

How to regulate cryptocurrencies in South Africa

by

Reabetsoe Balekani Phasha

Submitted in fulfilment of the requirements for the degree

LLM

In the Faculty of Law,
University of Pretoria

Date

2020 December

Supervisor: Corlia van Heerden

ACKNOWLEDGEMENTS

I would like to first and foremost thank God for the wisdom that He gave me to be able to complete this paper. To my supervisor Professor Corlia van Heerden, thank you for all your hard work and dedication which has helped me push through this difficult year and complete my paper. Emmanuel and Jeanette Phasha, my dearly beloved parents, your love and support is unparalleled. I thank God for your lives and for all you have done for me. To my friends and family who have carried me through this journey, I appreciate all of you.

ABSTRACT

The global economy is undergoing radical changes due to the significant proliferation of virtual currencies as well as other crypto assets. The international community is still grappling with this phenomenon and very few countries have started to regulate virtual currencies and related activities. South Africa is among the countries which has not yet drafted regulations to regulate and supervise the use of virtual currencies and related activities. There is, however, a need to regulate these activities in South Africa because of the growing interest among consumers to invest and participate in this market, the effect they will have on the country's financial sector and because they present substantial risks to the financial stability of the country.

This paper will have a general discussion about various aspects of virtual currencies and the risks that they present to the economy. It will briefly discuss international approaches to regulating virtual currencies before going into a detailed discussion and comparison on the regulatory approaches adopted by the United States of America and the People's Republic of China. Such regulatory response to virtual currencies and related activities will be discussed and following that discussion a regulatory framework for regulating virtual currencies in South Africa will be proposed. The paper will conclude with a summary of what was discussed and a proposal for the way forward.

Contents

ACKNOWLEDGEMENTS	1
ABSTRACT	2
Chapter One Introduction	4
1.1. Background and rationale for study	4
1.2. Research statement and objective of the study	5
1.3. Research objectives	6
1.4. Research Methodology	6
1.5. Chapter Layout	7
Chapter 2 Virtual Currency	8
2.1 General	8
2.2 Differentiation between e-money and virtual currencies	9
2.3 Functions of virtual currencies	10
2.4. Classifications	13
2.5. Virtual currency system participants	15
2.6. Risks that are related to the use of virtual currencies	17
Chapter 3 International approaches to the regulation of virtual currencies	22
3.1. General	22
3.2. Financial Action Task Force	23
3.3. United States of America	25
3.4. China	32
3.5. A comparison between the approaches of the USA and China	36
3.6. Conclusion	38
Chapter 4 Regulatory recommendations	39
4.1. General	39
4.2. Regulatory challenges	39
4.3. The South African regulatory response	43
4.4.3 My recommendations	53
Chapter 5 Conclusion	59
BIBLIOGRAPHY	60

1.1. Background and rationale for study

The global economy is undergoing radical change which is driven by new technologies.¹ Such technological innovations, which are of interest to regulators, include cryptography and the significant proliferation of virtual currencies as well as other crypto assets.² Since the introduction of Bitcoin in 2009, there has been an increasing hype surrounding virtual currencies to the extent that some merchants are even accepting virtual currencies as a form of payment.³

The approach to the regulation of virtual currencies differs significantly across jurisdictions.⁴ Some jurisdictions, such as New York City (in the United States of America (“USA”)), have attempted to formulate regulations that regulate virtual currencies hence the “Bitlicense”.⁵ While other jurisdictions The approach to the regulation of virtual currencies differs significantly across jurisdictions.⁶ Some jurisdictions, such as New York, like Vietnam, have put a blanket ban on using virtual currencies.⁷ In South Africa, the National Treasury alongside other financial regulators issued an initial public statement on virtual currencies, which primarily warned the

¹ International Monetary Fund ‘Virtual Currencies and Beyond: Initial Considerations’, available at <https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf>, accessed on 30 July 2019.

² European Parliament ‘Virtual currencies and Blockchain’, available at <http://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20virtual%20currencies%20and%20blockchain.pdf>, accessed on 29 August 2019.

³ OECD ‘How to deal with Bitcoin and other virtual currencies in the System of National Accounts?’, available at [http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=COM/SDD/DAF\(2018\)1&docLanguage=En](http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=COM/SDD/DAF(2018)1&docLanguage=En), accessed on 30 July 2019.

⁴ Coie ‘Digital Currencies: International Actions and Regulations’, available at <https://www.perkinscoie.com/en/news-insights/digital-currencies-international-actions-and-regulations.html#South%20Africa>, accessed on 05 August 2019.

⁵ New York State Department of Financial Services ‘Virtual Currency Business activity’, available at https://www.dfs.ny.gov/apps_and_licensing/virtual_currency_businesses, accessed 29 August 2019.

⁶ Coie ‘Digital Currencies: International Actions and Regulations’, available at <https://www.perkinscoie.com/en/news-insights/digital-currencies-international-actions-and-regulations.html#South%20Africa>, accessed on 05 August 2019.

⁷ Library of congress law ‘Regulation of Cryptocurrency Around the World’, available at [https://www.loc.gov/law/help/cryptocurrency/world-survey.php#:~:text=Some%20\(Algeria%2C%20Bolivia%2C%20Morocco,and%20all%20activities%20involving%20cryptocurrencies](https://www.loc.gov/law/help/cryptocurrency/world-survey.php#:~:text=Some%20(Algeria%2C%20Bolivia%2C%20Morocco,and%20all%20activities%20involving%20cryptocurrencies), accessed on 29 August 2019.

public about the risks associated with using virtual currencies.⁸ A position paper was then issued by the South African Reserve Bank (“SARB”), the central bank of South Africa.⁹ It highlighted that, currently, virtual currencies are not regulated in terms of any legislation in South Africa.¹⁰ Consequently there is great uncertainty regarding the effects that virtual currencies will have in relation to the national payment system, consumer protection as well as exchange control regulations.¹¹

Despite the uncertainty, there is a need to regulate virtual currencies and other crypto assets activities in South Africa. This is because there is a growing interest among consumers to invest and participate in this market; they form part of the financial technology (“fintech”)¹² innovations that will probably affect the country’s financial sector, either positively or negatively; the existing regulatory framework does not adequately regulate them; they may create conditions for regulatory arbitrage; and they may present substantial risks to the financial stability of the country.¹³

1.2. Research statement and objective of the study

Virtual currencies have many benefits as well as various drawbacks which may pose risks to financial consumers and the financial system. Consequently, it will not be prudent to leave them unregulated. Therefore, the objectives of this study are to consider the rationale for regulating virtual currencies and to suggest guidelines for a regulatory framework for virtual currencies in South Africa.

⁸ IFWG CAR WG ‘Consultation paper on policy proposals for crypto assets’, available at http://www.treasury.gov.za/comm_media/press/2019/CAR%20WG%20Consultation%20paper%20on%20crypto%20assets_final.pdf, accessed on 30 July 2019.

⁹Ibid.

¹⁰ Ibid.

¹¹ Ibid.

¹² Financial technology is the development or creation of new technological products and processes that have the potential to disrupt the traditional business models and processes in the financial market. Comizio, ‘Virtual Currencies: Growing Regulatory Framework and Challenges in the Emerging Fintech Ecosystem’ (2017) 21 *North Carolina Banking Institute* 131 at 131.

¹³ Ibid.

1.3. Research objectives

For purposes of addressing the research problem, the following research questions or objectives will be considered:

(a) What are virtual currencies?

(b) Why must virtual currencies be regulated?

(c) For purposes of informing a regulatory framework for South Africa, the different regulatory responses between The People's Republic of China ("China") and USA will be considered.

(d) How can South Africa design an appropriate framework for the regulation of virtual currency?

1.4. Research Methodology

This study will consist of doctrinal research comprising of an analysis of policy documents, legislation, textbooks, journal articles and case law. It will include a comparative appraisal of measures relating to the regulation of virtual currencies in the USA and China. This is because these two countries are at "war" over various economic activities and they are both leaders in terms of technological innovations.¹⁴ An example of this is that both countries want to be leaders in 5G technology and the use of artificial intelligence.¹⁵ In light of the above, it will be interesting to note the differences in the manner in which the two countries have dealt with the regulation of virtual currencies. Although these two countries are ahead in terms of technological innovations, their approaches to regulating virtual currencies are very different, almost on opposite ends of the spectrum.¹⁶

¹⁴The wall street journal 'The U.S. vs. China: Who Is Winning the Key Technology Battles?', available at <https://www.wsj.com/articles/the-u-s-vs-china-who-is-winning-the-key-technology-battles-11586548597>, accessed on 04 October 2020.

¹⁵ Ibid.

¹⁶ Alvarez, 'Comparative Analysis of Cryptocurrency Regulation in the United States, Nigeria, and China: The Potential Influence of Illicit Activities on Regulatory Evolution' (2018) 25(1) *ILSA Journal of International and Comparative Law* 33 at 53.

1.5. Chapter Layout

Chapter 1 of this dissertation provides an introduction to the paper, contains the research statement, the research objectives, research methodology as well as the chapter layout. Chapter 2 considers what virtual currencies entail, key definitions, necessary classifications and differentiations of virtual currencies and the risks that they pose. Chapter 3 includes a short discussion on the Financial Action Task Force (“FATF”) and compares how the USA and China have addressed the regulation of virtual currencies. Chapter 4 will deal with the challenges to regulating virtual currencies, South Africa’s regulatory response to virtual currencies and proposes a regulatory framework for South Africa. Chapter 5 is the final chapter of the dissertation and comprises of the conclusions reached and suggestions regarding the way forward for South Africa with respect to regulating virtual currencies.

2.1 General

The concept “virtual currency” can be best explained with reference to two words, “cryptography” and “currency”.¹⁷ Cryptography utilises algorithms¹⁸ to encrypt data, such that the data is transmitted in formats that can only be accessed by an authenticated user, who uses a key to decrypt the message.¹⁹ Therefore, during the process of transmitting the data, no unauthorised user is able to decode the data back into readable formats.²⁰ Currency is the money used in a jurisdiction which serves the purpose of functioning as a medium of exchange for goods and services and a way to store value.²¹ Thus, virtual currencies refer to an encrypted equation that is used to secure and process financial transactions.

Virtual currencies digitally represent value and they operate as a unit of account, a way to store value and a means of trading.²² These characteristics are similar to e-money, however, virtual currencies are not legal tender.²³ The differences between e-money and virtual currencies will be discussed in more detail below.

¹⁷Alkadri, 'Defining and Regulating Virtual currency: Fake Internet Money or Legitimate Medium of Exchange' (2018-2019) 17 *Duke Law & Technology Review* 71 at 75.

¹⁸ An algorithm is a formula or set of computational rules for the solution of a mathematically expressed problem. An algorithm can be automated to run data inputs to produce an output which is the solution to the problem. Mainka, 'Algorithm-based recruiting technology in the workplace' (2019) 5(3) *Texas A&M Journal of Property Law* 801 at 803; The most common algorithm used for cryptocurrencies is SHA-256. SHA stands for secure hash algorithm. This algorithm ensures that the information in the data set has not been changed from its original form. CoinPursuit 'An In-Depth Look at Cryptocurrency Mining Algorithms', available at <https://www.coinpursuit.com/articles/an-in-depth-look-at-cryptocurrency-mining-algorithms.179/>, accessed 10 September 2020.

¹⁹Goforth, 'The Lawyer's Cryptionary: A Resource for Talking to Clients about Crypto-transactions' (2019) 41(1) *Campbell Law Review* 47 at 56.

²⁰ Ibid.

²¹Alkadri, (2018-2019) 17 *Duke Law & Technology Review* 71 at 76.

²² Ibid.

²³ European Banking Authority 'Opinion on Virtual Currencies (2014)', available at <https://eba.europa.eu/sites/default/documents/files/documents/10180/657547/81409b94-4222-45d7-ba3b-7deb5863ab57/EBA-Op-2014-08%20Opinion%20on%20Virtual%20Currencies.pdf?retry=1>, accessed on 15 March 2020.

2.2 Differentiation between e-money and virtual currencies

E-money is an electronic representation of fiat currency²⁴ which is backed by a country's government, whereas virtual currencies are not issued by any country or jurisdiction and they are backed and guaranteed by complex mathematical algorithms and proof-of-work systems.²⁵ Virtual currency miners²⁶ have the ability to create additional units of the virtual currency and verify²⁷ the transfer of its value.²⁸ The value of a virtual currency is best described in relation to a free market theory based on supply and demand, free of any governmental influence or control.²⁹ That is, virtual currencies are valued based on a consumer's preference to use an independent peer-to-peer network as opposed to relying on a third party intermediary to process and settle a transaction.³⁰ The value of e-money is the value of the fiat currency it represents.³¹

²⁴ Fiat currency is a currency that has value that is guaranteed by the government that issues that currency if that currency has been declared to be legal tender by that government. As such fiat currency can satisfy claims, debts and obligations in that respective jurisdiction. Chung, 'Money as Simulacrum: The Legal Nature and Reality of Money' (2009) *Hastings Business Law Journal* 112 at 113.

²⁵ As described by Nakamoto, a proof of work system generates computational proof of transactions by using a peer-to-peer distributed timestamp server to validate transactions Nakamoto, 'Bitcoin: A peer-to-peer electronic cash system', available at <https://bitcoin.org/bitcoin.pdf>, accessed on 14 April 2020; Proof-of-work can also be described as the process of solving the cryptographic problem Brühl, 'Virtual Currencies, Distributed Ledgers and the Future of Financial Services' 2017 52(6) *Intereconomics Review of European Economic Policy* 370 at 378.

²⁶ The process of calculating and solving mathematical algorithms called hashes is known as mining and it is done by miners. Lemchuk Virtual whats: Defining virtual currencies in the face of conflicting regulatory guidances. (2017) 15(2) *Cardozo Public Law, Policy and Ethics Journal* 319 at 330; Miners also use their computing resources to confirm transactions and to ensure that the ledger reflects the transactions accurately Syska, 'Eight-years-young: How the new yorkbitlicense stifles bitcoin innovation and expansion with its premature attempt to regulate the virtual currency industry' (2017) 17(2) *Journal of High Technology Law* 313 at 320.

²⁷ Miners verify transactions by solving a complex cryptographic problem generated by the transaction. The verification process is competitive. The miner that solves the cryptographic problem first is given a new batch of cryptocurrencies, that are generated automatically by the software, as a reward. The creation of a new batch of cryptocurrencies is an incentive for the miners to participate in the mining process and it is a method for issuing new cryptocurrencies. Marian, 'A Conceptual Framework for the Regulation of Cryptocurrencies' (2015-2016) 82 *University of Chicago Law Review Dialogue* 53 at 55; Animashaun, 'Regulating virtual currency payment systems' (2019) 4(2), *Cambridge Law Review* 29 at 41.

²⁸ Van Adrichem 'Howey Should Be Distributing New Virtual currencies: Applying the Howey Test to Mining, Airdropping, Forking, and Initial Coin Offerings' (2019) 20(2) *Columbia Science and Technology Law Review* 388 at 395.

²⁹ Kates, *Free Market Economics: An Introduction for the General Reader* 3 ed (Edward Elgar Publishing Inc 2017); Reddy & Lawack, 'An overview of the regulatory developments in South Africa regarding the use of virtual currencies' (2019) *SA Merc LJ* 3 at 8.

³⁰ *Ibid.*

³¹ Chung, (2009) *Hastings Business Law Journal* 112 at 113.

Conventionally, electronic transactions are processed and cleared with the intervention of a trusted third party and not directly between persons.³² In South Africa, payment instructions are finalised by the South African Multiple Option Settlement (SAMOS).³³ SAMOS is a system provided by the South African Reserve Bank which automatically settles payments between banks, finally and irrevocably, on an almost immediate, real-time basis. This allows banks to discharge their obligations almost instantaneously.³⁴ This process and its participants are eliminated when using virtual currencies and instead a “peer-to-peer”³⁵ system which utilises cryptographic proof is used. This allows two interested participants to complete transactions directly with each other, eliminating the need of a trustworthy third party like a bank.³⁶

2.3 Functions of virtual currencies

2.3.1. Payment platform

As explained by Bollen, payment entails the transfer of economic value by taking money from a payor’s account and transferring that corresponding value to the payee’s account.³⁷ This results in a final and irrevocable extinction or settlement of claims between the payor and the payee.³⁸ A payment platform comprises of various components that enable and facilitate the transfer of economic value.³⁹ Payment platforms are governed by central rules, that regulate the clearing and settlement of

³²Spruyt ‘An assessment of the emergent functions of virtual currencies’ 2018 *TSAR* 707 at 708- 709; Goforth (2019) 41(1) *Campbell Law Review* 47 at 60-61.

³³The South African Reserve Bank ‘SAMOS System (South African’s Real Time Gross Settlement (RTGS) System)’ available at [https://www.resbank.co.za/RegulationAndSupervision/NationalPaymentSystem\(NPS\)/SAMOSSystem\(RTGS\)/Pages/SAMOSSystem\(RTGS\)-Home.aspx](https://www.resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/SAMOSSystem(RTGS)/Pages/SAMOSSystem(RTGS)-Home.aspx), accessed on 15 March 2020.

³⁴Ibid.

³⁵ A peer-to-peer transacting is a system uses technology wherein the nodes on a network can directly interact with each other without the need of a central server to facilitate the interaction between the nodes.

³⁶ Nakamoto, ‘Bitcoin: A peer-to-peer electronic cash system’, available at <https://bitcoin.org/bitcoin.pdf> accessed on 14 April 2020.

³⁷ Bollen, ‘What a Payment Is (and How it Continues to Confuse Lawyers)’ (2005) *Macquarie Journal of Business Law* 189 at 190.

³⁸Ibid.

³⁹ Ibid.

payments. These rules are entrenched within express contracts between the various payment platform participants.⁴⁰

Virtual currencies are designed in such a way that their underlying payment protocol validates and timestamps a payment which constitutes a permanent and irrevocable entry in the blockchain ledger.⁴¹ The timestamp proves that the transaction was effected.⁴² This payment protocol irreversibly settles individual payment instructions between the accounts of the payor and the payee in real-time.⁴³ This transaction structure does away with the need to have a third party intermediary that processes the payment instruction.⁴⁴ Thus, an inherent feature of a virtual currency is that it also functions as a payment platform.

2.3.2. Medium of exchange

Mandjee points out that a medium of exchange is an intermediary instrument which represents a standard of value that is designed for continuous transfer between buyers and sellers without being destroyed or consumed by the end-user.⁴⁵

Virtual currencies can be transferred and traded between users without being destroyed or consumed by the end-user.⁴⁶ Although virtual currencies have the properties of a medium of exchange, persons and merchants are not obligated to accept them as an adequate discharge of a financial obligation because they are not

⁴⁰ Bank of International settlements, 'The payment system in South Africa', available at <https://www.bis.org/cpmi/paysys/southafrica.pdf>, accessed on 01 May 2020; Spruyt, 2018 *TSAR* 707 at 715.

⁴¹A ledger is a database that records all transactions that have been effected. A ledger resembles a cash flow statement for the cryptocurrency. A cryptocurrency ledger records the ownership of the cryptocurrencies that have been transacted. Glass, 'What is digital currency' (2017) 57(3) *IDEA: The Journal of the Franklin Pierce Center for Intellectual Property* 455 at 484- 485; Morton, 'The future of cryptocurrency: An unregulated instrument in an increasingly regulated global economy' (2020) 16(1) *Loyola University Chicago International Law Review* 129 at 130.

⁴²Doguet, 'The nature of the form: Legal and regulatory issues surrounding the bitcoin digital currency system' (2013) 73(4) *Louisiana Law Review* 1119 at 1144; Reddy & Lawack, (2019) *SA Merc LJ* 3at 10-13; Rosner & Kang, 'Understanding and regulating twenty-first century payment systems: The ripple case study' (2016) 114(4) *Michigan Law Review* 649 at 652.

⁴³*Ibid.*

⁴⁴ *Ibid.*

⁴⁵Mandjee, 'Bitcoin, Its Legal Classification and Its Regulatory Framework' (2014) 15(2) *Journal of Business and Securities Law* 1 at 14; Spruyt 2018 *TSAR* 707 at 714.

⁴⁶Reddy &Lawack,(2019) *SA Merc LJ* 3 at 16.

legal tender.⁴⁷ Virtual currencies may theoretically function as a medium of exchange, but practically, it is at a merchant's discretion to decide whether they will accept the virtual currency as a means of trading and a discharge of a financial obligation.⁴⁸

2.3.3. Store of value

An asset that can function as a store of value is one that preserves its worth without depreciating and it can be utilized to transfer purchasing power from the present-day to the future.⁴⁹ For anything to be considered a store of value it must be reliable and secure.⁵⁰ An example of a dependable and safe store of value is gold.

Virtual currencies respond to market forces which result in price volatility, and as such they are generally a risky store of value.⁵¹ Spruyt indicates that for virtual currencies to be an effective store of value, there should be a realistic guarantee that their value will not suddenly depreciate.⁵² If there is a wider acceptance of virtual currencies, he opines that they can stabilize such that they maintain their value and can be a dependable way to store value.⁵³

2.3.4. Unit of account

A “unit of account” is an instrument that is used to measure and attribute worth to goods and services.⁵⁴ Mesk explains that the same way that we use centimetres to measure distance or length, we use a unit of account to determine the monetary worth of goods and services.⁵⁵ An efficient unit of account provides users with a relative

⁴⁷Ibid.

⁴⁸Mandjee, (2014) 15(2) *Journal of Business and Securities Law* 1 at 14.

⁴⁹Spruyt 2018 *TSAR* 707 at 716; Mandjee, (2014) 15(2) *Journal of Business and Securities Law* 1 at 13.

⁵⁰ Ibid.

⁵¹Mandjee, (2014) 15(2) *Journal of Business and Securities Law* 1 at 18; Doguet, (2013) 73(4) *Louisiana Law Review* 1119 at 1140.

⁵²Spruyt, 2018 *TSAR* 707 at 716-717.

⁵³ Ibid.

⁵⁴Mandjee, (2014) 15(2) *Journal of Business and Securities Law* 1 at 14-17; Spruyt, 2018 *TSAR* 707 at 715-716.

⁵⁵Mesk, 'Unit of Account', available at <https://www.binance.vision/glossary/unit-of-account>, accessed on 11 May 2020.

measure of worth such that they do not have to use their resources trying to determine the value of a thing.⁵⁶

Virtual currencies are denominated in their own units of account.⁵⁷ However, as indicated above, virtual currencies are volatile and fluctuate significantly daily.⁵⁸ Due to this price volatility, it is not effective to value goods and services in a virtual currency-denominated unit of account.⁵⁹ If virtual currencies stabilize over time and become more widely used, they could possibly serve as an appropriate unit of account.⁶⁰

From the above, it is seen that if virtual currencies are more widely accepted and used, they could perform all the functions of money and act as a payment platform simultaneously, however, they would still not be considered legal tender.

2.4. Classifications

Virtual currencies can either be convertible or non-convertible.⁶¹ This classification refers to their exchangeability. They can also be centralised or decentralised, which refers to their distribution of control in relation to who can administer the virtual currency.⁶²

Convertible virtual currencies can be changed in form, function and character by being converted into fiat currency.⁶³ Conversely, non-convertible virtual currencies are not exchangeable for fiat currency.⁶⁴ Non-convertible virtual currencies are only usable within a specific cyber community that the virtual currency was created for.⁶⁵ Although non-convertible virtual currencies may be transferred officially within the specific cyber

⁵⁶Mandjee, (2014) 15(2) *Journal of Business and Securities Law* 1 at 14-17.

⁵⁷ Ibid.

⁵⁸Doguet, (2013) 73(4) *Louisiana Law Review* 1119 at 1140; Mandjee, (2014) 15(2) *Journal of Business and Securities Law* 1 at 18.

⁵⁹Spruyt, 2018 *TSAR* 707 at 716.

⁶⁰Ibid.

⁶¹Syska, 'Eight-years-young: How the new york bitlicense stifles bitcoin innovation and expansion with its premature attempt to regulate the virtual currency industry' (2017) 17(2) *Journal of High Technology Law* 313 at 318-319.

⁶²Ibid.

⁶³ Nieman, 'Few South African cents' worth on bitcoin' (2015) 18(5) *Potchefstroom Electronic Law Journal* 1979 at 1982.

⁶⁴Ibid.

⁶⁵Ibid.

environment they were created for, they remain incapable of being converted into fiat currency.⁶⁶ While some non-convertible virtual currencies may be bought utilising fiat currency, it is not possible to convert them back to fiat currency after they have been so bought.⁶⁷

The administration and control⁶⁸ of a virtual currency refers to the major decision-making power and authority of the virtual currency. This includes: establishing the rules for using the virtual currency, maintaining the blockchain ledger, increasing the volume of available virtual currency, issuing the currency and withdrawing the virtual currency from circulation.⁶⁹ A centralised virtual currency has a management structure wherein there is a single administering authority that controls the administration of the virtual currency.⁷⁰ A decentralised virtual currency, in contrast, does not have a central administering authority, nor does it have a central monitoring or oversight authority.⁷¹ Therefore, the administration of the decentralised virtual currency can be done by various different persons.⁷² An advantage of a decentralised virtual currency, as stated by Vessio, is that where a centralised virtual currency is susceptible to a “single point of failure”,⁷³ the different nodes in a decentralised virtual currency can perform the function of being back-up sites should the need arise.⁷⁴

Virtual currencies can thus be convertible and decentralised,⁷⁵ convertible and centralised,⁷⁶ or non-convertible and centralized.⁷⁷ There are currently no examples of

⁶⁶Ibid.

⁶⁷ This would be in the case where you buy credits or currency for an online game using fiat currency. Once the conversion has been made from fiat currency to the currency used in the game, you cannot convert that currency back into fiat currency.

⁶⁸ This is referred to by Bech & Garrattas (as quoted by Vessio) as a “transfer mechanism” in Bech & Garratt ‘Central bank cryptocurrencies’ Bank for International Settlements Quarterly Review (2017) 55 at 55.

⁶⁹ Nieman, (2015) 18(5) *Potchefstroom Electronic Law Journal* 1979 at 1983.

⁷⁰ Ibid.

⁷¹ Ibid.

⁷² Ibid.

⁷³ Vessio, ‘To CBDC or not to CBDC? Exploring central bank digital currency’ *Annual Banking Law Update* (2020) 63 at 69.

⁷⁴ Ibid.

⁷⁵ An example of this is the popular bitcoin.

⁷⁶ An example of this is webmoney.

⁷⁷ An example of this is World of warcraft gold.

non-convertible decentralised virtual currencies.⁷⁸ This study focusses on convertible decentralised virtual currencies.

2.5. Virtual currency system participants

There are various role-players within the virtual currency system. A virtual currency “exchanger” and an “exchange” are closely linked concepts.⁷⁹ An exchange is an online platform⁸⁰ wherein an entity or person can trade their virtual currencies for other currencies, such as other virtual currencies or fiat currencies and other assets.⁸¹ The exchanger facilitates this transaction⁸² and charges a fee or commission for this service.⁸³

A “wallet” is a software program that stores digital currencies,⁸⁴ allows its user to monitor its balances and provides storage and transaction security to the user.⁸⁵ A “wallet provider” provides the software application that interacts with various digital protocols to create the “wallet” and gives the “wallet user” the ability to hold, store, receive and transfer the user’s private and public keys (that is the user’s virtual currency).⁸⁶ In the same way a physical wallet is used to store money, a “wallet” in this sense allows virtual currency users to store their virtual currencies.⁸⁷

“Intermediary service providers” are virtual currency trading platforms, vending machine facilities or any other entity facilitating virtual currency transactions, such as

⁷⁸ Financial Action Task Force (FATF) ‘Virtual Currencies: Key Definitions and Potential AML/CFT Risks’, available at <https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>, accessed on 15 April 2020.

⁷⁹ Takahashi, ‘Cryptocurrencies entrusted to an exchange provider: Shielded from the provider’s bankruptcy?’ *Annual Banking Law Review* (2018) 1 at 2.

⁸⁰ Ibid.

⁸¹ Financial Action Task Force (FATF) ‘Virtual Currencies: Key Definitions and Potential AML/CFT Risks’, available at <https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>, accessed on 15 April 2020.

⁸² Takahashi, *Annual Banking Law Review* (2018) 1 at 2.

⁸³ Ibid.

⁸⁴ Glass, (2017) 57(3) *IDEA: The Journal of the Franklin Pierce Center for Intellectual Property* 455 at 484.

⁸⁵ Kirby, ‘Virtually possible: How to strengthen bitcoin regulation within the current regulatory framework’ (2014) 93(1) *North Carolina Law Review* 195 at 207.

⁸⁶ Lemchuk, (2017) 15(2) *Cardozo Public Law, Policy and Ethics Journal* 319 at 348.

⁸⁷ Ibid.

banks, that offer the buying and selling of virtual currencies.⁸⁸ These service providers facilitate virtual currency transactions like trading and converting or exchanging virtual currencies, fiat currency and other virtual assets for one another.⁸⁹

An “administrator” controls the issuing and redemption of the virtual currency, maintains the payment ledger and establishes the rules for the use of the virtual currency.⁹⁰ A “user” is a natural or legal person that uses virtual currencies to make purchases, trades the virtual currency or holds it as an investment.⁹¹ Although the transactions of a user are recorded on a public ledger, the identity of the user remains hidden.⁹²

A “miner” solves difficult maths equations in a decentralised proof-of-work system to create new virtual currency units in the system.⁹³ Miners can either operate on a public, private or hybrid blockchain.⁹⁴ A public blockchain is open to public use and no permission is needed to be able to operate on the blockchain.⁹⁵ This was the original form of a blockchain.⁹⁶ A private blockchain has got restricted access and authorisation is necessary before a user can participate on the blockchain.⁹⁷ This means that all the participants on the blockchain are known.⁹⁸ A hybrid blockchain combines the public and private blockchain.⁹⁹ It allows the blockchain to be accessible or visible to the public, however, the control and modification of the blockchain ledger is restricted.¹⁰⁰

⁸⁸ Financial Action Task Force (FATF) ‘Virtual Currencies: Key Definitions and Potential AML/CFT Risks’, available at <https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>, accessed on 15 April 2020.

⁸⁹ *Ibid.*

⁹⁰ Nieman, (2015) 18(5) *Potchefstroom Electronic Law Journal* 1979 at 1983.

⁹¹ Mandjee, (2014) 15(2) *Journal of Business and Securities Law* 1 at 9.

⁹² Haynes & Yeoh, ‘Legal issues arising from the utilisation of blockchain-based products in the 4th industrial revolution’ *Annual Banking Law Update* (2020) 47 at 47.

⁹³ Nieman, (2015) 18(5) *Potchefstroom Electronic Law Journal* 1979 at 1994.

⁹⁴ Haynes & Yeoh, *Annual Banking Law Update* (2020) 47 at 50.

⁹⁵ *Ibid.*

⁹⁶ *Ibid.*

⁹⁷ *Ibid.*

⁹⁸ *Ibid.*

⁹⁹ *Ibid.*

¹⁰⁰ *Ibid.*

2.6. Risks that are related to the use of virtual currencies

The financial system and its role players function in an extremely regulated environment. This helps to maintain a sound and safe financial system.¹⁰¹ Virtual currencies operate without safety mechanisms similar to those in the rest of the financial system, which creates various financial and consumer risks.¹⁰² Some of these risks include the circumvention of exchange controls, money laundering and terrorist funding related-risks, consumer protection risks and risks to financial stability and the national payment system.¹⁰³ These will be discussed in more detail below.

2.6.1. Money Laundering and terrorist funding risks

Virtual currencies allow for more secrecy in terms of processing transactions than traditional non-cash payment methods.¹⁰⁴ Although both of these transaction methods are characterised by customer transactions that do not include face-to-face interactions with the customer, unlike the traditional non-cash payment means, virtual currency service providers do not need to comply with any anti-money laundering and countering the funding of terrorism (“AML/CFT”) laws, like identifying the customer.¹⁰⁵ Virtual currencies are created in such a way that there is no central server that keeps a historical record of transactions that are effected and associated with a person’s real-life identity.¹⁰⁶ Furthermore, virtual currency protocols do not monitor, report on nor identify suspicious transaction patterns.¹⁰⁷ This means that virtual currency transactions can be completed without the same AML/CFT security features and with greater anonymity than traditional online payment platforms that use fiat currency for

¹⁰¹National Treasury Policy Document ‘A Safer Financial Sector to Serve South Africa Better’ available at <http://www.treasury.gov.za/twinpeaks/20131211%20-%20Item%202%20A%20safer%20financial%20sector%20to%20serve%20South%20Africa%20better.pdf>, accessed on 15 October 2020.

¹⁰²IFWG CAR WG, ‘Consultation paper on policy proposals for crypto assets’, available at http://www.treasury.gov.za/comm_media/press/2019/CAR%20WG%20Consultation%20paper%20on%20crypto%20assets_final.pdf, accessed on 30 July 2020.

¹⁰³Ibid.

¹⁰⁴ Ibid.

¹⁰⁵ Ibid.

¹⁰⁶ Ibid.

¹⁰⁷ Ibid.

payments.¹⁰⁸ In this way, virtual currencies are able to perpetuate the laundering of money and the financing of terrorism.¹⁰⁹

2.6.2. The circumvention of exchange control regulations

The financial surveillance department of the SARB (“Finsurv”), as per its delegated authority by the minister of finance, is responsible for exchange control administration.¹¹⁰ This means that it monitors and controls the movement of capital in and out of South Africa.¹¹¹ Finsurv has reporting requirements for persons (legal and natural) who wish to transfer, remit or receive funds from abroad.¹¹² Unfortunately, currently, Finsurv does not explicitly allow companies to transfer funds abroad for purposes of purchasing virtual currencies.¹¹³ This is because virtual currencies are not legal tender nor have they been specifically designated to an asset class.¹¹⁴

Virtual currency transactions do not require a registered third-party intermediary to complete a transaction; therefore, companies can purchase virtual currencies abroad without complying with the regulatory reporting requirements that are required by Finsurv.¹¹⁵ In this way, transparency and accuracy may be lost in the financial system because it becomes difficult to have a precise record and complete information regarding the flow of capital funds in and out of South Africa.¹¹⁶ Furthermore, virtual currencies do not distinguish their users based on their location it is therefore hard to impose national laws and capital flow restrictions on virtual currency transactions.¹¹⁷

¹⁰⁸Ryan, Glass, Governatori, Lindsay, Lumsden, Nayyar, Salon, & Watt, ‘Sydney Node’ (2018) 1 *Stanford Journal of Blockchain Law & Policy* 90 at 108-111.

¹⁰⁹ Ibid.

¹¹⁰ South African Reserve Bank ‘Financial Surveillance’ available at <https://www.resbank.co.za/AboutUs/Departments/Pages/FinancialSurveillance.aspx>, accessed on 30 June 2020.

¹¹¹ Ibid.

¹¹² Ibid.

¹¹³ Ibid.

¹¹⁴ South African Reserve Bank ‘Crypto assets’ available at <https://www.resbank.co.za/RegulationAndSupervision/FinancialSurveillanceAndExchangeControl/FAQs/Pages/VirtualCurrenciesCryptocurrencies.aspx>, accessed 28 June 2020.

¹¹⁵ IFWG CAR WG, ‘Consultation paper on policy proposals for crypto assets’, available at http://www.treasury.gov.za/comm_media/press/2019/CAR%20WG%20Consultation%20paper%20on%20crypto%20assets_final.pdf, accessed on 30 July 2020.

¹¹⁶ Ibid.

¹¹⁷ Morton, (2020) 16(1) *Loyola University Chicago International Law Review* 129 at 142.

2.6.3. Risks to financial stability

The market capitalisation of virtual currencies is currently low as such it could take a while before their financial stability risks materialise.¹¹⁸ A factor which could increase the risks to financial stability caused by virtual currencies is if more registered financial institutions participate in the virtual currency environment either as a means to convert virtual currencies to fiat currencies or any facilitation of a virtual currency transaction and a failure from this interconnectedness occurs.¹¹⁹ This will trigger severe instability or a collapse in the financial industry.¹²⁰

If virtual currencies become more widely accepted as a means to discharge obligations, there are various transmission channels which pose systemic risks which could affect the financial stability of a country.¹²¹ These include the impact of the interconnectedness of virtual currencies with the regulated financial system, the exposure of regulated financial institutions to virtual currencies, consumer confidence effects and the ability for virtual currencies to finally and irrevocably settle payments in a traditional payment system.¹²²

Furthermore, if one country buys virtual currencies in an attempt to control its availability, it could negatively impact other countries who have widely accepted and use virtual currencies in their economy.¹²³ This could in turn have a spill-over effect to other economies in that the negative performance of one economy will begin to affect

¹¹⁸ IFWG CAR WG, 'Consultation paper on policy proposals for crypto assets', available at http://www.treasury.gov.za/comm_media/press/2019/CAR%20WG%20Consultation%20paper%20on%20crypto%20assets_final.pdf, accessed on 30 July 2020.

¹¹⁹ Goldsmith, 'The IMF must develop best practices before government-backed cryptocurrencies destabilize the international monetary system' 2020 34(2) *Emory International Law Review* 595 at 598.

¹²⁰ Ibid.

¹²¹ Financial stability board 'Crypto-asset markets Potential channels for future financial stability implications,' available at <https://www.fsb.org/wp-content/uploads/P101018.pdf>, accessed on 20 September 2020.

¹²² Rosner & Kang, (2016) 114(4) *Michigan Law Review* 649 at 652; IFWG CAR WG, 'Consultation paper on policy proposals for crypto assets', available at http://www.treasury.gov.za/comm_media/press/2019/CAR%20WG%20Consultation%20paper%20on%20crypto%20assets_final.pdf, accessed on 30 July 2020.

¹²³ Financial stability board 'Crypto-asset markets Potential channels for future financial stability implications,' available at <https://www.fsb.org/wp-content/uploads/P101018.pdf>, accessed on 20 September 2020.

the performance of other economies due to their interdependence and interconnectedness.¹²⁴

2.6.4. National payment system

Virtual currencies are created in such a way that they are in themselves able to settle transactions irrevocably and with finality.¹²⁵ As a result of this characteristic of virtual currencies, they are able to fulfil the payment function that is done by the traditional payment system.¹²⁶ As such, virtual currencies can create a parallel and disjointed financial system.¹²⁷

The risk of the creation of a parallel payment system is currently low as the adoption of the use of virtual currencies is currently low.¹²⁸ Should the use of virtual currencies be more widely accepted, they would compete with the current traditional payment system without being subjected to the same regulatory oversight and supervision.¹²⁹

The worth of a virtual currency is not based on any underlying asset or contractual claim and thus its price is highly speculative and experiences high levels of price volatility.¹³⁰ As a result of the high price volatility of virtual currencies, it could be difficult to use them for the payment and settlement of obligations in the traditional payment system.¹³¹

¹²⁴Ibid.

¹²⁵Doguet, 'The nature of the form: Legal and regulatory issues surrounding the bitcoin digital currency system' *Louisiana Law Review* (2013) 73(4) 1119 at 1144.

¹²⁶Reddy &Lawack,(2019) *SA Merc LJ* 3at 10-13; Rosner & Kang, 'Understanding and regulating twenty-first century payment systems: The ripple case study' (2016) 114(4) *Michigan Law Review* 649 at 652.

¹²⁷IFWG CAR WG, 'Consultation paper on policy proposals for crypto assets', available at http://www.treasury.gov.za/comm_media/press/2019/CAR%20WG%20Consultation%20paper%20on%20crypto%20assets_final.pdf, accessed on 30 July 2020.

¹²⁸ Ibid.

¹²⁹Rosner & Kang, (2016) 114(4) *Michigan Law Review* 649 at 652; IFWG CAR WG, 'Consultation paper on policy proposals for crypto assets', available at http://www.treasury.gov.za/comm_media/press/2019/CAR%20WG%20Consultation%20paper%20on%20crypto%20assets_final.pdf, accessed on 30 July 2020.

¹³⁰Goldsmith 2020 34(2) *Emory International Law Review* 595 at 627.

¹³¹IFWG CAR WG, 'Consultation paper on policy proposals for crypto assets', available at http://www.treasury.gov.za/comm_media/press/2019/CAR%20WG%20Consultation%20paper%20on%20crypto%20assets_final.pdf, accessed on 30 July 2020.

2.6.5. Consumer protection

In terms of consumer protection laws, virtual currencies do not need to comply with the same consumer protection regulations as other financial products.¹³² Therefore, in instances where a customer has recourse against a financial institution, for example in accordance with the National Credit Act 34 of 2005 (“National Credit Act”) or in accordance with the Financial Sector Regulation Act 9 of 2017 (“Financial Sector Regulation Act”), a virtual currency customer does not have the same protection afforded to them.¹³³

There is also a high frequency of hacking attacks on virtual currency service providers.¹³⁴ These hacking activities are big enough to destroy the business of a virtual currency service provider.¹³⁵ Despite this being known, there are still no consumer protection mechanisms for the consumer.¹³⁶ Therefore, if a private key is lost or a virtual currency service provider¹³⁷ is hacked or crashes, the consumer loses its money and has no legal recourse against the virtual currency service provider.¹³⁸

In addition, a virtual currency customer may not know the real identity of who they are transacting with and they have no way of knowing or assessing if that is a person that they wish to do business with or if that person is a sanctioned person as per the UN sanctions list.¹³⁹ In instances where central banks act as a “lender of last resort” for banks in cases where banks fail, if a virtual currency fails, a consumer’s money cannot be refunded because virtual currencies are not guaranteed by any government.¹⁴⁰

¹³²Tu & Meredith, ‘Rethinking virtual currency regulation in the bitcoin age’ (2015) 90(1) *Washington Law Review* 271 at 333.

¹³³ Tu & Meredith, (2015) 90(1) *Washington Law Review* 271 at 333.

¹³⁴ An example of this are the exchanges which have been hacked and have resulted in the loss of millions of dollars. Takahashi, *Annual Banking Law Review* (2018) 1 at 2.

¹³⁵ Takahashi, *Annual Banking Law Review* (2018) 1 at 2.

¹³⁶ Consumers are deemed to have taken and accepted all the risks that are associated with their virtual currency activities. Takahashi, *Annual Banking Law Review* (2018) 1 at 21.

¹³⁷ These will be further explained in chapter four as Crypto-Asset service providers.

¹³⁸Ponsford, ‘Comparative Analysis of Bitcoin and Other Decentralised Virtual Currencies: Legal Regulation in the People’s Republic of China, Canada, and the United States’ (2015) 9 *Hong Kong Journal of Legal Studies* 29 at 33; Lee, Long, McRae, Steiner, & Handler, ‘Bitcoin basics: primer on virtual currencies’ (2015) 16(1) *Business Law International* 21 at 37.

¹³⁹Marian, ‘Conceptual Framework for the Regulation of Cryptocurrencies’ (2015) 82 *University of Chicago Law Review Dialogue* 53 at 60.

¹⁴⁰Lee, Long, McRae, Steiner, & Handler, (2015) 16(1) *Business Law International* 21 at 37.

Chapter 3 International approaches to the regulation of virtual currencies

3.1. General

This chapter will begin with of a short discussion on the FATF because of its international importance in regulating money laundering and terrorist funding, which is one of the major risks posed by virtual currencies. It will then be followed by an overview of the approach that the USA and China have taken with respect to regulating virtual currencies. It will include a short discussion on the different approaches taken by China and the USA and thereafter conclude with a few principles that can be extracted pursuant to the said discussions.

With the advent of virtual currencies, regulators have scrambled to find the best approach to ensure the safety of their financial systems, while striking a balance of not stifling innovation. For example, in Australia, part 6A of their Anti-Money Laundering and Counter-Terrorism Financing Act 169 of 2006 requires virtual currency exchange providers to be registered. This section is divided into three divisions and makes provision for the manner in which the virtual currency exchange providers will be regulated in Australia. In 2014, the Canadian government passed Bill C31, for purposes of revising the Proceeds of Crime (Money Laundering) and Terrorist Financing Act 17 of 2000, to incorporate natural and legal persons who operate a business in Canada that involves the use of virtual currencies and other related activities in the scope of their regulation.¹⁴¹ In Japan, the Payment Services Act 59 of 2009, was revised in April 2017, and now requires virtual currency exchange businesses, operating in Japan, to register their business, take and implement security measures that will protect their customers and keep personal and transaction records of their customers. Virtual currency exchanges are also subject to money laundering regulations.¹⁴² A major reason for regulating virtual currencies has been their implications on AML/CFT initiatives and guidelines which are the primary focus of the FATF.

¹⁴¹Bill C31 amendments to The Proceeds of Crime (Money Laundering) and Terrorist Financing Act 2000 s256(2), available at <https://www.parl.ca/DocumentViewer/en/41-2/bill/C-31/royal-assent/page-347#38>, accessed on 02 June 2020.

¹⁴²Library of congress law Regulation of Virtual currency: Japan, available at [https://www.loc.gov/law/help/virtual currency/japan.php](https://www.loc.gov/law/help/virtual%20currency/japan.php), accessed on 31 May 2020.

3.2. Financial Action Task Force

As pointed out in Chapter two, one of the major risks that virtual currencies pose is that, due to their anonymous nature, they present an avenue to launder money and finance terrorism, hence many regulators have focussed their regulation of virtual currencies on mitigating against those potential risks. Given the risk that virtual currencies can be used to launder money and finance terrorist activities, it is necessary to consider the international role that is played in this regard by the FATF.

The FATF is an international inter-governmental body that is situated at the headquarters of the Organisation for Economic Co-operation and Development in Paris. The FATF sets international standards in an attempt to tackle money laundering and terrorist funding, by creating a co-ordinated global response to combating terrorism, corruption, and organised crime.¹⁴³ The FATF standards are called the “International Standards in Combating Money Laundering and the Financing of Terrorism and Proliferation” these are more popularly known as the FATF Recommendations.¹⁴⁴ Countries have different systems of governance, varied legal systems and diverse administrative and operational frameworks as such a “one size fits all” approach to countering money laundering and terrorist funding cannot work.¹⁴⁵ The FATF sets out standards which member countries need to implement according to their methods of governance and their legal framework with the intention of fighting money laundering and terrorist financing.¹⁴⁶

The FATF standards are continually reviewed to address new risks such as the risks presented by virtual currencies.¹⁴⁷ The FATF ensures that countries implement the FATF standards fully and effectively by conducting mutual evaluations.¹⁴⁸ Mutual

¹⁴³The Financial Action Task Force, ‘Who we are’, available at <https://www.fatf-gafi.org/about/>, accessed on 31 May 2020.

¹⁴⁴FATF, ‘International Standards on Combating Money Laundering and the Financing Of Terrorism & Proliferation- The FATF Recommendations’, available at <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>, accessed on 15 June 2020.

¹⁴⁵ Ibid.

¹⁴⁶ Ibid.

¹⁴⁷ Ibid.

¹⁴⁸ Ibid.

evaluations are in-depth assessments that assess, review and measure the effectiveness and compliance of the measures that a country has taken in an effort to tackle money laundering and terrorist funding.¹⁴⁹

The FATF Standards require member jurisdictions to enforce a risk-based approach, which encourages countries to focus their AML/CFT approach on allocating resources more effectively in places where there are higher risks or use better implementation methods for tackling money laundering and terrorist funding.¹⁵⁰

A risk-based approach is a principle of regulation wherein regulators and financial institutions allocate their resources in such a way that resources are allocated commensurately to the money laundering and terrorist financing risks that exist in the institution.¹⁵¹ This allows for an efficient allocation of resources in that the greatest risk areas that have been identified are given more attention in terms of the allocation of the available AML/CFT resources.¹⁵²

A risk-based approach is an involved process which includes, amongst other things, identifying a risk, assessing the risk to ensure that the risk is understood by the regulators and the financial institutions and developing methods to mitigate the risk that has been identified.¹⁵³ This process will involve developing processes which correspond with the risks that have been pointed out. Areas that pose greater money laundering and terrorist financing risks will be subject to enhanced procedures and areas that present lower risks will be subject to simplified procedures.¹⁵⁴ The procedures mentioned include customer due diligence checks and transaction monitoring processes.¹⁵⁵

Although the risk-based approach allows for more flexibility for FATF member countries, in that they can develop their policies according to the risks that they have

¹⁴⁹Ibid.

¹⁵⁰Ibid.

¹⁵¹The Financial Action Task Force 'Guidance for a Risk-Based Approach-Virtual Currencies' available at <https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf>, accessed on 01 July 2020.

¹⁵² Ibid.

¹⁵³ Ibid.

¹⁵⁴ Ibid.

¹⁵⁵ Ibid.

identified and assessed, their standards, laws, rules and regulations still need to be within the FATF recommendations framework and comply with the FATF principles.¹⁵⁶

The following discussion will take a closer look at the approach that the USA and China have taken with respect to regulating virtual currencies.

3.3. United States of America

The Financial Crimes Enforcement Network (FinCEN) was established as an agency in the Department of the Treasury in April 1990.¹⁵⁷ The FinCEN operates as the Financial Intelligence Unit of the USA and its responsibilities include protecting the USA's financial system from the infiltration of illicit funds and the use thereof.¹⁵⁸ The FinCEN is required to keep a database of financial transactions and use such information to analyse emerging trends, support law enforcement investigatory professionals and disseminate financial intelligence.¹⁵⁹

In 2013, the FinCEN issued a guidance dealing with virtual currencies.¹⁶⁰ Financial sector participants including regulators and law enforcement agencies sought clarity on how persons who partake in virtual currency transactions and related activities should be treated for regulatory purposes insofar as the Bank Secrecy Act of 1970 ("BSA") is applicable.¹⁶¹ The purpose of the guidance was thus to clarify the FinCEN's position on the use of virtual currencies and to give guidance and regulatory certainty for natural and legal persons engaged in one form or the other with virtual currency.¹⁶²

This FinCEN guidance considered whether virtual currencies could be classified as a money service business and more particularly, a money transmitter.¹⁶³ The FinCEN's

¹⁵⁶Ibid.

¹⁵⁷ 31 U.S. Code Section 310 (a).

¹⁵⁸ Ibid.

¹⁵⁹ 31 U.S. Code Section 310 (b)(2).

¹⁶⁰ Department of the Treasury Financial crimes enforcement Network, 'Application of FinCen's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies', available at <https://www.FinCen.gov/sites/default/files/shared/FIN-2013-G001.pdf>, accessed on 03 June 2020.

¹⁶¹ Ibid.

¹⁶² Ibid.

¹⁶³ Department of the Treasury Financial crimes enforcement Network, 'Application of FinCen's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies', available at <https://www.FinCen.gov/sites/default/files/shared/FIN-2013-G001.pdf>, accessed on 03 June 2020;

regulations define a “money transmitter” as a person or company that accepts value (in various forms) from one person and transfers such value by any process to another location or person or a person or company that offers such services.¹⁶⁴

The guidance focuses on convertible virtual currencies¹⁶⁵ and describes a virtual currency exchange as any “person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency”.¹⁶⁶ In the guidance, “real currency” is defined as legal tender that serves as a medium of exchange. The major distinction between real and virtual currencies as per the guidance is that virtual currencies are not legal tender.¹⁶⁷ When comparing a virtual currency exchange with a money transmission service provider, the FinCEN found that any exchange that accepts, sells, transfers or purchases convertible virtual currencies for any purpose whatsoever falls within the meaning of a money transmitter.¹⁶⁸

The importance of the above characterisation is that the BSA requires certain compliance obligations¹⁶⁹ for financial institutions,¹⁷⁰ and because virtual currency administrators and exchangers fall within the meaning of a financial institution as a money service business, they also need to comply with those obligations.¹⁷¹

Financial Crimes Enforcement Network, ‘Am I a MSB?’, available at <https://www.FinCen.gov/am-i-msb>, accessed on 03 June 2020.

¹⁶⁴ 31 Code of Federal Regulations s 1010.100(ff)(5)(i)(A).

¹⁶⁵ Department of the Treasury Financial crimes enforcement Network, ‘Application of FinCen’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies’, available at <https://www.FinCen.gov/sites/default/files/shared/FIN-2013-G001.pdf>, accessed on 03 June 2020; This type of virtual currency either has an equivalent value in real currency or acts as a substitute for real currency.

¹⁶⁶ Department of the Treasury Financial crimes enforcement Network, ‘Application of FinCen’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies’, available at <https://www.FinCen.gov/sites/default/files/shared/FIN-2013-G001.pdf> accessed on 03 June 2020.

¹⁶⁷ Ibid.

¹⁶⁸ Ibid.

¹⁶⁹ Money service businesses as financial institutions need to comply with registration requirements and AML obligations, such as, recordkeeping and reporting suspicious activities and cash transactions that exceed the threshold.

¹⁷⁰ In May 2013, the Department of Homeland Security seized assets owned by MutumSigillum because MutumSigillum was engaged in money transfers but had failed to register with FinCen pursuant to the March 2013 Guidance; 31 US Code s5330.

¹⁷¹ Department of the Treasury Financial crimes enforcement Network, ‘Application of FinCen’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies’, available at <https://www.FinCen.gov/sites/default/files/shared/FIN-2013-G001.pdf>, accessed on 03 June 2020.

The BSA regulates financial institutions in the USA and the USA's AML/CFT law is found primarily therein.¹⁷² The definition of a financial institution according to the BSA¹⁷³ is quite broad. The BSA imposes an obligation on financial institutions to assist the US government to tackle money laundering and terrorist funding by maintaining appropriate information regarding their clients and their transactions, filing reports of cash transactions that exceed the prescribed threshold¹⁷⁴ as well as reporting suspicious transaction activities that may signify criminal activities.¹⁷⁵

In 2014, due to many uncertainties regarding the mining of virtual currencies and software development and certain investment activities, the FinCEN issued two rulings to clarify these matters.¹⁷⁶ These rulings are the Application of FinCEN's Regulations to Virtual Currency Software Development and Certain Investment Activity¹⁷⁷ and the Application of FinCEN's Regulations to Virtual Currency Mining Operations.¹⁷⁸

FinCEN rulings are administrative letters that are issued by the FinCEN in accordance with its administrative authority conferred to it by the BSA.¹⁷⁹ FinCEN rulings provide clarity on any new issues that arise that fall within the scope of FinCEN's regulatory ambit such as virtual currencies, any new issues or cases that arises and differs

¹⁷²Financial Crimes Enforcement Network, 'FinCen's Mandate from Congress', available at <https://www.FinCen.gov/resources/statutes-regulations/FinCens-mandate-congress>, accessed on 03 June 2020.

¹⁷³ 31 U.S Code section 5312(a)(2).

¹⁷⁴ The threshold is currently a daily aggregate amount of \$10,000.

¹⁷⁵ Financial Crimes Enforcement Network, 'FinCen's Mandate from Congress', available at <https://www.FinCen.gov/resources/statutes-regulations/FinCens-mandate-congress>, accessed on 03 June 2020.

¹⁷⁶ Department of the Treasury Financial crimes enforcement Network, 'Application of FinCen's Regulations to Virtual Currency Software Development and Certain Investment Activity', available at <https://www.FinCen.gov/sites/default/files/shared/FIN-2014-R002.pdf>, accessed on 04 June 2020; Department of the Treasury Financial crimes enforcement Network, 'Application of FinCen's Regulations to Virtual Currency Mining Operations', available at <https://www.FinCen.gov/sites/default/files/shared/FIN-2014-R001.pdf>, accessed on 04 June 2020.

¹⁷⁷ Department of the Treasury Financial crimes enforcement Network, 'Application of FinCen's Regulations to Virtual Currency Software Development and Certain Investment Activity', available at <https://www.FinCen.gov/sites/default/files/shared/FIN-2014-R002.pdf>, accessed on 04 June 2020.

¹⁷⁸ Department of the Treasury Financial crimes enforcement Network, 'Application of FinCen's Regulations to Virtual Currency Mining Operations', available at <https://www.FinCen.gov/sites/default/files/shared/FIN-2014-R001.pdf>, accessed on 04 June 2020.

¹⁷⁹Department of the Treasury Financial crimes enforcement Network "Administrative Rulings" [https://www.fincen.gov/resources/statutes-regulations/administrative-rulings#:~:text=The%20Financial%20Crimes%20Enforcement%20Network%20\(%E2%80%9CFinCE N%E2%80%9D\)%20is%20issuing,involvement%20in%20transportation%20of%20currency](https://www.fincen.gov/resources/statutes-regulations/administrative-rulings#:~:text=The%20Financial%20Crimes%20Enforcement%20Network%20(%E2%80%9CFinCE N%E2%80%9D)%20is%20issuing,involvement%20in%20transportation%20of%20currency).

factually from previously considered matters and provides clarity on any new interpretation of any statute wherein the FinCEN has delegated authority.¹⁸⁰

The ruling on the Application of the FinCEN's Regulations to Virtual Currency Mining Operations explained that, whether a person or a company is required to register as a money service business is determined by the kind of activity that the person or company is engaged in and who benefits from such activities.¹⁸¹ Thus, a virtual currency miner does not need to be registered as a money service business if the activity that the miner is engaged in is for their personal use.

In the ruling on the Application of FinCEN's Regulations to Virtual Currency Software Development and Certain Investment Activity, the FinCEN clarified that even though the purchases and sales of virtual currencies may be considered as the transfer of value, if that activity is only for the user's personal use, then the person or company does not need to register as a money service business.¹⁸² Furthermore in this ruling, the FinCEN explained that software development and the sale thereof are not within the meaning of a money transmitter and as such software developers and distributors do not need to be registered as financial institutions even if such software facilitates the transfer of value of virtual currencies.¹⁸³

Money service businesses need to develop a risk-based compliance programme that corresponds with the risks that the business is exposed to, based on where it is located, how big the business is and the kind of financial services it provides.¹⁸⁴ This is to ensure that their businesses do not enable money laundering and terrorist funding.¹⁸⁵ In terms of the BSA regulations, money service businesses need to incorporate policies and protocols to ensure that they identify and verify their customers, file the necessary reports with the corresponding law enforcement

¹⁸⁰ Ibid.

¹⁸¹Department of the Treasury Financial crimes enforcement Network, 'Application of FinCen's Regulations to Virtual Currency Mining Operations', available at <https://www.FinCen.gov/sites/default/files/shared/FIN-2014-R001.pdf>, accessed on 04 June 2020.

¹⁸²Department of the Treasury Financial crimes enforcement Network, 'Application of FinCen's Regulations to Virtual Currency Software Development and Certain Investment Activity', available at <https://www.FinCen.gov/sites/default/files/shared/FIN-2014-R002.pdf>, accessed on 04 June 2020.

¹⁸³Ibid.

¹⁸⁴31 Code of Federal Regulations s1022.210(b).

¹⁸⁵ Ibid.

agencies, appoint personnel to administer their AML programme and designate various responsibilities to those personnel in that regard.¹⁸⁶ The risk-based compliance programme needs to include educational programmes as well as mechanisms for independent review, to evaluate whether the AML programme is commensurate with the risks faced by the business.¹⁸⁷

Businesses and persons may be held civilly or criminally liable for violating the BSA regulations and for violating any other AML and CFT law.¹⁸⁸ The main federal money laundering statutes that hold people criminally liable are sections 1956 and 1957 of the Federal Money Laundering Control Act of 1986. These provisions generally prohibit financial transactions that promote or facilitate money laundering.¹⁸⁹

The United States Internal Revenue Services ("IRS") issued a notice¹⁹⁰ that explained how virtual currencies would be regulated within the existing tax principles and decided that they would be considered property for the purposes of federal tax.¹⁹¹ Capital profits or losses will be accounted for in relation to the nature of the asset for the taxpayer.¹⁹² If the virtual currency is considered a capital asset, capital gains and losses will be accounted for accordingly.¹⁹³ In the same way that information reporting is required for a payment that is made in property, the same is required for virtual currency payments.¹⁹⁴ If a taxpayer accepts virtual currencies as a discharge of obligations of its creditors, when calculating the gross income of the taxpayer, the fair market value on the day when the payment in virtual currency was received will be used.¹⁹⁵ If virtual currency users fail to comply with tax laws, they may be subject to penalties that other taxpayers are subject to for non-compliance.¹⁹⁶ Such penalties

¹⁸⁶ Ibid.

¹⁸⁷ 31 Code of Federal Regulations s1022.210(d).

¹⁸⁸ 31 Code of Federal Regulations s1010.820.

¹⁸⁹ Gatto & Broeker, 'Bitcoin and beyond: Current and future regulation of virtual currencies' (2015) 9(2) *Ohio State Entrepreneurial Business Law Journal* 429 at 439.

¹⁹⁰ Internal Revenue Services, 'Notice 2014-21', available at <https://www.irs.gov/pub/irs-drop/n-14-21.pdf>, accessed on 04 June 2020.

¹⁹¹ Ibid.

¹⁹² Ibid.

¹⁹³ Ibid.

¹⁹⁴ Ibid.

¹⁹⁵ Ibid.

¹⁹⁶ Ibid.

include accuracy-related penalties¹⁹⁷ under 26 U.S Code section 6662 or information reporting penalties¹⁹⁸ for not timeously and accurately reporting virtual currency transactions in terms of 26 U.S. Code sections 6721 and 6722.

The Securities Exchange Commission of the USA was established in June 1934 to safeguard investors and to create a well-organised and fair market for its participants.¹⁹⁹ Pursuant to the Securities Exchange Commission's mission, it often issues investor alerts to warn them about investment risks.²⁰⁰ In 2014, the Securities and Exchange Commission gave an investor warning, alerting consumers to the risks associated with investing in virtual currencies.²⁰¹ It explained what bitcoin is, highlighted the heightened unique risks of making virtual currency investments such as the limited ability for an investor to recover their money in the case of fraud or theft and how virtual currency users can be targets of fraudulent or high-risk investment schemes.²⁰² The warning also gave an example of a case, (*SEC v Shavers*),²⁰³ that involved a bitcoin pyramid scheme. Gatto and Broeker remark that a notable distinction between this pyramid scheme and other pyramid schemes that are prosecuted throughout the year by the Securities and Exchange Commission is that this pyramid scheme used Bitcoin, a virtual currency, as an investment vehicle.²⁰⁴

In this case, Judge A Mazzant of the U.S. District Court in the Eastern Division of Texas ruled in favour of the Securities Exchange Commission stating that:

¹⁹⁷ This penalty applies in a situation where there has been an underpayment of tax. In this situation, the IRS will charge a penalty of 20% of the underpayment in addition to the underpayment that needs to be paid over to the IRS.

¹⁹⁸This penalty is applicable when a person has failed to file an information return before the required filing date or when the information included in the return is not a full disclosure of information and/or some of the information included is incorrect. The penalty payable in this instance is \$250 for each late or inaccurate return. The maximum cumulative penalty that can be imposed during any calendar year is \$3,000,000.

¹⁹⁹ US Securities and Exchange Commission, 'What we so' available at <https://www.sec.gov/about/what-we-do> accessed on 04 June 2020.

²⁰⁰ US Securities and Exchange Commission, 'Investor Alert: Bitcoin And Other Virtual Currency-Related Investments', available at https://www.sec.gov/oiea/investor-alerts-bulletins/investoralertsia_bitcoin.html, accessed on 04 June 2020.

²⁰¹Ibid.

²⁰²Ibid.

²⁰³*Securities and Exchange Commission v. Trendon T. Shavers and Bitcoin Savings and Trust* (Case No. 4:13-CV-416 United States Eastern District of Texas Sherman Division August 2013) ("*SEC V Shavers*").

²⁰⁴Gatto & Broeker, (2015) 9(2) *Ohio State Entrepreneurial Business Law Journal* 429 at 446.

'[i]t is clear that Bitcoin can be used as money and [t]he court finds that the [Bitcoin Savings & Trust] investments meet the definition of investment contracts, and as such are securities'.²⁰⁵

It can be concluded from the above that for purposes of the Security Exchange Commission, virtual currencies are deemed to be securities.²⁰⁶ In this context, securities are deemed to be such if they satisfy the test as set out by the Supreme Court in *Howey*.²⁰⁷ In *Sec v Shavers* the court noted that Bitcoins are not considered legal tender and stated that legal tender status is not required to determine that the Bitcoin investments are investment contracts.

The Commodity Futures Trading Commission of the USA is a federal agency designed to promote transparency and resilience in the derivatives market.²⁰⁸ In 2014 Tera Exchange,²⁰⁹ with the endorsement of the Commodity Futures Trading Commission, piloted a swap with Bitcoin as the underlying asset wherein customers were able to safeguard the value of their Bitcoin from market volatility by securing it in a dollar value.²¹⁰ The term "commodity" includes, amongst others, "all services, rights, and interests in which contracts for future delivery are presently or in the future dealt in".²¹¹ The Commodity Futures Trading Commission decided in 2015 that virtual currencies fall within this definition.²¹²

²⁰⁵Memorandum Opinion Regarding the Court's Subject Matter Jurisdiction (2013), *SEC v. Shavers* 413-CV-416 2013 at 2.

²⁰⁶Gatto&Broeker, (2015) 9(2) *Ohio State Entrepreneurial Business Law Journal* 429 at 446.

²⁰⁷*Securities and Exchange Commission v. W. J. Howey Co* (The Supreme Court of the United States of America, 1946) Under the *Howey* Test, a transaction is an investment contract if:

1. Money has been invested
2. Profits are expected from the investment
3. The investment of money is in a common enterprise
4. The profit is made as a result of the efforts of a third party

In the *Howey* case the Supreme Court created a test that looks at an investment's substance, rather than its form, as the determining factor for whether it is a security. (Form was disregarded for substance and emphasis placed upon economic reality).

²⁰⁸The Commodity Futures Trading Commission, 'The Commission', available at <https://www.cftc.gov/About/AboutTheCommission> accessed on 27 June 2020.

²⁰⁹Tera Exchange, 'Tera Exchange Launches First Regulated Bitcoin Derivatives Trading: Creates Tera Bitcoin Price Index as Global Benchmark', available at http://www.teraexchange.com/news/2014_09_12_Launches%20First%20Regulated%20Bitcoin%20Derivatives.pdf, accessed on 15 June 2020.

²¹⁰CFTC's Chilton' Eyes Bitcoin 'House of Cards' Risk (CNBC television broadcast May 7, 2013), available at <http://video.cnbc.com/gallery/?video=3000166533>, accessed on 24 June 2020.

²¹¹7 U.S. Code s1a.Definitions.

²¹²United States of America before the Commodity Futures Trading Commission 'In the Matter of: Coinflip, Inc., d/b/a Derivabit, and Francisco Riordan, Order Instituting Proceedings Pursuant to Sections 6(C) And 6(D) of The Commodity Exchange Act, Making Findings And Imposing Remedial Sanctions', available at

The primary public policy objectives that can be extracted from the above is that the regulation of virtual currencies in USA aims to protect consumers, prevent tax evasion, money laundering and terrorist funding and to uphold the security, soundness and reliability of the financial system.

3.4. China

In China, the People's Bank of China and several regulators²¹³ collectively issued a consumer warning, referred to as the Initial Coin Offering Rules ("ICO Rules"),²¹⁴ to protect investors and to minimise financial risk.²¹⁵

The ICO Rules warn consumers about the risks of the financial crimes that are associated with using virtual currencies such as fraud and pyramid schemes.²¹⁶ These ICO rules prohibit trading companies from changing virtual currencies to legal tender, or vice versa, selling or buying virtual currencies or making available similar or related services.²¹⁷ In terms of the ICO Rules, non-bank payment institutions and other financial service providers cannot provide financial or related services, such as clearing, opening bank accounts and trading, to entities engaged in virtual currency related activities.²¹⁸

Although China was initially wary of the use of virtual currencies, they have passed the Cryptography Law of the People's Republic of China, 2019 ("Cryptography

<https://www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfcoinfliporder09172015.pdf>, accessed on 10 June 2020.

²¹³ These regulators include the Cyberspace Administration of China, the China Banking Regulatory Commission, the State Administration for Industry and Commerce, the China Securities Regulatory Commission, the Ministry of Industry and Information Technology, and the China Insurance Regulatory Commission.

²¹⁴ PBOC, CAC, MIIT, SAIC, CBRC, CSRC, and CIRC, 'Announcement on Preventing Financial Risks from Initial Coin Offerings (2017)', available at, <http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/3374222/index.html> (in Chinese), accessed on 11 June 2020.

²¹⁵ *Ibid.*

²¹⁶ *Ibid.*

²¹⁷ *Ibid.*

²¹⁸ *Ibid.*

Law”)²¹⁹, that took effect on 01 January 2020. The Cryptography law seems to be a shift towards opening-up the virtual currency industry in China in a controlled manner.

In the Cryptography Law, chapter 1 contains the general provisions of the legislation. Article 1 of the Cryptography Law stipulates that the purpose of the Cryptography Law is to oversee and monitor the use and administration of cryptography, in order to promote innovation and the development of cryptography, whilst maintaining data security, national security and preserving the rights and interests of the natural and legal persons in China.²²⁰ The Cryptography Law seems to be a regulatory sandbox for the development and innovation of cryptography and the regulation thereof. Different levels of government have accordingly been allocated their scope of responsibility and management of cryptographic work within their respective regions.²²¹

Cryptography has been defined as the technologies, skills and methods used to encode and validate data and information and can either be categorized as core, common or commercial cryptography.²²² Core and common cryptography are used to protect and encrypt state secrets with the highest levels of protection being top secret and secret respectively.²²³ Commercial cryptography is used for commercial purposes that are not considered state secrets and persons and businesses may lawfully engage in the use thereof.²²⁴

Essentially chapter 1 of the Cryptography Law gives an introduction to the purposes for which the law was enacted and provides a brief outline of the respective classifications and the uses of cryptography. It also states the various responsibilities for the government, citizens and businesses with respect to the use of cryptography.²²⁵

²¹⁹ The National people’s Congress of the People’s Republic of China ‘Cryptography Law of the People’s Republic of China’ available at <http://www.npc.gov.cn/npc/c30834/201910/6f7be7dd5ae5459a8de8baf36296bc74.shtml>, accessed on 20 June 2020.

²²⁰ Ibid, article 1.

²²¹ Ibid, Article 5.

²²² Ibid Article 2.

²²³ Ibid.

²²⁴ Ibid Article 6 -8.

²²⁵ Ibid Chapter 1.

The focus of chapter 2 of the Cryptography law is to give a more detailed analysis of the purposes and uses of core and common cryptography. It is the responsibility of the Government (State) to have oversight on the improvement and management of core and common cryptography science and to ensure that there are security measures to safeguard core and common cryptography.²²⁶ According to the relevant State provisions and regulations, the processing and storage of State secret information sent on cable or wireless telecommunications must use core and common cryptography to encrypt, secure and verify State secrets.²²⁷ If anything is deemed to be a State secret, commercial cryptography cannot be used to encrypt the information or data. In addition, entities that are engaged in cryptography work bodies²²⁸ of core and ordinary cryptography products need to comply with strict compliance measures to maintain the security of core and common cryptography.²²⁹

Cryptographic work bodies of core and common cryptography need to cooperate with the government by consulting, sharing information, monitoring and issuing security alerts where necessary, to protect and enhance the cryptographic work.²³⁰ Strict supervision and compliance is expected from entities and employees of the entities that use core and common cryptography.²³¹ If there is a breach or suspected breach of security, responsive measures need to be carried out and such breach accordingly needs to be reported to the relevant state institution and if necessary, investigations need to be carried out to minimize and eliminate any potential risks or any further breach.²³²

Chapter 3 of the Cryptography law deals with commercial cryptography. Research, development and transformation are encouraged to create an open and competitive commercial cryptography industry, that allows for equal opportunities for foreign

²²⁶Ibid Article 13.

²²⁷Ibid Article 14.

²²⁸Ibid article 15; These cryptography work bodies include: research & development, manufacturing, sales, servicing, import & export.

²²⁹Ibid Article 15.

²³⁰Ibid Article 16-20.

²³¹ Ibid.

²³²Ibid Article 16-20.

investors also to participate in the market.²³³ Commercial cryptographic work units²³⁴ are expected to maintain national security and ensure that the rights and public interest of others are protected.²³⁵

In terms of the Cryptography Law, critical information infrastructure operators are required to use commercial cryptography to encrypt their data.²³⁶ These operators need to pass a national security test, that is done by the State Internet Information Department and other relevant departments, before they can purchase commercial cryptography products and services if such products and services are likely to affect national security.²³⁷ This requirement is congruous with Article 35 of the Cybersecurity Law of the People's Republic of China, 2017 which requires critical information infrastructure operators to undergo a national safety evaluation, that is organised by the State, if the products that they have purchased may affect national security.²³⁸ The State Cryptography Administration authenticates commercial cryptography products and the use of unauthenticated commercial cryptography products may attract a penalty from the State Cryptography Administration.²³⁹

Cryptography management departments are not permitted to force commercial cryptographic work units to disclose source codes and other proprietary cryptography-related information.²⁴⁰ This appears to be an endeavour to protect the business secrets of commercial cryptography operators. Administration authorities are strictly required to maintain the trade secrets and other confidential information that they may become aware of in the course of performing their duties.²⁴¹

Chapter four of the Cryptography Law details the possible liabilities and consequences that may be faced for the violation of the Cryptography Law.²⁴² These include

²³³Ibid Article 21.

²³⁴Ibid; Commercial cryptographic work units include researching, producing, selling, servicing, or importing or exporting commercial cryptography.

²³⁵Ibid Article 21.

²³⁶Ibid Article 27.

²³⁷Ibid.

²³⁸ Ibid Article 31.

²³⁹ Ibid Article 31.

²⁴⁰Ibid.

²⁴¹Ibid.

²⁴² Ibid Article 32-34.

warnings, sanctions, fines and directives instructing the relevant offender to adhere to the Cryptography Law requirements. Acts such as leaking core or common cryptography, theft of encryption protected information, trespassing activities and not using core or common cryptography when required to may attract criminal liability.²⁴³

The Cryptography law only focuses on encryption and does not address decryption which is the other aspect of cryptography.²⁴⁴ The scope of applicability to cryptography is thus limited to encryption and leaves doubt as to who, when and how data and information can be decrypted.²⁴⁵ Furthermore, the State has the power to decide what information should be considered State secrets and the State has a lot of control with respect to regulating the use of cryptography where State secrets are involved. This may put doubt in the mind of the investors as to how private and confidential their trade secrets will be and may make them reconsider investing in the Chinese cryptography industry.²⁴⁶

3.5. A comparison between the approaches of the USA and China

The USA recognized convertible virtual currency as a functional substitute for “real”²⁴⁷ currency. However, it highlighted that, although virtual currencies are a functional substitution for real currency, they are not recognized as legal tender.²⁴⁸ In contrast,

²⁴³ Ibid.

²⁴⁴Ibid; Article 2 of the Cryptography laws defines cryptography within the context of the law as technologies, products, and services that employ specified transformation methods to encrypt information or carry out security authentication. Decryption is not mentioned or covered in this definition.

²⁴⁵Ibid.

²⁴⁶Ibid Article 5 -6; China Briefing ‘Trade Secrets’ Protection in China: What is Changing?’ available at <https://www.china-briefing.com/news/trade-secrets-protection-in-china-changes-expected/> accessed on 17 June 2020.

²⁴⁷Department of the Treasury Financial crimes enforcement Network, ‘Application of FinCen’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies’, available at <https://www.FinCen.gov/sites/default/files/shared/FIN-2013-G001.pdf>, accessed on 03 June 2020. It defined real currency as

‘the coin and paper money of the United States or of any other country that [i] is designated as legal tender and that [ii] circulates and [iii] is customarily used and accepted as a medium of exchange in the country of issuance.’

²⁴⁸Ibid.

China stated that in the absence of virtual currency being recognized as legal tender, it cannot function as currency.²⁴⁹

The US regulators, such as the FinCEN and the IRS, brought virtual currencies into the scope of their regulation by categorising them as a functional substitute for “real” currency.²⁵⁰ The Commodity Futures Trading Commission and the Securities Exchange Commission gave consumer warnings and were able to identify how virtual currencies could and would fit into the scope of their regulation. As pointed out by Xie, the Chinese regulators, in contrast to those in the USA, sought to assert control over virtual currencies and the use thereof, thereby limiting the possibility of virtual currencies eroding the functioning of its current regulatory structure and efficiency.²⁵¹ The Chinese government exercised a strict and invasive approach with respect to regulating cryptography and was not direct about whether the Cryptography Law was directed at virtual currencies.²⁵² The other aspect of cryptography, being decryption, is not addressed at all, leaving much doubt as to how virtual currencies can and will interact with fiat currency and the current financial system in China.²⁵³

If China had included virtual currencies into its existing laws under monetary services and capital flows under the State Administration of Foreign Exchange, Xie points out that designated banks would have been overburdened with the unfeasible task of tracking and monitoring anonymous virtual currency transactions of Chinese users.²⁵⁴ Thus the Chinese government steered clear from giving financial institutions an impossible task.²⁵⁵

²⁴⁹Xie, ‘Why China Had to Ban Virtual currency but the U.S. Did Not: A Comparative Analysis of Regulations on Crypto-Markets between the U.S. and China’ (2019) 18(2) *Washington University Global Studies Law Review* 457.

²⁵⁰Ibid.

²⁵¹Ibid.

²⁵²The Cryptography Law speaks about Cryptography generally and does not specifically address virtual currencies.

²⁵³As previously mentioned, Article 2 of the Cryptography laws defines cryptography within the context of the law as technologies, products, and services that employ specified transformation methods to encrypt information or carry out security authentication. There is no mention of decryption in the Cryptography law and the focus of the entire law is encryption.

²⁵⁴Xie, (2019) 18(2) *Washington University Global Studies Law Review* 457.

²⁵⁵ Ibid.

From these two approaches, it is seen that China is less tolerant to regulatory uncertainty and wants to exert control over all that happens in the country that may cause a disruption to the current norm, while the USA is more open to disruptive technology²⁵⁶ even though it causes uncertainty.²⁵⁷

3.6. Conclusion

One can agree with Nathan who remarks that when it comes to regulating disruptive technology such as virtual currencies, the timing of regulation is important and every jurisdiction must adopt the approach best suited to its particular situation, taking into account its location, resources available and the risks posed to the country by the disruptive technology.²⁵⁸

Issuing a guidance warns consumers and gives the public and market participants an idea of what is permissible but also allows for flexibility making it possible for the government to retreat and revisit earlier positions if necessary.²⁵⁹ This is because a guidance is merely a form of soft law and has not been enacted as hard black letter law. This means it is easier to change and revise a guidance note that was issued.²⁶⁰ This allows regulatory bodies to customize their regulations in line with the development of the technology which they are directed at.²⁶¹

It should also be noted that under-regulation can present unforeseen risks while over-regulation can result in high opportunity costs.²⁶² It is thus left to jurisdictions to adopt a proportional and balanced regulatory approach that is best suited to them, based on the risks that virtual currencies may pose to their jurisdictions and their current regulatory system.²⁶³

²⁵⁶Disruptive technology refers to a new innovation that challenges or radically changes the way things have been done in a particular industry by creating new platforms or products that make use of new technologies. It 'turns an existing industry on its head'. Disruptive technologies often offer better value to customers McPeak, 'Disruptive technology and the ethical lawyer' (2019) 50(3) *University of Toledo Law Review* 457.

²⁵⁷ Xie, (2019) 18(2) *Washington University Global Studies Law Review* 457.

²⁵⁸ Nathan, 'Regulating Disruptive Innovation' (2014) 29(1) *Berkeley Technology Law Journal* 175.

²⁵⁹ Ibid.

²⁶⁰ Ibid.

²⁶¹ Ibid.

²⁶² Ibid.

²⁶³ Ibid.

Chapter 4 Regulatory recommendations

4.1. General

This chapter will propose a framework on how to regulate virtual currencies in South Africa in light of the regulatory challenges that exist and South Africa's current regulatory responses to virtual currencies. Notably, in the existing regulatory proposals, SARB refers to virtual currencies as "crypto assets" to avoid the possibility of confusion being made that virtual currencies are currencies that are considered legal tender and may be a substitution for the Rand.²⁶⁴ In this chapter, the term "crypto assets" will be used instead of "virtual currencies".

4.2. Regulatory challenges

The need to regulate crypto assets is largely anchored on the risks that they present to the current financial system as discussed in Chapter 2. Regulatory challenges also exist due to the inherent characteristics and nature of crypto assets.²⁶⁵ These regulatory challenges will be discussed in more detail below.

Crypto assets are stored as data on the blockchain on the internet.²⁶⁶ Holders of a crypto asset can access their accounts with little hassle, irrespective of which country they are in, by simply logging into their crypto asset accounts through the internet.²⁶⁷ Crypto assets are not denominated in any currency, thus, once the holders of the crypto assets have logged into their account, they can transact using their crypto assets provided that the merchant concerned accepts such crypto assets as compensation for goods and services rendered to the consumer.²⁶⁸ In this way, crypto

²⁶⁴ South African Reserve Bank National Payment System Department, 'Position Paper on virtual currencies', available at [https://www.resbank.co.za/RegulationAndSupervision/NationalPaymentSystem\(NPS\)/Legal/Documents/Position%20Paper/Virtual%20Currencies%20Position%20Paper%20%20Final_02of2014.pdf](https://www.resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/Legal/Documents/Position%20Paper/Virtual%20Currencies%20Position%20Paper%20%20Final_02of2014.pdf), accessed on 15 June 2020.

²⁶⁵ Lemchuk, (2017) 15(2) *Cardozo Public Law, Policy and Ethics Journal* 319 at 341.

²⁶⁶ Reiff, 'Blockchain explained', available at <https://www.investopedia.com/terms/b/blockchain.asp>, accessed on 15 July 2020.

²⁶⁷ Coinjar, 'How cryptocurrency breaks down the barriers for a borderless world', available at <https://blog.coinjar.com/2019/06/18/how-cryptocurrency-breaks-down-the-barriers-for-a-borderless-world/>, accessed on 15 July 2020.

²⁶⁸ Ibid.

assets are borderless.²⁶⁹ This may make it difficult for regulators to determine which country has jurisdiction over a crypto-asset transaction.²⁷⁰ Consequently, the responsibility of regulating crypto assets can cut across various regulators in various countries.²⁷¹ Cooperation and well-coordinated efforts are required at an international level for the effective and efficient regulation of crypto assets to ensure that there is no regulatory arbitrage.²⁷²

There is no universally accepted definition or characterisation of crypto assets.²⁷³ This new phenomenon is still nebulous and regulators are trying to figure out how to regulate them.²⁷⁴ Some jurisdictions classify them based on their economic functions and are thus able to bring them into the scope of their regulation, while others have completely banned the use thereof.²⁷⁵ Other regulators have taken a “wait-and-see” approach while issuing warnings and directives.²⁷⁶ Thus another challenge to regulating crypto assets is not knowing how to classify them in an international context.²⁷⁷ Having universally accepted principles pertaining to crypto assets may assist in creating uniformity across the globe and regulators within different countries can then pass laws and regulations in line with those principles.²⁷⁸

Businesses are inclined to choose the strategic option that has the least compliance red tape for them.²⁷⁹ Ensuring that a business is compliant with laws and regulations usually takes plenty of time and hiring compliance personnel can be a costly

²⁶⁹Morton, (2020) 16(1) *Loyola University Chicago International Law Review* 129 at 142.

²⁷⁰ Ibid.

²⁷¹ Ibid.

²⁷² Ibid.

²⁷³IFWG CAR WG, ‘Consultation paper on policy proposals for crypto assets’, available at http://www.treasury.gov.za/comm_media/press/2019/CAR%20WG%20Consultation%20paper%20on%20crypto%20assets_final.pdf, accessed on 30 July 2020.

²⁷⁴Ibid.

²⁷⁵Hughes & Middlebrook, ‘Advancing framework for regulating cryptocurrency payments intermediaries’ (2015) 32(2) *Yale Journal on Regulation* 495 at 546-549; IFWG CAR WG, ‘Consultation paper on policy proposals for crypto assets’, available at http://www.treasury.gov.za/comm_media/press/2019/CAR%20WG%20Consultation%20paper%20on%20crypto%20assets_final.pdf, accessed on 30 July 2020.

²⁷⁶ Ibid.

²⁷⁷Morton, (2020) 16(1) *Loyola University Chicago International Law Review* 129 at 142.

²⁷⁸Ibid.

²⁷⁹PriceWaterhouseCoopers, ‘The business – and cost – of compliance Practical strategies to optimize compliance cost and effectiveness’, available at <https://www.pwc.com/us/en/risk-assurance/publications/assets/pwc-business-of-compliance-4-5-18.pdf>, accessed on 15 July 2020.

exercise.²⁸⁰ If there are varying regulatory standards and degrees of strictness, this will result in a “race to the bottom”.²⁸¹ What this means is that, because crypto assets are borderless, users thereof will be more attracted to and move to jurisdictions that have less stringent crypto asset-related activity regulatory requirements.²⁸² The drawback of this is that it may result in a disintegrated international regulatory regime and regulatory arbitrage which might hinder the success of regulatory actions taken globally.²⁸³

It is important to note that crypto assets are pseudonymous.²⁸⁴ In the Oxford dictionary,²⁸⁵ a pseudonym is defined as a fictitious name or a disguise of one's real identity.²⁸⁶ Crypto assets have an account address made up of various numbers and letters, which is the address that is recorded on the blockchain when a transaction is effected.²⁸⁷ The transactions that are recorded on the distributed ledger are linked to the account address of the user, which account address can be seen as the pseudonym of the user.²⁸⁸ Thus, one of the biggest problems associated with regulating crypto assets is gathering information on the crypto asset users' real identity

²⁸⁰Darroll, 'Strategic partnerships for business growth in Africa: COUNTING THE COST OF RED TAPE for business in South Africa', available at http://www.sbp.org.za/uploads/media/Counting_the_cost_of_red_tape_for_business_in_South_Africa_Main_Report_June_2005.pdf, accessed on 15 July 2020.

²⁸¹*Louis K. Liggett Co. v. Lee* (1933) 288 U.S. 517 (United States of America Supreme Court), available at <https://caselaw.findlaw.com/us-supreme-court/288/517.html>, accessed on 20 July 2020; Chen, 'Race to the Bottom', available at <https://www.investopedia.com/terms/r/race-bottom.asp>, accessed 15 July 2020.

²⁸²*Ibid.*

²⁸³ IFWG CAR WG, 'Consultation paper on policy proposals for crypto assets', available at http://www.treasury.gov.za/comm_media/press/2019/CAR%20WG%20Consultation%20paper%20on%20crypto%20assets_final.pdf, accessed on 30 July 2019.

²⁸⁴Ponsford, (2015) 9 *Hong Kong Journal of Legal Studies* 29 at 33.

²⁸⁵ Oxford University Press (2010), available at <https://www.oxfordlearnersdictionaries.com/definition/english/pseudonym>, accessed 20 July 2020.

²⁸⁶ *Ibid.*

²⁸⁷Ponsford, (2015) 9 *Hong Kong Journal of Legal Studies* 29 at 33.

²⁸⁸ *Ibid.*

and beneficial owners²⁸⁹ behind crypto-asset transactions.²⁹⁰ Although every crypto-asset transaction is recorded in a distributed ledger that can be seen by the users of the crypto asset, a crypto-asset user is deemed to be anonymous as they can “hide” behind their account address.²⁹¹

As discussed in Chapter 2, crypto assets can be classified under various economic functions.²⁹² Crypto assets have the ability to perform the roles of a payment method, a unit of account, a means of trading and a way to store value.²⁹³ It can therefore be difficult to determine according to which function crypto assets should be regulated.²⁹⁴

South Africa is a member of international treaties²⁹⁵ and international groups such as the FATF, and the Eastern and Southern Africa Anti-Money Laundering Group.²⁹⁶ It is therefore important to implement and monitor the regulation of crypto assets in cooperation and coordination with these various groups.²⁹⁷ This will ensure that South Africa has an effective regulatory framework that does not contravene any international treaty, standard or principle of the various organisations that it is part of

²⁸⁹A beneficial owner as stated by the FATF in the general Glossary to the FATF Recommendations available at, <https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>, accessed on 20 July 2020:

‘refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.’

²⁹⁰Ponsford, (2015) 9 *Hong Kong Journal of Legal Studies* 29 at 33.

²⁹¹Hegerstrøm, *Virtual currency and its pseudonymous users: A decentralised system beyond the control of authorities* (unpublished LLD thesis, University of Oslo, 2017) 29-30).

²⁹²Spruyt, 2018 *TSAR* 707 at 713-717.

²⁹³ Ibid.

²⁹⁴ Hughes & Middlebrook, ‘Advancing a Framework for Regulating Cryptocurrency Payments Intermediaries’, (2015) 32(2) *Yale Journal on Regulation* 495 at 548.

²⁹⁵An example of such a treaty is ‘the Protocol against the Illicit Manufacturing of and Trafficking in Firearms Parts and Components and Ammunition, supplementing the United Nations Convention against Transnational Organised Crime(31 May 2001), available at http://www.dirco.gov.za/docs/2005pq/pq2_455.htm, accessed on 21 July 2020.

²⁹⁶ The subject matter of both these bodies is curbing financial crimes such as money laundering and terrorist financing.

²⁹⁷ The FATF conducts mutual evaluations (peer reviews) which are in-depth analysis of the effectiveness of a countries efforts and regulations to combat money laundering and the financing of terrorism. A report is given by the FATF which states to what degree a country is compliant with the FATF standards. FATF, ‘Mutual Evaluations’, available at [https://www.fatf-gafi.org/publications/mutualevaluations/more/more-about-mutual-evaluations.html?hf=10&b=0&s=desc\(fatf_releasedate\)](https://www.fatf-gafi.org/publications/mutualevaluations/more/more-about-mutual-evaluations.html?hf=10&b=0&s=desc(fatf_releasedate)), accessed on 21 July 2020.

and that South Africa has the best possible regulatory outcome aligned with international best practices.²⁹⁸

Crypto-asset-related activities have increased and at the time that the Intergovernmental Fintech Working Group Consultation Paper²⁹⁹ was published there were over 2 000 different crypto coins circulating in the market.³⁰⁰ Consumers and businesses are becoming more interested in the use of and investment in crypto assets. However, the exact market cap of crypto assets is difficult to determine and is currently unknown.³⁰¹ Hughes and Middlebrook observe that the increase in the use of crypto assets may put pressure on regulators to implement regulatory and supervisory measures sooner.³⁰² Their view is that, if regulators respond in a pressurized manner, it may result in over-regulation, under-regulation, regulatory arbitrage or the wrong regulatory tools and/or methods being utilised.³⁰³

4.3. The South African regulatory response

4.3.1. General

When considering a high-level overview of the current regulatory framework that impacts and affects South African banks and financial institutions, Spruyt points out that 53 acts of parliament, like the Financial Sector Regulation Act, the Financial Advisory and Intermediary Services Act 37 of 2002 and the Banks Act 94 of 1990, impact the financial sector specifically and another 149 acts of parliament, such as the Competition Act 89 of 1998, the Companies Act 71 of 2008, and the Protection of Personal Information Act 4 of 2013, impact the business sector in general.³⁰⁴ This means that there may be roughly 202 acts of parliament that will potentially affect crypto assets and related activities and the regulation thereof.

²⁹⁸IFWG CAR WG, 'Consultation paper on policy proposals for crypto assets', available at http://www.treasury.gov.za/comm_media/press/2019/CAR%20WG%20Consultation%20paper%20on%20crypto%20assets_final.pdf, accessed on 30 July 2020.

²⁹⁹ Ibid.

³⁰⁰ Ibid.

³⁰¹ Ibid.

³⁰² Hughes & Middlebrook, (2015) 32(2) *Yale Journal on Regulation* 495 at 546-549.

³⁰³ Ibid.

³⁰⁴ Spruyt, 2018 *TSAR* 707 at 715-717.

4.3.2. SARB Position Paper

The following section will discuss the SARB's position with respect to crypto assets. There is currently no specific act of parliament that has been passed in line with the SARB's mandate³⁰⁵ or otherwise to regulate crypto assets. However, the SARB released the SARB National Payment System Department Position Paper on virtual currencies³⁰⁶ ("SARB Position Paper"), in 2014, on crypto assets. The Intergovernmental Fintech Working Group Crypto Asset Regulators Working Group ("IFWG CAR WG") also released a consultation paper and position paper which will be discussed in more detail below.³⁰⁷ The SARB Position Paper is separated into five parts which are: the executive summary; the background of crypto assets; the classification of important terms and concepts; the risks posed by crypto assets; and the conclusion.

The executive summary of the SARB Position Paper highlights the need for the SARB to respond to crypto assets as far as they affect the SARB's mandate and responsibilities.³⁰⁸ It also provides a brief outline of the Position Paper.

³⁰⁵ Section 224(1) of the Constitution of the Republic of South Africa, 1996 states that 'The primary object of the South African Reserve Bank is to protect the value of the currency in the interest of balanced and sustainable economic growth in the Republic'.

³⁰⁶ South African Reserve Bank National Payment System Department, 'Position Paper on virtual currencies', available at [https://www.resbank.co.za/RegulationAndSupervision/NationalPaymentSystem\(NPS\)/Legal/Documents/Position%20Paper/Virtual%20Currencies%20Position%20Paper%20%20Final_02of2014.pdf](https://www.resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/Legal/Documents/Position%20Paper/Virtual%20Currencies%20Position%20Paper%20%20Final_02of2014.pdf), accessed on 15 June 2020.

³⁰⁷ SARB is also a member of the IFWG CAR WG; IFWG CAR WG, 'Consultation paper on policy proposals for crypto assets', available at http://www.treasury.gov.za/comm_media/press/2019/CAR%20WG%20Consultation%20paper%20on%20crypto%20assets_final.pdf, accessed on 30 July 2020; South African Reserve Bank National Payment System Department, 'Position Paper on virtual currencies', available at [https://www.resbank.co.za/RegulationAndSupervision/NationalPaymentSystem\(NPS\)/Legal/Documents/Position%20Paper/Virtual%20Currencies%20Position%20Paper%20%20Final_02of2014.pdf](https://www.resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/Legal/Documents/Position%20Paper/Virtual%20Currencies%20Position%20Paper%20%20Final_02of2014.pdf), accessed on 15 June 2020.

³⁰⁸ South African Reserve Bank National Payment System Department, 'Position Paper on virtual currencies', available at [https://www.resbank.co.za/RegulationAndSupervision/NationalPaymentSystem\(NPS\)/Legal/Documents/Position%20Paper/Virtual%20Currencies%20Position%20Paper%20%20Final_02of2014.pdf](https://www.resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/Legal/Documents/Position%20Paper/Virtual%20Currencies%20Position%20Paper%20%20Final_02of2014.pdf), accessed on 15 June 2020.

In the SARB Position Paper, a crypto asset is given the same definition³⁰⁹ as in the FATF Report³¹⁰ on virtual currencies. The SARB Position Paper gives a general brief discussion on convertible virtual currencies and it explains how virtual currencies perform similar functions as other functionalities in the financial system and also contrasts the differences between virtual currencies and other financial system functionalities. These have been discussed in paragraph 2.3 of Chapter 2.

An important clarification made in section 3 of the SARB Position Paper relates to the meaning of “legal tender”. The South African Reserve Bank Act 90 of 1989 (“SARB Act”) defines legal tender, in section 17, as a payment in the form of a banknote or otherwise wherein the SARB has taken responsibility in accordance with section 15(3)(c) of the Currency and Banking Act 31 of 1920 or in accordance with a contract entered into between the SARB and another bank. The SARB Act provides in section 14(1) that it is only the SARB that is able to legally issue legal tender in South Africa which can legally be given as payment to extinguish a debt wherein a creditor is obliged to accept such payment.³¹¹

As stated in the SARB Position Paper, crypto assets remain largely unregulated³¹² in South Africa.³¹³ Crypto assets are not legal tender, as discussed above, and creditors are not obliged to accept them as an adequate discharge of a debt or payment obligation.³¹⁴ There is no legal recourse or protection given at law for using crypto

³⁰⁹ ‘A virtual currency (VC) is a digital representation of value that can be digitally traded and functions as a medium of exchange, a unit of account and/or a store of value but does not have legal tender status.

³¹⁰ FATF Report, ‘Virtual Currencies: Key Definitions and Potential AML/CFT Risks’, available at <https://www.fatf-gafi.org/documents/documents/virtual-currency-definitions-aml-cft-risk.html>, accessed on 25 July 2020.

³¹¹ Section 14(1) of the SARB Act; South African Reserve Bank National Payment System Department, ‘Position Paper on virtual currencies’, available at [https://www.resbank.co.za/RegulationAndSupervision/NationalPaymentSystem\(NPS\)/Legal/Documents/Position%20Paper/Virtual%20Currencies%20Position%20Paper%20%20Final_02of2014.pdf](https://www.resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/Legal/Documents/Position%20Paper/Virtual%20Currencies%20Position%20Paper%20%20Final_02of2014.pdf), accessed on 15 June 2020.

³¹² The use of the words ‘largely unregulated’ is because the Taxation Laws Amendment Act 23 of 2018 has been amended to include the taxation of crypto assets in terms of tax laws. This will be discussed in more detail below.

³¹³ South African Reserve Bank National Payment System Department, ‘Position Paper on virtual currencies’, available at [https://www.resbank.co.za/RegulationAndSupervision/NationalPaymentSystem\(NPS\)/Legal/Documents/Position%20Paper/Virtual%20Currencies%20Position%20Paper%20%20Final_02of2014.pdf](https://www.resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/Legal/Documents/Position%20Paper/Virtual%20Currencies%20Position%20Paper%20%20Final_02of2014.pdf), accessed on 15 June 2020.

³¹⁴ Ibid.

assets in South Africa and the users thereof do so at their own risk.³¹⁵ The Position Paper discusses the risks posed by crypto assets but these have been thoroughly explained in Chapter 2.

Since the initial SARB Position Paper, there has not been any other statement released to alter the position of the SARB. The SARB Position Paper remains current and relevant save as to add that there has been a consultation paper³¹⁶ and position paper³¹⁷ issued by the IFWG CAR WG that considers the regulation of crypto assets in South Africa in more detail.

4.3.3. Taxation laws

The South African Revenue Service (“SARS”) released a media statement³¹⁸ in April 2018 on its position on how crypto assets will be treated in accordance with tax laws. Pursuant to the media statement, normal income tax rules now apply to crypto assets and crypto asset gains and losses must be declared as part of a taxpayer’s taxable income.³¹⁹ If taxpayers do not do so, they may incur penalties for such failure.³²⁰ Crypto assets are regarded as assets of an intangible nature by SARS and taxable income may be derived from mining for crypto assets, using crypto assets to pay for goods and services and trading with crypto assets.³²¹

The Taxation Laws Amendment Act 23 of 2018 has been promulgated in terms of which the Income Tax Act 58 of 1962 (“ITA”) and the Value Added Tax Act 89 of 1991

³¹⁵ Ibid.

³¹⁶ IFWG CAR WG, ‘Consultation paper on policy proposals for crypto assets’, available at http://www.treasury.gov.za/comm_media/press/2019/CAR%20WG%20Consultation%20paper%20on%20crypto%20assets_final.pdf, accessed on 30 June 2020.

³¹⁷ IFWG CAR WG, ‘Position Paper on crypto assets’, available at http://www.treasury.gov.za/comm_media/press/2020/20200414%20IFWG%20Position%20Paper%20on%20Crypto%20Assets.pdf, accessed on 29 June 2020.

³¹⁸ The South African Revenue Service, ‘Sars’s Stance On The Tax Treatment Of Cryptocurrencies’, available at <https://www.sars.gov.za/Media/MediaReleases/Pages/6-April-2018---SARS-stance-on-the-tax-treatment-of-cryptocurrencies-.aspx>, accessed on 15 June 2020.

³¹⁹ Ibid.

³²⁰ Ibid.

³²¹ Ibid.

(“VAT Act”) have been amended to include crypto assets within their regulatory ambit.³²²

The meaning of a financial instrument in section 1 of the ITA now includes crypto assets and section 20A of the ITA that addresses the ring-fencing of measured losses will also apply to crypto assets. The effect of this amendment is that investors can only offset their losses suffered from crypto asset related activities against future gains made from crypto-asset related activities and not against other forms of trade.³²³

Section 2 of the VAT Act has been modified to incorporate the “issue, acquisition, collection, buying or selling or transfer of ownership”³²⁴ of crypto assets as a financial service. The effect of this is that crypto-asset-related activity will be regarded as a VAT-exempt supply in line with section 12 of the VAT Act and will in effect be exempted from the taxes that are imposed in section 7(1)(a) of the VAT Act.

Although there is still much uncertainty with respect to the regulation of crypto assets, taxpayers are now aware of the tax implications associated with any crypto-asset-related activity they engage in.

4.3.4. Intergovernmental Fintech Working Group Crypto Asset Regulators Working Group

The IFWG CAR WG, that consists of several financial sector regulators,³²⁵ was formed in 2016 to monitor and assess the growth of fintech and innovation in South Africa, to determine how these developments affect the financial sector and what steps can be taken to optimize new opportunities presented by crypto assets, while mitigating against any possible risks that are posed to the effective and efficient functioning of

³²² Sections 1, 37 and 90 of The Taxation Laws Amendment Act 23 of 2018 contain the respective amendments to the ITA and VAT Act.

³²³ Section 20A of the ITA.

³²⁴ Section 2 of the VAT Act.

³²⁵ These financial sector regulators include: the National Treasury, the Financial Intelligence Centre, the Financial Sector Conduct Authority, the National Credit Regulator, the South African Reserve Bank and the South African Revenue Service.

South Africa's financial system.³²⁶ The IFWG CAR WG issued the Consultation Paper on policy proposals for crypto assets³²⁷ ("Consultation Paper"), for public discussion in January 2019.

The IFWG CAR WG included in its work attempts to unify terms used to refer to crypto assets. It has defined crypto assets as:

"...digital representations or tokens that are accessed, verified, transacted, and traded electronically by a community of users. Crypto assets are issued electronically by decentralised entities and have no legal tender status, and consequently are not considered as electronic money either. It therefore does not have statutory compensation arrangements. Crypto assets have the ability to be used for payments (exchange of such value) and for investment purposes by crypto asset users. Crypto assets have the ability to function as a medium of exchange, and/or unit of account and/or store of value within a community of crypto asset users."³²⁸

The Consultation Paper proposes a crypto asset regulatory approach that will be implemented in three phases. Phase one of the approach will be the registration process for crypto-asset service providers.³²⁹ The Consultation Paper does not stipulate who will be responsible for this registration process. The purpose of the registration process is for the financial sector regulators to know and gain insights from the market participants.³³⁰

The purposes of phase two will be to review whether crypto assets fit into the current regulatory framework.³³¹ Where it is seen that crypto-asset-related activity is not adequately regulated by the current regulatory framework in areas where it should be, the regulatory framework will be amended to bring such activity into the scope of its mandate and if it is unrealistic to do so, new regulations will be drafted.³³² This phase

³²⁶IFWG CAR WG 'Consultation paper on policy proposals for crypto assets', available at http://www.treasury.gov.za/comm_media/press/2019/CAR%20WG%20Consultation%20paper%20on%20crypto%20assets_final.pdf, accessed on 30 June 2020.

³²⁷ Ibid.

³²⁸ Ibid.

³²⁹ Ibid.

³³⁰ Ibid.

³³¹ Ibid.

³³² Ibid.

will cover the regulatory adjustments and amendments that need to be made, determine the services that will be covered, clarify definitions and it will also address the kind of protection that consumers transacting with crypto assets will be given.³³³

The final phase will be an appraisal of the regulatory actions implemented to determine whether the intended objectives of the regulatory actions were achieved.³³⁴ The Consultation Paper does not go on further to explain other details such as: benchmarks or key indicators for each phase, processes and approaches to be followed in each phase, nor are there any deadlines or other timelines given for the completion of each phase.³³⁵ The Position Paper on crypto assets³³⁶ (“Policy Paper”) issued in April 2020 is similar to the Consultation Paper in terms of structure and content with the exception of the policy recommendations that it proposes. This Position Paper on crypto assets will be discussed in more detail below, in relation to its policy recommendations, as part of the proposed regulatory framework.

4.4. Proposed framework

4.4.1 General

When considering how to regulate crypto assets a specific consideration to be borne in mind is whether the regulation of crypto assets should require new legislation or whether they should be regulated in the same way as the products that they compete with.³³⁷ For example, crypto assets can function as a payment method; thus it can be considered whether the current regulatory framework applicable to payment methods can be applied to crypto assets or whether new regulations need to be promulgated to bring crypto assets into the scope of regulation.³³⁸ The following section will make policy proposals for regulating crypto assets taking into consideration the Position

³³³ Ibid.

³³⁴ Ibid.

³³⁵ Reddy & Lawack, (2019) *SA Merc LJ* 3 at 16.

³³⁶ IFWG CAR WG ‘Position Paper on crypto assets’, Available at http://www.treasury.gov.za/comm_media/press/2020/20200414%20IFWG%20Position%20Paper%20on%20Crypto%20Assets.pdf, accessed on 29 June 2020.

³³⁷ Hughes & Middlebrook, (2015) 32(2) *Yale Journal on Regulation* 495 at 546-54.

³³⁸ IFWG CAR WG, ‘Consultation paper on policy proposals for crypto assets’, available at http://www.treasury.gov.za/comm_media/press/2019/CAR%20WG%20Consultation%20paper%20on%20crypto%20assets_final.pdf, accessed on 30 June 2020.

Paper³³⁹ on crypto assets published by the IFWG CAR WG and the recommendations made therein.

4.4.2 Position Paper on crypto assets

The IFWG CAR WG pointed out that regulators need to unify definitions and have a clear understanding of who will be covered within the scope of their regulation.³⁴⁰ Regulations in this regard should stipulate the functions and key activities of crypto-asset market participants and they should designate risks.³⁴¹ This will enable market participants to ascertain their risk exposure and allocate their resources accordingly, depending on their risk portfolio.³⁴²

Recommendation 1 of the Position Paper defines and classifies the framework's subject matter and covered participants of regulation as "crypto asset service providers" ("CASPs"). It defines the CASPs as well as the services offered by the CASPs that will be subject to regulation.³⁴³ This recommendation takes into account FATF recommendation 15,³⁴⁴ which imposes an obligation on regulators and financial service providers to consider the money laundering and terrorist funding risks that are related to new fintech innovations and to mitigate against these risks.³⁴⁵ This means

³³⁹ IFWG CAR WG 'Position Paper on crypto assets', Available at http://www.treasury.gov.za/comm_media/press/2020/20200414%20IFWG%20Position%20Paper%20on%20Crypto%20Assets.pdf, accessed on 29 June 2020.

³⁴⁰ Ibid.

³⁴¹ Ibid.

³⁴² Hughes & Middlebrook, (2015) 32(2) *Yale Journal on Regulation* 495 at 546-54.

³⁴³ IFWG CAR WG 'Position Paper on crypto assets', Available at http://www.treasury.gov.za/comm_media/press/2020/20200414%20IFWG%20Position%20Paper%20on%20Crypto%20Assets.pdf, accessed on 29 June 2020.

³⁴⁴ FATF recommendation 15 states that:

'Countries and financial institutions should identify and assess the money laundering or terrorist financing risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products. In the case of financial institutions, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. They should take appropriate measures to manage and mitigate those risks.'

FATF, 'International Standards on Combating Money Laundering and the Financing Of Terrorism & Proliferation- The FATF Recommendations', available at <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>, accessed on 15 June 2020.

³⁴⁵ Ibid.

that because CASPs are a new fintech development they need to be brought into the scope of AML/CFT regulations.³⁴⁶

For purposes of regulation, the following are regarded as crypto asset service providers in South Africa: any entity facilitating or providing crypto asset trading platforms;³⁴⁷ crypto asset vending machine providers;³⁴⁸ crypto-asset token issuer;³⁴⁹ crypto-asset fund or derivative service provider;³⁵⁰ crypto-asset custodial wallets; and crypto asset custodial services.³⁵¹ In addition, as suggested by Hughes and Middlebrook, a person who issues a crypto-asset payment or transaction instruction to any crypto-asset transaction or payment facilitator should be known as the “initiator”.³⁵² A “beneficiary” should be the person who is the recipient of the payment or transaction instruction issued by the initiator.³⁵³

It is suggested in the Position Paper that Schedule 1 to the Financial Intelligence Centre Act 38 of 2002 (“FICA”), should be amended to include CASPs to the listed accountable institutions.³⁵⁴ The implication of this is that legal requirements pursuant to chapter 3 of the FICA which includes customer due diligence,³⁵⁵ a duty to keep record,³⁵⁶ financial sanctions,³⁵⁷ responsibilities regarding reporting and allowing authorised personnel of the Financial Intelligence Centre to access needed information,³⁵⁸ and procedures to encourage compliance by accountable institutions,³⁵⁹ will be applicable to CASPs.

³⁴⁶ IFWG CAR WG, ‘Position Paper on crypto assets’, available at http://www.treasury.gov.za/comm_media/press/2020/20200414%20IFWG%20Position%20Paper%20on%20Crypto%20Assets.pdf, accessed on 29 June 2020.

³⁴⁷ These services include providing intermediary services for crypto assets related transactions such as buying and selling crypto assets, converting or exchanging crypto assets into fiat currency or other crypto assets and remittance services.

³⁴⁸ Ibid.

³⁴⁹ These include services related to initial coin offerings and the issuance of stablecoins.

³⁵⁰ These services include offering investment and derivative products with the underlying asset being a crypto asset.

³⁵¹ These services include providing the software to enable custodial services and offering custodial services including safeguarding and storage of a crypto asset belonging to another person.

³⁵² Hughes & Middlebrook, (2015) 32(2) *Yale Journal on Regulation* 495 at 546.

³⁵³ Ibid.

³⁵⁴ Position Paper on crypto assets recommendation 2, 11 and 20.

³⁵⁵ Part 1 of chapter 3 of FICA.

³⁵⁶ Part 2 of chapter 3 of FICA.

³⁵⁷ Part 2A of chapter 3 of FICA.

³⁵⁸ Part 3 of chapter 3 of FICA.

³⁵⁹ Part 4 of chapter 3 of FICA.

In terms of FICA, CASPs will thus be required to identify their customers satisfactorily and ensure the veracity of the information that they have regarding their clients on an ongoing basis.³⁶⁰ Where necessary enhanced due diligence measures will need to be applied.³⁶¹ They will be obliged to keep information regarding their customers, their business relationship with the said customer as well as transactions effected by the customer pursuant to the business relationship.³⁶² The records that are to be kept by the CASPs should be kept for five years either by the CASP or a third party.³⁶³ In addition, CASPs must report transactions and series of transactions that exceed the prescribed threshold,³⁶⁴ report transactions that they reasonably believe are suspicious or unusual³⁶⁵ and file reports on any property that they have under their control or in their possession that is associated with terrorist activity or terrorist organisations.³⁶⁶ CASPs will also be required to “develop, document, maintain and implement”³⁶⁷ a Risk Management and Compliance Programme that is able to categorise the CASPs’ different classes of risks that they face and allocate their resources proportionately to their various risk classes.³⁶⁸

Compliance with the FICA requirements by CASPs must be monitored and non-compliance will attract remedial action and where such remedial action does not have the desired effect, administrative sanctions can be imposed.³⁶⁹ The FIC will be responsible for this supervisory oversight, in relation to AML/CFT, to ensure compliance by CASPs.³⁷⁰

³⁶⁰ Sections 20A-21H of FICA.

³⁶¹ Ibid.

³⁶² Sections 22-25 of FICA.

³⁶³ Ibid.

³⁶⁴ The current cash transaction threshold is R24 999.99.

³⁶⁵ Section 29 of FICA.

³⁶⁶ Section 28 of FICA.

³⁶⁷ Section 42 of FICA.

³⁶⁸ Ibid.

³⁶⁹ IFWG CAR WG, ‘Position Paper on crypto assets’, available at http://www.treasury.gov.za/comm_media/press/2020/20200414%20IFWG%20Position%20Paper%20on%20Crypto%20Assets.pdf, accessed on 29 June 2020.

³⁷⁰ Ibid.

Furthermore, it is suggested that section 3(1) of the Financial Sector Regulation Act and the Conduct of Financial Institutions Bill³⁷¹ should be amended to include CASPs under the definition of a financial service.³⁷² It is also suggested that the Financial Markets Act 19 of 2012 should be amended to include crypto assets as a financial instrument.³⁷³ However, there should be restrictions with respect to which investment vehicles are allowed to use crypto assets.³⁷⁴

Regulators such as the Financial Sector Conduct Authority (FSCA), Prudential Authority (PA), SARB, SARS, and National Treasury need to consider their respective responsibilities as regulators and determine how their respective scope of regulation will need to be amended to incorporate crypto assets and the use thereof into the scope of their regulation.³⁷⁵ For example, the PA needs to determine prudential and reporting requirements for CASPs.³⁷⁶

Monitoring the development and use of crypto assets will be an ongoing process³⁷⁷ whilst holding the position that crypto assets are not legal tender.³⁷⁸ The IFWG CAR WG suggests that crypto assets should not interact with SAMOS for the time being until the National Payment Systems Department³⁷⁹ has determined how crypto-asset-related transactions will be recorded and settled. Similarly, other financial market infrastructure should not interface with crypto assets until it is determined how crypto assets will be regulated.³⁸⁰

4.4.3 My recommendations

³⁷¹National Treasury, 'Conduct Of Financial Institutions Bill'.available at <http://www.treasury.gov.za/twinpeaks/Conduct%20of%20Financial%20Institutions%20Bill.pdf>, accessed on 30 June 2020.

³⁷² Position Paper on crypto assets recommendation 9.

³⁷³ Position Paper on crypto assets recommendation 22-24, such as 'over-the-counter' financial instruments.

³⁷⁴ For example, they should not be used for collective investment schemes and potentially pension funds asset spreading.

³⁷⁵ IFWG CAR WG, 'Position Paper on crypto assets', available at http://www.treasury.gov.za/comm_media/press/2020/20200414%20IFWG%20Position%20Paper%20on%20Crypto%20Assets.pdf, accessed on 29 June 2020.

³⁷⁶ Position Paper on crypto assets recommendation 10-18.

³⁷⁷ Position Paper on crypto assets recommendation 4.

³⁷⁸ Position Paper on crypto assets recommendation 5.

³⁷⁹ Position Paper on crypto assets recommendation 21.

³⁸⁰ Position Paper on crypto assets recommendation 6.

In addition to the recommendations made by the IFWG CAR WG, regulators can consider regulations related to the timing and effect of a crypto-asset transaction, the obligations and responsibilities of a CASP when they receive a payment instruction, to what extent crypto assets discharge the underlying obligation, fees and fee disclosures and any other miscellaneous issue, which can include matters such as offering crypto-asset-related credit services.³⁸¹ In light of this, I would recommend the following:

As recommended by the IFWG CAR WG, CASPs should not interface with the national payment system until it has been clearly established how this will be done.³⁸² It is further recommended that it should be a requirement for any CASP that interfaces with the national payment system to be duly registered as a legal person so that the CASP can be held legally accountable.³⁸³ Furthermore, a fiduciary duty should be imposed on CASPs to uphold the integrity of the national payment system and all other core functions related thereto.³⁸⁴ CASPs must also adhere to and comply with the regulatory and supervisory requirements of the overall payment system as required by the National Payments Systems Act 78 of 1998 and the Payment Association of South Africa.³⁸⁵

Consumer financial protection laws should be enacted and amended to protect consumers against financial risks that arise from using crypto assets.³⁸⁶ These laws can include requirements for corporate governance for the management of a crypto asset company, prudential, liquidity and capital requirements and the requirement to

³⁸¹ Hughes & Middlebrook, (2015) 32(2) *Yale Journal on Regulation* 495 at 546-54.

³⁸² Position Paper on crypto assets Recommendation 6.

³⁸³ Virga, 'International criminals and their virtual currencies: The need for an international effort in regulating virtual currencies and combating cybercrime' (2015) 12(2) *Brazilian Journal of International Law* 512 at 522.

³⁸⁴ 'Blockchain development and fiduciary duty' (2019) 2(2) *Stanford Journal of Blockchain Law & Policy* 1 at 3, 8-9.

³⁸⁵ The legal foundation governing participation in a particular payment system in the PASA environment is contained in a Payment Clearing House ('PCH') agreement. Specific transaction types and Clearing Rules are agreed upon amongst participating members. PCH Systems Operator (PSO) facilitate clearing of payment instructions between the banks. The participation of members and the PSO is managed through adherence to Service Level Agreements. Payment association of South Africa, 'legal and regulatory framework', available at <http://www.pasa.org.za/national-payment-system/legal-regulatory-framework>, accessed on 31 July 2020.

³⁸⁶ Lee, Long, McRae, Steiner, & Handler, (2015) 16(1) *Business Law International* 21 at 40.

be transparent and accountable to regulators³⁸⁷ - these measures would be aimed at protecting individual users.³⁸⁸ Laws that protect consumers like the National Credit Act and the Financial Sector Regulation Act can be expanded to incorporate CASPs in the scope of their application.³⁸⁹ Some consumer protection laws, such as the National Credit Act, protect individual customers and small businesses that fall within a prescribed limit.³⁹⁰ In a similar way, crypto-asset laws can limit the scope of their application to individual consumers and small businesses that do not specialise in cryptographic work.

It is further agreed (as Godlove suggests) that regulators should consider implementing a consumer financial protection law that regulates electronic fund transfers and the risk allocation and obligations in that regard.³⁹¹ This will also assist in determining how the risks should be allocated between a consumer and a CASP.³⁹² In these regulations, the rights and obligations of consumers, CASPs, the beneficiaries of the transaction and other businesses that may be needed to conclude the transaction should be clearly stipulated.³⁹³ This will allow market participants to know what is expected of them and for them also to know what they can expect.³⁹⁴ The purpose of these regulations should be to protect the consumers in the transactions.³⁹⁵

I also agree with Rusch that minimum security procedures and requirements that include how the CASP will verify that the instruction was given by the consumer need to be included.³⁹⁶ These security procedures can also stipulate how unauthorised instructions will be identified and dealt with as well as transmission and conversion

³⁸⁷ For example, CASPS can be required to disclose their audited or reviewed financial statements to regulators such as the Prudential Authority.

³⁸⁸ Hughes & Middlebrook, (2015) 32(2) *Yale Journal on Regulation* 495 at 546-54.

³⁸⁹ Lee, Long, McRae, Steiner, & Handler (2015) 16(1) *Business Law International* 21 at 40.

³⁹⁰ In terms of a legal person, the NCA is applicable to a company whose asset value or annual turnover, together with the combined asset value or annual turnover of all related juristic persons, at the time the credit agreement is made, does not exceed R 1 000 000. The NCA protects and applies to all natural persons.

³⁹¹ Godlove 'Regulatory Overview of Virtual Currency' 2014 (10) *Oklahoma Journal of Law and Technology* 1 at 43.

³⁹² *Ibid.*

³⁹³ *Ibid.*

³⁹⁴ *Ibid.*

³⁹⁵ *Ibid.*

³⁹⁶ Rusch, 'Reimagining payment systems: Allocation of risk for unauthorized payment inception' (2008) 83(2) *Chicago-Kent Law Review* 561 at 583-4.

errors.³⁹⁷ This can be done as an industry practice, that can be captured like the Code of Banking Practice.³⁹⁸ In this industry practice, CASPs would be required to stipulate the scope and extent of their responsibility and that of the customer when an instruction has been issued, received and processed.³⁹⁹ CASPs should also not be forced to accept or process payment or transaction instructions that do not adhere to the minimum security procedures that are required.⁴⁰⁰

As suggested by Hughes and Middlebrook, a regulation should be enacted that provides for the resolution of errors in three areas,⁴⁰¹ namely: where the incorrect amount has been paid over to the beneficiary; if the funds are not made available to the beneficiary on the stipulated date; and where the payment was made to the incorrect recipient.⁴⁰² The time period wherein the error should be reported can be adjusted with industry practice and a time period that is practical can be used based on the feedback from the market.⁴⁰³

Paragraph 6.6 of the Code of Banking Practice states that banks will inform their customers about the relevant fees and charges that they charge for the products and services that a customer chooses. Banks use various platforms to alert their customers to these fees and charges.⁴⁰⁴ The costs of transactions, services and products are also made available to the customer to enable them to compare prices with other banks.⁴⁰⁵ The Code of Banking Practice further states that banks will notify their customers 20 business days before any change to the fees and charges charged to the customer takes effect and also state the basis for that change in at least two of the manners stated in paragraph 6.6.6 of the Code of Banking Practice.⁴⁰⁶ The Code of

³⁹⁷ Ibid.

³⁹⁸ The Banking association of South Africa, 'Code of Banking Practice', Available at <https://www.banking.org.za/wp-content/uploads/2019/04/Code-of-Banking-Practice-2012.pdf>, accessed on 01 July 2020.

³⁹⁹ Ibid.

⁴⁰⁰ Ibid.

⁴⁰¹ Hughes & Middlebrook, (2015) 32(2) *Yale Journal on Regulation* 495 at 546.

⁴⁰² Ibid.

⁴⁰³ Ibid.

⁴⁰⁴ Code of Banking Practice paragraph 6.6.

⁴⁰⁵ Ibid.

⁴⁰⁶ Ibid. These methods include: letters, statement messages or other personal notices; notices or leaflets in branches or outlets; ATM or electronic banking system messages; telephonic announcements, e-mail or short message service; announcements on our website or any other electronic media; media advertisements or any other communication channel available to the banks.

Banking Practice is not legislation but simply a voluntary standard that banks adhere to that sets the minimum standards and conduct that customers (natural persons and small businesses) can expect from banks.⁴⁰⁷ I recommend that a similar standard code of practice relating to fees and fees disclosures should be written and adhered to by CASPs so that customers are aware of what they can expect with respect to the fees charged by CASPs.

Paragraph 7.7 of the Code of Banking Practice includes provisions for protecting the account of the customer. It is the customer's responsibility to keep the bank up to date with respect to their personal information such as their phone number and email address.⁴⁰⁸ Furthermore, customers need to take reasonable care to ensure that their banking information including their personal identification number and online account information is not disclosed to other people.⁴⁰⁹ The passwords that are used by the customer should not be easy to guess such as a customer's name or date of birth.⁴¹⁰ Similar requirements can be imposed on crypto-asset customers to ensure that their accounts are protected and not easily hackable. Crypto-asset transactions are "computationally impractical to reverse";⁴¹¹ therefore it is important that customers protect their accounts in such a manner or manners that the account is not hacked, as reversing an incorrect transaction may not be feasible, practical or even possible.

Paragraph 7.8 of the Code of Banking Practice provides the responsibility that the bank will take if a customer's bank account is misused. The responsibility of the customer is to demonstrate that they did not act fraudulently, negligently or without the necessary care.⁴¹² CASPs should also provide some sort of recourse if the customer can show that they were not the author of their own misfortune.

The compliance requirements for CASPs can be implemented in stages to ensure that regulators do not stifle the growth of the industry while at the same time being able to

⁴⁰⁷ Code of Banking Practice.

⁴⁰⁸ Ibid.

⁴⁰⁹ Ibid.

⁴¹⁰ Ibid.

⁴¹¹ Animashaun, 'Regulating virtual currency payment systems' (2019) 4(2) Cambridge Law Review 29 at 41.

⁴¹² Code of Banking Practice.

monitor, regulate and supervise CASPs and being able to ensure the financial stability of the economy and the protection of the consumers.⁴¹³

⁴¹³ Similar to the three-phase approach that was proposed in the IFWG Crypto Assets Regulatory Working Group, 'Consultation paper on policy proposals for crypto assets', available at http://www.treasury.gov.za/comm_media/press/2019/CAR%20WG%20Consultation%20paper%20on%20crypto%20assets_final.pdf, accessed on 30 July 2019.

Chapter 5 Conclusion

This paper has discussed various aspects of virtual currencies including the differentiation between e-money and virtual currencies, their various functions, classifications and virtual currency payment system participants. The importance of regulating virtual currencies stems from the risks that they pose to the current financial system. These risks were discussed and international approaches were also considered with a particular focus on the USA and China. Chapter 4 discussed the challenges to regulating virtual currencies, considered South Africa's current regulatory response and proposed a regulatory framework for regulating virtual currencies in South Africa.

Virtual currencies have been widely discussed by various international regulatory agencies as well as national regulators to determine how, if possible, to fit them into their current regulatory frameworks.⁴¹⁴ If used properly, this new fintech has potential benefits for the financial system but can also be detrimental if the risks that it poses materialise.⁴¹⁵ Due to the differences in approaches taken by different countries to regulating virtual currencies, it could take a while to synergise a holistic global approach for using and regulating virtual currencies.⁴¹⁶ In the interim, the regulation of virtual currencies can be dealt with in a piecemeal fashion with various international regulators, such as the FATF or the Bank of International Settlement issuing their own directives regarding how to approach the supervision and use of virtual currencies.⁴¹⁷

Regulating virtual currencies is important for the smooth integration of virtual currencies into the current financial system, to level the playing field between this currently unregulated market that competes directly with the regulated financial system, to increase consumer protection and to ensure that as virtual currencies interact with the real economy, financial stability is not compromised.⁴¹⁸

⁴¹⁴Lemchuk, (2017) 15(2) *Cardozo Public Law, Policy and Ethics Journal* 319 at 350.

⁴¹⁵ Ibid.

⁴¹⁶Goldsmith, 2020 34(2) *Emory International Law Review* 595 at 637.

⁴¹⁷Ibid.

⁴¹⁸ Morton, (2020) 16(1) *Loyola University Chicago International Law Review* 129 at 143.

BIBLIOGRAPHY

Legislation

Banks Act 94 of 1990

Bill C31 amendments to The Proceeds of Crime (Money Laundering) and Terrorist Financing Act 2000

Companies Act 71 of 2008

Competition Act 89 of 1998

Constitution of the Republic of South Africa, 1996

Consumer Protection Act 68 of 2008

Currency and Exchanges Act 9 of 1933

Financial Advisory and Intermediary Services Act 37 of 2002

Financial Intelligence Centre Act 38 of 2001

Financial Markets Act 19 of 2012

Financial Sector Regulatory Act 9 of 2017

Income Tax Act 58 of 1962

National Credit Act 34 of 2005

Protection of Personal Information Act 4 of 2013

South African Reserve Bank Act 90 of 1989

Taxation Laws Amendment Act 23 of 2018

The Code of Federal Regulations

The United States Code

Value Added Tax Act 89 of 1991

Journal articles

Alvarez M, 'Comparative Analysis of Cryptocurrency Regulation in the United States, Nigeria, and China: The Potential Influence of Illicit Activities on Regulatory Evolution' (2018) 25(1) ILSA Journal of International and Comparative Law 33

Alkadri S, 'Defining and Regulating Virtual currency: Fake Internet Money or Legitimate Medium of Exchange' (2018-2019) 17 Duke Law & Technology Review 71

Animashaun S, 'Regulating virtual currency payment systems' (2019) 4(2) Cambridge Law Review 29

Bech & Garratt 'Central bank cryptocurrencies' Bank for International Settlements Quarterly Review (2017) 55

'Blockchain development and fiduciary duty' (2019) 2(2) Stanford Journal of Blockchain Law & Policy 1

Bollen R, 'What a Payment Is (and How it Continues to Confuse Lawyers)' (2005) Macquarie Journal of Business Law 189

Brühl V, 'Virtual Currencies, Distributed Ledgers and the Future of Financial Services' 2017 52(6) Intereconomics Review of European Economic Policy 370

Chung J, 'Money as Simulacrum: The Legal Nature and Reality of Money' (2009) Hastings Business Law Journal 112

Comizio V, 'Virtual Currencies: Growing Regulatory Framework and Challenges in the Emerging Fintech Ecosystem' (2017) 21 North Carolina Banking Institute 131

Cortez N, 'Regulating Disruptive Innovation' (2014) 29(1) Berkeley Technology Law Journal 175

Doguet J, 'The nature of the form: Legal and regulatory issues surrounding the bitcoin digital currency system' (2013) 73(4) Louisiana Law Review 1119

Gatto J & E Broeker, 'Bitcoin and beyond: Current and future regulation of virtual currencies' (2015) 9(2) Ohio State Entrepreneurial Business Law Journal 429

Glass J, 'What is digital currency' (2017) 57(3) IDEA: The Journal of the Franklin Pierce Center for Intellectual Property 455

Godlove N 'Regulatory Overview of Virtual Currency' 2014 (10) Oklahoma Journal of Law and Technology

Goforth C, 'The Lawyer's Cryptionary: A Resource for Talking to Clients about Crypto-transactions' (2019) 41(1) Campbell Law Review 47

Goldsmith J, 'The IMF must develop best practices before government-backed cryptocurrencies destabilize the international monetary system' 2020 34(2) Emory International Law Review 595

Haynes & Yeoh, 'Legal issues arising from the utilisation of blockchain-based products in the 4th industrial revolution' Annual Banking Law Update (2020) 47

Hughes S & Middlebrook S, 'Advancing framework for regulating cryptocurrency payments intermediaries' (2015) 32(2) Yale Journal on Regulation 495

Kirby P, 'Virtually possible: How to strengthen bitcoin regulation within the current regulatory framework' (2014) 93(1) North Carolina Law Review 195

Lee J, Long A, McRae M, Steiner J, & Handler S, 'Bitcoin basics: primer on virtual currencies' (2015) 16(1) Business Law International 21

Lemchuk A, 'Virtual whats: Defining virtual currencies in the face of conflicting regulatory guidances' (2017) 15(2) Cardozo Public Law, Policy and Ethics Journal 319

Mainka S, 'Algorithm-based recruiting technology in the workplace' (2019) 5(3) Texas A&M Journal of Property Law 801

Marian O, 'A Conceptual Framework for the Regulation of Cryptocurrencies' (2015-2016) 82 University of Chicago Law Review Dialogue 53

Mandjee T, 'Bitcoin, Its Legal Classification and Its Regulatory Framework' (2014) 15(2) Journal of Business and Securities Law 1

McPeak A, 'Disruptive technology and the ethical lawyer' (2019) 50(3) University of Toledo Law Review 457

Morton D, 'The future of cryptocurrency: An unregulated instrument in an increasingly regulated global economy' (2020) 16(1) Loyola University Chicago International Law Review 129

Ponsford M, 'Comparative Analysis of Bitcoin and Other Decentralised Virtual Currencies: Legal Regulation in the People's Republic of China, Canada, and the United States' (2015) 9 Hong Kong Journal of Legal Studies 29

Reddy E & Lawack V, 'An overview of the regulatory developments in South Africa regarding the use of virtual currencies' (2019) SA Merc LJ 3

Rosner M & Kang A, 'Understanding and regulating twenty-first century payment systems: The ripple case study' (2016) 114(4) Michigan Law Review 649

Rusch L, 'Reimagining payment systems: Allocation of risk for unauthorized payment inception' (2008) 83(2) Chicago-Kent Law Review 561

Ryan P, Glass H, Governatori G, Lindsay D, Lumsden A, Nayyar R, Salon B, & Watt M, 'Sydney Node' (2018) 1 Stanford Journal of Blockchain Law & Policy 90

Spruyt W 'An assessment of the emergent functions of virtual currencies' 2018 TSAR 707

Syska S, 'Eight-years-young: How the new york bitlicense stifles bitcoin innovation and expansion with its premature attempt to regulate the virtual currency industry' (2017) 17(2) Journal of High Technology Law 313

Tu K & Meredith M, 'Rethinking virtual currency regulation in the bitcoin age' (2015) 90(1) Washington Law Review 271

Van Adrichem B 'Howey Should Be Distributing New Virtual currencies: Applying the Howey Test to Mining, Airdropping, Forking, and Initial Coin Offerings' (2019) 20(2) Columbia Science and Technology Law Review 388

Vessio, 'To CBDC or not to CBDC? Exploring central bank digital currency' *Annual Banking Law Update* (2020) 63

Virga J, 'International criminals and their virtual currencies: The need for an international effort in regulating virtual currencies and combating cybercrime' (2015) 12(2) *Brazilian Journal of International Law* 512

Xie R, 'Why China Had to Ban Virtual currency but the U.S. Did Not: A Comparative Analysis of Regulations on Crypto-Markets between the U.S. and China' (2019) 18(2) *Washington University Global Studies Law Review* 457

Case law

Louis K. Liggett Co. v. Lee (1933) 288 U.S. 517

Securities and Exchange Commission v. Trendon T. Shavers and Bitcoin Savings and Trust (2013) 4:13-CV-416 (United States Eastern District of Texas Sherman Division August)

Securities and Exchange Commission v. W. J. Howey Co (1946) 328 U.S. 293

Thesis

Hegerstrøm, Virtual currency and its pseudonymous users: A decentralised system beyond the control of authorities (unpublished LLD thesis, University of Oslo, 2017) 29-30)

Internet sources

Bank of International settlements, 'The payment system in South Africa', available at <https://www.bis.org/cpmi/paysys/southafrica.pdf>, accessed on 01 May 2020

CFTC's Chilton' Eyes Bitcoin 'House of Cards' Risk (CNBC television broadcast May 7, 2013), available at <http://video.cnbc.com/gallery/?video=3000166533>, accessed on 24 June 2020.

Coie 'Digital Currencies: International Actions and Regulations', available at

<https://www.perkinscoie.com/en/news-insights/digital-currencies-international-actions-and-regulations.html#South%20Africa>, accessed on 05 August 2019.

The Banking association of South Africa, 'Code of Banking Practice', Available at <https://www.banking.org.za/wp-content/uploads/2019/04/Code-of-Banking-Practice-2012.pdf>, accessed on 01 July 2020.

Coinjar, 'How cryptocurrency breaks down the barriers for a borderless world', available at <https://blog.coinjar.com/2019/06/18/how-cryptocurrency-breaks-down-the-barriers-for-a-borderless-world/>, accessed on 15 July 2020.

CoinPursuit 'An In-Depth Look at Cryptocurrency Mining Algorithms', available at <https://www.coinpursuit.com/articles/an-in-depth-look-at-cryptocurrency-mining-algorithms.179/>, accessed 10 September 2020

Darroll, 'Strategic partnerships for business growth in Africa: COUNTING THE COST OF RED TAPE for business in South Africa', available at http://www.sbp.org.za/uploads/media/Counting_the_cost_of_red_tape_for_business_in_South_Africa_Main_Report_June_2005.pdf, accessed on 15 July 2020.

Department of the Treasury Financial crimes enforcement Network "Administrative Rulings" [https://www.fincen.gov/resources/statutes-regulations/administrative-rulings#:~:text=The%20Financial%20Crimes%20Enforcement%20Network%20\(%E2%80%9CFinCEN%E2%80%9D\)%20is%20issuing,involvement%20in%20transportation%20of%20currency.](https://www.fincen.gov/resources/statutes-regulations/administrative-rulings#:~:text=The%20Financial%20Crimes%20Enforcement%20Network%20(%E2%80%9CFinCEN%E2%80%9D)%20is%20issuing,involvement%20in%20transportation%20of%20currency.)

Department of the Treasury Financial crimes enforcement Network, 'Application of FinCen's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies', available at <https://www.FinCen.gov/sites/default/files/shared/FIN-2013-G001.pdf>, accessed on 03 June 2020.

Department of the Treasury Financial crimes enforcement Network, 'Application of FinCen's Regulations to Virtual Currency Mining Operations', available at <https://www.FinCen.gov/sites/default/files/shared/FIN-2014-R001.pdf>, accessed on 04 June 2020.

Department of the Treasury Financial crimes enforcement Network, 'Application of FinCen's Regulations to Virtual Currency Software Development and Certain Investment Activity', available at <https://www.FinCen.gov/sites/default/files/shared/FIN-2014-R002.pdf>, accessed on 04 June 2020.

European Banking Authority 'Opinion on Virtual Currencies (2014)', available at <https://eba.europa.eu/sites/default/documents/files/documents/10180/657547/81409b94-4222-45d7-ba3b-7deb5863ab57/EBA-Op-2014-08%20Opinion%20on%20Virtual%20Currencies.pdf?retry=1>, accessed on 15 March 2020.

European Parliament 'Virtual currencies and Blockchain', available at <http://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20virtual%20currencies%20and%20blockchain.pdf>, accessed on 29 August 2019.

Financial Action Task Force 'Glossary to the FATF Recommendation's available at, <https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>, accessed on 20 July 2020:

Financial Action Task Force 'Guidance for a Risk-Based Approach-Virtual Currencies' available at <https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf>, accessed on 01 July 2020

Financial Action Task Force, 'International Standards on Combating Money Laundering and the Financing Of Terrorism & Proliferation- The FATF Recommendations', available at <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>, accessed on 15 June 2020.

Financial Action Task Force, 'Mutual Evaluations', available at [https://www.fatf-gafi.org/publications/mutualevaluations/more/more-about-mutual-evaluations.html?hf=10&b=0&s=desc\(fatf_releasedate\)](https://www.fatf-gafi.org/publications/mutualevaluations/more/more-about-mutual-evaluations.html?hf=10&b=0&s=desc(fatf_releasedate)), accessed on 21 July 2020.

Financial Action Task Force Report, 'Virtual Currencies: Key Definitions and Potential AML/CFT Risks', available at <https://www.fatf-gafi.org/documents/documents/virtual-currency-definitions-aml-cft-risk.html>, accessed on 25 July 2020

Financial Action Task Force 'Virtual Currencies: Key Definitions and Potential AML/CFT Risks', available at <https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>, accessed on 15 April 2020.

Financial Action Task Force, 'Who we are', available at <https://www.fatf-gafi.org/about/>, accessed on 31 May 2020.

Financial Crimes Enforcement Network, 'Am I a MSB?', available at <https://www.FinCen.gov/am-i-msb>, accessed on 03 June 2020.

Financial Crimes Enforcement Network, 'FinCen's Mandate from Congress', available at <https://www.FinCen.gov/resources/statutes-regulations/FinCens-mandate-congress>, accessed on 03 June 2020.

Financial stability board 'Crypto-asset markets Potential channels for future financial stability implications,' available at <https://www.fsb.org/wp-content/uploads/P101018.pdf>, accessed on 20 September 2020

IFWG Crypto Assets Regulatory Working Group 'Consultation paper on policy proposals for crypto assets', available at http://www.treasury.gov.za/comm_media/press/2019/CAR%20WG%20Consultation%20paper%20on%20crypto%20assets_final.pdf, accessed on 30 July 2019

Internal Revenue Services, 'Notice 2014-21', available at <https://www.irs.gov/pub/irs-drop/n-14-21.pdf>, accessed on 04 June 2020.

International Monetary Fund 'Virtual Currencies and Beyond: Initial Considerations', available at <https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf>, accessed on 30 July 2019.

Library of congress law Regulation of Virtual currency: Japan, available at https://www.loc.gov/law/help/virtual_currency/japan.php, accessed on 31 May 2020.

Mesk, 'Unit of Account', available at <https://www.binance.vision/glossary/unit-of-account>, accessed on 11 May 2020.

Nakamoto, 'Bitcoin: A peer-to-peer electronic cash system', available at <https://bitcoin.org/bitcoin.pdf>, accessed on 14 April 2020;

National Treasury, 'Conduct Of Financial Institutions Bill '.available at <http://www.treasury.gov.za/twinpeaks/Conduct%20of%20Financial%20Institutions%20Bill.pdf>, accessed on 30 June 2020.

National Treasury Policy Document 'A Safer Financial Sector to Serve South Africa Better' available at <http://www.treasury.gov.za/twinpeaks/20131211%20-%20Item%202%20A%20safer%20financial%20sector%20to%20serve%20South%20Africa%20better.pdf>, accessed on 15 October 2020.

New York State Department of Financial Services 'Virtual Currency Business activity', available at https://www.dfs.ny.gov/apps_and_licensing/virtual_currency_businesses, accessed 29 August 2019.

OECD 'How to deal with Bitcoin and other virtual currencies in the System of National Accounts?', available at [http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=COM/SDD/DAF\(2018\)1&docLanguage=En](http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=COM/SDD/DAF(2018)1&docLanguage=En), accessed on 30 July 2019.

Oxford University Press (2010), available at <https://www.oxfordlearnersdictionaries.com/definition/english/pseudonym>, accessed 20 July 2020.

Payment association of South Africa, 'legal and regulatory framework', available at <http://www.pasa.org.za/national-payment-system/legal-regulatory-framework>, accessed on 31 July 2020.

PBOC, CAC, MIIT, SAIC, CBRC, CSRC, and CIRC, 'Announcement on Preventing Financial Risks from Initial Coin Offerings (2017)', available at, <http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/3374222/index.html> (in Chinese), accessed on 11 June 2020.

PriceWaterhouseCoopers, 'The business – and cost – of compliance Practical strategies to optimize compliance cost and effectiveness', available at <https://www.pwc.com/us/en/risk-assurance/publications/assets/pwc-business-of-compliance-4-5-18.pdf>, accessed on 15 July 2020.

Reiff, 'Blockchain explained', available at <https://www.investopedia.com/terms/b/blockchain.asp>, accessed on 15 July 2020.

South African Reserve Bank 'Crypto assets' available at <https://www.resbank.co.za/RegulationAndSupervision/FinancialSurveillanceAndExchangeControl/FAQs/Pages/VirtualCurrenciesCryptocurrencies.aspx>, accessed 28 June 2020

South African Reserve Bank 'Financial Surveillance' available at <https://www.resbank.co.za/AboutUs/Departments/Pages/FinancialSurveillance.aspx>, accessed on 30 June 2020.

South African Reserve Bank National Payment System Department, 'Position Paper on virtual currencies', available at [https://www.resbank.co.za/RegulationAndSupervision/NationalPaymentSystem\(NPS\)/Legal/Documents/Position%20Paper/Virtual%20Currencies%20Position%20Paper%20%20Final_02of2014.pdf](https://www.resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/Legal/Documents/Position%20Paper/Virtual%20Currencies%20Position%20Paper%20%20Final_02of2014.pdf), accessed on 15 June 2020.

South African Reserve Bank 'Project Khoka', available at https://www.resbank.co.za/Lists/News%20and%20Publications/Attachments/8491/SARB_ProjectKhokha%2020180605.pdf, accessed on 01 July 2020.

South African Reserve Bank 'SAMOS System (South African's Real Time Gross Settlement (RTGS) System)' available at [https://www.resbank.co.za/RegulationAndSupervision/NationalPaymentSystem\(NPS](https://www.resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)

) /SAMOSSystem(RTGS)/Pages/SAMOSSystem(RTGS)-Home.aspx, accessed on 15 March 2020.

Tera Exchange, 'Tera Exchange Launches First Regulated Bitcoin Derivatives Trading: Creates Tera Bitcoin Price Index as Global Benchmark', available at http://www.teraexchange.com/news/2014_09_12_Launches%20First%20Regulated%20Bitcoin%20Derivatives.pdf, accessed on 15 June 2020.

The National people's Congress of the People's Republic of China 'Cryptography Law of the People's Republic of China' available at <http://www.npc.gov.cn/npc/c30834/201910/6f7be7dd5ae5459a8de8baf36296bc74.shtml>, accessed on 20 June 2020.

The Protocol against the Illicit Manufacturing of and Trafficking in Firearms Parts and Components and Ammunition, supplementing the United Nations Convention against Transnational Organised Crime(31 May 2001), available at http://www.dirco.gov.za/docs/2005pq/pq2_455.htm, accessed on 21 July 2020

The South African Revenue Service, 'Sars's Stance On The Tax Treatment Of Cryptocurrencies', available at <https://www.sars.gov.za/Media/MediaReleases/Pages/6-April-2018---SARS-stance-on-the-tax-treatment-of-cryptocurrencies-.aspx>, accessed on 15 June 2020.

The wall street journal 'The U.S. vs. China: Who Is Winning the Key Technology Battles?', available at <https://www.wsj.com/articles/the-u-s-vs-china-who-is-winning-the-key-technology-battles-11586548597>, accessed on 04 October 2020.

United States of America before the Commodity Futures Trading Commission 'In the Matter of: Coinflip, Inc., d/b/a Derivabit, and Francisco Riordan, Order Instituting Proceedings Pursuant to Sections 6(C) And 6(D) of The Commodity Exchange Act, Making Findings And Imposing Remedial Sanctions', available at <https://www.cftc.gov/sites/default/files/idc/groups/public/@Irenforcementactions/documents/legalpleading/enfcoinfliporder09172015.pdf>, accessed on 10 June 2020.

US Securities and Exchange Commission, 'Investor Alert: Bitcoin And Other Virtual Currency-Related Investments', available at https://www.sec.gov/oiea/investor-alerts-bulletins/investoralertsia_bitcoin.html, accessed on 04 June 2020.

Yu 'China to stamp out virtual currency trading completely with ban on foreign platforms', available at <https://www.scmp.com/business/banking-finance/article/2132009/china-stamp-out-virtual-currency-trading-completely-ban>, accessed on 29 August 2019