22(2) of the POPI Act.
[1837] Section 22(3) of the POPI Act.

notification via registered post or last known physical address; published in the news media; placed on the website of the responsible party or as may be directed by the Regulator.[1838] The notification to the data subject must contain sufficient information to allow the data subject to take protective measures against the consequences of the compromise.[1839] The notification to the data subject should clearly contain a description of the possible consequences of the security compromise.[1840] It is very difficult for a responsible party to reasonably foresee all the possible consequences of any security compromise. In my view, the type and form of information that is unlawfully retrieved can determine the severity of the impact to the data subject. For example, the unauthorised access of sensitive plain text tax information can be more severe to a data subject than the unauthorised access of anonymised tax information. The consequences cannot be the same because it is very difficult to link anonymised information to any data subject. Plain text information can be easily deciphered and used to the detriment of a data subject.

The notification to a data subject must contain a description of the measures that a responsible party intends to take or has taken to address the security compromise.[1841] The notification must also contain recommended measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise.[1842] If possible, the responsible party must make known the identity of the unauthorised person who accessed the personal information.[1843] The Information Regulator can direct a responsible party to publicise any compromise to the integrity or confidentiality of personal information if the Information Regulator has reasonable grounds to believe that publication would protect a data subject.[1844]

6.5.2 The right to access information

A data subject has the right to request access to their personal information. This right includes establishing whether a responsible party holds personal information of that

[1838] Section 22(4) of the POPI Act.
[1839] Section 22(5) of the POPI Act.
[1840] Section 22(5)(a) of the POPI Act.
[1841] Section 22(5)(b) of the POPI Act.
[1842] Section 22(5)(c) of the POPI Act.
[1843] Section 22(5)(d) of the POPI Act.
[1844] Section 22(6) of the POPI Act.

data subject.[1845] A data subject can request a responsible party to confirm whether that party holds personal information about the data subject. The confirmation is free of charge and the data subject is required to provide positive identification.[1846] A data subject can also request from a responsible party all records or descriptions of personal information about the data subject held by the responsible party including the identity of all third parties who have or who had access to the information.[1847] The responsible party is required to furnish the requested information within a reasonable time, subject to a prescribed fee, in a reasonable manner and format, and in a form that is generally understandable.[1848]

Once a request to access to information is made in terms of section 23(1) of the POPI Act, a data subject must be advised of the right to have their information corrected in terms of section 24 of the POPI Act.[1849] When a data subject makes a request in terms of section 23(1) of the POPI Act, and a responsible party requires a fee to be paid in in terms of section 23(1)(b), the responsible party must give the data subject a written estimate of the fee before providing the services and the responsible party may require the data subject to pay a deposit for all or part of the fee.[1850] A request for access to information can be denied in terms of sections 33 – 46 of the Promotion of Access to Information Act 2 of 2000 (PAI Act).[1851] A refusal for access to information made by a responsible party in terms of section 24(a) of the POPI Act does not preclude every other part from being disclosed.[1852]

6.5.3 The right to rectification

A data subject has the right to have his or her personal information corrected, destroyed, or deleted.[1853] A data subject can request a responsible party to correct or delete personal information that is inaccurate, irrelevant, out of date, incomplete,

[1845] Section 5(b) of the POPI Act.
[1846] Section 23(1)(a) of the POPI Act.
[1847] Section 23(1)(b) of the POPI Act.
[1848] Section 23(1)(b) of the POPI Act.
[1849] Section 23(2) of the POPI Act. The provisions of section 24 are discussed in paragraph 6.5.3 below.
[1850] Section 23(3) of the POPI Act.
[1851] Section 23(4)(a) of the POPI Act.
[1852] Section 23(5) of the POPI Act.
[1853] Section 5(c) of the POPI Act.

misleading, excessive, or obtained unlawfully.[1854] A data subject can also request for their personal information be deleted or destroyed provided that the responsible party is no longer authorised to retain that information.[1855] Section 14 of the POPI Act states that a responsible party must not retain personal information any longer than is necessary unless the retention of the record is required or authorised by law; the responsible party requires the record for lawful purposes related to its functions or activities; the retention is required by a contract between the parties or the data subject consents to the retention of the record.[1856]

When a responsible party receives a request by the data subject to delete, correct, or destroy personal information, a responsible party must do so as soon as possible.[1857] Once information has been altered, a responsible party must notify each party to whom the personal information has been disclosed.[1858] The responsible party must advise the data subject of all the relevant steps taken when a request for rectification has been received.[1859]

6.5.4 The right to object to the processing of information

A data subject has the right to object to the processing of his or her personal information.[1860] The objection may be given at any time unless legislation provides otherwise.[1861] If a data subject makes an objection to the processing of his or her personal information, the responsible party may no longer process the personal information.[1862] The right to object applies to direct marketing.[1863] Section 69(3) states that a responsible party may only process the personal information of a data subject (customer) if the responsible party has obtained the contact details of the data subject

[1854] Section 24(1)(a) of the POPI Act.
[1855] Section 24(1)(b) of the POPI Act.
[1856] Section 14(1) of the POPI Act.
[1857] Section 24(2) of the POPI Act.
[1858] Section 24(3) of the POPI Act.
[1859] Section 24(4) of the POPI Act.
[1860] Section 5(d) of the POPI Act.
[1861] Section 11(3)(a) of the POPI Act.
[1862] Section 11(4) of the POPI Act.
[1863] Section 1 of the definition of 'direct marketing' reads: "to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of - (a) promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or (b) requesting the data subject to make a donation of any kind for any reason."

in the context of the sale of a product or service. The responsible party can only process the personal information for the purpose of direct marketing of the responsible party's own similar products and services. Lastly, the responsible party can only process a data subject's personal information if the data subject has been given the opportunity to object to the use of their electronic details at the time when the information was collected. The data subject has the right to object to direct marketing on each direct marketing communication from the responsible party if the data subject has not initially refused such use.[1864]

6.5.5 The right to be free from unsolicited electronic communications

A data subject has the right not to have their personal information processed for purposes of directing marketing by means of unsolicited electronic communications.[1865] A responsible party is prohibited from processing a data subject's personal information for the purpose of direct marketing by means of any form of electronic communication, including automatic calling machines, facsimile machines, short message service (SMS) or electronic mail unless a data subject consents to the processing or if the data subject is a customer of the responsible party.[1866]

6.5.6 The right to be free from profiling

A data subject has the right not to have his or her personal information processed automatically for the sole purpose of providing a profile of such a person.[1867] A data subject must not be subject to automated decision making which is based on the automated processing of personal information intended to provide a profile of such a person including their performance at work, their credit worthiness, reliability, location, health, or personal preferences.[1868] There are exceptions to this rule. For instance, the provisions above do not apply if the decision is governed by a law or code of conduct in which appropriate measures[1869] are specified for the legitimate interests of data

[1864] Section 69(3) of the POPI Act.
[1865] Section 5(f) of the POPI Act.
[1866] Section 69(1) of the POPI Act.
[1867] Section 5(g) of the POPI Act.
[1868] Section 71(1) of the POPI Act.
[1869] Section 72(3) reads: "The appropriate measures, referred to in subsection (2)(a)(ii), must—a) provide an opportunity for a data subject to make representations about a decision referred to

subjects.[1870] Additionally, the provisions above do not apply if a decision has been made for purposes of executing a contract and the request of the data subject in terms of the contract has been met or if appropriate measures have been taken to protect the interests of the data subject.[1871]

6.5.7 The right to complain to the Information Regulator

A data subject has the right to complain to the Information Regulator if there is alleged interference with the protection of the personal information of a data subject. This right includes the submission of a complaint to the Regulator in respect of a determination made by an adjudicator.[1872] A complaint may be submitted in the prescribed manner and form alleging interference with the protection of personal information of a data subject.[1873] Subject to section 63(3),[1874] a responsible party or a data subject may submit a complaint to the Regulator in the prescribed manner and form if he, she or it is aggrieved by the determination of an adjudicator.[1875]

6.5.8 The right to institute legal proceedings

A data subject has the right to institute legal proceedings for the alleged interference with the protection of their personal information.[1876] A data subject can institute legal proceedings against a responsible party for breaching any provision in the POPI Act whether the breaches are negligent or conducted with intent.[1877] A responsible party can raise the following defences against the data subject: (i) *vis major* (ii) consent (iii) fault by the data subject (iv) compliance was not reasonably practicable in the

in subsection (1); and (b) require a responsible party to provide a data subject with sufficient information about the underlying logic of the automated processing of the information relating to him or her to enable him or her to make representations in terms of paragraph (a)."

[1870] Section 71(2)(b) of the POPI Act.

[1871] Section 71(2)(a) of the POPI Act.

[1872] Section 5(h) of the POPI Act.

[1873] Section 74(1) of the POPI Act.

[1874] Section 63(3) of the POPI Act reads: "A responsible party or data subject who is aggrieved by a determination, including any declaration, order or direction that is included in the determination, made by an adjudicator after having investigated a complaint relating to the protection of personal information under an approved code of conduct, may submit a complaint in terms of section 74(2) with the Regulator against the determination upon payment of a prescribed fee."

[1875] Section 74(2) of the POPI Act.

[1876] Section 5(i) of the POPI Act.

[1877] Section 99(1) of the POPI Act.

circumstances of the particular case or (v) the Regulator has granted an exemption in terms of section 37.[1878]

6.6 The conditions for the processing of personal information

The POPI Act prescribes conditions that a responsible party must follow for the processing personal information to be considered lawful.[1879] This section discusses the eight conditions for the lawful processing of personal information.

6.6.1 Accountability

A responsible party must ensure that all the measures in the POPI Act are complied with at the time of the determination of the purpose and means of the processing and when processing occurs.[1880] The practical implication of this provision is that a responsible party can be fined for non-compliance with the POPI Act.[1881] Generally, the Information Regulator may impose a fine not exceeding R10 million for non-compliance with the provisions of the POPI Act.[1882] Where a data breach has occurred, and personal information has been compromised by an unauthorised third party, the onus rests on the responsible party to notify the data subject.[1883]

[1878] Section 99(2) of the POPI Act. See discussion of the provisions of section 37 in paragraph 6.4.6 above.

[1879] Section 4(1) of the POPI Act.

[1880] Section 8 of the POPI Act.

[1881] Pienaar, C., Munro, V., van Wyk, R., & Ameer-Mia, F. (2018). *Information Technology Contracts* LexisNexis at 158.

[1882] See section 109 of the POPI Act. In March 2022, it was reported that TransUnion (a credit bureau) suffered a cyberattack. The hackers allegedly compromised personal information relating to at least 3 million consumers. The Information Regulator ordered TransUnion to publicise the data breach and divulge the information of those affected. These included names, ID numbers, contact details, marital status, gender, and vehicle identity number. According to the Information Regulator, TransUnion did not explain how it would mitigate the risks. See Child, K. (2022). "TransUnion ordered to inform those whose information was compromised in hack." Available at https://www.businesslive.co.za/bd/national/2022-03-25-transunion-ordered-to-inform-those-whose-information-was-compromised-in-hack/. Accessed 4 April 2022.

[1883] See section 22 of the POPI Act; Child, K. (2022). "TransUnion ordered to inform those whose information was compromised in hack." Available at https://www.businesslive.co.za/bd/national/2022-03-25-transunion-ordered-to-inform-those-whose-information-was-compromised-in-hack/. Accessed 4 April 2022.

6.6.2 Processing limitation

Personal information must be processed lawfully and in a reasonable manner that does not infringe the privacy of the data subject.[1884] This entails that personal information must only be processed if the processing is adequate, relevant, and not excessive.[1885] This requirement is often known as the principle of minimality[1886] or in the European context, data minimisation.[1887] According to Pienaar *et al*, the principle of minimality means "processing only such personal information of a data subject as is needed by the responsible party to meet the purpose behind the processing."[1888] Put simply, a responsible party must process relevant personal information. What constitutes 'relevant information' will differ from case to case. It is important to consider each case on its own merit. For example, in the context of VAT collection on a blockchain, the name and address of the recipient of the digital goods constitutes 'relevant information' for purposes of section 10 of the POPI Act. In exchange of information, countries exchange information that is 'foreseeably relevant' for purposes of carrying out the provisions of the Model Tax Convention on Income and Capital.[1889] Additionally, SARS can require a taxpayer to submit relevant material[1890] for the

[1884] Section 9 of the POPI Act.

[1885] Section 10 of the POPI Act.

[1886] Pienaar, C., Munro, V., van Wyk, R., & Ameer-Mia, F. (2018). *Information Technology Contracts* LexisNexis at 158.

[1887] Article 5(1)(c) of the EU GDPR reads: "Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed."

[1888] Pienaar, C., Munro, V., van Wyk, R., & Ameer-Mia, F. (2018). *Information Technology Contracts* LexisNexis at 158.

[1889] Article 26(1) of the Model Tax Convention on Income and Capital; see also Fritz, C. (2021). "South African Taxpayer's Right to Privacy in Cross-Border Exchange of Tax Information" *Constitutional Court Review* 11(1): 419.

[1890] Section 1 of the definition of 'relevant material' in the Tax Administration Act reads: "any information, document or thing that in the opinion of SARS is foreseeably relevant for the administration of a tax Act as referred to in section 3." Section of the Tax Administration Act reads: "(1) SARS is responsible for the administration of this Act under the control or direction of the Commissioner. (2) Administration of a tax Act means to - (a) obtain full information in relation to - (i) anything that may affect the liability of a person for tax in respect of a previous, current or future tax period; (ii) a taxable event; or (iii) the obligation of a person (whether personally or on behalf of another person) to comply with a tax Act; (b) ascertain whether a person has filed or submitted correct returns, information or documents in compliance with the provisions of a tax Act; (c) establish the identity of a person for purposes of determining liability for tax; (d) determine the liability of a person for tax; (e) collect tax debts and refund tax overpaid; (f) investigate whether a tax offence has been committed, and, if so - (i) to lay criminal charges; and (ii) to provide the assistance that is reasonably required for the investigation and prosecution of the tax offence; (g) enforce SARS' powers and duties under a tax Act to ensure that an obligation imposed by or under a tax Act is complied with; (h) perform any other administrative function necessary to carry out the provisions of a tax Act; (i) give effect to the obligation of the Republic to provide assistance under an international tax agreement; and (j) purposes of the administration of a tax Act.[1891] These provisions illustrate the broad scope of information that is required to administer taxes. For these reasons, it can be argued that applying the data minimisation principle in the administration of taxes can prove to be challenging for tax authorities.

The third requirement that must be complied with under processing limitation is for the responsible party to obtain the consent from the relevant data subject.[1892] The definition of consent has been defined above.[1893] The onus rests on the responsible party to show that the data subject consented to the processing of their personal information.[1894] A data subject has the right to withdraw their consent at any given time provided that the withdrawal does not affect the lawfulness of processing of personal information.[1895] As already discussed,[1896] a data subject has the right to object to the processing of personal information at any time.[1897]

The last requirement states that a data subject's personal information must be collected directly from the data subject to certain exceptions.[1898]

give effect to an international tax standard. (3) If SARS, in accordance with— (a) an international tax agreement—(i) received a request for, is obliged to exchange or wishes to spontaneously exchange information, SARS may disclose or obtain the information for transmission to the competent authority of the other country as if it were relevant material required for purposes of a tax Act and must treat the information obtained as taxpayer information; (ii) received a request for the conservancy or the collection of an amount alleged to be due by a person under the tax laws of the requesting country, SARS may deal with the request under the provisions of section 185; or (iii) received a request for the service of a document which emanates from the requesting country, SARS may effect service of the document as if it were a notice, document or other communication required under a tax Act to be issued, given, sent or served by SARS; or (b) an international tax standard, obtained information of a person, SARS may retain the information as if it were relevant material required for purposes of a tax Act and must treat the information obtained as taxpayer information.

[1891] Section 46(1) of the Tax Administration Act 28 of 2011; see also Fritz, C. (2021). "South African Taxpayer's Right to Privacy in Cross-Border Exchange of Tax Information" *Constitutional Court Review* 11(1): 419.

[1892] Section 11(1) of the POPI Act.

[1893] Paragraph 6.5.1 above.

[1894] Section 11(2)(a) of the POPI Act.

[1895] Section 11(2)(b) of the POPI Act. In terms of section 11(1) of the POPI Act, personal information may only be processed if – "(a) the data subject or a competent person where the data subject is a child consents to the processing; (b) processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party; (c) processing complies with an obligation imposed by law on the responsible party; (d) processing protects a legitimate interest of the data subject; (e) processing is necessary for the proper performance of a public law duty by a public body; or (f) processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied."

[1896] Paragraph 6.5.4.

[1897] Section 11(3) of the POPI Act.

[1898] Section 12 of the POPI Act.

6.6.3 Purpose specification

A responsible party must collect a data subject's personal information for a specific, explicit, and lawful purpose related to the function of the responsible party.[1899] The responsible party must ensure that the data subject is aware of the purpose of the collection of the information.[1900] A responsible party must not retain personal information any longer than is necessary.[1901] In practice, it is possible for a responsible party to retain personal information longer than is necessary. For example, where the retention of the record is authorised by law; or where the responsible party requires the record for lawful purposes related to its functions or activities; or where retention is required by a contract between the parties; or where the data subject consents to the retention.[1902] Section 11(6) of the POPI Act makes provision for a responsible party to restrict processing of personal information under certain circumstances. First, if a data subject contests the accuracy of their personal information, a responsible party must not process that information until it has been verified.[1903] This implies that should personal information prove to be inaccurate, the onus rests on the responsible party to rectify the inaccuracy. Second, the processing of information is limited to the reason(s) or purpose for which the collection and processing originally took place.[1904] Third, a data subject requests for the restriction of their personal information where the initial processing was unlawful, and the data subject opposed the deletion or destruction of their personal information.[1905] Lastly, restrictions are imposed where a data subject requests that their personal information be transmitted to another automated processing system.[1906]

[1899] Section 13(1) of the POPI Act.

[1900] Section 13(2) of the POPI Act. See also Pienaar, C., Munro, V., van Wyk, R., & Ameer-Mia, F. (2018). *Information Technology Contracts* LexisNexis at 158.

[1901] Section 14(1) of the POPI Act.

[1902] Section 14(1) of the POPI Act.

[1903] Section 14(6)(a) of the POPI Act.

[1904] Section 14(6)(b) of the POPI Act.

[1905] Section 14(6)(c) of the POPI Act.

[1906] Section 14(6)(d) of the POPI Act.

6.6.4 Further processing limitation

Generally, further processing of personal information must be compatible with the original purpose of collection.[1907] A responsible party must not use the personal information for any other purpose other than for the reason it was initially collected.[1908] There are exceptions to this rule. First, a data subject can consent to the further processing of their personal information.[1909] Second, further processing is possible where a data subject's personal information is derived from a public record or where the data subject has made their personal information public.[1910] Third, further processing is necessary to maintain the law, to enforce legislation concerning the collection of revenue, to conduct court proceedings or if further processing is in the interest of national security.[1911] Fourth, it is possible to process information further if it is necessary to prevent an imminent threat to public health.[1912] Fifth, further processing can take place if information is used for historical, statistical or research purposes.[1913] Last, further processing is possible if it is done in accordance with an exemption as prescribed in section 37 of the POPI Act.[1914]

[1907] Section 15(1) of the POPI Act. See also Pienaar, C., Munro, V., van Wyk, R., & Ameer-Mia, F. (2018). *Information Technology Contracts* LexisNexis at 158.

[1908] Pienaar, C., Munro, V., van Wyk, R., & Ameer-Mia, F. (2018). *Information Technology Contracts* LexisNexis at 158.

[1909] Section 15(3)(a) of the POPI Act.

[1910] Section 15(3)(b) of the POPI Act.

[1911] Section 15(3)(c) of the POPI Act.

[1912] Section 15(3)(d) of the POPI Act.

[1913] Section 15(3)(e) of the POPI Act.

[1914] Section 15(3)(f) of the POPI Act. Section 37 of the POPI Act reads: "The Regulator may, by notice in the *Gazette*, grant an exemption to a responsible party to process personal information, even if that processing is in breach of a condition for the processing of such information, or any measure that gives effect to such condition, if the Regulator is satisfied that, in the circumstances of the case—(a) the public interest in the processing outweighs, to a substantial degree, any interference with the privacy of the data subject that could result from such processing; or (b) the processing involves a clear benefit to the data subject or a third party that outweighs, to a substantial degree, any interference with the privacy of the data subject or third party that could result from such processing. (2) The public interest referred to in subsection (1) includes— a) the interests of national security; (b) the prevention, detection, and prosecution of offences; (c) important economic and financial interests of a public body; (d) fostering compliance with legal provisions established in the interests referred to under paragraphs (b) and (c); (e) historical, statistical or research activity; or (f) the special importance of the interest in freedom of expression. (3) The Regulator may impose reasonable conditions in respect of any exemption granted under subsection (1)."

6.6.5 Information quality

In terms of this condition, a responsible party must ensure that a data subject's personal information is complete, accurate, and not misleading. This entails that the responsible party must ensure that where information is found to be inaccurate, it must be updated accordingly.[1915] A responsible party must have regard to the purpose for which personal information was collected when ensuring information quality.[1916]

6.6.6 Openness

A responsible party is required to document all the processing operations in terms of the Promotion of Access to Information Act 2 of 2000 (PAIA).[1917] For example, section 14 of PAIA requires that an information officer of a responsible party must produce a manual containing the purpose for processing a data subject's personal information; the categories of data subjects and information relating to those data subjects; the recipients to whom personal information may be supplied; any plans relating to the cross-border flow of personal information; the security measures implemented to ensure that a data subject's personal information is subject to confidentiality, integrity, and availability when it is processed.[1918]

According to Pienaar *et al*, the openness condition promotes transparency in a responsible party's management of a data subject's personal information.[1919] A responsible party can, upon request by a data subject, make available information about its policies and practices relating to the management of personal information.[1920] A data subject can consult a responsible party's privacy policy document if they require clarity on the security measures employed to protect a subject's personal information.[1921] In my view, this form of transparency can build trust because a data

[1915] Section 16(1) of the POPI Act.
[1916] Section 16(2) of the POPI Act.
[1917] Section 17 of the POPI Act.
[1918] Section 14(1)(c) of PAIA.
[1919] Pienaar, C., Munro, V., van Wyk, R., & Ameer-Mia, F. (2018). *Information Technology Contracts* LexisNexis at 158.
[1920] Pienaar, C., Munro, V., van Wyk, R., & Ameer-Mia, F. (2018). *Information Technology Contracts* LexisNexis at 158.
[1921] See Pienaar, C., Munro, V., van Wyk, R., & Ameer-Mia, F. (2018). *Information Technology Contracts* LexisNexis at 158.

subject may be more willing to provide their personal information to a responsible party. A responsible party ensures that a data subject's personal information is always protected.

6.6.7 Security safeguards

It is crucial for a responsible party to implement appropriate security safeguards when processing personal information. In fact, it can be argued that security safeguards are the most important condition for the lawful processing of personal information. In my view, security safeguards should be the most important condition and a prerequisite before any personal information can be processed. If one considers that the purpose of the POPI Act is to give effect to the right to privacy by safeguarding personal information,[1922] then a data subject's personal information cannot be adequately protected if adequate security safeguards are not implemented.[1923] Without safeguards, it is easy for unauthorised parties to access a data subject's personal information. The unlawful or unauthorised possession of personal information is detrimental to a data subject because illegal activities such as fraud, and identity theft can be committed in the name of the data subject whose information has been retrieved. This can result in significant financial loss for a data subject.

Section 19 of the POPI Act makes provision for a responsible party to secure the integrity and confidentiality of a data subject's personal information by taking appropriate, reasonable technical and organisational measures to prevent loss and

[1922] Section 2(a) of the POPI Act.

[1923] In this regard, Pienaar *et al* recommend best practices and frameworks for data protection and data security. For example, the ISO published standards pertaining to information security. One of the standards, the ISO 27001:2013 looks at security techniques and information security management systems. The ISO 27001:2013 'specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization.' See https://www.iso.org/standard/54534.html. Accessed 21 July 2022; see also Pienaar, C., Munro, V., van Wyk, R., & Ameer-Mia, F. (2018). *Information Technology Contracts* LexisNexis at 168. It should be noted that this specific standard is under review and will be replaced by ISO/IEC FDIS 27001. See https://www.iso.org/standard/82875.html. Accessed 21 July 2022. Another relevant standard to consider is the ISO/IEC 27000:2018. This standard 'provides the overview of information security management systems (ISMS). It also provides terms and definitions commonly used in the ISMS family standards'. See https://www.iso.org/standard/73906.html. Accessed 21 July 2022.

unauthorised access to personal information.[1924] A responsible party must foresee internal and external risks to personal information in its possession. A responsible party must regularly verify that the safeguards are effectively implemented and ensure that the safeguards are continuously updated in response to new risks.[1925]

Interestingly, a responsible party can delegate the processing of personal information to an 'operator'. Section 1 of the POPI Act defines an 'operator' as "a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party."[1926] It is unclear why the drafters of the POPI Act included provisions relating to an 'operator'. The EU GDPR refers to a 'processor'. A 'processor' is defined as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."[1927] It is clear that a 'processor' and 'operator' are identical and perform the functions mandated to them by a controller and responsible party respectively.[1928]

An operator can only process a data subject's personal information with the knowledge and authority of a responsible party. Additionally, an operator must treat all personal information with confidentiality and such information must not be disclosed to any other party unless a disclosure is required by law or required for the proper performance of duties.[1929] It should be noted that an operator must adhere to the same security measures as a responsible party. An operator must notify a responsible party if it suspects any data breaches.[1930] As discussed above,[1931] the onus rests on the responsible party to notify the Information Regulator and the data subject when a data breach has occurred. Pienaar *et al* highlight the contrast between the POPI Act and the EU GDPR in so far as the time period for notification is concerned.[1932] Section 22 provides that a notification must be made as soon as is 'reasonably possible after the

[1924] Section 19(1) of the POPI Act.

[1925] Section 19(2) of the POPI Act.

[1926] Section 1 of the definition of 'operator' in the POPI Act.

[1927] Article 4(8) of the EU GDPR.

[1928] See also Pienaar, C., Munro, V., van Wyk, R., & Ameer-Mia, F. (2018). *Information Technology Contracts* LexisNexis at 155.

[1929] Section 20 of the POPI Act.

[1930] Section 21 of the POPI Act.

[1931] Paragraph 6.5.1.

[1932] Pienaar, C., Munro, V., van Wyk, R., & Ameer-Mia, F. (2018). *Information Technology Contracts* LexisNexis at 166.

discovery of the compromise', while the EU GDPR requires a data subject to be notified no later than 72 hours after becoming aware of the breach.[1933] It is clear that article 33(1) of the EU GDPR provides more certainty when it comes to notifying a data subject of a breach. Section 22(2) of the POPI Act is vague because what constitutes 'reasonable' depends on the facts of the case. A plain reading of section 22(2) of the POPI Act suggests that the actions of law enforcement agencies should be considered before notifying a data subject. It can also be argued that section 22(2) of the POPI Act can only be invoked *after* (my emphasis) a responsible party has attempted to determine the extent of the compromise and attempts have been made to restore integrity to the party's information system.[1934] In my view, this is irritational because the issue here is not the speed at which law enforcement agencies and the responsible parties can recover the stolen data. Rather, the issue should be the promotion of a data subject's right to privacy. The right to information privacy cannot be enforced if a data subject waits for third parties to determine if there was an actual breach. It is also unrealistic for a data subject to potentially rely on law enforcement's ability or inability to investigate the extent of the breach. In any case, the ability to recover data does not necessarily mean that data was not unlawfully appropriated to begin with. Moreover, a closer reading of the section 22(2) of the POPI Act also suggests that the data subject is reliant on the investigative capabilities of law enforcement agencies and personnel of the responsible party. If the investigative capabilities of the law enforcement agencies and other relevant personnel is lacking or if personnel are not adequately trained or equipped to know what to look for, then a data subject bears the brunt of inefficient investigative work. For these reasons, it may be more suitable for section 22(2) of the POPI Act to be amended to make provision for a notification time similar to that of article 33(1) of the EU GDPR. This is to ensure legal certainty and to promote a data subject's right to privacy. It also makes responsible parties more accountable. It should be noted that the sooner a data subject is notified, the sooner they can also take preventative measures to ensure that they are not adversely affected by the data breach. It can be argued that notifying a data subject of a data breach within 72 hours is reasonable if personal information is

[1933] Section 22(2) of the POPI Act read with article 33(1) of the EU GDPR. See also Pienaar, C., Munro, V., van Wyk, R., & Ameer-Mia, F. (2018). *Information Technology Contracts* LexisNexis at 166.

[1934] See section 22(2) of the POPI Act.

transferred to another country via a blockchain. Given the complexities of identifying a perpetrator in a foreign jurisdiction, providing a notification to data subject within 72 hours seems logical.

Pienaar *et al* correctly submit that a responsible party should respond decisively and judiciously when a data breach occurs.[1935] This can be done by establishing defined processes and procedures and setting out internal measures to be followed if a data breach occurs.[1936] For example, it may be necessary to install incident management communications and procedures within a responsible party's structure.[1937] This can ensure that notifications are sent out to the data subject and to the Information Regulator within a specified timeframe.[1938]

6.6.8 Data subject participation

I discuss a data subject's right to access their personal information held by a responsible party above.[1939] As such, the discussion shall not be repeated here. It must be noted that the right to access personal information is one of the conditions for the lawful processing of personal information.[1940]

6.7 Application of the POPI Act to blockchain

It is important to consider the effects and possible challenges regarding the application of the POPI Act to blockchain. It should be noted that the effects and challenges can largely vary depending on the type of blockchain, the location of the responsible party or parties, the way information is processed, the type of tax collected/remitted, and whether information constitutes 'personal information' for purposes of POPI.

[1935] Pienaar, C., Munro, V., van Wyk, R., & Ameer-Mia, F. (2018). *Information Technology Contracts* LexisNexis at 166.

[1936] Pienaar, C., Munro, V., van Wyk, R., & Ameer-Mia, F. (2018). *Information Technology Contracts* LexisNexis at 166.

[1937] Pienaar, C., Munro, V., van Wyk, R., & Ameer-Mia, F. (2018). *Information Technology Contracts* LexisNexis at 166.

[1938] Pienaar, C., Munro, V., van Wyk, R., & Ameer-Mia, F. (2018). *Information Technology Contracts* LexisNexis at 166.

[1939] See paragraphs 6.5.2 and 6.5.3.

[1940] See section 23(1) of the POPI Act.

6.7.1 Responsible party

It is important to determine who qualifies as a 'responsible party' for purposes of POPI. A responsible party has an important role to play in so far as enforcing the rights of data subjects is concerned. It can be argued that without a responsible party, it is difficult for a data subject to enforce their right to privacy. If a data breach occurs, the responsible party is held accountable. The responsible party must ensure that all the conditions for the lawful processing of personal information and all the measures that give effect to such conditions are complied with at any given time.[1941]

As mentioned above,[1942] it is important to consider the type of blockchain in use when establishing the identity of a responsible party. In a private blockchain, a responsible party can easily be identified as the central administrator. The central administrator is often the one that: (i) determines who has access to the network, (ii) screen participants, (iii) is responsible for governance rules, (iv) is responsible for maintaining the network infrastructure, and (v) determines the purpose of blockchain. An important issue that must be considered is whether the recipients of personal information on a private blockchain qualify as 'responsible parties' for purposes of POPI. The question is important because it can have repercussions for participants on blockchain. As discussed earlier, a responsible party is a public or private body or any other person that processes personal information in conjunction with others.[1943] In a private blockchain, once information is stored on a node all the participants have access to that information. To access blockchain network, a participant requires a node. The instantaneous receipt of information by all the participants on a private blockchain qualifies the latter participants as 'responsible parties' for purposes of POPI. The participants collect, receive, record, and store personal information on their respective nodes. These actions constitute 'processing' for purposes of POPI.[1944] In essence, the central administrator and the participants are '*co-responsible parties*'. The same duties and responsibilities that are granted to the central administrator at the initial stages are, by necessary implication, are granted to all the participants on the private

[1941] Section 8 of the POPI Act.
[1942] See Paragraph 6.7.
[1943] See section 1 of the definition of 'responsible party' in the POPI Act.
[1944] See section 1 of the definition of 'processing' in the POPI Act.

blockchain. Should a data subject institute legal proceedings against a responsible party for breaches to the POPI Act, all the participants in blockchain can be held jointly and severely liable because they are responsible parties. It is important to look at this issue in context. I make use of another example.

Example 10

SARS receives a request for tax information from His Majesty's Revenue and Customs (HMRC). The request relates to a British citizen residing and working in South Africa. SARS transmits that tax information to HMRC via blockchain. Since the United Kingdom (UK) consists of England, Scotland, Wales, and Northern Ireland, the tax information is automatically transmitted to all HMRC offices in the respective countries. The tax information is not anonymised.

For purposes of this example, SARS and HMRC are *co-responsible parties*. Both revenue authorities processed personal information. It can also be argued that the processing of the taxpayer's personal information has been processed at a multiplicity of locations. Under ordinary circumstances, SARS, and HMRC (in its entirety) should comply with the provisions of the POPI Act. A taxpayer can institute legal proceedings against the two tax authorities should a data breach occur, and the taxpayer suffers damage because of the data breach. In principle, HMRC should also be compliant with POPI because HMRC processes personal information in South Africa. Blockchain network originates in South Africa and HMRC makes use of an 'automated means' in South Africa.[1945] In my view, this confirms the POPI Act's potential extra-territorial application. Generally, the POPI Act applies to the place or territory where the processing of personal information occurs.[1946] In my view, the use of blockchain can broaden the territorial scope of the POPI Act's application.

In the context of VAT collection, the provisions of the POPI Act can apply. During the VAT collection process, a digital invoice is transmitted to the relevant tax authority. The digital invoice contains personal information. For example, suppliers of electronic

[1945] See section 3(1)(b) of the POPI Act.

[1946] Giles, J. (2020). *Must I comply with the POPI Act?* Available at https://www.michalsons.com/blog/must-i-comply-with-the-popi-act/41827. Accessed 22 March 2022.

services must insert the name and address of the recipient of the electronic services.[1947] This information constitutes personal information for POPI purposes. This means that the provisions of POPI apply to SARS (the relevant tax authority) and the supplier of electronic services. In my view, requiring foreign suppliers of electronic services to comply with the POPI Act, in addition to the VAT Act and the Tax Administration Act, increases their compliance burden. The reason for this is clear. If an electronic supplier of services is considered a *co-responsible party*, then the latter must comply with all the provisions of the POPI Act. For example, the foreign supplier of electronic services must ensure that the conditions for lawful processing are always adhered to. The lack of compliance with the POPI Act or a security breach that is unaccounted for may result in the institution of legal proceedings or hefty fines towards foreign suppliers of electronic services. This can have a negative impact on the collection of revenue because foreign suppliers may deem it too risky or even too costly to supply electronic services to South Africa. Other supplies may cease supplying electronic services to South Africa altogether. In turn, this can lead to revenue loss for SARS.

Another important point to consider is whether a responsible party can be identified when a public blockchain is used. The nature of a public blockchain makes it difficult to identify the responsible party. This is because no single node can determine the purposes and means of data processing.[1948] All nodes on a public blockchain can perform the same functions. Moreover, any person who joins a public blockchain can make changes to blockchain itself. As a result, there is no central administrator that qualifies as the dominant responsible party. All nodes on the network become responsible parties. Finck correctly points out that if all the nodes on a public blockchain are considered responsible parties, significant challenges can arise.[1949] For instance, it is difficult to establish the location and identity of each node on the public network.[1950] If a node cannot be identified, then a data subject's rights cannot be

[1947] See SARS (2016). *Binding General Ruling (VAT) No 28 Issue 2* at 2. Available at https://www.sars.gov.za/wp-content/uploads/Legal/Rulings/BGR/LAPD-IntR-R-BGR-2015-03-BGR28-Electronic-Services.pdf. Accessed 15 July 2021; see also paragraph 3.2.2 above.

[1948] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 99.

[1949] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 100.

[1950] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 100.

enforced. It can be extremely difficult to force a node to comply with the necessary data protection laws.[1951] Finck points out that nodes can be forced to stop running a blockchain if the rights entrenched in data protection laws cannot be achieved through alternative means.[1952]

Moreover, the location of multiple nodes in various countries can raise issues around conflict of laws especially if the nodes are situated in different countries around the world. The application of data protection laws on public blockchain does, however, provide interesting scenarios. Finck questions whether data subjects who gain access to their data via a private key on a blockchain become data controllers (responsible parties).[1953] The definition of a responsible party includes "any other person which, alone or in conjunction with others, determines the purpose and means of processing personal information."[1954] Based on this definition, it is clear that a natural person who gains access to a public blockchain in order to process personal information (whether their own or that of another person) becomes a responsible party for purposes of the POPI Act.[1955] A natural person who qualifies as a responsible party is required to ensure compliance with the provisions of the POPI Act. The key factor to consider whether a person or entity is a responsible person is whether they can determine the 'means of processing personal information'.[1956] Ordinarily, the means of processing data on a blockchain are determined by miners, software developers or nodes.[1957] In my view, merely accessing a blockchain network is insufficient for one to be considered as a responsible party. An actor must demonstrate that they have the means to determine how data/personal information is processed on blockchain network.

[1951] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 100.

[1952] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 100.

[1953] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 101.

[1954] See the definition of 'responsible party' in section 1 of the POPI Act.

[1955] See also Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 101.

[1956] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 101.

[1957] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 101.

6.7.2 The rights of data subjects on blockchain

It is important to consider the rights that can be affected by the application of the POPI Act on blockchain. This section limits the discussion to the rights that pose the greatest challenges to the application of POPI on blockchain in a VAT collection scenario.

6.7.2.1 The right to object to the processing of personal information

Section 5 of the POPI Act provides that a data subject has the right to object to the processing of their personal information. Section 11 of the POPI Act provides that objection can be made at *any time*. Section 11 of the POPI Act compels a responsible party to cease processing of personal information once an objection has been made. The time of objection is crucial in blockchain ecosystem. An objection made *before* the actual processing is done on blockchain can work. However, it is difficult for a responsible party to adhere to an objection made by a data subject *after* processing has taken place. This is because a responsible party cannot simply delete, stop, pause, resume, change, destroy, or alter the processing once it has started because blockchain is immutable in nature. In my view, an objection made by a data subject once processing has already occurred can frustrate the tax administration process. This is true where, after the fact, it was established that the objection did not have merit. I do not argue that data subjects should not be given the opportunity to object to the processing of their personal information. It is important to look at each case on a case-by-case basis. The most efficient way to address this challenge is by inserting a proviso in the POPI Act that reads: “an objection can only be made before processing of personal information takes place where a responsible party facilitates the processing on a blockchain. The objection must reach the responsible party before processing takes place.”

6.7.2.2 The right to rectification

Section 5(c) of the POPI Act makes provision for a data subject to request for the correction, destruction, or deletion of their personal information. This right is similar to the EU GDPR's right to rectification.[1958] It is difficult for a data subject to exercise the right to rectification on a blockchain. First, a blockchain is inherently immutable in nature. Any changes, deletion, and correction on blockchain cannot be effected due to blockchain's immutable.[1959] Second, exercising the right to rectification entails identifying all the nodes on blockchain to request for the rectification of personal information.[1960]

6.7.2.3 The right to access information

Section 5(b) of the POPI Act makes provision for a data subject to establish whether a responsible party holds their personal information and for a data subject to request access to that information. Enforcing this right presupposes that the data subject has knowledge or has reason to believe that a responsible party is processing their personal information. Upon becoming aware, a data subject must identify the responsible party. It is much easier to identify a responsible party that has a permanent fixed establishment in the jurisdiction where the data subject is domiciled. Challenges arise where a responsible party exists exclusively on the Internet. Even if a responsible party has been identified, that entity can easily mask their location by changing their IP address.[1961] On a decentralised public blockchain, a responsible party does not have the resources to identify which nodes handle encrypted or hashed data.[1962] As a result, it is difficult for a responsible party to establish whether a data subject's personal information has been processed.[1963] Even if a data subject were to access blockchain network in order to obtain a copy of all the information on the network, it may not necessarily reveal the identity of the party that processed their information. Finck questions whether obtaining a copy of all the data on a blockchain network is a

[1958] Article 16 of the EU GDPR.

[1959] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 105.

[1960] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 105.

[1961] See Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 101 at footnote 94.

[1962] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 106.

[1963] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 106.

satisfactory solution to a data subject's right to access information.[1964] In my view, the outcome is not satisfactory because the issue is not merely retrieving information from a database. The issue is establishing the identity of all the parties who determined the means of processing and establishing the identity of *all* the parties who had access to a data subject's personal information. Without those identities, enforcing the right to access personal information remains trivial.

The likelihood of enforcement increases if a data subject identifies the parties in a private or consortium network. The design of a private network makes it possible for the central administrator to determine the identities of all the participants on the network. A data subject can merely make a request to the responsible parties to ascertain whether personal information has been processed, and to confirm the identity of the parties who have access to that information.

6.7.2.4 Purpose specification condition

Section 13(1) of the POPI Act provides that personal information must be collected for a specific, explicitly defined, and lawful purpose related to a function of the responsible party. Simply put, the collection and processing of personal information should be achieved for a specified purpose. If the collection and processing of personal information is unspecified and unlawful, then the processing and collection can breach the provisions of the POPI Act. The purpose specification condition requires responsible parties to retain records for as long as it is necessary to achieve the purpose for which information was collected.[1965] One of the conditions set out in the POPI Act is for the deletion, destruction, or de-identification of personal information by the responsible party after the purpose for which it was attained has materialised.[1966] Moreover, the deletion or destruction must be done a way that prevents any person from reconstructing it.[1967] It is very difficult for a responsible party to comply with the purpose specification condition when using blockchain because blockchain is append-

[1964] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 106.

[1965] Section 14(1) of the POPI Act.

[1966] Section 14(4) of the POPI Act.

[1967] Section 14(5) of the POPI Act.

only.[1968] As correctly pointed out by Finck, information stored on a blockchain continuously exists on blockchain.[1969] As data is continuously stored, blockchain grows in size and accumulates more blocks in the process.[1970] The more nodes join the network, the more difficult it is for compliance of the purpose specification requirement to take place.[1971] Information stored on blockchain cannot be destroyed or deleted. However, if data is stored in an anonymised manner, it can be difficult for any person to reconstruct it. But the permanent destruction of anonymised data cannot be achieved.

6.7.2.5 Information quality

The responsible party can have challenges to ensure that personal information is always complete, accurate, and updated. As already mentioned, it is not possible to make changes to blockchain. Once data is stored, it cannot be altered. A responsible party cannot update information if the latter is found to be inaccurate. The responsible party stores the information it initially retrieved irrespective of its accuracy.

6.7.2.6 Data subject participation

One of the requirements of data subject participation is for a data subject to request for the correction of their personal information.[1972] This also entails that a data subject can request that their personal information be destroyed.[1973] With the application of blockchain, any correction or destruction of personal information is not possible. A responsible party making use of blockchain to process personal information can be considered non-compliant with the provisions of the POPI Act.

[1968] See also Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 104.

[1969] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 104.

[1970] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 104.

[1971] See Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 104.

[1972] See section 24 of the POPI Act.

[1973] Section 24(2)(b) of the POPI Act.

6.8 Addressing the tension between the POPI Act and blockchain

It has been shown that a responsible party that uses blockchain to process personal information infringes the provisions of the POPI Act. A data subject cannot enforce their right to rectification, the right to object to the processing of information, and the right to access their personal information. Additionally, a responsible party is unable to meet all the conditions for the lawful processing of personal information. The non-compliance of all the conditions necessary for lawful processing can potentially render the processing of personal information on a blockchain unlawful. In my view, all the requirements for the lawful processing of personal information must be met before the processing of personal information can be considered lawful.

This section discusses the measures that can be implemented to render the processing of personal information on a blockchain lawful in terms of the conditions set out in the POPI Act.

6.8.1 Exclusion/exemption of POPI on blockchain users

Blockchain can be excluded from the provisions of the POPI Act. In doing so, blockchain users can be deemed to be compliant with the provisions of the POPI Act. It should be noted that a blanket exclusion of blockchain is not recommended. This is to prevent entities, organisations, and other persons from using blockchain to process personal information indiscriminately. These entities can be cognisant of the fact that no penalties for breaching data privacy will be imposed on them. Put simply, a blanket approach should not be followed because it can facilitate entities' violation of the provisions of the POPI Act.[1974] In my view, the exclusion can only apply to facilitate the collection of VAT and any other taxes on blockchain. SARS can use blockchain to collect VAT from foreign suppliers of digital goods without violating the provisions of the POPI Act. Blockchain exclusion reduces the compliance burden for foreign suppliers of digital goods because no additional costs are incurred for ensuring compliance with provisions of the POPI Act.

[1974] See Mirchandani, A. (2019). "The GDPR-blockchain paradox: exempting permissioned blockchains from the GDPR" *Fordham Intellectual Property, Media & Entertainment Law Journal* 29(4): 1234.

Currently, the POPI Act makes provision for the Information Regulator to grant an exemption to a responsible party that processes personal information even if the processing is in breach of a condition provided the Information Regulator is satisfied that the breach is in the public interest or if the processing involves a clear benefit to the data subject.[1975] It can be argued that SARS' use of blockchain to collect VAT on the cross-border supply of digital goods is necessary to raise revenue for the *fiscus*. It can also be argued that for SARS to effectively adopt blockchain, it is necessary to breach the conditions for the lawful processing of personal information as prescribed in the POPI Act. In my view, it can also be argued that since SARS has a duty to provide an effective and efficient method to collect VAT,[1976] it is necessary to use blockchain because blockchain makes the administration of VAT efficient. In doing so, additional revenue is collected which is in the public's best interest[1977] because more funds are allocated to fund public expenditure. Moreover, section 38[1978] of the POPI Act can be amended to make provision for SARS to be exempted from the provisos for the lawful processing of personal information. This is subject to SARS performing a 'relevant function'[1979] as per the requirements of the POPI Act. For this to be practicable, the phrase 'relevant function' should be amended to include the collection of revenue by SARS on blockchain. Moreover, the POPI Act can be amended to exclude SARS from the provisions of the POPI Act because the TAA provides sufficient security safeguards.

[1975] Section 37(1)(a) and (b) of the POPI Act.

[1976] See the preamble of the Tax Administration Act.

[1977] For purposes of section 37(1) of the POPI Act, public interest includes: "(a) the interests of national security; (b) the prevention, detection and prosecution of offences; (c) important economic and financial interests of a public body; (d) fostering compliance with legal provisions established in the interests referred to under paragraphs (b) and (c); (e) historical, statistical or research activity; or (f) the special importance of the interest in freedom of expression."

[1978] Section 38(1) of the POPI Act reads: "Personal information processed for the purpose of discharging a relevant function is exempt from sections 11(3) and (4), 12, 15 and 18 in any case to the extent to which the application of those provisions to the personal information would be likely to prejudice the proper discharge of that function."

[1979] Section 38(2) of the POPI Act reads: "for purposes of subsection (1), means any function— (a) of a public body; or (b) conferred on any person in terms of the law, which is performed with the view to protecting members of the public against— (i) financial loss due to dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons concerned in the provision of banking, insurance, investment or other financial services or in the management of bodies corporate; or (ii) dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons authorised to carry on any profession or other activity."

6.8.2 Anonymise personal information

As discussed above,[1980] the provisions of the POPI Act do not apply to de-identified data. Anonymised data is data that can no longer be linked to a data subject. If a responsible party or a blockchain user stores anonymised data, the provisions of the POPI Act do not apply. A responsible party or a blockchain user cannot be deemed to be non-compliant because the provisions of the POPI Act do not apply to anonymised data. The processing of anonymised data by suppliers of digital goods decreases their compliance burden. These parties do not need to incur compliance costs associated with data privacy laws.

Mirchandani is of the view that hashed data can be considered as anonymous data. There are two reasons for this view. First, it is highly improbable for a person to link hashed data to a data subject. Second, the storage of hashed data on a permissioned blockchain provides better security.[1981] Mirchandani further argues that the growth of blockchain and the development of future use cases should not be stifled simply because there is a likelihood of linking personal information stored on a blockchain to a data subject.[1982] While Mirchandani's argument has merit, it is important to consider the reasons for adopting blockchain in any given scenario. If blockchain is only used for storage of personal information, then it is recommended that traditional databases be used for this purpose. If the storage of personal information is secondary to the main reason for using blockchain, then a blockchain can be used. Second, the classification of 'hashed data' as anonymous should only prevail if blockchain data security makes it impossible to identify a data subject. In my view, if data security measures are lacking or inadequate, then 'hashed data' must be considered as personal data.

[1980] Paragraph 6.4.2 above.

[1981] Mirchandani, A. (2019). "The GDPR-blockchain paradox: exempting permissioned blockchains from the GDPR" *Fordham Intellectual Property, Media & Entertainment Law Journal* 29(4): 1239 – 1240.

[1982] Mirchandani, A. (2019). "The GDPR-blockchain paradox: exempting permissioned blockchains from the GDPR" *Fordham Intellectual Property, Media & Entertainment Law Journal* 29(4): 1239.

6.8.3 Amendments to the POPI Act

The provisions for the POPI Act can be amended to make it more inclusive of blockchain technology users. It should be noted that the POPI Act was clearly designed to cater for centralised silos that store, collect, and process personal information.[1983] Put simply, the POPI Act was not designed for a decentralised technology capable of seamlessly transcending borders. Finck correctly points out that the application of the data privacy laws on blockchains has the effect of rendering blockchain operations unlawful, possibly stifling the growth of this novel technology.[1984] It is also possible for blockchain users to move underground simply because they do not want to be seen as 'non-compliant' with the provisions of the POPI Act. Moreover, the limited use cases for blockchain make it difficult for the technology to fully develop. An undeveloped blockchain is of benefit to no one unless users and developers fully harness the technology and its capabilities. It is important to note that blockchain is a relatively new technology. It is highly probable that new features and use cases can materialise in later stages as the use of the technology becomes widespread. Any legislative changes to the POPI Act should be made while taking the above factors into consideration.

6.8.4 Storing personal information off-chain

As discussed above,[1985] it is possible to store personal information outside blockchain. Personal information can be stored on a traditional database. When this is done, the data can be linked to the data stored on blockchain using a hash. The hash of this data is stored on blockchain and serves as a link to the data stored on the database.[1986] If the personal information on the traditional database is destroyed, then

[1983] See also Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 110.

[1984] Finck, M. (2019). *Blockchain Regulation and Governance in Europe* Cambridge University Press at 88.

[1985] Paragraph 5.5.2.

[1986] De Meijer, C. R. W. (2016). *Blockchain versus GDPR and who should adjust most*. Available at https://www.finextra.com/blogposting/16102/blockchain-versus-gdpr-and-who-should-adjust-most. Accessed 19 April 2022; Mirchandani, A. (2019). "The GDPR-blockchain paradox: exempting permissioned blockchains from the GDPR" *Fordham Intellectual Property, Media & Entertainment Law Journal* 29(4): 1229.

the link to the hashed data on blockchain is also destroyed.[1987] In doing so, it is easier for a data subject to enforce their right to rectification under the POPI Act.[1988] It should be noted that there are risks to this method. First, it is difficult for a data subject to know if their data has been accessed by an unauthorised third party. Hence, splitting data storage between blockchain and an off-chain database makes it easier for hackers to target a data subject's information.[1989] Second, De Meijer reasons that the complex method of storing personal data off-chain makes it difficult for blockchain global standards to be adopted, which can limit its deployment in sectors such as finance.[1990] Third, storing data off-chain lacks transparency.[1991] It is difficult for data subjects to know who had access to their personal information stored on an off-chain database.[1992] Fourth, there is a viewpoint that storing information off-chain is tantamount to storing information on a traditional database. Off-chain databases have the same cybersecurity issues that are associated with traditional databases.[1993] The only difference is that a traditional database lacks immutability. Instead, this method makes the process of data storage more complex and inefficient.[1994]

[1987] De Meijer, C. R. W. (2016). *Blockchain versus GDPR and who should adjust most*. Available at https://www.finextra.com/blogposting/16102/blockchain-versus-gdpr-and-who-should-adjust-most. Accessed 19 April 2022; Mirchandani, A. (2019). "The GDPR-blockchain paradox: exempting permissioned blockchains from the GDPR" *Fordham Intellectual Property, Media & Entertainment Law Journal* 29(4): 1229.

[1988] See De Meijer, C. R. W. (2016). *Blockchain versus GDPR and who should adjust most*. Available at https://www.finextra.com/blogposting/16102/blockchain-versus-gdpr-and-who-should-adjust-most. Accessed 19 April 2022; Mirchandani, A. (2019). "The GDPR-blockchain paradox: exempting permissioned blockchains from the GDPR" *Fordham Intellectual Property, Media & Entertainment Law Journal* 29(4): 1229.

[1989] De Meijer, C. R. W. (2016). *Blockchain versus GDPR and who should adjust most*. Available at https://www.finextra.com/blogposting/16102/blockchain-versus-gdpr-and-who-should-adjust-most. Accessed 19 April 2022.

[1990] De Meijer, C. R. W. (2016). *Blockchain versus GDPR and who should adjust most*. Available at https://www.finextra.com/blogposting/16102/blockchain-versus-gdpr-and-who-should-adjust-most. Accessed 19 April 2022.

[1991] De Meijer, C. R. W. (2016). *Blockchain versus GDPR and who should adjust most*. Available at https://www.finextra.com/blogposting/16102/blockchain-versus-gdpr-and-who-should-adjust-most. Accessed 19 April 2022; Mirchandani, A. (2019). "The GDPR-blockchain paradox: exempting permissioned blockchains from the GDPR" *Fordham Intellectual Property, Media & Entertainment Law Journal* 29(4): 1230.

[1992] Mirchandani, A. (2019). "The GDPR-blockchain paradox: exempting permissioned blockchains from the GDPR" *Fordham Intellectual Property, Media & Entertainment Law Journal* 29(4): 1230.

[1993] Mirchandani, A. (2019). "The GDPR-blockchain paradox: exempting permissioned blockchains from the GDPR" *Fordham Intellectual Property, Media & Entertainment Law Journal* 29(4): 1230.

[1994] Mirchandani, A. (2019). "The GDPR-blockchain paradox: exempting permissioned blockchains from the GDPR" *Fordham Intellectual Property, Media & Entertainment Law Journal* 29(4): 1230.

6.8.5 Implementing privacy by design

Privacy by Design (PbD) is a concept developed by Dr Ann Cavoukian in the 1990s.[1995] In terms of the PbD concept, systems should be built on privacy from the outset as opposed to introducing privacy measures at the end.[1996] PbD[1997] is proactive rather than reactive in the sense that privacy related challenges are anticipated and prevented before they materialize.[1998] PbD does not rely on compliance with legislation and other regulatory frameworks but follows a preventative approach wherein a system's default setting is based on privacy.[1999] In practical terms, a developer of a blockchain must consider privacy at the initial stages of development.[2000] Kianieff correctly argues that a PbD approach must be multi-disciplinary in safeguarding privacy.[2001] For example, blockchain developers must consider potential threats to privacy from the perspective of disciplines such as statistics, economics, computer science, psychology, business, and law for a clearer picture when designing systems for users.[2002]

[1995] Information and Privacy Commissioner Ontario (2009). *Privacy by Design* at 1. Available at https://www.ipc.on.ca/wp-content/uploads/2013/09/pbd-primer.pdf. Accessed 27 April 2022.

[1996] Information and Privacy Commissioner Ontario (2009). *Privacy by Design* at 1. Available at https://www.ipc.on.ca/wp-content/uploads/2013/09/pbd-primer.pdf. Accessed 27 April 2022; see also Berberich, M., & Steiner, M. (2016). "Blockchain technology and the GDPR how to reconcile privacy and distributed ledgers" *European Data Protection Law Review* 2(3): 425.

[1997] Privacy by Design is founded on seven foundational principles. (1) Privacy by Design is proactive and not reactive; preventative and not remedial. Privacy issues are identified from the start and preventative measures are incorporated into the system during the development process. (2) Privacy must be the default setting. Designers must ensure that personal data is automatically protected when designing a system. (3) Privacy is embedded into the design of the system. Privacy must form part of the design and architecture of the system. (4) Privacy must be fully functional. No trade-offs must be made. (5) End-to-end security. Systems should embed security measures from the start and throughout the system's life cycle. (6) Transparency. The system and its operations must remain visible and transparent to the relevant parties. (7) Respect. The interests of individuals must be protected by implementing measures such as privacy defaults, and notices if or when the need arises. See Information and Privacy Commissioner Ontario (2009). *Privacy by Design* at 1. Available at https://www.ipc.on.ca/wp-content/uploads/2013/09/pbd-primer.pdf. Accessed 27 April 2022.

[1998] Information and Privacy Commissioner Ontario (2009). *Privacy by Design* at 1 – 2. Available at https://www.ipc.on.ca/wp-content/uploads/2013/09/pbd-primer.pdf. Accessed 27 April 2022.

[1999] Information and Privacy Commissioner Ontario (2009). *Privacy by Design* at 1. Available at https://www.ipc.on.ca/wp-content/uploads/2013/09/pbd-primer.pdf. Accessed 27 April 2022.

[2000] Kianieff, M. (2019) *Blockchain Technology and the Law Opportunities and Risks* Routledge Publishing (UK) at 179.

[2001] Kianieff, M. (2019) *Blockchain Technology and the Law Opportunities and Risks* Routledge Publishing (UK) at 179.

[2002] Kianieff, M. (2019) *Blockchain Technology and the Law Opportunities and Risks* Routledge Publishing (UK) at 179 – 180.

The idea of implementing PbD practices at the development stages of an IT system originated from Recital 46 of Directive 95/46[2003] of the EU.[2004] Recital 46 made it mandatory for the relevant actors to adopt appropriate technical and organisational measures at the time of the design of the IT system and at the time of processing personal data.[2005] Schaar correctly points out that PbD is not limited to merely maintaining security in an IT system but includes the practice that technology systems should be designed and constructed in a manner that reduces the amount of personal data stored on a system.[2006] To give effect to this practice, Schaar recommends the separation of personal identifiers and content data, making use of pseudonyms, employing anonymisation techniques, or the deletion of personal data in its entirety.[2007]

Berberich and Steiner correctly point out that a blockchain that has strong encryption and data security can be compatible with PbD.[2008] Berberich and Steiner also note that introducing measures such as the addition of 'noise'[2009] to data stored on a blockchain can make blockchains compatible with PbD.[2010] Additionally, Berberich and Steiner also highlight the techniques employed in the ENIGMA project.[2011] ENIGMA is a decentralised computation platform that guarantees privacy by enabling developers to

[2003] Recital 46 of the 1995 EU Directive reads: "Whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing; whereas it is incumbent on the Member States to ensure that controllers comply with these measures; whereas these measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected."

[2004] Schaar, P. (2010). "Privacy by Design" *Identity in the Information Society* (3) at 267. Available at https://doi.org/10.1007/s12394-010-0055-x. Accessed 14 June 2022.

[2005] European Parliament (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&rid=5. Accessed 14 June 2022. See also Schaar, P. (2010). "Privacy by Design" *Identity in the Information Society* (3) at 267. Available at https://doi.org/10.1007/s12394-010-0055-x. Accessed 14 June 2022.

[2006] Schaar, P. (2010). "Privacy by Design" *Identity in the Information Society* (3) at 267 – 268. Available at https://doi.org/10.1007/s12394-010-0055-x. Accessed 14 June 2022.

[2007] Schaar, P. (2010). "Privacy by Design" *Identity in the Information Society* (3) at 268. Available at https://doi.org/10.1007/s12394-010-0055-x. Accessed 14 June 2022.

[2008] Berberich, M., & Steiner, M. (2016). "Blockchain technology and the GDPR how to reconcile privacy and distributed ledgers" *European Data Protection Law Review* 2(3): 425.

[2009] See paragraph 3.8.5 above.

[2010] Berberich, M., & Steiner, M. (2016). "Blockchain technology and the GDPR how to reconcile privacy and distributed ledgers" *European Data Protection Law Review* 2(3): 425.

[2011] Berberich, M., & Steiner, M. (2016). "Blockchain technology and the GDPR how to reconcile privacy and distributed ledgers" *European Data Protection Law Review* 2(3): 425.

build PbD end-to-end decentralisation applications without trusted third parties.[2012] ENIGMA uses a network of computers that store and execute queries.[2013] ENIGMA uses multi-party computation (MPC) where a PC only sees a piece of data.[2014] In other words, data (which is encrypted at all times) is not stored at a single location but at different nodes. No party has access to a person's data in its entirety.[2015] If a party requires access to a person's data, computations are run on that data. Blockchain stores proof of who owns the data.[2016] If the owner of the data wishes to share their data with an inquisitor, they do so by providing 'shares'[2017] of that data.[2018]

It may be necessary for developers to adopt privacy enhancing technologies (PETs) at the start of blockchain system design. PETs have been defined as "a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data all without losing the functionality of the data system."[2019] Although PETs were designed to enable users to control and disseminate their personal information,[2020] it is submitted that these technologies can be designed into ICT systems to promote privacy.

[2012] Zyskind, G., Nathan, O. & Pentland, A. (2015). "Enigma: Decentralized Computation Platform with Guaranteed Privacy" at 2. Available at https://arxiv.org/pdf/1506.03471.pdf. Accessed 3 July 2022.

[2013] Hardjono, T., Shrier, D. L., & Pentland, A. (2019). *Trusted Data: A New Framework for Identity and Data Sharing* The MIT Press at 161.

[2014] Hardjono, T., Shrier, D. L., & Pentland, A. (2019). *Trusted Data: A New Framework for Identity and Data Sharing* The MIT Press at 161; Zyskind, G., Nathan, O. & Pentland, A. (2015). "Enigma: Decentralized Computation Platform with Guaranteed Privacy" at 2. Available at https://arxiv.org/pdf/1506.03471.pdf. Accessed 3 July 2022.

[2015] Zyskind, G., Nathan, O. & Pentland, A. (2015). "Enigma: Decentralized Computation Platform with Guaranteed Privacy" at 2. Available at https://arxiv.org/pdf/1506.03471.pdf. Accessed 3 July 2022; Hardjono, T., Shrier, D. L., & Pentland, A. (2019). *Trusted Data: A New Framework for Identity and Data Sharing* The MIT Press at 161.

[2016] Hardjono, T., Shrier, D. L., & Pentland, A. (2019). *Trusted Data: A New Framework for Identity and Data Sharing* The MIT Press at 162.

[2017] Shares is a process where data is split into several random pieces. See Hardjono, T., Shrier, D. L., & Pentland, A. (2019). *Trusted Data: A New Framework for Identity and Data Sharing* The MIT Press at 162.

[2018] Hardjono, T., Shrier, D. L., & Pentland, A. (2019). *Trusted Data: A New Framework for Identity and Data Sharing* The MIT Press at 162; Zyskind, G., Nathan, O. & Pentland, A. (2015). "Enigma: Decentralized Computation Platform with Guaranteed Privacy" at 3. Available at https://arxiv.org/pdf/1506.03471.pdf. Accessed 3 July 2022

[2019] Borking, J. J. & Raab, C. D. (2001). "Laws, PETs and Other Technologies for Privacy Protection" *The Journal of Information, Law and Technology* 2001(1) at 1.

[2020] Office of the Privacy Commissioner of Canada (2017). *Privacy Enhancing Technologies – A Review of Tools and Techniques*. Available at https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/pet_201711/#fn6. Accessed 27 April 2022.

The importance of adopting PbD for the cross-border collection of VAT from the supply of digital goods cannot be overstated. For example, suppliers that make use of blockchain technology for the remittance of VAT may not necessarily have the relevant IT skills to implement security measures by themselves in order to protect their own information and the personal information of taxpayers.[2021] For this reason, it is advisable for tax authorities that develop blockchain specifically for the purpose of collecting VAT to ensure that suppliers and taxpayer's data is protected by providing the necessary privacy tools that facilitate data protection.[2022] By enabling automatic data protection from the onset, tax authorities can create an architecture of trust.[2023] For example, the architecture of trust can reduce the compliance burden for foreign suppliers of digital goods because compliance with data privacy laws is not required. This is because a PbD designed blockchain is inherently, and by default, compliant with data privacy laws. From a taxpayer's perspective, trust, and confidence in the PbD designed blockchain can enable greater tax compliance. Tax authorities benefit from the PbD designed blockchain because their administrative burden is reduced. Tax authorities can count on greater tax compliance to generate more revenue.

6.9 Conclusion

The advent of the POPI Act has brought change to the South African privacy discussion landscape. The primary objective of the POPI Act is to ensure that a data subject's right to information privacy is protected. The POPI Act establishes conditions that must be complied with before the processing of personal information is considered lawful. It is likely that if any one of the conditions is absent, then the processing of personal information can be unlawful. The Information Regulator can impose

[2021] See Schaar, P. (2010). "Privacy by Design" *Identity in the Information Society* (3) at 267. Available at https://doi.org/10.1007/s12394-010-0055-x. Accessed 14 June 2022.

[2022] See Schaar, P. (2010). "Privacy by Design" *Identity in the Information Society* (3) at 267. Available at https://doi.org/10.1007/s12394-010-0055-x. Accessed 14 June 2022.

[2023] According to Werbach, an 'architecture' is the way the components of a system interact with one another. There are three types of architectures. A Peer-to-Peer (P2P) architecture system is based on relationships and shared norms. For example, P2P architectures formulate a set of self-governing principles that must be adhered to by all the users. The second form of architecture is the Leviathan model where a central authority governs the system and prevents others from forcefully imposing their will. The last model is the Intermediary model. In this model, emphasis is placed on the local rules and the reputation of intermediaries. See Werbach, K. (2018). *The Blockchain and the New Architecture of Trust* Massachusetts Institute of Technology Press (US) at 25 – 28.

administrative penalties on a responsible party that commits an offence in terms of the POPI Act.[2024]

The use of blockchain for revenue collection purposes is currently incompatible with certain provisions of the POPI Act. A data subject's: (i) right to rectification, (ii) right object to the processing of personal information, (iii) right to access information, (iv) data subject participation, (v) information quality, and (vi) the purpose specific condition cannot be enforced on blockchain. However, there are measures that can be implemented to make the use and application of blockchain more compliant with the POPI Act.[2025]

The collection of VAT on blockchain raises data privacy issues. A taxpayer's information on a digital invoice can be transmitted on blockchain from the foreign supplier to the relevant tax authority. To ensure compliance with data privacy laws, it is necessary to anonymise taxpayer information supplied on the digital invoice. Since a foreign supplier is considered a data subject for purposes of the POPI Act,[2026] it is also sensible to anonymise the foreign supplier's information when VAT collection occurs on blockchain. This is to ensure that the protection afforded to natural persons in terms of the POPI Act is extended to foreign suppliers of digital goods.

In the final chapter, I make recommendations based on the discussion and findings in this thesis.

[2024] See section 109 of the POPI Act.
[2025] See paragraph 6.8 above.
[2026] See the definition of 'person' in section 1 of the POPI Act.

CHAPTER 7: RECOMMENDATIONS AND CONCLUSION

7.1 Introduction

VAT remains an important source of revenue for governments around the world. It stands to reason that the administration of VAT must be modernised to ensure that it is efficiently collected. The rise of e-commerce and the recent lockdown during the 2019 COVID pandemic have led to an increase in the demand for digital goods and services. Local consumers continue to purchase digital goods and services from foreign suppliers. By nature, the digital goods and services are intangible and tax authorities struggle to tax these transactions adequately. Tax authorities do not have the facilities nor the resources to track and audit online purchases of digital goods and services. The lack of resources to track and trace these transactions adequately means that tax liability and compliance cannot be ascertained. If the consumer or taxpayer cannot be identified, VAT goes uncollected. The inability to collect VAT on the cross-border supply of digital goods has the potential to erode the tax base. It is important for tax authorities to address the taxation issues linked to e-commerce by introducing mechanisms that can make the collection of VAT on cross-border supply of digital goods more efficient. This mechanism should not impose an additional compliance burden on foreign suppliers of digital goods. The mechanism must also reduce the administrative burden on tax authorities while making the administration of taxes simpler in the process.

The aim of this thesis is to determine whether blockchain can be used as an effective mechanism for the collection VAT on the cross-border supply of digital goods. The discussion in this thesis sought to answer the following questions:

i) What are the interjurisdictional aspects associated with implementing blockchain for the collection of VAT on cross-border trade in digital goods?

ii) What are the benefits of using blockchain to collect and administer VAT?

iii) How can SARS effectively use blockchain to collect VAT on the cross-border trade in digital goods?

iv) What are the legal considerations, if any, that must be considered as a result of implementing blockchain for VAT collection?

v) What enforcement measures can SARS have after implementing blockchain for VAT administration?

These questions formed the basis upon which the discussion in this thesis was conducted. During this study, it has emerged that blockchain shows potential as a viable tool for the collection of VAT on the cross-border supply of digital goods in South Africa. Despite its numerous advantages,[2027] there are significant drawbacks that can inhibit the successful adoption of blockchain technology.[2028] These challenges cannot be surmounted by merely making amendments to the VAT Act and the Tax Administration Act.[2029] The adoption of blockchain requires unprecedented levels of cooperation at local and international level. Tax authorities must allocate resources to reform tax policies, IT infrastructure must be modernised, data security must be strengthened, skilled personnel must be hired, and cybersecurity must be enhanced to assist tax authorities in executing their duties.[2030]

In this chapter, I consider whether this thesis has answered the questions posed above and at the beginning of this study.[2031] Thereafter, I make recommendations based on the findings I have made in this thesis.

7.2 The interjurisdictional aspects of blockchain

As I have already mentioned,[2032] blockchain is a computer code. It runs on computer nodes that can transcend borders. In other words, a copy of a blockchain ledger can

[2027] See paragraph 3.4 above.
[2028] See paragraph 3.5 above.
[2029] Act 89 of 1991 and Act 28 of 2011 respectively.
[2030] See Van Zyl, S. P. (2013). *The collection of Value Added Tax on online cross-border trade in Digital Goods*. Unpublished LLD thesis (UNISA) at 346.
[2031] See paragraph 1.2 above.
[2032] See paragraph 3.3.1 above.

be accessed anywhere around the world depending on the type of blockchain and access rights. A foreign supplier merely requires a computer, good Internet connectivity, and sufficient storage space to gain access to blockchain. A foreign supplier simply downloads a copy of the ledger on their computer and starts recording transactions on blockchain using a smart contract. From a supplier's perspective, a dedicated team can be tasked with ensuring that VAT is transmitted to the relevant tax authority. It is a tax authority's responsibility to ensure that the transactions are recorded on blockchain for audit purposes. Since the tax authority is responsible for running blockchain, it is important to develop a legal framework in the country where blockchain has been setup.[2033] To put this into context, the VAT Act and the Tax Administration Act should be amended to make provision for the collection of VAT on blockchain. For example, the amendments to the VAT Act must contain a statutory legal definition of blockchain. The inclusion of a legal definition provides legal certainty for suppliers. Suppliers want to be certain that the preferred method for VAT remittance has been legislated in the country of consumption. Also, the proposed rules around this collection model should be clear and simple to understand. The simpler the rules are, the more likely that compliance will be high. Clear, and simple rules can entice foreign suppliers to trade in South Africa.

At present, the bilateral and multilateral tax treaties provide, generally, for the mutual assistance between countries. These treaties do not provide for specific VAT collection mechanisms. Yet, for VAT collection using blockchain technology, minimum standards must be adopted by revenue authorities in the countries with which South Africa trades. This aspect is crucial for the successful adoption of blockchain for VAT collection. Accordingly, SARS must develop a blockchain based on universal accepted standards. If SARS uses a standalone blockchain system,[2034] then SARS might be isolated from the international community. Moreover, a standalone blockchain adopted by SARS can be incompatible with blockchains developed by tax authorities in other countries. A standalone blockchain can also be incompatible with blockchains developed by other government departments. For example, a standalone blockchain developed by the South African Reserve Bank (SARB) can be incompatible with a

[2033] The setup can take place in the country where the goods and services are consumed.

[2034] For purposes of this thesis, a standalone blockchain is one that is programmed solely by one entity without considering internationally accepted standards.

blockchain developed by SARS. As a result, the two systems can be incompatible with each other which can lead to fragmentation.[2035]

It is possible for SARS to enforce extra-territorial powers on blockchain if bilateral agreements have been concluded. However, it is difficult for SARS to enforce its extra-territorial powers if the corresponding jurisdiction is not familiar with the programming language used by SARS's blockchain. The code can be unreadable and incompatible with the systems employed in the corresponding jurisdiction. If that is the case, a standalone blockchain can cause delays in the enforcement, collection, and administration of VAT on the cross-border supply of digital goods.

7.2.1 Setting the scene for the development of international agreements and standards

There are three ways to create and adopt standards: (i) by convention; (ii) by law or (iii) by negotiation.[2036] In the first criteria, standards can be adopted by repetition and use.[2037] In the second criteria, standards can be imposed by governments or other institutions. And in the third criteria, standards can be agreed upon by stakeholders in an activity or enterprise.[2038] SARS can test blockchain locally by requesting businesses to use the system to remit VAT.[2039] Blockchain best practices and use cases can be established, enabling SARS to learn from these cases and transpose the experiences at international level. Once SARS has established a blueprint, the practices for VAT remittance on blockchain can be sent to the Institute of Electrical

[2035] See discussion at paragraph 3.5.10 above.

[2036] World Economic Forum (2020). *Global Standards Mapping Initiative: An overview of blockchain technical standards* at 7. Available at https://www3.weforum.org/docs/WEF_GSMI_Technical_Standards_2020.pdf. Accessed 26 August 2023.

[2037] World Economic Forum (2020). *Global Standards Mapping Initiative: An overview of blockchain technical standards* at 7. Available at https://www3.weforum.org/docs/WEF_GSMI_Technical_Standards_2020.pdf. Accessed 26 August 2023.

[2038] World Economic Forum (2020). *Global Standards Mapping Initiative: An overview of blockchain technical standards* at 7. Available at https://www3.weforum.org/docs/WEF_GSMI_Technical_Standards_2020.pdf. Accessed 26 August 2023.

[2039] Before deployment, SARS must test the technology in a controlled environment to determine the pros and cons of the technology.

and Electronics Engineers Standards Association (IEEE SA)[2040] for approval. In 2018, Tencent and the Shenzhen's tax bureau developed a blockchain e-invoice platform.[2041] Blockchain system provides a platform for the issuer and recipient of the invoice to mediate with the tax authority to monitor the reimbursement, reporting, and circulation process.[2042] The primary purpose of the of this system is to prevent VAT fraud.[2043] After use cases and practices in Shenzhen province (China) materialised, IEEE SA approved and published the standards in 2019 and 2021 respectively. The IEEE Recommended Practice for E-Invoice Business Using Blockchain Technology[2044] "is the world's first international standard for blockchain-based applications for e-invoice business."[2045] The IEEE SA's approval of China's blockchain e-invoice technology means that it has gained acknowledgment from international authoritative institutions and this development contributes to the standardisation and guidance of relevant applications globally.[2046] If SARS follows a similar approach, it

[2040] The IEEE "is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity." See IEEE (2023). *About*. Available at https://www.ieee.org/about/index.html?utm_source=dhtml_footer&utm_medium=hp&utm_campaign=learn-more. Accessed 27 August 2023. The IEEE SA "IEEE Standards Association (IEEE SA) is a leading consensus building organization that nurtures, develops and advances global technologies, through IEEE. We bring together a broad range of individuals and organizations from a wide range of technical and geographic points of origin to facilitate standards development and standards related collaboration. With collaborative thought leaders in more than 160 countries, we promote innovation, enable the creation and expansion of international markets and help protect health and public safety. Collectively, our work drives the functionality, capabilities and interoperability of a wide range of products and services that transform the way people live, work, and communicate." See IEEE SA (2023). *About us*. Available at https://standards.ieee.org/about/. Accessed 27 August 2023.

[2041] See Shenzhen Daily (2021). "City introduces world's 1st international standardization for blockchain e-invoice". Available at http://www.sz.gov.cn/en_szgov/business/news/content/post_8675244.html. Accessed 26 August 2023.

[2042] Wight, M. (2020). China to use blockchain-based system to tackle fraudulent invoices. Available at https://theblockchainland.com/2020/03/13/china-blockchain-based-system-fraudulent-invoices/. Accessed 26 August 2023; see also Post, D. & Cipollini, C. (2022). Fundamental elements of a blockchain-based tax system – when to use blockchain for tax? *World Tax Journal* 14(4): 557.

[2043] Wight, M. (2020). China to use blockchain-based system to tackle fraudulent invoices. Available at https://theblockchainland.com/2020/03/13/china-blockchain-based-system-fraudulent-invoices/. Accessed 26 August 2023; see also Post, D. & Cipollini, C. (2022). Fundamental elements of a blockchain-based tax system – when to use blockchain for tax? *World Tax Journal* 14(4): 557.

[2044] IEEE Std 2142.1™- 2021.

[2045] See Shenzhen Daily (2021). "City introduces world's 1st international standardization for blockchain e-invoice". Available at http://www.sz.gov.cn/en_szgov/business/news/content/post_8675244.html. Accessed 26 August 2023.

[2046] See Shenzhen Daily (2021). "City introduces world's 1st international standardization for blockchain e-invoice". Available at http://www.sz.gov.cn/en_szgov/business/news/content/post_8675244.html. Accessed 26 August 2023.

can set the scene for the approval of international standards on the use of blockchain for VAT remittance.[2047]

7.2.2 How can suppliers (taxpayers) be incentivised to use blockchain?

For blockchain to be successfully adopted to collect VAT, it may be necessary to incentivise taxpayers. In other words, are there any incentives for suppliers to use blockchain to remit VAT to the relevant tax authorities? It is possible to provide incentives for taxpayers so that they can participate in blockchain.[2048] This is because taxpayers must invest in technology and other resources to run a blockchain-based VAT.[2049] One strategy that has been proposed is for the introduction of tax incentives.[2050] It should be noted that this strategy can work if local suppliers of goods and services are treated in the same manner as their international counterparts. It does not make sense to give tax incentives to foreign suppliers and exclude local suppliers because this would be contrary to the VAT neutrality principle.

Post and Cipollini[2051] mention that taxpayers can be incentivised to use blockchain if the following benefits accrue to them:

i) Manual submissions are eliminated, and audits can be automated;

ii) If all parties use the same ecosystem, they have access to the same data. This reduces the likelihood of legal disputes;

iii) The immutable version of the truth can be accessible to all the relevant parties potentially reducing fraud in the process;

iv) Processes such as real-time data analytics and siloed systems can be integrated in a single environment;

[2047] It should be noted that South Africa does not have the same influence on the international stage like China. For this reason, South Africa can set standards for blockchain on the African continent. In doing so, SARS can set blockchain standards that are specific to Africa.

[2048] Setyowati, M. S. *et al* (2023). “Strategic factors in implementing blockchain technology in Indonesia’s value-added tax system” *Technology in Society* (72): 102169.

[2049] Setyowati, M. S. *et al* (2023). “Strategic factors in implementing blockchain technology in Indonesia’s value-added tax system” *Technology in Society* (72): 102169.

[2050] Setyowati, M. S. *et al* (2023). “Strategic factors in implementing blockchain technology in Indonesia’s value-added tax system” *Technology in Society* (72): 102169.

[2051] Post, D. & Cipollini, C. (2022). Fundamental elements of a blockchain-based tax system – when to use blockchain for tax? *World Tax Journal* 14(4): 519 – 572.

v) Increased transparency;

vi) Taxpayers could be required to take better control of the quality of their data;

vii) Real-time taxation can provide insight into the tax position of a taxpayer, enabling the tax function at companies to act faster and more directly;

viii) Blockchain can provide a single source of truth with updated tax rules. This can be achieved by using software *oracle*s, which make it possible for smart contracts to interact with real-time events. Interactions can include determining the taxable base and tax rate. This can promote and simplify tax compliance for taxpayers.[2052]

Another important way to incentivise suppliers is by making the use of blockchain legally enforceable and mandatory under domestic laws.[2053] Simply put, the country of consumption can compel foreign suppliers to use blockchain to remit VAT in terms of the domestic VAT laws. This strategy, albeit extreme, can work if all the role players have the infrastructure and resources to use blockchain to remit VAT. A lack of resources can deter suppliers from supplying digital goods to the country of consumption. Moreover, I propose that this strategy be implemented as a last resort if all avenues have been exhausted. In my view, it is necessary for SARS to incentivise suppliers to use blockchain. Recently, SARS announced that it intended to modernise the VAT administration process.[2054] To encourage uptake and participation among foreign suppliers, SARS proposes that the initial costs of implementing the new system be deducted for income and VAT purposes as a means of complying with the new VAT administrative framework.[2055]

From the strategies I have just discussed, the proposal by Post and Cipollini to highlight the benefits of blockchain use seems to be the most favourable at this stage. Therefore, SARS should highlight the advantages of using the technology and propose

[2052] Post, D. & Cipollini, C. (2022). Fundamental elements of a blockchain-based tax system – when to use blockchain for tax? *World Tax Journal* 14(4): 547 – 548.

[2053] See Post, D. & Cipollini, C. (2022). Fundamental elements of a blockchain-based tax system – when to use blockchain for tax? *World Tax Journal* 14(4): 547.

[2054] SARS (2023). *Discussion Paper: Value-Added Tax Modernisation*. Available at https://www.sars.gov.za/wp-content/uploads/Docs/VAT/Discussion-Paper-on-Value-Added-Tax-Modernisation.pdf. Accessed 4 October 2023.

[2055] SARS (2023). *Discussion Paper: Value-Added Tax Modernisation* at 6. Available at https://www.sars.gov.za/wp-content/uploads/Docs/VAT/Discussion-Paper-on-Value-Added-Tax-Modernisation.pdf. Accessed 4 October 2023.

it to the suppliers. The benefits clearly demonstrate that the suppliers' compliance burden in the tax administration process is reduced. If all the benefits are highlighted, and all the role players come on board, SARS can proceed to introduce blockchain for VAT collection.

7.2.3 Considerations of topics for international blockchain agreements

I propose that the following topics be considered with international counterparts:

i) Blockchain definition: It is important for parties to agree on the definition of blockchain. A consistent definition promotes legality and avoids uncertainty. This implies that countries should regulate blockchain. Other elements of blockchain that must be addressed include the type of source code that runs blockchain, the consensus mechanism used to validate transactions, the software code for the smart contract, and all other applications that run on blockchain.

ii) Security management: Security is a key component of blockchain. Parties must agree on how the security of blockchain will be managed. Adequate security ensures that the nodes, networks, and services work optimally.[2056]

iii) Privacy management: Parties should agree on the type of privacy enhancing techniques that will be used on blockchain. For example, I propose that parties use zero-knowledge proof or anonymisation techniques to protect taxpayer's data.

iv) Private key management: The management of private keys should be addressed. Parties must determine who will be responsible for the management of private keys. If the private keys are not adequately catered for, data may be retrieved by unauthorised parties.

v) Governance: The governance of blockchain architecture should be performed by the tax authority. This is to ensure that the compliance burden of the suppliers is kept to a minimum. An international agreement should contain governance best practice and standards.[2057]

[2056] See European Commission (2022). *Blockchain Standards*. Available at https://digital-strategy.ec.europa.eu/en/policies/blockchain-standards. Accessed 30 August 2023.

[2057] See European Commission (2022). *Blockchain Standards*. Available at https://digital-strategy.ec.europa.eu/en/policies/blockchain-standards. Accessed 30 August 2023.

vi) Smart contracts: Smart contracts can play a significant role in the collection of VAT. For that reason, establishing smart contract best practices and standards to ensure smart contracts are safe and secure,[2058] could prove crucial.

vii) Interoperability: Blockchains and DLT protocols must be interoperable in an international setting for easy exchange of data and for seamless communication with each other.[2059]

viii) General blockchain taxonomy: It is imperative for tax authorities to agree on the terminology and definitions of all the components of blockchain.

ix) Digital invoice system:[2060] Tax authorities must agree on the standards that will be used to adapt a blockchain-based digital invoice system. Additionally, the standards must prescribe what sort of information should be on a digital invoice.

x) Regulatory framework: It would be irrational for countries to agree on blockchain standards if the respective jurisdictions lack a regulatory framework. A regulatory framework supports mainstream blockchain adoption and mitigates risks associated with blockchain use.[2061]

xi) Harmonisation of VAT rules: In my view, this step is the most basic. If governments cannot agree on a uniform set of VAT rules for the cross-border collection of VAT on the supply of digital goods, then it is extremely unlikely that they would agree on blockchain standards for VAT collection.

I therefore recommend the following amendments to the VAT Act:[2062]

Section 1 of the VAT Act should be amended as follows:

> Definitions. – (1) In this Act, unless the context otherwise indicates –
>
> **“Blockchain technology”** means a decentralised database based on a software protocol, which is cryptographically verified and secured, which may be public or private, may require an admission permission or not, may be controlled by (an)

[2058] See European Commission (2022). *Blockchain Standards*. Available at https://digital-strategy.ec.europa.eu/en/policies/blockchain-standards. Accessed 30 August 2023.

[2059] See European Commission (2022). *Blockchain Standards*. Available at https://digital-strategy.ec.europa.eu/en/policies/blockchain-standards. Accessed 30 August 2023.

[2060] Mazur, O. (2022). “Can blockchain revolutionize tax administration?” *Penn State Law Review* 127(1): 161.

[2061] Mazur, O. (2022). “Can blockchain revolutionize tax administration?” *Penn State Law Review* 127(1): 159.

[2062] Act 89 of 1991.

operator(s) or not, may be immutable or not, and in which it is intended that certain trust results from the foregoing principles inherently.[2063]

"Blockchain" means blockchain technology that is programmed and run by SARS.

"Node" means a computer linked to other computers on the Internet based on a software protocol.[2064]

"Operator" means SARS.

I recommend the following amendments to the Tax Administration Act:[2065]

Section 1 of the Tax Administration Act should be amended as follows:

"**International tax agreement**" means -
(a) an agreement entered into with the government of another country in accordance with a tax Act; or
(b) any other agreement entered into between the competent authority of the Republic and the competent authority of another country relating to the automatic exchange of information under an agreement referred to in paragraph (a);
(c) an agreement entered into with the government of another country from which a supplier of electronic services originates or has a permanent establishment.

"International tax standard" means -
(a) the OECD Standard for Automatic Exchange of Financial Account Information in Tax Matters;
(b) the Country-by-Country Reporting Standard for Multinational Enterprises specified by the Minister; or
(c) any other international standard for the exchange of tax-related information between countries specified by the Minister, or

[2063] See definition provided in Richter, T., *Blockchain Regulation* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 160.

[2064] See definition provided in Richter, T., *Blockchain Regulation* in Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* Kluwer Law International at 160.

[2065] Act 28 of 2011.

(d) an internationally developed blockchain standard for the collection of value-added tax between countries specified by the Minister.

7.3 The benefits of using blockchain to collect and administer VAT

I have already highlighted the benefits that blockchain brings to the administration of VAT on a blockchain.[2066] As such, I shall not repeat all the benefits here. This section pinpoints the critical aspects of blockchain that I believe should be incorporated in the VAT and Tax Administration Acts.

It is important to reiterate the importance of a digital invoice in the collection and administration of VAT on blockchain. A digital invoice is issued electronically by a supplier. The submission of a digital invoice is beneficial because it reduces a supplier's compliance burden by removing paper-based invoices. The digital invoice is signed electronically by a supplier using PKI. It is not possible to falsify a digital signature due to PKI.[2067] This feature has the potential to reduce VAT fraud. The obligation to append a digital signature on a tax invoice authenticates the data on the invoice.[2068] Currently, neither the Tax administration Act nor the VAT Act contain a definition of a digital signature.[2069] SARS can consider a binding general ruling (BGR)[2070] to clarify and interpret matters on PKI.

Most transactions on blockchain can be done using a smart contract. As already discussed,[2071] smart contracts are computer code that execute instructions instantaneously. In my view, the use of a smart contract reduces the time it takes for suppliers to file VAT returns.[2072] If the requirement to submit VAT returns is removed, a supplier's compliance burden is reduced. Suppliers are encouraged to trade in South Africa because the costs associated with trading in South Africa is low. The ripple

[2066] See paragraph 3.4 above.

[2067] See paragraph 3.3.3 above.

[2068] See discussion at paragraph 3.3.3 above.

[2069] It should be noted that sections 237 and 255 of the Tax Administration Act briefly mentions digital signatures.

[2070] A binding general ruling is a document issued by SARS on matters of general interest or importance and clarifies SARS' application and interpretation of tax law. See https://www.sars.gov.za/legal-counsel/legal-advisory/published-binding-rulings/binding-general-rulings-bgrs/. Accessed 5 January 2023.

[2071] See paragraph 2.8 above.

[2072] See discussion at paragraph 3.4.1 above.

effect is that more digital goods and services are made available to South African consumers. More options on the e-commerce marketplace means an increase in e-commerce transactions, which translates to additional revenue for the *fiscus*. Moreover, transaction costs for foreign suppliers and tax authorities are reduced.[2073] A financial intermediary may not be required to process the payments. The remittance of VAT on a blockchain using a smart contract is done in real-time, making tax information available for tax authorities. Real-time reporting that takes place on blockchain enables tax authorities to have information in real-time. Audits can be performed timeously, and any errors are identified immediately. Errors are also resolved timeously. For example, if a digital invoice contains an error, a supplier can merely reconfigure the digital invoice and resend it to SARS.

The use of blockchain to collect VAT can remove the statutory requirement for suppliers to keep records as required by the TAA.[2074] The statutory provision enables SARS to conduct audits on taxpayers. Generally, the costs of keeping records are high. The costs of keeping records are doubled because tax authorities and taxpayers keep separate records.[2075] Ideally, the records kept by taxpayers should match the records kept by tax authorities.[2076] Blockchain can synchronise record-keeping to ensure that taxpayers' and tax authorities' records match.[2077]

With blockchain, tax authorities can perform audits because the identity of the supplier is known. The audit can be conducted on blockchain itself. For this reason, it is not necessary for suppliers to keep records. All transactions are recorded on blockchain, and SARS can complete the VAT returns on the supplier's behalf. In doing so, a supplier's compliance burden is reduced.

Moreover, the introduction of blockchain for the administration of VAT can signal the end of the reverse-charge and registration mechanisms in South Africa.[2078] For

[2073] See discussion at paragraph 3.4.5 above.
[2074] See section 29 of the TAA.
[2075] Delmotte, C. (2022). "The Promises and Pitfalls of a Blockchain Driven Tax System" at 20. Available at https://ssrn.com/abstract=4187919. Accessed 6 October 2022.
[2076] Delmotte, C. (2022). "The Promises and Pitfalls of a Blockchain Driven Tax System" at 20. Available at https://ssrn.com/abstract=4187919. Accessed 6 October 2022.
[2077] Delmotte, C. (2022). "The Promises and Pitfalls of a Blockchain Driven Tax System" at 20. Available at https://ssrn.com/abstract=4187919. Accessed 6 October 2022.
[2078] See discussion at paragraphs 3.4.9 and 3.4.10 above.

starters, a consumer will no longer be required to account for and remit VAT to SARS when the latter imports services or digital goods into South Africa.[2079] With blockchain, the onus rests on the supplier to account for and remit VAT to the tax authorities. This way, VAT is remitted instantaneously, and SARS does not lose out on revenue. The registration mechanism can also be removed altogether from the VAT Act. A foreign supplier will not be required to register as a VAT vendor in South Africa. With blockchain, a foreign supplier simply remits VAT to SARS on a blockchain. The registration threshold[2080] can be removed from the VAT Act. These changes can reduce a foreign supplier's compliance.

Having considered the above, I recommend the following amendments to the VAT Act: Section 1 of the VAT Act should be amended by inserting the following definitions:

> **"Digital invoice"** means an electronic invoice signed electronically using public key infrastructure and is issued on a blockchain.
>
> **"Digital signature"** means an electronic signature signed cryptographically with a public and private key.
>
> **"Private key"** means cryptographically created characters used to encrypt and decrypt information.
>
> **"Public key"** means cryptographically created characters used to encrypt information.
>
> **"Public key infrastructure"** means a set of rules that ensures authenticity on a blockchain.
>
> **"Smart contract"** means a self-executing program run on a blockchain.
>
> **"VATCoin/TVACoin"** means a digital tax currency issued by SARS on a blockchain.

[2079] Section 14(1) of the VAT Act.
[2080] Currently at R1 million.

Section 14 of the VAT Act should be amended by inserting the following provision:

> (1A) For purposes of this Act, the provisions of subsection (1) do not apply where a supplier of imported services or electronic services remits value-added tax on a blockchain.

Section 14 of the VAT Act should be amended by inserting the following provision:

14A. Collection of value-added tax on blockchain

(1) Where tax is payable in terms of section 7(1)(c) in respect of the supply of imported services, a supplier must –

(a) Remit tax on a blockchain using a smart contract; and

(b) Send a digital invoice to a blockchain using a smart contract; and

(c) Ensure that a digital invoice contains encrypted or anonymised particulars as prescribed by section 20(4) of this Act; and

(d) Ensure that the digital invoice is signed with the supplier's private key.

(2) Where a supplier remits tax in terms of section 14A, tax must be paid using a node connected to a blockchain run by SARS.

14B. Collection of value-added tax on blockchain using VATCoin/TVACoin

(1) Where tax is payable in terms of section 7(1)(c) in respect of the supply of imported services, a supplier must -

(a) Remit tax on a blockchain using VATCoin/TVACoin; and

(b) Send a digital invoice on a blockchain using smart contract; and

(c) Ensure that a digital invoice contains encrypted or anonymised particulars as prescribed by section 20(4) of this Act; and

(d) Ensure that the digital invoice is signed with the supplier's private key.

(2) Where a supplier remits tax in terms of section 14(B), output tax can be paid in VATCoin/TVACoin.

(3) Where a supplier remits tax in terms of section 14A, tax must be paid using a node connected to a blockchain run by SARS.

Section 23 of the VAT Act should be amended by inserting the following provision:

> (1B) Every person who carries on any enterprise as contemplated in paragraph (b)(vi) or (vii) of the definition of "enterprise" in section 1 who is registered for and maintains value-added tax compliance on a blockchain is not required to register as a vendor in terms of paragraph (1A) of the provisions in section 23 of this Act.

Section 28 of the VAT Act should be amended by inserting the following provision:

> (10) A supplier shall not be required to furnish the Commissioner with a return reflecting such information as may be required for the purpose of the calculation of tax in terms of section 14 or 16 if that supplier remits tax on a blockchain.

Section 55 of the VAT Act should be amended by inserting the following provision:

> (5) Unless the context indicates otherwise, the provisions of subsection (1) do not apply to a supplier who remits tax under this Act on a blockchain.

I recommend the following amendments to the TAA:

Section 1 of the TAA should be amended by inserting the following provision:

> **"Digital signature"** means the definition given in section 1 of the Value-Added Tax Act 89 of 1991.
>
> **"Blockchain"** means the definition given in section 1 of the Value-Added Tax Act 89 of 1991.

Section 25 of the TAA should be amended by inserting the following provision:

> (9) Subsections (1) to (8) does not apply to a person who remits a tax under a tax Act on a blockchain.

Section 29 of the TAA should be amended by inserting the following provision:

> (4) The requirements of this Act to keep records, books of account or documents for a tax period do not apply to a person who remits a tax under a tax Act on a blockchain.

7.4 How SARS can effectively use blockchain to collect VAT on the cross-border supply of digital goods

For SARS to effectively use blockchain as a VAT collection tool, a good strategy[2081] is required. A good strategy involves identifying three key elements: establishing a diagnosis, adopting a guiding policy, and implementing a coherent action plan.[2082] A diagnosis identifies the nature of the problem.[2083] Once the correct diagnosis is made, it is easier to identify the most critical aspects of the problem that must be addressed. Addressing the critical aspects makes the problem less complex.[2084] The second aspect to consider is the introduction of a guiding policy. A guiding policy is the approach chosen to manage the problems identified in the diagnosis.[2085] Lastly, active coherent steps must be taken to ensure that the measures identified in the guiding policy are accomplished.[2086]

From SARS's perspective, a successful diagnosis can entail identifying the issues that can curtail blockchain's adoption. A budget must be set aside to ensure that funds are available. National Treasury can play a vital role in this process by ensuring that funds are allocated to SARS. If funds are available, SARS can recruit software developers, programmers, data analysts, data architects, and quality assurers.[2087] The success of

[2081] Rumelt defines a 'good strategy' as: "a coherent action backed up by an argument, an effective mixture of thought and action with a basic underlying structure called the *kernel*". A kernel consists of a diagnosis, a guiding policy, and a set of coherent actions. See Rumelt, R. (2017). *Good Strategy Bad Strategy: The difference and why it matters* Profile Books Ltd (London) at 7, 77 – 93.

[2082] Rumelt, R. (2017). *Good Strategy Bad Strategy: The difference and why it matters* Profile Books Ltd (London) at 7.

[2083] See Rumelt, R. (2017). *Good Strategy Bad Strategy: The difference and why it matters* Profile Books Ltd (London) at 77.

[2084] Rumelt, R. (2017). *Good Strategy Bad Strategy: The difference and why it matters* Profile Books Ltd (London) at 77.

[2085] Rumelt, R. (2017). *Good Strategy Bad Strategy: The difference and why it matters* Profile Books Ltd (London) at 77.

[2086] Rumelt, R. (2017). *Good Strategy Bad Strategy: The difference and why it matters* Profile Books Ltd (London) at 77.

[2087] This is not an exhaustive list. See also paragraph 3.5.1 above.

blockchain can hinge on the recruitment and training of skilled personnel in these respective fields.[2088] It is also important for SARS to have the necessary IT systems and infrastructure in place to facilitate blockchain use. Issues such as blockchain governance and blockchain security should be addressed at the initial phases of implementation.[2089] The strength of SARS's IT systems and infrastructure can have a direct impact on data privacy. A weak or compromised IT system can lead to system vulnerabilities. These vulnerabilities can be exploited by unauthorised parties. If unauthorised parties gain access to blockchain system, data theft can take place. Cybersecurity must be actively pursued to ensure that data leaks do not take place.

By introducing blockchain, SARS, and by implication South Africa, can be the leading authority in so far as establishing blockchain standards is concerned.[2090] Adopting blockchain in the tax sector can set the benchmark for other sectors like insurance, banking, and health to also consider blockchain. The widespread use of blockchain can aid its development.

As I have discussed earlier,[2091] political will is a concern that must be addressed at the initial stages of blockchain development. Government backing, or the lack thereof, has a direct impact on the pace at which blockchain is introduced in the tax sector. It is important for the relevant role players to actively engage and lobby the government to ensure that government backing is obtained, and perhaps more importantly, sustained.

Once all the issues have been identified,[2092] a set of guiding principles must be introduced. SARS can use the guidelines as a 'to do' list to ascertain if all the problems owing to blockchain development have been identified. A guiding policy sets the approach(es) chosen to overcome the issues identified in the diagnosis phase.[2093] A guiding policy can provide a method of grappling with the challenges identified while

[2088] See paragraph 3.5.2 above.

[2089] See paragraphs 3.5.12 and 3.4.11 respectively.

[2090] See paragraph 3.5.10.

[2091] See paragraph 3.5.4 above.

[2092] It should be borne in mind that other issues can materialise at the initial stages of blockchain development. It is also possible that issues, not considered in this thesis, can materialise at the initial stages of development.

[2093] Rumelt, R. (2017). *Good Strategy Bad Strategy: The difference and why it matters* Profile Books Ltd (London) at 77.

also ruling out an array of actions.[2094] In the context of VAT collection, SARS can adopt a policy on the collection of VAT on the cross-border supply of digital goods. For instance, SARS can publish a comprehensive interpretation note[2095] on the rules pertaining to the collection of VAT on a blockchain. The interpretation note can assist and guide suppliers (both local and foreign) on the interpretation and application of the relevant provisions of the VAT Act and the TAA that pertain to the use of blockchain for the collection and administration of VAT.[2096] An interpretation note can be quickly amended, in line with legislation and any other tax policy developments.[2097] It should be noted that interpretation notes are not substitutes for legislation. Legislation remains the primary source of tax rules and tax administration guidance.[2098]

The last step to implement is the coherent action plan. The action plan should be coherent.[2099] An action plan entails taking steps that are coordinated with one another to achieve the goals set out in the guiding policy.[2100] For example, SARS must obtain political backing before all the other steps are followed. Political will can make blockchain development process much easier. As already mentioned, funds and resources can be made available to enable SARS to: (i) hire and train personnel, (ii) improve IT systems and infrastructure, and (iii) strengthen cybersecurity. This can lay the foundation for the successful adoption of blockchain technology in South Africa.

7.5 Addressing privacy on blockchain

The most important constitutional aspect to consider when adopting blockchain is the right to privacy. More pertinently, a taxpayer's right to information privacy. The reason

[2094] Rumelt, R. (2017). *Good Strategy Bad Strategy: The difference and why it matters* Profile Books Ltd (London) at 84.

[2095] Interpretation notes "are intended to provide guidelines to stakeholders on the interpretation and application of the provisions of the legislation administered by the Commissioner". See SARS (2022). "Interpretation Notes" Available at https://www.sars.gov.za/legal-counsel/legal-advisory/interpretation-notes/. Accessed 2 December 2022.

[2096] See SARS (2022). "Interpretation Notes" Available at https://www.sars.gov.za/legal-counsel/legal-advisory/interpretation-notes/. Accessed 2 December 2022.

[2097] See SARS (2022). "Interpretation Notes" Available at https://www.sars.gov.za/legal-counsel/legal-advisory/interpretation-notes/. Accessed 2 December 2022.

[2098] See Bal, A. (2019). "Developing a regulatory framework for the taxation of virtual currencies" *Intertax* 47(2): 229.

[2099] Rumelt, R. (2017). *Good Strategy Bad Strategy: The difference and why it matters* Profile Books Ltd (London) at 91.

[2100] Rumelt, R. (2017). *Good Strategy Bad Strategy: The difference and why it matters* Profile Books Ltd (London) at 77.

for this is that once adopted, taxpayer's information can be processed on a blockchain. As I have already discussed,[2101] it is possible for all the participants on blockchain to view the transactions on blockchain. The transactions can contain metadata. If the metadata is combined with certain identifiers, it can reveal a taxpayer's information. It is important to have security safeguards when processing taxpayer information on a blockchain.

Chapter four has shown that anonymising taxpayer information makes it difficult for a person to reveal the original information. For this reason, anonymised data affords the best possible route to protect data on a blockchain. While there are tensions between privacy laws and blockchain, it must be noted that blockchain can provide adequate security safeguards to protect the privacy of taxpayers. Moreover, zero-knowledge proof can be used to share confidential information with specific participants without revealing the same information with other participants on blockchain.[2102]

The emergence of the POPI Act has brought significant changes in so far as the protection of a person's privacy is concerned. The POPI Act applies to the processing of personal information in South Africa. It sets the conditions for the lawful processing of personal information. While the definition of personal information is broad, it is my view that taxpayer information constitutes personal information for purposes of the POPI Act. It can be concluded that the provisions of POPI apply to the processing of taxpayer information. However, this thesis has shown that the application of blockchain for revenue collection is currently incompatible with certain provisions of the POPI Act.[2103]

To remedy this defect, I recommend the following amendments to the POPI Act:

The definition of 'personal information' in section 1 of the POPI Act should be amended by inserting the following provision:

[2101] See paragraph 2.5 above.

[2102] Post, D. & Cipollini, C. (2022). Fundamental elements of a blockchain-based tax system – when to use blockchain for tax? *World Tax Journal* 14(4): 525.

[2103] See paragraph 6.9 above.

(i) Hashed data and encrypted data.

Section 3(1) of the POPI Act should be amended by inserting the following provision:

(c) In the context of the activities of a responsible party or operator in the Republic, irrespective of whether the processing takes place in the Republic or not.

Section 6 of the POPI Act should be amended by inserting the following provision:

(1)(f) by the South African Revenue Service to enforce legislation concerning the collection of revenue on a blockchain.

Section 11 of the POPI Act should be amended by inserting the following provision:

(5) The provisions of subsection (3)(a) do not apply where a responsible party or operator facilitates the processing of personal information on a blockchain.

Section 68 of the TAA should be amended by inserting the following provision:

(4) The provisions of subsection (3) do not apply where SARS administers a tax under a tax Act on a blockchain.

Section 69 of the TAA should be amended by inserting the following provision:

(9) The provisions in this section do not apply where SARS administers a tax under a tax Act on a blockchain.

Section 46 of the PAIA should be amended by inserting the following provision:

46A. The provisions of section 46 of this Act do not apply where the South African Revenue Service enforces legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act on a blockchain.

7.6 Enforcement measures for SARS on blockchain

Blockchain can strengthen SARS's enforcement powers. Blockchain's features make it conducive for SARS to identify suppliers. SARS can perform tax audits on suppliers in real-time. Once a defaulting supplier has been identified on blockchain, SARS can proceed to impose penalties or interest on non-compliant suppliers.[2104] As already mentioned above,[2105] SARS cannot enforce its extra-territorial powers without concluding a tax treaty with the country in which enforcement measures are to be conducted.[2106] It may be necessary for SARS to conclude bilateral and multilateral treaties with other countries to ensure that the provisions of the TAA are enforced.[2107]

I have already made recommendations for the TAA to be amended to include an international tax agreement concluded between South Africa and other countries for the collection of VAT on blockchain.[2108]

7.7 Blockchain and VAT rules

VAT rules predate blockchain technology. The adoption of blockchain for the cross-border collection of VAT raises question around the application of VAT rules. It must be borne in mind that without harmonised VAT rules, the application of blockchain for the cross-border collection of VAT can prove difficult. In other words, it is impractical to implement a blockchain system across various jurisdictions if there are no uniform VAT rules. Thus, a uniform set of VAT rules is a prerequisite if blockchain is to be considered as a technology tool to collect VAT across multiple jurisdictions. As discussed above,[2109] blockchain offers a tool, called an *oracle*, which aligns blockchain with real-time events.[2110] With the aid of an *oracle*, a smart contract can interact with

[2104] Van Zyl, S. P. (2013). *The collection of Value Added Tax on online cross-border trade in Digital Goods*. Unpublished LLD thesis (UNISA) at 357 – 358.

[2105] Paragraph 3.4.6 above.

[2106] Van Zyl, S. P. (2013). *The collection of Value Added Tax on online cross-border trade in Digital Goods*. Unpublished LLD thesis (UNISA) at 357 – 358.

[2107] See Van Zyl, S. P. (2013). *The collection of Value Added Tax on online cross-border trade in Digital Goods*. Unpublished LLD thesis (UNISA) at 358.

[2108] See Paragraph 7.2 above.

[2109] See Paragraph 2.8 above.

[2110] Post, D. & Cipollini, C. (2022). Fundamental elements of a blockchain-based tax system – when to use blockchain for tax? *World Tax Journal* 14(4): 572.

online databases and tax rules to ascertain the taxable base and the relevant tax rate.[2111] Taxpayers can remain tax compliant as long as the *oracle* performs its role as an agent who verifies applicable tax rules from reliable and updated databases.[2112] To contextualise this, a supplier can interact with an *oracle* using a smart contract to determine if the appropriate VAT rate has been selected. Moreover, the supplier interacts with the *oracle* to determine the *place of supply* rules for consumption purposes. *Place of supply* rules help identify the jurisdiction where the supplies are to be taxed for VAT purposes as well as the appropriate VAT rate.[2113] If *place of supply* rules are lacking, there is a possibility that a transaction can be taxed twice or not at all.[2114] If a jurisdiction does not have specific *place of supply* rules, proxies are used. For example, the VAT Act currently makes use of proxies. Once the proxies in the VAT Act[2115] have been identified and applied, the *oracle* can supply the relevant information to the supplier using a smart contract. The smart contract contains information regarding the location of the consumer and the relevant VAT rate (currently fifteen per cent) on the supply. Thereafter, the smart contract remits the relevant VAT amount to SARS in real-time. If there are changes to the VAT Act or any other VAT legislation (for example, the VAT rate increases to sixteen per cent), the online database is updated by the tax authorities in real-time. Once the rate has been amended, the *oracle* interacts with the database and each time a transaction takes place, the supplier remits the correct amount of VAT to SARS. In theory, a supplier can be compliant with various tax laws and VAT rates if the *oracle* provides accurate information. This can only happen if the tax authorities update the databases when amendments are made to the VAT laws. It should be noted that a supplier cannot identify where the transaction originates. The supplier relies on information provided by the consumer to determine the place of consumption. If the consumer provides unreliable data, this affects the VAT administration process. That is why it is important

[2111] Post, D. & Cipollini, C. (2022). Fundamental elements of a blockchain-based tax system – when to use blockchain for tax? *World Tax Journal* 14(4): 547.

[2112] Post, D. & Cipollini, C. (2022). Fundamental elements of a blockchain-based tax system – when to use blockchain for tax? *World Tax Journal* 14(4): 547.

[2113] Visser, A. (2023). "*Uncertainty over 'place of supply' rules for cross-border transactions*". Available at https://www.moonstone.co.za/uncertainty-over-place-of-supply-rules-for-cross-border-transactions/. Accessed 19 October 2023.

[2114] Visser, A. (2023). "*Uncertainty over 'place of supply' rules for cross-border transactions*". Available at https://www.moonstone.co.za/uncertainty-over-place-of-supply-rules-for-cross-border-transactions/. Accessed 19 October 2023.

[2115] Act 89 of 1991.

for the VAT Act to make provision for specific *place of supply* rules. The proxies in the VAT Act aid the supplier to ascertain whether the consumer is from South Africa. A human *oracle* can also be used to ascertain the accuracy of information supplied by a consumer by consulting relevant sources. Alternatively, a consensus *oracle* can also be employed to attain even greater accuracy due to the multiple *oracles* that are deployed. The different oracles can significantly aid tax administrators and foreign suppliers to ascertain the place of consumption, the supplier's location, and the location of the consumer.

To provide certainty, I propose that VAT rules should be harmonised internationally. This ensures that suppliers adhere to a uniform and universal set of VAT rules. In doing so, suppliers' compliance burden can be reduced which can lead to an increase in trade around the world.

Having considered the above, I recommend the following amendments to the VAT Act: The definition of 'enterprise' in the VAT Act should be amended as follows:

> (viii) the place of supply for electronic services performed by a vendor or supplier from a place in an export country is the residence of the person paying for the supply.[2116]

7.8 Concluding remarks

This thesis has considered the use of blockchain technology to collect and administer VAT on the cross-border supply of digital goods. The current collection models in the VAT Act are inefficient in so far as the collection of VAT on the cross-border supply of digital goods and services is concerned. This thesis has provided an outline for VAT to be collected on blockchain under the auspices of SARS. The implementation of blockchain does face significant challenges. This thesis provides the consideration

[2116] See ATAF (date unknown). *Value-Added Tax technical note on digital financial assets (cryptocurrencies)* at 5. Available at https://events.ataftax.org/media/documents/83/documents/vat-technical-n_49843292.pdf. Accessed 16 October 2023.

factors for policymakers in implementing blockchain technology as a VAT collection tool. It is by no means a blueprint.

The implementation of blockchain reduces the administrative burden on tax authorities and it also reduces the compliance burden on foreign suppliers. Blockchain can assist SARS to collect revenue in an efficient manner.

Blockchain is a novel technology that is continuously growing. New discoveries and features can come to the fore in years to come. Policymakers must carefully assess these new developments to ascertain if and how it can benefit revenue collection. Chapter three has also highlighted the need for countries to collaborate with each other. The implementation of blockchain cannot successfully take off without international cooperation and the development of international standards.

It is also crucial for VAT rules to be harmonised globally. VAT legislation must explicitly provide for the taxation of cross-border supplies of digital goods. These laws must contain *place of supply* rules. If the *place of supply* rules is harmonised, then the collection and administration of VAT by blockchain can also be harmonised internationally. Jurisdictions can then apply the VAT rules based on the requirements prescribed in their legislative framework.

BIBLIOGRAPHY

Books and chapters in books

Adam, K. (2022). *Blockchain Technology for Business Processes: Meaningful use of the new technology in business* (Springer Nature, Germany).

Artzt, M., & Richter, T. (eds) (2020). *Handbook of Blockchain Law: A guide to understanding and resolving the legal challenges of blockchain technology* (Kluwer Law International, the Netherlands).

Bal, A., (2019). *Taxation, Virtual Currency and Blockchain* (Kluwer Law International, The Netherlands).

Bardopoulos, A., M., (2015). *eCommerce and the effects of technology on taxation: could VAT be the eTax solution?* (Springer International Publishing, Switzerland).

Basu, S. (2007). *Global perspectives on e-commerce taxation law* (Routledge, UK).

Bennett, C., J. (1992). *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Cornell University Press, USA).

Bird, R. M. & Gendron, P. P. (2007). *The VAT in developing and transitional countries* (Cambridge University Press, New York).

Brafman, O., & Beckstrom, A., R., (2006). *The Starfish and the Spider: The unstoppable power of leaderless organizations* (Portfolio Penguin, USA).

Brito, J. (2015) *et al The Law of Bitcoin* (iUniverse, USA).

Bygrave, L., A. (2014). *Data Privacy Law: An International Perspective* (Oxford University Press, UK).

Cappiello, B., & Carullo, G., (eds) (2020). *Blockchain, Law and Governance* (Springer Nature, Switzerland).

Croome, B. (ed) *et al* (2013). *Tax Law: an introduction* (Juta & Company (Pty) Ltd, Cape Town).

Cnossen, S. (2019). *Modernizing VATs in Africa* (Oxford University Press, UK).

De Filippi, P., & Wright, A., (2018). *Blockchain and the Law: The Rule Code* (Harvard University Press, USA).

De Leeuw, K., & Bergstra, J., (eds) (2007) *The History of Information Security: A Comprehensive Handbook"* (Elsevier, UK).

Dugard, J. (2011). *International Law: A South African Perspective* (Juta & Co Ltd, Cape Town).

Ebrill, L. Keen, M. Bodin, J.P. Summers, V. (2001). *The Modern VAT* (International Monetary Fund, Washington DC).

Finck, M. (2019). *Blockchain Regulation and Governance in Europe* (Cambridge University Press, UK).

Gambetta, D. (1988). *Can We Trust Trust?* in Gambetta, D. (ed.) *Trust: Making and Breaking Cooperative Relations* (Basil Blackwell Ltd, UK).

Gries, M., Gurges, K., & Tobai, M. *Blockchain in Tax and Customs Processes* in Owens, J., & Risse, R. (eds) (2021). *Tax Law and Digitalization: The New Frontier for Government and Business: Principles, Use Cases and Outlook* (Kluwer Law International, The Netherlands).

Gudgeon, L. *et al*, *SoK: Layer-Two Blockchain Protocols* in Bonneau, J. & Heninger, N. (eds) (2020) *Financial Cryptography and Data Security* (Springer Nature, Switzerland).

Gutwirth, S. *et al* (eds) (2009). *Reinventing Data Protection?* (Springer Science Business Media, The Netherlands).

Hacioglu, U., (ed) (2019). *Blockchain Economics and Financial Market Innovation: Financial Innovations in the Digital Age* (Springer Nature, Switzerland).

Hacker, P., Lianos, L., Dimitropoulos, G., Eich, S., (eds) (2019) *Regulating Blockchain: Techno-social and Legal challenges* (Oxford University Press, New York).

Hardjono, T., Shrier, D. L., & Pentland, A. (2019). *Trusted Data: A New Framework for Identity and Data Sharing* (The MIT Press, USA).

Herian, R., (2019). *Regulating Blockchain: Critical perspectives in law and technology* (Routledge publishing, UK).

IT Governance Privacy Team (2017). *EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide* (2nd edition) (IT Governance Publishing, UK).

Kianieff, M. (2019) *Blockchain Technology and the Law Opportunities and Risks* (Routledge Publishing, UK).

Kolb, W. R. (ed) (2010). *Lessons from the financial crisis: causes, consequences and our economic future* (John Wiley & Sons Inc, New Jersey).

Lessig, L. (2006). *Code: Version 2.0* (Basic Books, USA).

Lloyd, J., I. (2011). *Information Technology Law* 6th edition (Oxford University Press, New York).

Narayanan, A., *et al* (2016). *Bitcoin and Cryptocurrency technologies: A comprehensive introduction* (Princeton University Press, USA).

Oxford Advanced Learner's Dictionary (2005) 7th edition (Oxford University Press, Oxford).

Papadopoulos, S. & Snail ka Mtuze, S. (eds) (2022). *Cyberlaw@SA: the law of the internet in South Africa* (4th edition) (Van Schaik Publishers, Pretoria).

Pienaar, C., Munro, V., van Wyk, R., & Ameer-Mia, F. (2018). *Information Technology Contracts* (LexisNexis, Johannesburg).

Rubin, P., H. & Thomas, M., L. (2002). *Privacy and the Commercial use personal information* (Springer Science & Business Media, New York).

Rumelt, R. (2017). *Good Strategy Bad Strategy: The difference and why it matters* (Profile Books Ltd, London).

Schwab, K., (2016). *The Fourth Industrial Revolution* (Crown Business Publishing, New York).

Sharrock, R. (ed) *et al* (2016). *The Law of Banking and Payment in South Africa* (Juta & Co Ltd, Cape Town).

Solove, D. J., (2004). *The digital person: technology and privacy in the information age* (New York University Press, USA).

Solove, D., J. (2008). *Understanding Privacy* (Harvard University Press, USA).

Swan, M. (2015). *Blockchain: Blueprint for a new economy* (O'Reilly Media, USA).

Tamò-Larrieux, A., (2018). *Designing for Privacy and its Legal Framework: Data Protection by Design and Default for the Internet of Things* (Springer Nature, Switzerland).

Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the technology behind bitcoin is changing money, business and the world* (Portfolio Penguin, New York).

Himma, K., E., & Tavani, H., T., (eds) (2008). *The Handbook of Information and Computer Ethics* (John Wiley & Sons Inc, USA).

Thaler, R. & Sunstein, C. (2008). *Nudge: Improving decisions about health, wealth and happiness* (Penguin Books, UK).

Vigna, P., & Casey, M., J. (2016). *The Age of Cryptocurrency: How Bitcoin and the Blockchain are Challenging the Global Economic order* (Picador, USA).

Voigt, P., & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer International Publishing, Switzerland).

Werbach, K. (2018). *The Blockchain and the New Architecture of Trust* (Massachusetts Institute of Technology Press, USA).

Wheeler, T. (2019). *From Gutenberg to Google: The History of our Future* (Brookings Institution Press, Washington).

Zambrano, R. *Using New Technologies to Improve Existing VAT/GST Systems* in Owens, J., & Risse, R. (eds) (2021). *Tax Law and Digitalization: The New Frontier for Government and Business: Principles, Use Cases and Outlook* (Kluwer Law International, The Netherlands).

Case Law

Arena Holdings (Pty) Limited t/a Financial Mail v SARS and others (CCT 365/21) [2023] ZACC 13; 2023 (8) BCLR 905 (CC); 2023 (5) SA 319.

Journal Articles

Abdulrauf, L. (2014). Do we need to bother about protecting our personal data: Reflections on neglecting data protection in Nigeria *Yonsei Law Journal* 5(2): 163 – 191.

Andhov, A. (2020). Corporations on blockchain: Opportunities & challenges *Cornell International Law Journal* 53(1): 1 – 40.

Atzori, M. (2017). Blockchain technology and decentralized governance: is the states still necessary? *Journal of Governance and Regulation* 6(1): 45 – 62.

Azam, R. & Mazur, O. (2019). Cloudy with a chance of taxation *Florida Tax Review* 22(2): 500 – 570.

Bacon, J., Millard, C., & Singh, J. (2018). Blockchain Demystified: A technical and Legal Introduction to Distributed and Centralised Ledgers *Richmond Journal of Law & Technology* 25(1): 1 – 106.

Bacon, J. *et al* (2017). Blockchain Demystified *Queen Mary University of London, School of Law Legal Studies Research Paper No. 268/2017* 2 - 53. Available https://papers.ssrn.com/sol3/papers.cfm?Abstract_id=3091218. Accessed 5 January 2020.

Bal, A. (2019). Developing a regulatory framework for the taxation of virtual currencies *Intertax* 47(2): 219 – 233.

Basu, S. (2004). E-government and developing countries: an overview *International Review of Law, Computers & Technology* 18(1): 109 – 132.

Basu, S. (2008). International taxation of e-commerce: persistent problems and possible developments *Journal of Information Law and Technology* at 7 - 20.

Basu, S. (2004). To tax or not to tax? That is the question? Overview of options in consumption taxation of e-commerce *The journal of information, law and technology* Vol 1 1 – 25.

Beling, C. T. (1983). Transborder Data Flows: International Privacy Protection and the Free Flow of Information *Boston College International and Comparative Law Review* 6(2): 591 – 624.

Belu, G. M. (2020). Blockchain Technology and Customs Procedures *The Romanic Economic Journal* Year XXIII issue 78: 13 – 26.

Berberich, M. & Steiner, M. (2016). Blockchain technology and the GDPR - how to reconcile privacy and distributed ledgers *European Data Protection Law Review* 2(3): 422-426.

Beretta, G. (2018). "VAT and the Sharing Economy" *World Tax Journal* 10(3): 381 – 425.

Bird, M. R. and Zolt M., E. (2008). Technology and taxation in developing countries: from hand to mouse *National Tax Journal* 61(4): Part 2 791 – 821.

Birnhack, M., D. (2008). The EU Data Protection Directive: An engine of a global regime *Computer Law & Security Review* 24(6): 508 – 520.

Bitjoka, G. B. & Edoa, M., M., N. (2020). Blockchain in the Implementation of VAT Collection *American Journal of Computer Science and Technology* 3(2): 18 – 26.

Borking, J. J. & Raab, C. D. (2001). Laws, PETs and Other Technologies for Privacy Protection *The Journal of Information, Law and Technology* 2001(1) 1 – 13.

Brinkerhoff, D., W. (2000). "Assessing political will for anti-corruption efforts: an analytic framework" *Public Administration and Development* 20(3): 239 – 252.

Bygrave, L. A. (1998). Data protection pursuant to the right to privacy in human rights treaties *International Journal of Law and Information Technology* 6(3): 247 – 284.

Cannas, F. (2017). Sharing economy: Everyone can be an entrepreneur for two days…but what about a VAT taxable person? *World Journal of VAT* 6(2): 82 – 99.

Cassim, F. (2015). Protecting Personal Information in the era of Identity Theft: Just How Safe is our Personal Information from identity thieves? *Potchefstroom Electronic Law Journal* 18(2): 69 – 110.

Chang, Y. *et al* (2020). Blockchain in global supply chains and cross-border trade: a critical synthesis of the state-of-the-art, challenges and opportunities International *Journal of Production Research* 58(7): 2082 – 2099. Available at https://doi.org/10.1080/00207543.2019.1651946. Accessed 25 September 2022.

Ciocchetti, C. A. (2007). E-commerce and information privacy: Privacy policies as personal information protectors *American Business Law Journal* 44(1): 55 – 126.

Cockfield, A. J. 2010. "Protecting Taxpayer Privacy Rights Under Enhanced Cross-border Tax Information Exchange: Toward A multilateral Taxpayer Bill of Rights" *UBC Law Review* 42(2): 419 – 471.

Cockfield, J. A (2002). The law and Economics of digital taxation: challenges to traditional tax laws and principles *Bulletin for International Fiscal Documentation* 56(12): 606 – 619.

Coetzee, L. & Meiring, M. (2016). Value-Added Tax on imported electronic services: A critical evaluation of the newly enacted South African legislation *Journal of Economic and Financial Sciences* 9(1): 28 – 42.

Debelva, F. & Mosquera, I. (2017). “Privacy and Confidentiality in Exchange of Information Procedures: Some Uncertainties, Many Issues but Few Solutions” *Intertax* 45(5): 362 – 381.

De Filippi, P. (2016). The interplay between decentralization and privacy: the case of blockchain technologies *Journal of Peer Production Alternative Internets* 1 – 18.

De Filippi, P. & Hassan, S. (2016) *Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code***.** Available at https://arxiv.org/ftp/arxiv/papers/1801/1801.02507.pdf. Accessed 19 December 2019.

Duarte, D. G. (2019). An Introduction to Blockchain Technology from a Legal Perspective and Its Tensions With the GDPR *Cyberlaw Journal of the Cyberlaw Research Centre of the University of Lisbon School of Law 2019* 1 – 58. Available at SSRN: https://ssrn.com/abstract=3545331. Accessed 5 February 2021.

Duperrut, J., Thevoz, P., Ilves, L., Migai, C. & Owens, J. (2019). Why – and How – African Countries Should Use Technology for Automatic Information Exchange *Tax Notes International* 96(2): 919 – 925.

Emigh, A. (2006). The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond *Journal of Digital Forensic Practice* 1(3): 245 – 260.

Erbguth, J. (2019). Five ways to GDPR-compliant use of blockchains *European Data Protection Law Review* 5(3): 427 – 433.

Fairfield, J. (2014). Smart Contracts, Bitcoin Bots, and Consumer Protection *Washington and Lee Law Review Online* 71: 33 – 50.

Finck, M. (2018). Blockchains and data protection in the European Union *European Data Protection Law Review* 4(1): 17 – 35.

Finck, M. (2018). Blockchains: Regulating the Unknown *German Law Journal* 19(4): 665 – 691.

Finck, M. & Pallas, F. (2020). They who must not be identified – distinguishing personal from non-personal data under the GDPR *International Data Privacy Law Journal* 10(1): 11 – 36.

Fritz, C. (2021). South African Taxpayer's Right to Privacy in Cross-Border Exchange of Tax Information *Constitutional Court Review* 11(1): 411 – 432.

Gabison, G. (2016). Policy Considerations for the Blockchain Technology Public and Private Applications *SMU Science and Technology Law Review* 19(3): 327 – 350.

Gjems-Onstad, O. (2013). Cross-border electronic services and the need for international cooperation: the Norwegian experience *World Journal of VAT/GST Law* 2(3) 243 – 252.

Grayson, B. (2006). Personal Information in Government Records: Protecting the Public Interest in Privacy *Saint Louis University Public Law Review* 25(1): 63 – 121.

Groos, D. & van Veen, E. (2020). "Anonymised Data and the Rule of Law" *European Data Protection Law Review* 6(4): 498 – 508.

Gutuza, T. (2010). Tax and e-commerce: where is the source *South African Law Journal* 127(2): 328 – 338*.*

Hondius, F. W. (1980). Data Law in Europe *Stanford Journal of International Law* (16): 87 – 111.

Huckle, S. *et al* (2016). Internet of things, Blockchain and Shared Economy applications *Procedia Computer Science* 98: 461 – 466.

Jimenez-Gomez, B. (2020). Risks of blockchain for data protection: European approach *Santa Clara High Technology Law Journal* 36(3): 281 – 343.

Kabwe, R. (2020). The VAT Treatment of Cryptocurrencies in South Africa: Lessons from Australia *Obiter* 41(4): 767 – 786.

Kabwe, R. & van Zyl, S.P. (2021). The value-added tax in the digital economy: a fresh look at the South African dispensation *Obiter* 42(3): 499 – 528.

Kianieff, M. (2012) The Evolution of Consumer Privacy Law: How Privacy by Design Can Benefit from Insights in Commercial Law and Standardization *Canadian Journal of Law and Technology* 10(1): 1 – 28.

Kim, Y. (2022). Blockchain initiatives for tax administration *University of California Los Angeles Law Review* 69(1): 240 – 317.

Kiviat, T. I. (2015). Beyond bitcoin: Issues in regulating blockchain transactions *Duke Law Journal* 65(3): 569 – 608.

Knittel, M., Pitts, S., & Wash R. (2019) *The Most Trustworthy Coin: How Ideology Builds and Maintains Trust in Bitcoin* Proceedings of the ACM Human Computer Interact Vol 3, CSCW, Article 36 (November 2019) 1 – 23. https://doi.org/10.1145/3359138. Accessed 15 December 2019.

Kerber, W. & Schweitzer, H. (2017). Interoperability in the digital economy *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 8(1): 39 – 58.

Lamensch, M. (2012). Are reverse charging and the one-stop-scheme efficient ways to collect VAT on digital supplies? *World Journal of VAT/GST Law* 1(1): 1 – 20.

Ligthart, J. E. (2004). Consumption Taxation in a Digital World: A Primer *CentER Discussion Paper* Vol. 2004-102. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=625044. Accessed 10 December 2022.

Lynch, J. (2005). Identity theft in cyberspace: Crime control methods and their effectiveness in combating phishing attacks *Berkeley Technology Law Journal* 20(1): 259 – 300.

Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique *Big Data and Society* 1 – 13. Available at https://journals.sagepub.com/doi/pdf/10.1177/2053951714541861. Accessed 5 August 2020.

Mai, J. E. (2016). Big data privacy: The datafication of personal information *The Information Society* 32(3): 192 – 199. Available at https://doi.org/10.1080/01972243.2016.1153010. Accessed 5 July 2020.

Makulilo, A. B. (2012). Privacy and data protection in Africa: a state-of-the-art *International Data Privacy Law* 2(3): 163 – 178.

Makulilo, A. B. (2017). The GDPR implications for data protection and privacy protection in Africa *International Journal for the Data Protection Officer, Privacy Officer and Privacy Counsel* 1(2): 12 – 19.

Mayer, R., C., Davis, J., H., and Schoorman, F., D. (1995). An Integrative Model of Organizational Trust *The Academy of Management Review* Vol 20(3) 709 – 734.

McClurg, A. J. (2003). A thousand words are worth a Picture: A Privacy tort response to consumer data profiling *Northwestern University Law Review* 98(1): 63 – 144.

Meijas, U. A. & Couldry, N. (2019). Datafication *Internet Policy Review* 8(4): 1 – 10.

Melnyk, R. & Barikova, A. (2019). Cross-border public administration: Prospects for introducing blockchain jurisdiction *Informatologia* 52 1-2, 74 – 89.

Merkx, M. (2019). VAT and Blockchain: Challenges and Opportunities Ahead *EC Tax Review* 28(2): 83 – 89.

Merkx, M. & Verbaan, N. (2019). Technology: A key to solve VAT Fraud? *EC Tax Review* 28(6) at 300 – 306.

Millar, R. (2008) Jurisdictional Reach of VAT *University of Sydney Law School*: Legal research paper 8(64): 175. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1162510. Accessed on 2 April 2017.

Milne, G. *et al* (2004). Consumers' Protection of Online Privacy and Identity *The Journal of Consumer Affairs* 38(2): 217 – 232.

Mirchandani, A. (2019). The GDPR-blockchain paradox: exempting permissioned blockchains from the GDPR *Fordham Intellectual Property, Media & Entertainment Law Journal* 29(4): 1201 – 1241.

Moerel, L. (2019). Blockchain & Data Protection…and Why They Are Not on a Collision Course *European Preview of Private Law* 26(6): 825 – 852.

Moosa, F. (2020) Does the Bill of Rights Apply Extraterritorially for Tax Administration Purposes? *Stellenbosch Law Review* 31(1): 37 – 54.

Muller, R. (2020). Proposal for an Automated Real-Time VAT Collection Mechanism in B2C E-Commerce Using Blockchain Technology *International VAT Monitor* 31(3): 135 – 138.

Murphy, R. S. (1996). Property rights in personal information: An economic defense of privacy *Georgetown Law Journal* 84: 2381 – 2418.

Owens, J. & De Jong, J. (2017). Taxation on the Blockchain: Opportunities and Challenges *Tax Notes International* 87(6): 601 – 612.

Owens, J. & Hodžić, S. (2022). Blockchain technology: potential for digital tax administration *Intertax* Vol 50(11): 813 – 823.

Perl, M. W. (2003). It's not always about the money: Why the state identity theft laws fail to adequately address criminal record identity theft *Journal of Criminal Law & Criminology* 94(1): 169 – 208.

Post, D. & Cipollini, C. (2023). Fundamental Elements of a Blockchain-Based Tax System: Governance, Legal and Technology Aspects *World Tax Journal* 15(3): 5. [unpublished version]

Post, D. & Cipollini, C. (2022). Fundamental elements of a blockchain-based tax system – when to use blockchain for tax? *World Tax Journal* 14(4): 519 – 572.

Potnuru, M. (2012). Limits of the Federal Wiretap Act's Ability to Protect Against Wi-Fi Sniffing *Michigan Law Review* 111(1): 89 – 117.

Prewet K., W, Prescott G., L, Phillips K. (2020) Blockchain adoption is inevitable—Barriers and risks remain *Journal of Corporate Accounting & Finance* 31: 21 – 28. Available at https://doi.org/10.1002/jcaf.22415. Accessed 5 May 2021.

Roos, A. (2006). Core principles of data protection law *Comparative and International Law Journal of Southern Africa* 39(1): 102 – 130.

Roos, A. (2007). Data protection: Explaining the international backdrop and evaluating the current South African position *South African Law Journal* 124(2): 400 – 433.

Rosen, J. (2012). The Right to Be Forgotten *Stanford Law Review Online* 64: 88 – 92.

Sapienza, P. & Zingales, L. (2012). "A Trust crisis" *International Review of Finance* 12(2):123 – 131. Available at https://doi.org/10.1111/j.1468-2443.2012.01152.x. Accessed 2 March 2020.

Schaar, P. (2010). "Privacy by Design" *Identity in the Information Society* (3) at 267 – 274. Available at https://doi.org/10.1007/s12394-010-0055-x. Accessed 14 June 2022.

Schwartz, P. (1992). Data Processing and Government Administration: The Failure of the American Legal Response to the Computer *Hastings Law Journal* 43(5): 1321 – 1389.

Setyowati, M. S. *et al* (2020). Blockchain Technology Application for Value-Added Tax Systems *Journal of Open Innovation: Technology, Market and Complexity* 6(156): 1 – 27.

Setyowati, M. S. *et al* (2023). Strategic factors in implementing blockchain technology in Indonesia's value-added tax system *Technology in Society* (72): 102169.

Solove, D. J. (2002). Access and aggregation: Public records, privacy and the constitution *Minnesota Law Review* 86(6): 1137 – 1218.

Solove, D. J. (2002). Identity theft, privacy, and the architecture of vulnerability *Hastings Law Journal* 54(4): 1227 – 1276.

Solove, D. J. (2001). Privacy and power: Computer databases and metaphors for information privacy *Stanford Law review* 53(6): 1393 – 1462.

Solove, D. J. (2006). Taxonomy of privacy *University of Pennsylvania Law Review* 154(3): 477 – 564.

Steyn, T. (2010). VAT and e-commerce: still looking for answers? *South African Mercantile Law Journal* 22(2): 230 – 258.

Sullins, L. L. (2006). Phishing for solution: Domestic and international approaches to decreasing online identity theft *Emory International Law Review* 20(1): 397 – 434.

Tavani, H. T. (1999). Informational privacy, data mining, and the Internet *Ethics and Information Technology* 1 137 – 145.

Temte, M. N. (2019). "Blockchain challenges traditional contract law: Just how are smart contracts" *Wyoming Law Review* 19(1): 87 – 118.

Van der Merwe, B. A. (2003). VAT and e-commerce *South African Mercantile Law Journal* 15(3): 371 – 387.

Van Dijk, J. (2014). Datafication, dataism and dataveillance: Big Data between paradigm and ideology *Surveillance and Society* 12(2): 197 – 208.

Volokh, E. (1999). Freedom of speech and information privacy: The troubling implications of a right to stop people from speaking about you *Stanford Law Review* 50(5): 1049 – 1124.

Warren, S. D. & Brandeis, L., D., (1890). The right to privacy *Harvard Law Review* 4(5): 193 – 220.

Westin, A. F. (1966) Science, Privacy, and Freedom: Issues and Proposals for the 1970's. Part I--The Current Impact of Surveillance on Privacy *Columbia Law Review* 66(6): 1003 – 1050.

Winn, J. & Wrathall, J. R. (2000). Who owns the customer the emerging law of commercial transactions in electronic customer data *Business Lawyer* (ABA) 56(1): 213 – 272.

Yilma, K. M. (2019) The United Nations data privacy system and its limits *International Review of Law, Computers & Technology* 33(2): 224-248.

Ziegeldorf, J. H., Morchon, O., G., & K., Wehrle (2013). Privacy in the Internet of Things: Threats and challenges *Security and Communications Network* 7 2728 – 2742.

Legislation

(Australia)

A New Tax System (Goods and Services Tax) Act 1999.

Australian Tax and Superannuation Laws Amendment (2016 Measures No 1) Act 2016 (52 of 2016).

(European Union)

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

The General Data Protection Regulation.

(Italy)

Article 8 *ter* of Law Decree No. 135 of 14 December 2018.

(South Africa)

Bank's Act 94 of 1990.

Birth and Death Registration Act 51 of 1992.

Companies Act 71 of 2008.

Copyright Act 98 of 1978.

Customs and Excise Act 91 of 1964.

Electronic Communications and Transactions Act 25 of 2002.

Government Gazette No. 36433 (10 May 2013).

Government Gazette No. 38405 (20 January 2015).

Government Gazette No. 37067 (26 November 2013).

Identification Act 68 of 1997.

Income Tax Act 58 of 1962.

Promotion of Administrative Justice Act 3 of 2000.

Promotion of Access to Information Act 2 of 2000.

The Constitution of the Republic of South Africa, 1996.

The Protection of Personal Information Act 4 of 2013.

Tax Administration Act 28 of 2011.

Value Added Tax Act 89 of 1991.

(The United States of America)

The Foreign Account Tax Compliance Act.

Reports

Ainsworth, R., T. & Alwohaibi, M. (2017). Blockchain, Bitcoin and VAT in the GCC: The Missing Trader Example *Boston University School of Law, Law & Economics Working Paper No. 17-05* at 8. Available at http://www.bu.edu/law/files/2017/03/BLOCKCHAIN-BITCOIN-VAT-in-the-GCC.pdf. Accessed 21 May 2021.

Article 29 Data Protection Working Party Opinion 05/2012 on Cloud Computing (WP 196). Available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf. Accessed 9 February 2021.

ATAF (date unknown). *Value-Added Tax technical note on digital financial assets (cryptocurrencies)* at 5. Available at https://events.ataftax.org/media/documents/83/documents/vat-technical-n_49843292.pdf. Accessed 16 October 2023.

Baker, P. & Pistone, P. (2015). *General Report, The Practical Protection of Taxpayers' Fundamental Rights* (IFA Cahiers 2015 – Volume 100B) (SDU publishing, the Hague).

Bank of England (2020). *Central bank digital currency: opportunities, challenges and design* Future of Money Discussion Paper. Available at https://www.bankofengland.co.uk/-/media/boe/files/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design.pdf. Accessed 30 December 2022.

Clarke, R. (1994). *The Digital Persona and its Application to Data Surveillance*. Available at http://www.rogerclarke.com/DV/DigPersona.html#DV. Accessed 5 August 2020.

Chang, H., (2017). *Blockchain: Disrupting data protection?* Privacy Law and Business International Report University of Hong Kong Faculty of Law Research Paper No. 2017/041 at 2. Available at SSRN: https://ssrn.com/abstract=3093166. Accessed 22 September 2020.

Christl, W., (2017). How Companies use personal data against people: Automated disadvantage, personalized persuasion, and the societal ramifications of the commercial use of personal information *working paper by Cracked Labs*. Available at https://crackedlabs.org/dl/CrackedLabs_Christl_DataAgainstPeople.pdf. Accessed 16 July 2020.

Data Protection Working Party (2014). "Opinion 05/2014 on Anonymisation Techniques" *Article 29 Data Protection Working Party EU* at 2 – 11. Available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. Accessed 22 September 2020.

Davis Tax Committee (2014). *Addressing Base Erosion and profit shifting in South Africa: Davis Tax Committee interim report.* Available at http://www.taxcom.org.za/docs/New_Folder/2%20DTC%20BEPS%20Interim%20Report%20on%20Action%20Plan%201%20-%20Digital%20Economy,%202014%20deliverable.pdf. Accessed 18 March 2019.

De Filippi, P. & McMullen, G. (2018). "Governance of blockchain systems: Governance of and by distributed infrastructure" *Blockchain Research Institute and COALIA*. Available at https://hal.science/hal-02046787/document. Accessed 15 October 2023.

Deutsche Energie-Agentur (Publisher) (dena, 2023) "Rethinking Blockchain's Electricity Consumption – A Guide to Electricity- Efficient Design of Decentralized Data-Infrastructure". Available at https://www.dena.de/fileadmin/dena/Publikationen/PDFs/2023/Guide_Rethinking_Blockchain_s_Energy_Consumption.pdf. Accessed 22 June 2024.

Financial Conduct Authority (2017). *Discussion Paper on distributed ledger technology*. Available at https://www.fca.org.uk/publication/discussion/dp17-03.pdf. Accessed 23 August 2022.

GAO (2002). *Identity Theft: Greater Awareness and Use of Existing Data Are Needed*. Available at https://www.gao.gov/assets/240/234959.pdf. Accessed 6 August 2020.

Green paper on electronic commerce for South Africa (2000). Available at https://www.gov.za/sites/default/files/gcis_document/201409/electroniccommerce1.pdf. Accessed 17 March 2019.

Information and Privacy Commissioner Ontario (2009). *Privacy by Design*. Available at https://www.ipc.on.ca/wp-content/uploads/2013/09/pbd-primer.pdf. Accessed 27 April 2022.

KPMG. (2017). *VAT/GST treatment of cross-border services*. Available at https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2017/11/ess-survey-13-nov-17.pdf. Accessed 19 March 2018.

OECD (2012). *Automatic Exchange of Information: What it is, How it works, Benefits, What remains to be done*. Available at https://www.oecd.org/ctp/exchange-of-tax-information/automatic-exchange-of-information-report.pdf. Accessed 27 January 2022.

OECD (2017). *Mechanisms for the effective collection of VAT/GST*. https://www.oecd.org/tax/tax-policy/mechanisms-for-the-effective-collection-of-VAT-GST.pdf. Accessed 29 March 2019.

OECD (2022). *Measuring the Information Economy*. Available at https://www.oecd.org/sti/ieconomy/1835738.pdf. Accessed 10 December 2022.

OECD (2005). *Facilitating collection of consumption taxes on business-to-consumer cross-border e-commerce transactions*. Available https://www.oecd.org/tax/consumption/34422641.pdf. Accessed 10 June 2017.

OECD (2017). *International VAT/GST Guidelines*. Available at https://www.oecd-ilibrary.org/docserver/9789264271401-en.pdf?expires=1553858743&id=id&accname=guest&checksum=548681052C34CEC274E3A3887BFCB279. Accessed 29 March 2019.

OECD (2000). *Report by the Technology Technical Advisory Group*. Available at http://www.oecd.org/tax/consumption/1923248.pdf. Accessed 8 March 2017.

OECD (2008). *Scoping Paper on Online Identity Theft*. Available at http://www.oecd.org/internet/consumer/40644196.pdf. Accessed 6 August 2020.

OECD (2013). *The OECD Privacy Framework*. Available at http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. Accessed 12 December 2020.

Office of the Privacy Commissioner of Canada (2017). *Privacy Enhancing Technologies – A Review of Tools and Techniques*. Available at https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/pet_201711/#fn6. Accessed 27 April 2022.

PWC (2016). *How blockchain technology could improve the tax system*. Available at https://www.pwc.co.uk/issues/futuretax/assets/documents/how-blockchain-could-improve-the-tax-system.pdf. Accessed 24 March 2021.

PWC (2017). *VAT compliance: the impact on business and how technology can help*. Available at https://www.pwc-tls.it/it/assets/docs/pwc-vat-compliance-paying-taxes-2017.pdf. Accessed 17 November 2017.

SARS (2023). *Discussion Paper: Value-Added Tax Modernisation*. Available at https://www.sars.gov.za/wp-content/uploads/Docs/VAT/Discussion-Paper-on-Value-Added-Tax-Modernisation.pdf. Accessed 4 October 2023.

SARS and National Treasury (2023). *Tax statistics 2023*. Available at https://www.sars.gov.za/wp-content/uploads/2023-Tax-Statistics-Main-Publication-compressed.pdf. Accessed 7 June 2024.

UK Government Chief Scientific Adviser (2016). *Distributed Ledger Technology: Beyond Block Chain* (London: Government Office for Science) (Blackett Review). Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf. Accessed 11 December 2022.

Vienna University of Economics and business (2017). *Blockchain: taxation and regulatory challenges and opportunities*. Available at https://www.wu.ac.at/fileadmin/wu/d/i/taxlaw/institute/WU_Global_Tax_Policy_Center/Tax___Technology/Backgrd_note_Blockchain_Technology_and_Taxation_03032017.pdf. Accessed 23 March 2019.

World Economic Forum (2020). *Global Standards Mapping Initiative: An overview of blockchain technical standards*. Available at https://www3.weforum.org/docs/WEF_GSMI_Technical_Standards_2020.pdf. Accessed 26 August 2023.

Zyskind, G., Nathan, O. & Pentland, A. (2015). *Enigma: Decentralized Computation Platform with Guaranteed Privacy*. Available at https://arxiv.org/pdf/1506.03471.pdf. Accessed 3 July 2022.

Master's and Doctoral Theses

Abdulrauf, L. A. (2015). *The Legal Protection of Data Privacy in Nigeria: Lessons from Canada and South Africa* Unpublished LLD thesis (University of Pretoria).
Bal, M., A. (2014). *Taxation of virtual currency* PhD thesis (University of Leiden).

Bardopoulos, M. A. (2012). *The impact of technology on taxation and is VAT the eTax solution?* PhD thesis University of Cape Town.

Kabwe, K., R. (2017). *Consumption tax collection models in online trade in digital goods* unpublished LLM mini dissertation (UNISA).

Lidstrom, C. (2020). *EU VAT and the sharing economy: The relationship between the concept of "taxable person" and Airbnb and Uber* unpublished LLM thesis (Uppsala Universitet).

Lubbe, H. (2015). *Alternatives to the enforceability of VAT on imported digital purchases in South Africa*. Unpublished LLM mini dissertation (North West University of South Africa).

Makulilo, A. B. (2012). *Protection of Personal Data in sub-Saharan Africa* published *Dr Jur* thesis (Universität Bremen).

Manrique, S. (2018). *Blockchain: A Proof of Trust* Master thesis (Delft University of Technology).

Miller, A. (2019). *Data protection on blockchain in the context of the General Data Protection Regulation* Master's thesis (University of Tartu).

Moller, L. (2016). *An analysis of the current framework for the exchange of taxpayer information, with special reference to the taxpayer in South Africa's constitutional rights to privacy and just administrative action* MCom mini dissertation (University of Cape Town).

Ramsey, S. (2018). *The General Data Protection Regulation vs The Blockchain – A legal study on the compatibility between blockchain technology and the GDPR* Thesis in Law and Informatics (Stockholm University).

Roberta, F. (2017). *Blockchain and individuals' control over personal data in European data protection law* Master's thesis (Tilburg University).

Roos, A. (2003). *The law of data (privacy) protection: a comparative and theoretical study* (unpublished LLD thesis, UNISA).

Van Zyl, S. P. (2013). *The collection of Value Added Tax on online cross-border trade in Digital Goods*. Unpublished LLD thesis (UNISA).

Websites

Accenture (2016). “Accenture Debuts Prototype of ‘Editable’ Blockchain for Enterprise and Permissioned Systems”. Available at https://newsroom.accenture.com/news/accenture-debuts-prototype-of-editable-blockchain-for-enterprise-and-permissioned-systems.htm. Accessed 13 August 2023.

Accenture (2017). *Accenture, Microsoft create Blockchain Solution to support ID2020*. Available at https://newsroom.accenture.com/news/accenture-microsoft-create-blockchain-solution-to-support-id2020.htm. Accessed 24 September 2020.

Accenture (2016). “*Editing the Uneditable Blockchain: Why distributed ledger technology must adapt to an imperfect world”* Accenture at 7*.* Available at https://www.accenture.com/_acnmedia/pdf-33/accenture-editing-uneditable-blockchain.pdf. Accessed 30 June 2020.

Ainsworth, R. T., Alwohaibi, M., Cheetham, M., & Tirand, C., V. (2018). A VATCoin Solution to MTIC Fraud: Past Efforts, Present Technology and the EU’s 2017 Proposal *Boston University Scool of Law, Law and Economics Research Paper No. 18-08*. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3151394. Accessed 24 May 2021.

Ainsworth, R., T. & Alwohaibi, M. (2017). Blockchain, Bitcoin and VAT in the GCC: The Missing Trader Example *Boston University School of Law, Law & Economics Working Paper No. 17-05*. Available at http://www.bu.edu/law/files/2017/03/BLOCKCHAIN-BITCOIN-VAT-in-the-GCC.pdf. Accessed 21 May 2021.

Ainsworth, R., T. & Todorov, G. (2013). *DICE – Digital Invoice Customs Exchange* Boston University School of Law Working Paper No 13-40. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2314478. Accessed 15 July 2021.

Ainsworth, R. T. & Madzharova, B. (2012). “Real-Time Collection of the Value-Added Tax: Some Business and Legal Implications” *Boston University School of Law, Law and Economics Research paper* 12-51. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2166316. Accessed 26 March 2021.

Ainsworth, R., T., Alwohaibi, M., & Cheetham, M. (2016). *VATCOIN: The GCC’s Cryptotaxcurrency*. Available at https://www.law.upenn.edu/live/files/5955-gcc-vatcoin.pdf. Accessed 9 April 2021.

AWS (2023). *What is an API (Application Programming Interface)?* Available at https://aws.amazon.com/what-is/api/#:~:text=API%20stands%20for%20Application%20Programming,of%20service%20between%20two%20applications. Accessed 24 August 2023.

Baghla, S. (2017). *Origin of Bitcoin: A brief history from 2008 crisis to present times*. Available at https://www.analyticsindiamag.com/origin-bitcoin-brief-history/. Accessed 7 September 2019.

Batmunkh, D. (2018). *Private blockchain consensus mechanisms*. Available at https://medium.com/@arigatodl/private-blockchain-consensus-mechanisms-8e6fc48c8fb. Accessed 10 June 2024.

Beniiche, A. (2020). *A study of blockchain oracles*. Available at https://arxiv.org/pdf/2004.07140.pdf. Accessed 18 October 2023.

Binamite (2023). *5 blockchain layers you should know in 2023*. Available at https://binamite.com/blockchain-layers/. Accessed 16 October 2023.

Bird & Bird. *Private Blockchains*. Available at https://www.twobirds.com/~/media/pdfs/in-focus/blockchain/private-blockchain-briefing-note.pdf. Accessed 26 April 2021.

Bitcoin. Available at https://bitcoin.org/en/vocabulary#bit. Accessed 23 August 2022.

Bitstamp Learn (2022). *What is block size?* Available at https://www.bitstamp.net/learn/crypto-101/what-is-block-size/#:~:text=The%20size%20of%20a%20block,as%20the%20block%20size%20limit. Accessed 24 August 2023.

Blake Finucane (2019) *Bitcoin Market Cycles and Price Swings – What You Need to Know*. Available at https://financial-news-now.com/bitcoin-market-cycles-and-price-swings-what-you-need-to-know/. Accessed 24 February 2020.

Blockchain Bundesverband (2018). *Blockchain, Data protection and GDPR*. Available at https://www.bundesblock.de/wp-content/uploads/2019/01/GDPR_Position_Paper_v1.0.pdf. Accessed 21 September 2020.

Blockchain Smart Solutions (2023). *Public vs Private Blockchains: Which one id the best for your business?* Available at https://www.linkedin.com/pulse/public-vs-private-blockchains-which-one-best#:~:text=Transaction%20speed%3A,limited%20number%20of%20authorized%20entities. Accessed 4 October 2023.

Bossa, G. & de Paiva Gomes, E. (2019). *Blockchain: Technology as a Tool for Tax information Exchange or an instrument Threatening the Taxpayer's Privacy?* Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3540277. Accessed 19 July 2019.

BSI (2017). *Distributed Ledger Technologies/Blockchain: Challenges, opportunities and the prospects for standards*. Available at https://www.bsigroup.com/LocalFiles/zh-tw/InfoSec-newsletter/No201706/download/BSI_Blockchain_DLT_Web.pdf. Accessed 13 June 2021.

Businesstech staff writer (2020). *It's time to change the way our VAT system works*. Available at https://businesstech.co.za/news/finance/386705/its-time-to-change-the-way-our-vat-system-works-tax-expert/. Accessed 6 April 2021.

Businesstech staff Writer (2018). *What you need to know before writing or developing code in South Africa*. https://businesstech.co.za/news/it-services/257135/what-you-need-to-know-before-writing-or-developing-code-in-south-africa/. Accessed 3 May 2021.

Buterin, V. (2015). *On Public and Private Blockchains*. Available at https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/. Accessed 8 January 2020.

Buterin, V. (2015). *Privacy on the Blockchain*. Available at https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/. Accessed 24 September 2020.

Caron, F. (2017). *Blockchain: Identifying Risk on the Road to Distributed Ledgers*. Available at https://www.isaca.org/resources/isaca-journal/issues/2017/volume-5/blockchain-identifying-risk-on-the-road-to-distributed-ledgers. Accessed 8 May 2021.

Catalinin, C. & Gans, J., S. (2016). "Some Simple Economics of the Blockchain". Available at https://ccl.yale.edu/sites/default/files/files/SSRN%20--%20Some%20Simple%20Economics%20About%20Blockchain.pdf. Accessed 16 April 2021.

Child, K. (2022). *TransUnion ordered to inform those whose information was compromised in hack*. Available at https://www.businesslive.co.za/bd/national/2022-03-25-transunion-ordered-to-inform-those-whose-information-was-compromised-in-hack/. Accessed 4 April 2022.

Christl, W. (2017). *Corporate Surveillance in Everyday Life. How Companies Collect, Combine, Ana-lyze, Trade, and Use Personal Data on Billions* Report by Cracked Labs June 2017. Available at: http://crackedlabs.org/en/corporate-surveillance. Accessed 18 July 2020.

Commission Nationale de l'informatique et de Libértes (2018). *Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data*. Available at https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data. Accessed 20 September 2020.

CoE (1981). *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. Available at https://rm.coe.int/1680078b37. Accessed 13 December 2020.

CoE (1973). *Resolution on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector*. Available at https://rm.coe.int/1680502830. Accessed 14 December 2020.

CoE (1974). *Resolution on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector*. Available at https://rm.coe.int/16804d1c51. Accessed 14 December 2020.

Compuscan. https://compuscan.co.za/2020/02/17/how-a-credit-bureau-affects-financial-inclusion/. Accessed 17 July 2020.

Council of Europe. Available at https://www.coe.int/en/web/about-us/who-we-are. Accessed 13 December 2020.

Corruption Watch (2019). *Trust inequality at all-time high globally*. https://www.corruptionwatch.org.za/trust-inequality-at-all-time-high/. Accessed 19 December 2019.

Crypton Studio (2022). *Frontend developer on a blockchain project*. Available at https://medium.com/coinmonks/frontend-developer-on-a-blockchain-project-9d0c496fd38. Accessed 20 August 2023.

Deer, M. (2023). *How to check an Ethereum transaction*. Available at https://cointelegraph.com/news/how-to-check-an-ethereum-transaction#:~:text=How%20long%20does%20an%20Ethereum,at%20the%20time%20of%20processing. Accessed 21 August 2023.

De la Feria, R. & Schoeman, A. (2019). Addressing VAT fraud in developing countries: the tax policy-administration symbiosis. Available at https://repository.up.ac.za/bitstream/handle/2263/77923/DelaFeria_Addressing_2019.pdf?sequence=1. Accessed 29 December 2022.

Deloitte (2016). *Blockchain Enigma Paradox Opportunity*. Available at https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-blockchain-full-report.pdf. Accessed 13 June 2021.

Deloitte (2017). *Blockchain technology and its potential in taxes*. Available https://www2.deloitte.com/content/dam/Deloitte/pl/Documents/Reports/pl_Blockchain-technology-and-its-potential-in-taxes-2017-EN.PDF. Accessed 14 January 2020.

Deloitte (2019). *Blockchain: Legal implications, questions, opportunities and risks*. Available at https://www2.deloitte.com/content/dam/Deloitte/za/Documents/legal/za_legal_implications_of_blockchain_14052019.pdf. Accessed 14 January 2020.

Deloitte (2017). *Blockchain Technology and its potential in taxes*. Available at https://www2.deloitte.com/content/dam/Deloitte/pl/Documents/Reports/pl_Blockchain-technology-and-its-potential-in-taxes-2017-EN.PDF. Accessed 6 May 2021.

De Meijer, C. R. W. (2016). *Blockchain versus GDPR and who should adjust most*. Available at https://www.finextra.com/blogposting/16102/blockchain-versus-gdpr-and-who-should-adjust-most. Accessed 19 April 2022.

Delmotte, C. (2022). *The Promises and Pitfalls of a Blockchain Driven Tax System*. Available at https://ssrn.com/abstract=4187919. Accessed 6 October 2022.

Dog, D. (2021). *How long does a Bitcoin Transaction Take?* Available at https://coinmarketcap.com/alexandria/article/how-long-does-a-bitcoin-transaction-take#:~:text=little%20bit*%20longer.-,How%20Long%20Does%20Bitcoin%20Take%20to%20Send%3F,activity%2C%20hashrate%20and%20transaction%20fees. Accessed 21 August 2023.

Eberhardt, J. & Tai, S. (2017). On or off the Blockchain? Insights on off-chaining Computation and Data *Information Systems Engineering*. Available at http://www.ise.tu-berlin.de/fileadmin/fg308/publications/2017/2017-eberhardt-tai-offchaining-patterns.pdf. Accessed 22 September 2020.

Edelman Trust Barometer. Available at https://www.edelman.com/trust-barometer. Accessed 19 December 2019.

Edwood, F. (2020). *Block size and scalability, explained*. Available at https://cointelegraph.com/explained/block-size-and-scalability-explained#:~:text=behind%20the%20scenes.-,What%20are%20the%20arguments%20for%20and%20against%20increasing%20block%20size,will%20lead%20to%20greater%20centralization. Accessed 24 August 2023.

Ethereum.org (2023) *Blocks.* Available at https://ethereum.org/en/developers/docs/blocks/#:~:text=Each%20block%20has%20a%20target,(2x%20target%20block%20size). Accessed 24 August 2023.

Ethereum (2023). *Proof-of-stake (POS)*. Available https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/. Accessed 21 August 2023.

European Commission (2024). *European blockchain regulatory sandbox for distributed ledger technologies*. Available at https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Sandbox+Project. Accessed 16 June 2024.

European Commission (2022). *Legal and regulatory framework for blockchain*. Available at https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-blockchain. Accessed 16 October 2023.

European Commission (2019). *Taxation and Customs Union: VAT Gap*. Available at https://taxation-customs.ec.europa.eu/business/vat/vat-gap_en. Accessed 24 September 2022.

European Convention of Human Rights. Available at https://www.echr.coe.int/documents/convention_eng.pdf. Accessed 13 December 2020.

European Justice. *National Legislation*. https://e-justice.europa.eu/content_member_state_law-6-en.do. Accessed 3 February 2021.

Everledger. Available at https://www.everledger.io/about-us/about. Accessed 17 December 2019.

Eyewitness News. *Government partners with Vodacom for COVID-19 data collection*. Available at https://www.youtube.com/watch?v=7p3DhOn3Kp4. Accessed 12 November 2023.

Federal Trade Commission (2003). *ID Theft: When Bad Things Happen to your Good Name* at 3. Available at http://www.iwar.org.uk/ecoespionage/resources/id-theft/idtheft.pdf. Accessed 15 August 2020.

Finck, M. (2018). Blockchain and Data Protection in the European Union *Max Planck Institute for Innovation and Competition Research Paper No. 18-01* at 6. Available at https://cybersecurity.master.di.unimi.it/articoli/blockchain%20gdpr.pdf. Accessed 21 September 2020.

Finnish Social Science Data Archive. *Anonymisation and Personal Data*. Available at https://www.fsd.tuni.fi/aineistonhallinta/en/anonymisation-and-identifiers.html. Accessed 9 September 2020.

Ganne, E. (2018). *Can Blockchain revolutionize international trade?* World Trade Organisation at 35. Available at https://theblockchaintest.com/uploads/resources/WTO%20-%20Can%20Blockchain%20revolutionize%20international%20trade%20-%202018.pdf. Accessed 25 September 2022.

Garfinkel, L., S. (2015). De-Identification of Personal Information *National Institute of Standards and Technology* at 2. Available at https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf. Accessed 22 September 2020.

G DATA Blog (2020). *How secure are smart contracts?* Available at https://www.gdatasoftware.com/blog/2020/12/36570-how-secure-are-smart-contracts. Accessed 17 June 2021.

Ghimiray, D. (2022). *What is cryptography and how does it work?* Available at https://www.avast.com/c-cryptography#:~:text=How%20does%20cryptography%20work%3F,all%20except%20the%20intended%20recipient. Accessed 22 August 2023.

Giles, J. (2020). *Must I comply with the POPI Act?* Available at https://www.michalsons.com/blog/must-i-comply-with-the-popi-act/41827. Accessed 22 March 2022.

GSMA (2021). *The Mobile economy: Sub-Saharan Africa*. Available at https://www.gsma.com/mobileeconomy/wp-content/uploads/2021/09/GSMA_ME_SSA_2021_English_Web_Singles.pdf. Accessed 5 October 2022.

Hertig, A., (2017). *Why Are Miners Involved in Bitcoin Code Changes Anyway?* Available at https://www.coindesk.com/miners-involved-bitcoin-code-changes-anyway. Accessed 17 December 2019.

Higgins, S. (2017). “Accenture awarded patent for ‘editable blockchain’ tech”. Available at https://www.coindesk.com/markets/2017/09/28/accenture-awarded-patent-for-editable-blockchain-tech/. Accessed 13 August 2023.

Higginson, M. *et al* (2019). *Blockchain and retail banking: Making the connection*. Available at https://www.mckinsey.com/industries/financial-services/our-insights/blockchain-and-retail-banking-making-the-connection#. Accessed 16 January 2021.

Hoffman, M. R. (2018). *Can Blockchains and Linked Data Advance Taxation?* Available at https://dl.acm.org/doi/fullHtml/10.1145/3184558.3191555. Accessed 6 October 2022.

Hyson, P. & Ancrum, S. (2023). *Unleashing the power of cryptocurrency: Exploring Transactions per second (TPS) and its impact*. Available at https://www.miamiherald.com/software-business/article274817896.html#:~:text=Bitcoin%2C%20the%20first%20cryptocurrency%2C%20has,around%207%20transactions%20per%20second. Accessed 21 August 2023.

IEEE (2023). *About*. Available at https://www.ieee.org/about/index.html?utm_source=dhtml_footer&utm_medium=hp&utm_campaign=learn-more. Accessed 27 August 2023

IEEE SA (2023). *About us*. Available at https://standards.ieee.org/about/. Accessed 27 August 2023.

IEEE. *Blockchain smartphones – going mobile*. Available at https://innovationatwork.ieee.org/blockchain-smartphones-going-mobile/. Accessed 22 April 2021.

IBM. *What is Blockchain Security?* Available at https://www.ibm.com/topics/blockchain-security. Accessed 17 June 2021.

Information Commissioner's Office (ICO). *What are identifiers and related factors*? Available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-are-identifiers-and-related-factors/. Accessed 21 July 2022.

Iredale, G. (2019). *Introduction to Permissioned Blockchains*. Available at https://101blockchains.com/permissioned-blockchain/. Accessed 3 May 2021.

ISO. Available at https://www.iso.org/about-us.html. Accessed 15 July 2021.

ISO. *Blockchain standards*. https://www.iso.org/search.html?PROD_isoorg_en%5Bquery%5D=blockchain&PROD_isoorg_en%5Bmenu%5D%5Bfacet%5D=standard. Accessed 16 June 2024.

ISO. *ISO/DTR 3242 Blockchain and distributed ledger technologies – use cases*. Available at https://www.iso.org/standard/79543.html. Accessed 15 July 2021.

ISO. *ISO/IEC 27001:2022 Information technology, cybersecurity and privacy protection – Information security management systems – requirements*. Available at https://www.iso.org/standard/82875.html. Accessed 21 July 2022.

ISO. *ISO/IEC 27000:2018 Information technology – security techniques – information security management systems – Overview and vocabulary*. Available at https://www.iso.org/standard/73906.html. Accessed 21 July 2022.

ISO. *ISO/IEC 27001:2013 Information technology – security techniques – information security – management systems – requirements*. Available at https://www.iso.org/standard/54534.html. Accessed 21 July 2022.

Janse van Rensburg, R. (2020). *POPI Act officially in effect*. Available at https://solidariteit.co.za/en/popi-act-officially-in-effect/. Accessed 15 March 2020.

John, F., Oleh, M. & Luciano, C. (2023). *Blockchain architecture layers: a comprehensive guide*. Available at https://hacken.io/discover/blockchain-architecture-layers/. Accessed 16 October 2023.

Kasireddy, P., (2017). *Fundamental challenges with public blockchains*. Available at https://medium.com/@preethikasireddy/fundamental-challenges-with-public-blockchains-253c800e9428. Accessed 13 January 2020.

Kasireddy, P. (2018). *What do mean by 'blockchains are trustless?* https://medium.com/@preethikasireddy/eli5-what-do-we-mean-by-blockchains-are-trustless-aa420635d5f6. Accessed 15 December 2019.

Keen, M. & Smith, S. (2007). VAT fraud and evasion: what do we know, and what can be done? *IMF working paper WP/07/31*. Available at https://www.imf.org/external/pubs/ft/wp/2007/wp0731.pdf. Accessed 29 December 2022

Kim, R., C. (2021). Blockchain Initiatives for Tax Administration *University of Utah College of Law Research Paper No 427*. Available at https://ssrn.com/abstract=3798136. Accessed 26 June 2021.

Kurahashi-Sofue, J. *What is a blockchain validator?* Available at https://support.avax.network/en/articles/4064704-what-is-a-blockchain-validator. Accessed 6 October 2023.

Lalav, R. (2023). *Blockchain with the highest transaction speed*. Available at https://bitpowr.com/blog/blockchains-with-the-highest-transaction-speeds. Accessed 9 June 2024.

M6T (2021). *How long does a shipment take to clear customs in South Africa?* Available at https://www.m6t.co.za/how-long-does-a-shipment-take-to-clear-customs-in-south-africa/. Accessed 25 September 2022.

Mainelli, M. (2017). *Blockchain could help us Reclaim control of Our personal Data*. Available at https://hbr.org/2017/10/smart-ledgers-can-help-us-reclaim-control-of-our-personal-data. Accessed 24 September 2020.

Mammadzada, K. *et al* (2020). "Blockchain Oracles: A framework for blockchain-based applications" at 3. Available at https://www.researchgate.net/publication/344079826_Blockchain_Oracles_A_Framework_for_Blockchain-Based_Applications/link/5f53cef992851c250b967e95/download?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19. Accessed 16 June 2024.

Marquit, M. & Adams, M. (2022). *Fannie Mae and Freddie Mac*. Available at https://www.forbes.com/advisor/investing/fannie-mae-and-freddie-mac/#:~:text=Fannie%20Mae%20and%20Freddie%20Mac%20played%20a%20starring%20role%20in,functioning%20of%20the%20mortgage%20market. Accessed 21 June 2024.

Martin, A. & Martinovic, I. (2016). *Security and Privacy Impacts of a Unique Personal Identifier*. Available at https://ora.ox.ac.uk/catalog/uuid:90cf14a1-beb3-4322-b18d-deffe8c7f861/download_file?file_format=application%2Fpdf&safe_filename=workingpaperno4martinmartinovic.pdf. Accessed 21 July 2022.

Masekesa, F. (2020). *Nigeria, South Africa and Kenya dominate the e-commerce industry in Sub-Saharan Africa*. Available at https://www.theasianbanker.com/updates-and-articles/nigeria,-south-africa-and-kenya-dominate-the-e-commerce-industry-in-sub-saharan-africa. Accessed 21 April 2021.

Mazur, O. (2021). *Can Blockchain Revolutionize Tax Administration?* SMU Dedman School of Law Legal Studies Research Paper No. 510. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3841785. Accessed 23 June 2021.

Mboweni, T. T. (2019). 2019 *Budget Speech*. Available at http://www.treasury.gov.za/documents/national%20budget/2019/speech/speech.pdf. Accessed 2 March 2019.

Mishra, M. (2023). *List of 10 Biggest and Largest Industries in the World*. Available at https://www.edudwar.com/biggest-industries-in-the-world/. Accessed 22 August 2023.

Mohammed J., K., (2018). "*Big Data Deidentification, Reidentification and Anonymization*" ISACA Journal. Available at https://www.isaca.org/resources/isaca-journal/issues/2018/volume-1/big-data-deidentification-reidentification-and-anonymization. Accessed 24 June 2020.

Momtaz, P. P., Rennertseder, K., and Schröder, H. (2019). *Token Offerings: A Revolution in Corporate Finance?* Available at https://ssrn.com/abstract=3346964. Accessed 24 December 2022.

Moore, T. & Edelman, B., (2010). Measuring the Perpetrators and Funders of Typosquatting 14th International Conference on Financial Cryptography and Data Security at 1. Available at https://www.benedelman.org/typosquatting/typosquatting.pdf. Accessed 15 August 2020.

Mual, M. (2019). *TymeBank, the first digital – only bank in South Africa*. Available at https://thepaypers.com/expert-opinion/tymebank-the-first-digital-only-bank-in-south-africa--780573. Accessed 17 July 2022.

Mzekandaba, S. (2020). *SA's smartphone penetration surpasses 90%*. Available at https://www.itweb.co.za/content/xA9PO7NZRad7o4J8. Accessed 22 April 2021.

Napoletano, E. & Curry, B. (2024). *Proof of work explained*. Available at https://www.forbes.com/advisor/investing/cryptocurrency/proof-of-work/. Accessed 9 June 2024.

Nedbank. *Tax Reporting*. https://www.nedbank.co.za/content/nedbank/desktop/gt/en/personal/tools-and-guidance/bank-anytime-anywhere/FATCA.html. Accessed 15 March 2022.

Newman, G., R. (2004). *Identity Theft* US Department of Justice. Available at https://secure.goozmo.com/user_files/19180.pdf. Accessed 15 August 2020.

Nguyen, V-C. *et al* (2019). *Digitizing Invoice and Managing VAT payment Using Blockchain Smart Contract*. Available at https://www.researchgate.net/profile/Pham-Hoai-Luan/publication/334167437_Digitizing_Invoice_and_Managing_VAT_Payment_Using_Blockchain_Smart_Contract/links/5f50ac6992851c250b8c5aac/Digitizing-Invoice-and-Managing-VAT-Payment-Using-Blockchain-Smart-Contract.pdf. Accessed 5 April 2021.

Odlysko, A. (2003) *Privacy, Economics, and Price Discrimination on the Internet*. Available at https://dl.acm.org/doi/pdf/10.1145/948005.948051. Accessed 12 December 2022.

OECD (1980). *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Available at http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Accessed 10 December 2020.

OECD (2021). *Jurisdictions Participating in The Convention on Mutual Administrative Assistance in Tax Matters Status – 15 July 2021*. Available at https://www.oecd.org/tax/exchange-of-tax-information/Status_of_convention.pdf. Accessed 19 July 2021.

OECD (2020). *Tracking and tracing COVID: Protecting privacy and data while using apps and biometrics*. Available at https://www.oecd.org/coronavirus/policy-responses/tracking-and-tracing-covid-protecting-privacy-and-data-while-using-apps-and-biometrics-8f394636/. Accessed 15 July 2022.

Okafor, C. *Unveiling the depths of blockchain cryptography*. Available at https://www.linkedin.com/pulse/unveiling-depths-blockchain-cryptography-collins-okafor. Accessed 7 June 2024.

Orenes-Lerma, L. (2023). *What is a blockchain validator?* Available at https://www.ledger.com/academy/what-is-a-blockchain-validator. Accessed 7 October 2023.

Parliament of Malta. *Innovative technology arrangements and Services Act*. Available at https://www.parlament.mt/en/13th-leg/bills/bill-no-043-innovative-technology-arrangements-and-services-bill/. Accessed 16 October 2023.

Parliament of Malta. Malta digital Innovation Authority Act. Available at https://parlament.mt/13th-leg/bills/bill-no-045-malta-digital-innovation-authority-bill/. Accessed 16 October 2023.

Parliament of Malta. *Virtual Financial Assets Bill*. Available at https://parlament.mt/13th-leg/bills/bill-no-044-virtual-financial-assets-bill/. Accessed 16 October 2023.

Panayi, C. H. J. I. (2016). Current trends on automatic exchange of information *University School of Accountancy Research Paper*. Available at https://accountancy.smu.edu.sg/cet/sites/accountancy.smu.edu.sg.cet/files/Current%

20Trends%20on%20Automatic%20Exchange%20of%20Information.pdf. Accessed 15 March 2022.

Peterson, A. (2014). *The Sony Pictures Hack, explained*. Available at https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/. Accessed 6 August 2020.

Phemex (2021). *Who are the blockchain validators: network users powering the blockchain functionality*. Available at https://phemex.com/academy/blockchain-validator-process. Accessed 7 October 2023.

Post Office (2022). *"Rates Brochure"*. Available at https://www.postoffice.co.za/questions/Postalrates.pdf. Accessed 24 September 2022.

Quaderno (2022). *Digital Taxes Around the World*. Available at https://quaderno.io/blog/digital-taxes-around-world-know-new-tax-rules/. Accessed 19 March 2018.

RapidSSonline. *The difference between public key and private key explained*. Available at https://www.rapidsslonline.com/ssl/difference-between-public-and-private-key/. Accessed 5 January 2020.

Rikken, O. (2017). *Blockchain Real Time Tax*. Available at https://www.linkedin.com/pulse/blockchain-real-time-tax-olivier-rikken. Accessed 6 April 2021.

SARS (2021). *Automatic Exchange of Information*. Available at https://www.sars.gov.za/businesses-and-employers/third-party-data-submission-platform/automatic-exchange-of-information/. Accessed 26 June 2021.

SARS (2022). *Binding General Rulings (BGRs)*. Available at https://www.sars.gov.za/legal-counsel/legal-advisory/published-binding-rulings/binding-general-rulings-bgrs/. Accessed 5 January 2023.

SARS (2016). *Binding General Ruling (VAT) No 28 Issue 2*. Available at https://www.sars.gov.za/wp-content/uploads/Legal/Rulings/BGR/LAPD-IntR-R-BGR-2015-03-BGR28-Electronic-Services.pdf. Accessed 15 July 2021.

SARS (2022). *Double Taxation Agreements & Protocols*. Available at https://www.sars.gov.za/legal-counsel/international-treaties-agreements/double-taxation-agreements-protocols/. Accessed 14 June 2021.

SARS (2022). *Interpretation Notes*. Available at https://www.sars.gov.za/legal-counsel/legal-advisory/interpretation-notes/. Accessed 2 December 2022.

SARS (2021). *IRS Criminal Investigation and SARS join forces to fight international crimes*. Available at https://www.sars.gov.za/media-release/irs-criminal-investigation-and-sars-join-forces-to-fight-international-crimes/. Accessed 7 July 2021.

SARS (2023). *Supply of electronic services by foreign suppliers and foreign intermediaries* at 4. Available at https://www.sars.gov.za/wp-content/uploads/Ops/Guides/VAT-REG-02-G02-Supply-of-Electronic-Services-by-Foreign-Suppliers-and-Foreign-Intermediaries-External-Guide.pdf. Accessed 12 October 2023.

SARS (2019). *VAT 404 – Guide for Vendors*. Available at https://www.sars.gov.za/wp-content/uploads/Ops/Guides/LAPD-VAT-G02-VAT-404-Guide-for-Vendors.pdf. Accessed 14 May 2021.

SARS (2023). *VAT Connect Issue 16 (August 2023)*. Available at https://www.sars.gov.za/businesses-and-employers/my-business-and-tax/newsletters/vat-connect-issue-16-august-2023/#:~:text=Registration%20of%20foreign%20electronic%20service,any%20consecutive%2012%2Dmonth%20period. Accessed 12 October 2023.

SARS (2022). *VAT News*. Available at https://www.sars.gov.za/legal-counsel/legal-counsel-archive/vatnews/. Accessed 14 May 2021.

SARS (2002). *VAT news 20*. Available at https://www.sars.gov.za/wp-content/uploads/Docs/VATNews/LAPD-IntR-VATN-Arc-2013-20-VATNews-20-September-2002.pdf. Accessed 14 May 2021.

SARS (2021). *What is a unique identifier?* Available at https://www.sars.gov.za/faq/faq-what-is-a-unique-identifier/. Accessed 21 July 2022.

Senga, E. (2024). *Crypto: here is the fastest blockchain in the world!* Available at https://www.cointribune.com/en/crypto-here-is-the-fastest-blockchain-in-the-world/#:~:text=Solana%20stands%20out%20as%20the,5%20times%20faster%20than%20Polygon. Accessed 9 June 2024.

Sharma, T. K. (2024). *Types of blockchains explained – public vs private vs consortium*. Available at https://www.blockchain-council.org/blockchain/types-of-blockchains-explained-public-vs-private-vs-consortium/. Accessed 9 June 2024.

Shenzhen Daily (2021). *City introduces world's 1st international standardization for blockchain e-invoice*. Available at http://www.sz.gov.cn/en_szgov/business/news/content/post_8675244.html. Accessed 26 August 2023.

SARS (2022). *SARS eFiling*. Available at https://www.sarsefiling.co.za. Accessed 12 December 2022.

Schneider, F. (2016). *Taxation and the exponential growth in e-commerce*. Available at https://www.bdo.co.za/en-za/insights/2016/tax/taxation-and-the-exponential-growth-in-e-commerce. Accessed 19 March 2018.

Schwab, J. & Ohnesorge, J. (2019). Potential Blockchain Technology for Trade Integration of Developing Countries *German Development Institute Briefing Paper 4/2019*. Available at https://www.die-gdi.de/en/briefing-paper/article/potential-of-blockchain-technology-for-trade-integration-of-developing-countries/. Accessed 21 April 2021.

Sguazzin, A. (2022). *Who unplugged South Africa?* Available at https://www.washingtonpost.com/business/energy/who-unplugged-south-africa/2022/12/13/33128cb8-7aac-11ed-bb97-f47d47466b9a_story.html. Accessed 13 December 2022.

Shah, P. *et al* (2019). "Blockchain Technology: Data Privacy Issues and Potential Mitigation Strategies" *Thomson Reuters Practical Law* at 7. https://www.davispolk.com/files/blockchain_technology_data_privacy_issues_and_potential_mitigation_strategies_w-021-8235.pdf. Accessed 17 June 2020.

Shenzhen Daily (2021). "City introduces world's 1st international standardization for blockchain e-invoice". Available at http://www.sz.gov.cn/en_szgov/business/news/content/post_8675244.html. Accessed 26 August 2023.

Sillaber, C., & Waltl, B., (2017). *Life Cycle of Smart Contracts in Blockchain Ecosystems*. Available at https://csillaber.q-e.at/pdfs/SW_DuD_SmartContracts_preprint.pdf. Accessed 21 February 2020.

Sim, S., Owens, J., Petruzzi, R., Tavares, R., J., S., & Migai, C. (2017). Blockchain, Transfer Pricing, Customs Valuations, and Indirect Taxes: Transforming the Global Tax Environment *Tax and Accounting Center* at 2. Available at https://www.wu.ac.at/fileadmin/wu/d/i/taxlaw/institute/WU_Global_Tax_Policy_Center/Tax___Technology/BNA_WU_Blockchain_article_June17_final_online_version.pdf. Accessed 1 July 2021.

Spiekermann, S. *et al* (2015). The challenges of personal data markets and privacy. Available https://link.springer.com/article/10.1007/s12525-015-0191-0. Accessed 18 July 2020.

Spydra (2023). *Everything you need to know about cryptography in blockchain*. Available at https://www.linkedin.com/pulse/everything-you-need-know-cryptography-blockchain-spydra. Accessed 22 August 2023.

Stepanek, M. (2000) *Weblining*. Available at https://www.bloomberg.com/news/articles/2000-04-02/weblining. Accessed 7 September 2020.

Szabo, N. (1996). *Smart Contracts: Building Blocks for the Digital Markets*. Available at https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html. Accessed 8 September 2022.

Takyar, A. *How to determine the cost of blockchain implementation?* Available at https://www.leewayhertz.com/cost-of-blockchain-implementation/. Accessed 16 April 2021.

Techskill Brew (2022). *Cryptography in Blockchain (Part 6-Blockchain series)*. Available at https://medium.com/techskill-brew/cryptography-in-blockchain-part-6-blockchain-basics-129ec058c574. Accessed 7 June 2024.

The General Secretariat of the Cooperation Council for the Arab States of the Gulf. Available at https://www.gcc-sg.org/en-us/Pages/default.aspx. Accessed 10 April 2021.

Thompson, A. (2019). Banks and financial apps in South Africa are sharing your personal information - here's how to stop them *Business Insider SA.* Available at https://www.businessinsider.co.za/banking-apps-share-your-information-2019-11. Accessed 17 July 2020.

Tobin, A., & Reed, D. (2016). The Inevitable Rise of Self-Sovereign Identity *Sovrin Foundation* at 9 – 13. Available at https://sovrin.org/wp-content/uploads/2017/06/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf. Accessed 24 September 2020.

Trotino, G. (2024). *What is k anonymity and why data pros care*. Available at https://www.k2view.com/blog/what-is-k-anonymity. Accessed 6 June 2024.

UNCTAD (2020). The UNCTAD B2C E-commerce Index 2020: Spotlight on Latin America and the Caribbean *UNCTAD Technical Notes on ICT for Development No 17*. Available at https://unctad.org/system/files/official-document/tn_unctad_ict4d17_en.pdf. Accessed 21 April 2021.

Vashishtha, G. (2023). *Consensus mechanism for permissioned blockchain protocols*. Available at https://www.zeeve.io/blog/consensus-mechanisms-for-permissioned-blockchain-protocols/. Accessed 10 June 2024.

Visser, A. (2023). "*Uncertainty over 'place of supply' rules for cross-border transactions*". Available at https://www.moonstone.co.za/uncertainty-over-place-of-supply-rules-for-cross-border-transactions/. Accessed 19 October 2023.

Volmink, P. (2020). *Is it safe to do business with government?* Available at https://www.news24.com/fin24/opinion/opinion-is-it-safe-to-do-business-with-government-20200127. 15 June 2020.

Wight, M. (2020). *China to use blockchain-based system to tackle fraudulent invoices*. Available at https://theblockchainland.com/2020/03/13/china-blockchain-based-system-fraudulent-invoices/. Accessed 26 August 2023.

Worldcoin (2023). *What's Ethereum 2.0? A complete guide*. Available at https://worldcoin.org/articles/whats-ethereum-2-0#:~:text=In%20terms%20of%20processing%20speed,which%20is%20a%20massive%20jump. Accessed 21 August 2023.

Other

Aïmeur, E., & Schőnfeld, D. (2011). The ultimate invasion of privacy: Identity theft *2011 Ninth Annual International Conference on Privacy, Security and Trust*. Available at https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5971959&casa_token=U2s7CN1Sa1QAAAAA:wAzrdGlSn_pY2T4FCAlp80-uUeu4xz_IXH9TXQJtyqwqSpTSRlkFef5taOkf5Lgchq5wB50k7ZfM&tag=1. Accessed 5 August 2020.

Bains, P. (2022). “Blockchain Consensus Mechanisms: A Primer for Supervisors” *International Monetary Fund* at 8.

Bal, A. (2018). Does the Tax Sector Need Blockchain? *White Paper IBFD* 1 – 8.

Ben-Sasson, E. *et al* (2014). Zerocash: Decentralized Anonymous Payments from Bitcoin *IEEE Symposium on Security and Privacy* at 459 – 474.

Buterin, V. (2013). *Ethereum White Paper: a next generation smart contract & decentralized application platform*. Available at https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf. Accessed 24 February 2020.

European Commission (2016). *Communication from the commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the regions: A European agenda for the collaborative economy*.

European Parliament (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&rid=5. Accessed 14 June 2022.

EU directive 95/46/EC of the European Parliament and the Council of 24 October 1995.

Frøstad, P. & Holm, J. (2015). "Blockchain: Powering the Internet of Value" *White Paper Evry Labs*. Available at https://blockchainlab.com/pdf/bank-2020---blockchain-powering-the-internet-of-value---whitepaper.pdf. Accessed 25 June 2024.

Gazzetta Ufficiale (2019). https://www.gazzettaufficiale.it/atto/serie_generale/caricaArticolo?art.versione=1&art.idGruppo=0&art.flagTipoArticolo=0&art.codiceRedazionale=19A00934&art.idArticolo=8&art.idSottoArticolo=3&art.idSottoArticolo1=10&art.dataPubblicazioneGazzetta=2019-02-12&art.progressivo=0. Accessed 18 October 2023.

Government General Notice No. 36742 (808 of 2013).

Godkin, E. L. (1890). The Rights of the Citizen, IV—To His Own Reputation *Scribner's Magazine* vol 8(1): 58 – 67.

Honkanen, P. Nylund, M. Westerlund, M. (2021). "Organizational Building Blocks for Blockchain Governance: A Survey of 241 Blockchain White Papers" *Frontiers in Blockchain* 4 (2021) at 5. Available at https://www.theseus.fi/bitstream/handle/10024/510748/Blockchain_Nylund_et_al.pdf?sequence=1. Accessed 12 November 2023.

Marwala, T. & Xing, B. (2018). *Blockchain and Artificial Intelligence*. Available at https://arxiv.org/pdf/1802.04451.pdf. Accessed 8 September 2022.

Model Tax Convention on Income and on Capital.

Nakamoto, S. (2008) *Bitcoin: A Peer-to-Peer Electronic Cash System*. Available at https://bitcoin.org/bitcoin.pdf. Accessed 7 December 2019.

OECD (2021). *The Impact of the Growth of the Sharing and Gig Economy on VAT/GST Policy and Administration* OECD Publishing, Paris.

OECD/WBG/ATAF (2023). *VAT Digital Toolkit for Africa* OECD Paris at 114. Available at https://www.oecd.org/tax/consumption/vat-digital-toolkit-for-africa.pdf. Accessed 12 August 2023.

Olyniwun Ajayi LP (2019). *Examining the Italian legal framework on distributed ledger technology and smart contracts* . Available at https://www.olaniwunajayi.net/blog/wp-content/uploads/2019/03/Examining-the-Italian-Legal-Framework-on-Distributed-Ledger-Technology-and-Smart-Contracts.pdf. Accessed 18 October 2023.

Pelouze, F. A. (2009). “Fannie Mae and Freddie Mac and the 2008 Financial Crisis”. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1424456. Accessed 21 June 2024.

Pillay, L. (2014). The partial commencement of the Protection of Personal Information Act 2013 *Without Prejudice* at 54.

Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data COM(90) 314 final – SYN 287.

SARS (2016). *Binding General Ruling (VAT) No 28 Issue 2*. Available at https://www.sars.gov.za/wp-content/uploads/Legal/Rulings/BGR/LAPD-IntR-R-BGR-2015-03-BGR28-Electronic-Services.pdf. Accessed 15 July 2021.
UN General Assembly Guidelines for the Regulation of Computerized Personal Data Files A/RES/45/95 of 14 December 1990.

UN General Assembly Resolution on Human Rights and Scientific and Technological Developments 2450 of 19 December 1968.

UN General Assembly (1948). *The Universal Declaration of Human Rights*. Available at https://www.ohchr.org/en/udhr/documents/udhr_translations/eng.pdf. Accessed 18 February 2021.

UN General Assembly International Covenant on Civil and Political Rights adopted on 19 December 1966. Available at https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf. Accessed 10 December 2020.

UN General Assembly Resolution 217A (III) A/RES/3/217A 10 December 1948.