



UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

**THE POTENTIAL ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM
FINANCING RISKS AND IMPLICATIONS OF VIRTUAL CURRENCIES ON THE
PREVAILING SOUTH AFRICAN REGULATORY AND SUPERVISORY REGIME**

by

Rynhard Botha

Submitted in accordance with the
requirements for the degree of

LLM Banking Law

In the faculty of Law
University of Pretoria

31 October 2019

Supervisor: Professor Reghard Brits



Acknowledgements

I am firstly immeasurably grateful to God, who has provided me with grace, wisdom and strength to embark on a lifelong journey of learning. He has bestowed me with the indispensable intellect, knowledge and aptitude to be able to exceed with my studies.

I am appreciative towards my supervisor, Professor Reghard Brits, for his continuous support and dedication during my research. He provided me with exceedingly virtuous recommendations and guidance to transition me into a master of laws. I appreciate his knowledge, assiduousness and determination throughout the journey.

I am thankful to my mentor, Hettie-Annette Nel, who is a seasoned financial crime analyst and she has provided me with practical anti-money laundering and counter-terrorism financing (AML/CTF) investigative, regulatory and supervisory skills and knowledge. She has assisted me to transition from a university graduate into an experienced AML/CTF analyst. She has contributed to the development of my career and has enhanced my interest and knowledge in financial crime, AML/CTF, forensic auditing and cybercrime.

I would also like to express my profound gratitude to my parents, André and Hendrina Botha, for all the years of moral support, motivation and unconditional love.

I am grateful to my sister, Cherise Botha, who is an experienced researcher and she has proved to be a true leader who has inspired me throughout my studies. She has provided me with emotional support throughout my life.



Declaration of originality

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

R Botha

October 2019



Executive summary

The purpose of this mini-dissertation is to analyse and establish the potential money laundering and terrorism financing risks and implications of virtual currencies on the prevalent South African regulatory and supervisory architecture. The South African financial system is exceedingly regulated and supervised to ensure that it is prudent and reputable, and to enhance the safety and soundness thereof. Recently, technological innovations and developments have created immense issues especially from a financial regulatory and supervisory perspective. Financial technology has produced mysterious phenomena such as blockchain, insuretech, crowdfunding and virtual currencies. Presently, virtual currencies, which will be the focus of this study, do not fall within the ambits of the South African financial regulatory or supervisory regime and have thus created a regulatory arbitrage. This poses a significant number of risks and implications to the South African context, namely tax evasion; cross-border illicit flow of funds; contravention of exchange control regulations; financial instability; monetary policy uncertainty; inaccurate economic statistics; non-reporting of balance of payment requirements; and money laundering and terrorist financing (ML/TF). The study aims to construct a clear description and categorisation of virtual currencies within a South African context. Secondly, the study will set out the risks and implications that virtual currencies pose to the South African financial system from a ML/TF perspective. Finally, the study will present a possible solution to close the current regulatory arbitrage presented by virtual currencies in the South African financial sector.



Table of contents

Acknowledgements	i
Declaration of originality	ii
Executive summary	iii
Table of contents	iv
Chapter 1: Introduction	1
1.1 Context of the study	1
1.2 The purpose of the study	2
1.3 Structure	2
Chapter 2: The notion and classification of virtual currencies and regulatory arbitrage	4
2.1 Introduction	4
2.2 Virtual currencies	5
2.2.1 Background of virtual currencies	5
2.2.2 Concept of virtual currencies	5
2.2.3 Conventional fiat currency	7
2.2.4 Technology and fiat currency.....	9
2.2.5 Classification of virtual currencies	12
2.2.5.1 Classified as a currency	12
2.2.5.2 Classified as an asset or commodity	13
2.3 Regulatory arbitrage of virtual currencies.....	14
2.3.1 International perspective.....	14
2.3.1.1 United Kingdom.....	14
2.3.1.2 China.....	15
2.3.1.3 Switzerland.....	15
2.3.1.4 New Zealand	16
2.3.1.5 Estonia	16
2.3.2 South African perspective.....	17
2.3.2.1 Prudential and conduct regulation	17
2.3.2.2 Deposit acceptance.....	18
2.3.2.3 Payment system.....	19
2.3.2.4 Investment schemes and portfolios	20
2.3.2.5 Foreign currency and securities	21



2.3.2.6 Derivatives	22
2.4 Conclusion	23
Chapter 3: The potential ML/TF risks that virtual currencies pose in South Africa.....	24
3.1 Introduction	24
3.2 AML/CTF regulatory and supervisory regime.....	25
3.2.1 Background	25
3.2.1.1 Money laundering.....	25
3.2.1.2 Terrorism financing.....	26
3.2.1.3 Financial Action Task Force	26
3.2.1.4 South Africa.....	28
(a) Prevention of Organised Crime Act (POCA).....	28
(b) Protection of Constitutional Democracy against Terrorist and Related Activities Act (POCDATARA)	29
(c) Financial Intelligence Centre Act (FICA).....	30
3.2.2 Characteristics of virtual currencies	31
3.2.2.1 Anonymity and pseudonymity.....	31
3.2.2.2 Decentralised system	32
3.2.3 The South African AML/CTF regime.....	33
3.2.3.1 Customer due diligence.....	33
3.2.3.2 Enhanced due diligence	35
(a) Ultimate beneficial ownership	35
(b) Prominent persons	36
3.2.3.3 Duty to keep record	37
3.2.3.4 Terrorism financing and weapons of mass destruction	37
3.2.3.5 Cash transactions.....	38
3.2.3.6 Suspicious and unusual transactions	39
3.2.3.7 Cash conveyances	40
3.2.3.8 International and domestic fund transfers	40
3.2.3.9 Powers of the FIC.....	42
3.3 Analysis of the South African AML/CTF regime and virtual currencies	43
3.3.1 Customer due diligence and enhanced due diligence	44
3.3.2 Record keeping	45
3.3.3 Terrorism property and sanctions	46
3.3.4 Reporting duties	46



3.3.5	Wire transfers	47
3.3.6	Powers of the FIC	48
3.4	Conclusion	48
Chapter 4: Potential AML/CTF policy recommendations for virtual currencies		50
4.1	Introduction	50
4.2	Difficulties of virtual currency regulation	51
4.3	Virtual currency regulation	51
4.3.1	International commitments	51
4.3.2	Regulatory approaches	52
4.3.3	South African approach	53
4.4	Virtual currency regulatory frameworks	54
4.4.1	Self-regulation	54
4.4.2	Government regulation	56
4.5	South African regulatory action to be taken	57
4.5.1	General regulation	57
4.5.2	AML/CTF regulation	57
4.6	Conclusion	58
Chapter 5: Conclusion		60
Bibliography		64
	International and foreign guidance	64
	Internet sources	65
	Journal articles and dissertations	66
	Legislation and regulations	69
	South African regulatory guidance, directives and position papers	69
	Press statements, notifications and speeches	70
List of abbreviations		71



Chapter 1: Introduction

1.1 Context of the study

The purpose of this mini-dissertation is to analyse the probable anti-money laundering and counter-terrorist financing (AML/CTF) risks and implications of virtual currencies to the prevalent South African regulatory and supervision regime. Recently, a technological revolution has disrupted the current financial sector with the introduction of robust and dynamic technological financial developments. This technological revolution has *inter alia* produced mysterious phenomena such as: robo-advisors; insurtech; crowdfunding platforms; mobile payments; budgeting, investment and share trading applications; blockchain and virtual currencies. The introduction of these unchartered technological innovations is peculiar and almost incomprehensible for most lay persons. The financial technology (fintech) revolution creates immense uncertainty for traditional financial distribution channels, financial products and services, financial “brick and mortar” firms, and financial intermediation, which might become obsolete.

The South African financial system is exceedingly regulated and strictly supervised to ensure the safety and soundness of the financial system as a whole. In reaction to the Global Financial Crisis of 2007/2008, South Africa has introduced a number of new financial regulatory bills before parliament and enacted legislation, *inter alia* the Financial Sector Regulation Act 9 of 2017, the Insurance Act 18 of 2017, the Financial Intelligence Centre Amendment Act 1 of 2017, the Conduct of Financial Institutions (COFI) Bill 42114 of 2018, the South African Reserve Bank Amendment Bill 41657 of 2018, the Banks Amendment Bill 41657 of 2018 and the Financial Sector Law Amendment Bill 41955. The aforementioned statutes and bills intend to enhance a safer, prudent, reputable and reliable financial sector in South Africa.

Presently, the South African financial regulation and supervisory architecture do not provide for the regulation and supervision of fintech in any manner. Thus, fintech largely operates outside the parameters of the law and creates a foundation for exposing the South African financial system to malpractice and abuse. This risk will be analysed in this study in an attempt to comprehend different technological



innovations, to discover a practical and appropriate regulatory and supervisory regime, and to include fintech within the ambits of the South African law.

1.2 The purpose of the study

This study will focus specifically on the potential money laundering and terrorism financing (ML/TF) risks that virtual currencies pose to the South African financial system, as these currencies presently operate outside the ambits of third party intermediaries and circumvent the current regulatory and supervisory framework in the country. A number of risks and implications that virtual currencies pose in the South African context have already been identified and include *inter alia*: tax evasion; illicit cross-border flows of funds; contravention of exchange control regulations; financial instability; monetary policy uncertainty; inaccurate economic statistics; non-reporting of balance of payment requirements; and ML/TF.

Virtual currencies are considered to be a technological innovation that has disrupted the current regulatory and supervisory framework. This has created a possible regulatory and supervisory arbitrage in South Africa. Indeed, the lack of appropriate classification and definition of virtual currencies have created momentous issues for consumers, legal policy-makers, governments, law-enforcement agencies and financial institutions. Virtual currencies are completely decentralised from the conventional financial system and are associated with anonymity and pseudonymity, which form the foundation of significant ML/TF risks.

It is essential that the current regulatory and supervisory framework should be reviewed from an AML/CTF prospective. A regulatory framework and supervisory approach that includes virtual currencies will have to be established either through the amendment of prevailing legislation and regulatory requirements, or the drafting of entirely new legislation and regulatory requirements.

1.3 Structure

This mini-dissertation is structured in five chapters that introduces the legal problem and provide the foundation thereof. It identifies the potential implications and risks associated with the identified problem and provides a potential solution thereto. Chapter one is the introductory chapter which provides the broad context and background of this study which supports the intention and purpose of the study.



Chapter two focusses on the lack of appropriate classification and definition of virtual currencies, which have created regulatory arbitrage. This chapter examines the definitions and characteristics of fiat currencies, electronic money and digital money. The aforementioned definition and characteristic are compared to virtual currencies as a way to understand the nature of virtual currencies and to reduce confusion surrounding it. The third chapter investigates the potential ML/TF risks that virtual currencies pose in a South African context. The focus in this chapter will be on the anonymity, pseudonymity and decentralisation of virtual currencies and how users thereof could abuse the financial system. Chapter four will analyse the potential policy proposals of international organisations and conduct a comparison of different jurisdictions' legal approaches. Additionally, this chapter will suggest a new or amended policy architecture for the South African current financial regulatory and supervisory regime.

Chapter five is the final chapter of this mini-dissertation and will form the conclusion of this study. The concluding chapter will provide an overview of the complete study and raise certain issues that should be addressed to prevent ML/TF risks associated with virtual currencies and to construct an effective legal framework to mitigate the ML/TF risks of virtual currencies. The notion of a new regulatory and supervisory architecture will assist in the combat of organised crime and prevent the financial abuse and malpractice of the financial system. It will support and enhance the reputation and assist the safety and soundness of the South African financial system.



Chapter 2:

The notion and classification of virtual currencies and regulatory arbitrage

2.1 Introduction

The introduction of virtual currencies into the financial marketplace has led to new methods of transacting and for the payment of goods and services. It has caused a disruption of the traditional financial intermediary system. Virtual currencies possess similar characteristics to that of assets and conventional fiat currencies, and there have been arguments that virtual currencies may ultimately replace both. Since virtual currencies are a fairly new and complex concept that stems from technological innovation, it understandably seems difficult for persons outside the technological sphere to comprehend.

It is an especially problematic concept for legal scholars, policy-makers, central banks, regulators and supervisors as they have found the concept particularly hard to unpack. This has caused virtual currencies to remain unregulated even though it poses significant uncertainty and risks to the financial system. From a legal perspective, it is necessary to firstly understand the meaning and classification of virtual currencies, before a decision can be taken on how to effectively regulate it.

In the second chapter of my dissertation, I intend to discuss the background, definition and different classifications of virtual currencies. In this discussion, it will be important to first discuss conventional fiat currency and other closely associated phenomena. The chapter will conclude with an examination of the regulatory arbitrage that exists in relation to virtual currencies both from an international and South African perspective.

2.2 Virtual currencies

2.2.1 Background of virtual currencies

The financial industry is reinventing itself by streamlining internal processes, the introduction of new technology, reshaping well-established products, and the reformation of its financial value chain.¹ Nevertheless, financial institutions have found it difficult to combine physical distribution channels, internet-based delivery channels and the management of multiple distribution channels.²

Financial institutions have struggled to create more technologically advanced delivery channels which resulted in the development of block-chain technology to facilitate instant payments without the need of a central banking system and traditional financial intermediaries.³ This new form of technology provides a digital platform for virtual currencies to be traded on and users can initiate direct web-based payments in real-time over a peer-to-peer computer network which is secure, fast and cost-effective.⁴ Virtual currencies are not created through the formulation and implementation of monetary policies, commercial banks or other financial participants, but rather through a peer-to-peer incentive computing network that proves authenticity of encrypted transactions with a mathematical algorithm.⁵

2.2.2 Concept of virtual currencies

The idea of greater access to digital forms of conventional currencies has previously been considered by central banks to form part of its responsibilities.⁶ The concept and use of virtual currencies have recently been inspired by a number of contributing aspects: firstly, a technological curiosity in the financial industry; secondly, the entrance of new participants in financial payments and intermediation; thirdly, the declining use of traditional fiat currencies; and lastly, the increase in the use of private digital tokens.⁷

¹ V Brühl “Virtual currencies, distributed ledgers and the future of financial services” (2017) 6 *Leibniz Information Centre for Economics* 370-378 370 (hereafter Brühl).

² *Ibid.*

³ *Ibid.*

⁴ Brühl *supra* n 1 371.

⁵ *Ibid.*

⁶ See J Tobin “Financial innovation and deregulation in perspective” (1985) 635 *Cowles Foundation Papers*; Bank for International Settlements Committee on Payments and Market Infrastructures “Central Bank digital currencies” 2018 (hereafter BIS Report 2018).

⁷ 2018 BIS Report *supra* n 6.



A number of international organisations have provided various definitions to attempt an understanding of virtual currencies as a technological innovation. The European Banking Authority (EBA) describes the concept of a virtual currency as a digital representation of value which is not determined by a public institution, public authority or central bank; based on the value of fiat currency; and is accepted by natural and legal persons as a means of exchange which can be transacted, stored and conveyed electronically.⁸ The European Central Bank (ECB) defines virtual currencies as unregulated digital money which is controlled by its inventors and is used and acknowledged by the participants of a specific cyber community.⁹ The Financial Action Task Force's (FATF) definition of virtual currencies is similar to that of the EBA and acknowledges it as a digital representation of value that can be transacted digitally and functions as a medium of exchange; unit of account; and a store of value but it has no function as a legal tender.¹⁰

As delineated above, the FATF defines virtual currencies as a representation of a digital value and can function as a medium of exchange, unit of account and a store of value, but it is distinguishable from conventional currency as virtual currencies are not issued by an authority, and it has therefore no legal tender status and is not guaranteed in any manner.¹¹ Virtual currencies fulfil the aforementioned functions only by a peer-to-peer digital arrangement within the participants of the virtual community.

It is important to note that virtual currencies have certain characteristics of conventional fiat currencies which will be discussed below. Virtual currencies are not pegged or linked to a commodity or conventional fiat currency in any manner and have therefore no intrinsic value.¹² Virtual currencies are similar to both assets and conventional fiat currencies as it has the ability to move from one place to another electronically, is accepted as tender for good and services, and is based on trust between the buyer and the seller.

⁸ See European Banking Authority Report "EBA opinion of virtual currencies" 2014 (hereafter EBA report).

⁹ See European Central Bank Report "Virtual currencies scheme" 2012.

¹⁰ See Financial Action Task Force Report "Virtual currencies key definitions and potential AML/CFT risks" 2014 (hereafter FATF 2014 Report).

¹¹ *Ibid.*

¹² M Dabrowski & L Janikowski Monetary Dialogue "Virtual currencies and central bank's monetary policies: challenges ahead" (2018) Request by ECON Committee of the European Parliament 1-31 7.



2.2.3 Conventional fiat currency

Conventional fiat currency is government issued currency notes and coins which is the nominated legal tender of a particular jurisdiction; which is inconvertible; circulates the hands of its citizenry; is widely recognised; and is customarily accepted as a medium of exchange within a jurisdiction.¹³ Conventional fiat currency is also referred to as national currency, real currency, real money or monetary money.¹⁴ In the South African context, the South African Reserve Bank (SARB) has the powers and duties to manufacture, issue and destroy bank notes and coins (rands and cents) that may be used in South Africa.¹⁵ The SARB has the sole right to issue bank notes and coins which will be lawfully in circulation and represents the legal tender in the Republic.¹⁶

It is important to emphasise that currency will only qualify as fiat currency once the following three characteristics are present: firstly, the currency must be declared as the legal tender by a government; secondly, the currency must have the functionality of being used as a medium of exchange; and lastly, the currency must have an intrinsic value.¹⁷ Additionally, currency should also not be backed with any tangible asset such as gold.¹⁸ An expanded discussion on the characteristics of fiat currency characteristics will be provided below.

¹³ FATF 2014 Report *supra* n 10 3.

¹⁴ *Ibid.*

¹⁵ S 10(1) of the South African Reserve Bank Act 90 of 1989 (hereafter SARB Act).

¹⁶ S 14(1) of the SARB Act.

¹⁷ D Dang “Macroeconomics and blockchain” (2014) European Business Administration Metropolia University of Applied Sciences 1-32 8 (hereafter Dang).

¹⁸ C Goforth “The lawyer’s cryptonary: a resource for talking to clients about crypto-transactions” (2019) 41 *Campbell Law Review* 47-122 83 (hereafter Goforth).



2.2.3.1 Legal tender

The concept of legal tender can be separated into two parts: firstly, 'legal' and secondly, 'tender'. In the context of fiat currency, the sovereign government of a state will provide the status of a currency that it issues as lawful with special rights and obligations attached thereto.¹⁹ Thus, government issued currency that is declared as lawful will be permitted and allowed to be used for payment as it is heavily regulated and managed by the state and central banks through monetary policy and regulatory standards.²⁰ The Bank of England explains that legal tender means the settling of debts rather than the payment for goods and service.²¹ It can therefore be accepted that currency that is lawfully declared to have rights and obligations attached thereto and that is used to settle debt obligations, will fulfil the requirement of legal tender.

2.2.3.2 Medium of exchange

The second requirement of fiat currency, namely medium of exchange, necessitates that the currency should be generally acknowledged as a measure of value and a means of payment.²² It acts as a denominator of value and can be used to effect economic and pecuniary transactions, and can easily be substituted for economic goods and services.²³ Therefore, currency circulates through the economy and lawfully transfers value between different economic participants to settle debts.

2.2.3.3 Intrinsic value

The third and final requirement of fiat currency, namely intrinsic value, refers to the store of value where economic participants can hold it as a form of wealth. The concept of wealth enables holders of currency to save, store, salvage and tender it for the payment of economic goods and services, as well as the settling of debts.²⁴ The intrinsic value bestows the holders of currency a procuring power that provides economic opulence and fortune.

¹⁹ Dang *supra* n 17 7.

²⁰ E Reddy & A Minnaar "Cryptocurrency: a tool and target for cybercrime" (2018) 31(3) *Acta Criminologica: Southern African Journal for Criminology* 71-92 72.

²¹ Bank of England "What is legal tender?" (2019) Available at: <https://www.bankofengland.co.uk/knowledgebank/what-is-legal-tender> (Accessed 27 Apr. 2019).

²² G Kalbaugh "Virtual currency, not a currency?" (2016) 16 *Journal of International Business and Law* 26-35 28 (hereafter Kalbaugh).

²³ *Ibid.*

²⁴ Dang *supra* n 17 3.

It is important to take cognisance that the objective of this part of the dissertation is to describe and characterise fiat currency in the context of the circulation of traditional bank notes and coins (*specie*), and the tendering of cheques and intermediation methods that the financial system have traditionally used. The next section of the dissertation will analyse two different types of currency which fall within the ambits of the definition of fiat currency and its characteristics. It involves, however, a certain degree of technology as the financial system matured over time.

2.2.4 Technology and fiat currency

As mentioned above, financial intermediation has transformed significantly as conventional currency has been combined with technology to enhance the effectiveness of payment for economic goods and services. The need had arisen for the transformation of fiat currency as it was not compatible in a modern and innovative society which is substantially focused on consumerism founded by capitalism. The focus of this part of the study will be on two technological phenomena, namely electronic money and digital money, which has been combined with fiat currency to improve the latter's role and effectiveness in society.

2.2.4.1 Electronic money

By the end of the previous century, traditional forms of payment had started to fade away as the demand for newer types of money increased to prevent the loss in confidence in real value of transactions and to maintain the faith between debtors and creditors.²⁵ At the turn of the millennium, the United States of America transmitted on average \$2 trillion a day through electronic and computer technology.²⁶

Electronic money (hereafter e-money) is the use of a chip or smart banking card which is linked to an electronic wallet that enables the card holder to transact at participating retailers with the available balance in the electronic wallet.²⁷ The European Union has issued a directive to define the concept of e-money to distinguish it from conventional money as the aforementioned uses technology to transfer the value equivalent of fiat currency which is stored in the electronic wallet, and accessed

²⁵ W G Schulze "Smart Cards and e-Money: New Developments Bring New Problems" (2004) 16 *South African Mercantile Law Journal* 703-715 703 (hereafter Schulze).

²⁶ *Ibid.*

²⁷ Schulze *supra* n 25 708.



and transferred by an electronic device.²⁸ The directive defines e-money as electronic currency which stores pecuniary value magnetically where the holder is entitled to claim on the issuer of the currency to make payment for transactions which is represented by a claim on the issuer to make payments for transactions which is then accepted by the holder of the currency other than the currency issuer.²⁹

E-money can be classified into two different types: firstly, account-based products, which is a traditional bank account where value can be transferred by electronic means; and secondly, token-based products, which allows participants to exchange electronic tokens without relying on an account.³⁰ Account-based e-money allows the payment initiating institution to maintain the instruction to effect payment by use of technology services of other institutions (i.e. debit and credit cards, electronic funds transfers, internet banking, and automated teller machines.³¹ Token-based products involve the conversion of fiat currency into electronic tokens in an electronic account where it can then be accessed.³²

Regulation of e-money is focused on the provision of payment services and not the technology itself.³³ This allows for flexible means for payment services as regulation thereof tends to be regulation-unbiased. In South Africa, the evolution of e-money has lead the SARB to issue a position paper on this matter and indicated that e-money may require a need for regulatory modification or intervention to ensure that the national payment system of South African maintains its integrity, confidence and limits any risk, to provide consumers with protection against unfair practices, fraud and financial loss and the promotion of law enforcement in averting criminal activity.³⁴ Stemming from the analysis, it appears that e-money is an electronic monetary representation of fiat currency to enable transactions through an account or to effect payment through electronic tokens.

²⁸ M D Tuba “The regulation of electronic money institutions in the SADC region: some lessons from the EU” (2014) 17 *Potchefstroom Electronic Law Journal* 2269-2312 2272 (hereafter Tuba 2014).

²⁹ Article 2(2) Payment of Services Directive 2009/110/EC Official Journal of the European Union 11.

³⁰ Tuba 2014 *supra* n 28 2273 2274.

³¹ Tuba 2014 *supra* n 28 2274.

³² *Ibid.*

³³ M D Tuba “The technology-neutral approach and electronic money regulation in the EU: identifying the promises and challenges for future regulation in South Africa” *Paper presented at the 10th Annual International Conference on Law, 8–11 July 2013, Athens, Greece* 372-400 382 (hereafter Tuba 2013).

³⁴ National Payment Systems Department “Position paper on electronic money” (2009) South African Reserve Bank NPS 01/2009 1-10 4 (hereafter NPS 01/2009).

2.2.4.2 *Digital currency*

In contrast to e-money, digital currency is the digital representation of either virtual currency (non-fiat currency) or e-money (fiat currency) and is commonly used interchangeably with the term virtual currencies.³⁵ Digital currency has the ability to electronically store value, be used as a medium of exchange and to function as a unit of account, and can therefore qualify as fiat currency.³⁶ In cases where electronic value is transferred through a peer-to-peer network, and it is issued and controlled by the developer in a decentralised system, the digital currency is regarded as a virtual currency, and then qualifies as a non-fiat currency.³⁷

It is important to note that there are similarities between e-money and digital currency as both types of currencies are transacted over an electronic money-based payment system to enable it as a payment instrument or to facilitate transactions.³⁸ In the context where digital currency represents fiat currency, neither digital currency nor e-money are regarded as separate currencies.³⁹ These currencies instead represent the monetary value of fiat currency in an electronic form, is regulated by a central bank and can only be issued by commercial banks.⁴⁰

It can be concluded from the analysis above that in cases where digital currency represents the value of a decentralised peer-to-peer virtual currency (non-fiat) without a legal tender status, there is a possibility that digital currency can be regarded as a separate currency. Nonetheless, in this instance the digital currency is dependent on the legal classification and status of virtual currencies. In certain cases where digital currency represents an electronic value of a virtual asset, virtual commodity or even a virtual currency, the digital currency might not be classified as a currency at all.

The next part of the chapter will analyse the legal status and classification of virtual currencies as it can play different roles and be used for a variety of purposes. As discussed in the introduction of this chapter, there remains a legal uncertainty as to how to regulate virtual currencies. It does not wholly fit within the ambit of any legal classification and has therefore created an absence of an appropriate legal status.

³⁵ FATF Report 2014 *supra* n 10.

³⁶ H A Nel "Know-Your-Customer measures: mitigating money-laundering risks in mobile banking transactions" (2017) LLM dissertation University of the North West 1-208 20 (hereafter Nel).

³⁷ Nel *supra* n 36 21.

³⁸ Nel *supra* n 36 19.

³⁹ *Ibid.*

⁴⁰ NPS 01/2009 *supra* n 36; Nel *supra* n 36 19.



2.2.5 Classification of virtual currencies

As mentioned above, the appearance of virtual currencies in the financial system has presented significant issues for legal scholars, policy-makers, central banks, conventional banks, financial regulators and supervisors as it is a difficult concept to fully comprehend. The different role players in the financial system have attempted to classify and categorise this technological innovation to create an understanding and the appropriate approach.

In the next part of this chapter, there will be a focus on the different classifications of virtual currencies as this forms the foundation for a decision on a suitable regulatory policy and framework. Virtual currencies have been considered to be a currency or an asset, and in certain instances these concepts are used interchangeably which may create added confusion.

2.2.5.1 Classified as a currency

The United States Federal Reserve System (Federal Reserve), the Internal Revenue Service (IRS) and the Financial Crime Enforcement Network (FinCEN) have all provided guidance and positions on virtual currencies in respect of the classification of virtual currencies for monetary, taxation and financial crime purposes, respectively.⁴¹ FinCEN has taken the decision to classify virtual currencies as a currency due to the fact that it is used as a medium of exchange, has the equivalent value of fiat currency and can be used to purchase goods and services.⁴² The Federal Reserve has measured virtual currency exchanges against foreign sovereign currency exchanges through the application of a technical empirical analysis and found that the transaction volume of virtual currencies is nearly equal to the daily transactions volume of the US payment system.⁴³ The IRS has instructed that all tax payers are obliged to calculate the fair market value of virtual currencies in US dollars when payment is made for property using virtual currencies and will therefore be taxable.⁴⁴

⁴¹ S Litwack "Bitcoin: currency or fool's gold: a comparative analysis of the legal classification of Bitcoin" (2015) 29 *International and Comparative Law Journal* 309-348 331 (hereafter Litwack).

⁴² See Department of the Treasury Financial Crimes Enforcement Network Guidance "Application of FinCEN's regulations to persons administering, exchanging or using virtual currencies" issued 18 March 2013 FIN 2013-G001.

⁴³ See Finance and Economics Discussion Series Divisions of Research & Statistics and Monetary Affairs Federal Reserve Board "Bitcoin: technical background and data analysis" issued 7 October 2014.

⁴⁴ See Internal Revenue Service Notice 2014-21 (issued March 2014).



The nature of virtual currencies implies that the lack of physical currency and recognition of the value are not enforced by a third party authority such as a government.⁴⁵ Virtual currency itself is argued to be a logical good itself and the parties to a transaction agree upon the value thereof without the need for a third party authority.⁴⁶ It is evident that the parties to a transaction and third party government authorities have determined that virtual currencies can be used as a currency for transaction and payment purposes.

2.2.5.2 Classified as an asset or commodity

It can be argued that the purchasing or transacting of virtual currencies itself can be viewed as the trading of assets or commodities as conventional currencies are exchanged for an object with a value. A commodity investment is any tangible or intangible object which is subject to sale or trading and has the ability to store value.⁴⁷ Virtual currencies can be considered as commodities as they qualify as goods which can be traded in a market with a uniform quality and value.⁴⁸ Virtual currencies can be viewed as a new class of assets rather than claims upon an object with an underlying asset.⁴⁹ If a virtual currency is used for speculative investment purposes, it can be regarded as a virtual asset rather than a virtual currency.⁵⁰ The value of virtual currencies is derived and created from the actual agreement between two parties and the replication of the asset which then establishes a virtual asset.⁵¹

The classification of virtual currencies has led to voluminous arguments to establish the legal status thereof. The absence of a classification of virtual currencies has had regulatory impacts which resulted in a regulatory arbitrage. The next part of the chapter will conclude with an explanation of the regulatory arbitrage that virtual currencies has brought to the worldwide financial system.

⁴⁵ A I Stankovic, R A Mihajlovic & A R Mihajlovic "Crypto-currency and e-financials" (2014) 4 *International Journal for Economics and Law* 132-137 134 (hereafter Stankovic).

⁴⁶ Stankovic *supra* n 45 135.

⁴⁷ Litwack *supra* n 41 339.

⁴⁸ N Fusco "Financial regulation - regulating a new sector: how should regulatory agencies classify and regulate virtual currencies - CFTC v. McDonnell" (2018) 4 *Journal of Trial and Appellate Advocacy* 136-143 140.

⁴⁹ S Bayern "Dynamic common law and technological change: the classification of bitcoin" (2014) 71 *Washington and Lee Law Review* 22-50 30.

⁵⁰ Goforth *supra* n 18 55.

⁵¹ E Howden "The crypto-currency conundrum: regulating an uncertain future" (2019) 29 *Emory International Law Review* 742-798 767.

2.3 Regulatory arbitrage of virtual currencies

The introduction of virtual currencies in the financial system has created immense ambiguity especially from a legal perspective. Virtual currencies are an entirely new financial phenomenon which prove difficult to understand and to classify to establish its legal status. The lack of appropriate classification and legal status has led to virtual currencies falling outside the ambits of the financial regulation framework, which has created a regulatory arbitrage.

The presence of regulatory arbitrage holds a considerable risk for the financial sector, which risk will be analysed and discussed in chapter three of this study. The final part of this chapter will therefore focus on the regulatory arbitrage that the inadequate classification of virtual currencies has caused in a number of countries.

2.3.1 *International perspective*

Virtual currencies are not regulated by a central authority but rather through its users in a central peer-to-peer network and therefore falling wholly outside legal and regulatory parameters.⁵² The design of virtual currencies has the ability to prevent central authorities from protecting the financial system as they have no central control over the workings of virtual currencies.⁵³ Regulators' approaches vary by jurisdiction in an attempt to prevent regulatory arbitrage and uncertainty in the financial system.

2.3.1.1 *United Kingdom*

The Financial Conduct Authority (FCA) has remained generic regarding the classification of virtual currencies and has indicated that certain virtual currencies may constitute the transfer of securities.⁵⁴ The FCA issued regulatory guidance in respect of virtual currencies and indicated that virtual currencies will fall within the FCA's regulatory parameters if a virtual currency is used for: specified investments under the FCA's Regulatory Activities Order; financial instruments in the markets under Financial Instruments Directive II; e-money under the Electronic Money Regulations; and

⁵² D Sonderegger "A regulatory and economic perplexity: bitcoin needs just a bit of regulation" (2015) 47 *Washington University Journal of Law and Policy* 175-216 175 (hereafter Sonderegger).

⁵³ Sonderegger *supra* n 52 176.

⁵⁴ P Maume & M Fromberger "Regulations of initial coin offerings: reconciling U.S. and E.U. securities laws" (2019) 19 *Chicago Journal of International Law* 548-585 567 (hereafter Maume).



payments under the Payment Systems Regulator.⁵⁵ If virtual currencies are not used for any of the aforementioned purposes, then it remains unregulated and thus consumers in the United Kingdom should take caution against the use thereof.⁵⁶

2.3.1.2 China

In 2013, the Chinese government refused to officially endorse the use of virtual currencies as a legitimate form of payment and conventional banks were prohibited from accepting it.⁵⁷ At the time, the government still required online virtual currency exchanges to report trading records to mitigate money laundering activities.⁵⁸ In the fight against corruption and capital outflow the Chinese government has completely banned virtual currencies in 2018 and has instructed that all exchanges should discontinue business.⁵⁹ China has not provided any regulatory stance on virtual currencies and it decided to take the more stringent approach by outlawing it all together.

2.3.1.3 Switzerland

Switzerland has probably the most progressive position on virtual currencies as the Swiss Financial Market Supervisory Authority (FINMA) has issued guidelines on the use of virtual currencies.⁶⁰ Virtual currencies remain financially unregulated in Switzerland as FINMA recognises innovative distributed ledger or blockchain technology to develop the Swiss financial centre.⁶¹ Nonetheless, FINMA is still concerned about virtual currencies as it relates to certain financial laws that regulate banking, money laundering and terrorism finance; collective investment schemes; and securities trading.⁶²

⁵⁵ Financial Conduct Authority “Guidance on cryptoassets: feedback and final guidance to CP 19/3” issued July 2019 *Policy Statement* 1-54 30.

⁵⁶ Maume *supra* 567 n 54.

⁵⁷ S Small “Bitcoin: the napster or currency” (2015) 37 *Houston Journal of International Law* 581 641 613 (hereafter Small).

⁵⁸ Small *supra* n 57 614.

⁵⁹ European Parliament “Virtual currencies and central banks’ monetary policy: challenges ahead” Monetary Dialogue issued July 2018 ECON Committee PE 619.009 1-30 16 (hereafter PE 619.009).

⁶⁰ PE 619.009 *supra* n 59 17.

⁶¹ FINMA Guidance 04/2017 “Regulatory treatment of initial coin offerings” issued 29 September 2017 1-4 2.

⁶² *Ibid.*

2.3.1.4 New Zealand

Virtual currency trading in New Zealand has remained relatively low and is presumed to be used for investment purposes rather than for effecting payments.⁶³ New Zealand has no regulatory framework for virtual currencies in place and regulators are attempting to apply existing promulgated financial law to regulate virtual currencies.⁶⁴

2.3.1.5 Estonia

The Central Bank of Estonia has voiced its concerns that virtual currencies hold the potential of qualifying as a Ponzi scheme, subsequently followed by the Tax and Customs Board of Estonia that declared it to be a substitute method of payment.⁶⁵ Estonia does not regard virtual currencies as a security nor as electronic money. Estonia has indicated that it is progressively researching blockchain technology but it remains unclear as to how virtual currencies will be treated.⁶⁶

Virtual currencies as an object remain largely unregulated, however the activity behind virtual currencies might be an indication of the appropriate regulatory approach.⁶⁷ It is important to determine the equilibrium between the failure to regulate technology, which can lead to a distortion of the financial system, and the over-regulation of technology, which can lead to a demand for less regulated channels or jurisdictions.⁶⁸ *Ex ante* regulation can provide the incentive for regulatory arbitrage as it is impossible to regulate the financial system to avoid every failure and it is also undesirable to do so.⁶⁹ It is evident that there is an absence of virtual currency regulatory frameworks across the world as nations attempt to apply existing financial laws aimed at regulating the traditional financial intermediary system to virtual currencies. The final section of the chapter will focus on the regulatory arbitrage from a South African perspective.

⁶³ A Sims, K Kariyawasam & D Mayes “Regulating cryptocurrencies in New Zealand” (2018) *The Law Foundation New Zealand* 1-179 78 (hereafter Sims).

⁶⁴ Sims *supra* n 63 79.

⁶⁵ Sims *supra* n 63 92.

⁶⁶ Sims *supra* n 63 93.

⁶⁷ E Mokhtarian & A Lindgren “Rise of the crypto hedge fund: operational issues and best practices for an emergent investment industry” (2018) 23 *Stanford Journal of Law, Business and Finance* 112-158 151.

⁶⁸ S J Hughes & S T Middlebrook “Advancing a framework for regulating cryptocurrency payments intermediaries” (2015) 32 *Yale Journal on Regulation* 495-559 499.

⁶⁹ C L Reyes “Moving beyond bitcoin to an endogenous theory of decentralized ledger technology regulation: an initial proposal” (2016) 61 *Villanova Law Review* 191-234 211.

2.3.2 South African perspective

South Africa has a comprehensive and stringent financial regulation regime that has the objective to protect and promote the safety and soundness of the financial system as a whole. The South African financial legal framework follows an *ex ante* approach to financial regulation as it attempts to regulate based on forecasts rather than on actual events.

The last section of chapter two will discuss the most prominent South African financial laws which do not cater directly for the regulation of virtual currencies. Additionally, this section will attempt to link virtual currencies to the various financial sector regulation laws should they be applicable to virtual currencies. The National Credit Act⁷⁰ and the Consumer Protection Act⁷¹ may also be applicable to virtual currencies but these laws are focused on consumer protection rather than on financial regulation, and will therefore be excluded from this study.

2.3.2.1 Prudential and conduct regulation

The enactment of the Financial Sector Regulation Act⁷² has provided, in conjunction with existing financial legislation, a regulatory and supervisory architecture that *inter alia* promotes the safety and soundness of financial institutions; fair treatment and protection of financial customers; efficiency and integrity of the financial system; prevention of financial crime; and confidence of the financial system.⁷³ The FSRA has established the Prudential Authority, which is empowered to regulate and supervise financial institutions that provide financial products and services as well as market infrastructures.⁷⁴

The Act affords the power to the Prudential Authority to issue prudential standards to financial institutions in respect of the financial products and services that they provide,⁷⁵ market infrastructure to prevent financial crime and to ensure the safety and soundness of financial institutions.⁷⁶ The FSRA stipulates that any person who

⁷⁰ National Credit Act 34 of 2005.

⁷¹ Consumer Protection Act 68 of 2008.

⁷² Financial Sector Regulation Act 9 of 2017 (hereafter FSRA).

⁷³ S 7(1) of FSRA.

⁷⁴ S 34(1)(a) of FSRA.

⁷⁵ S 105(1) of FSRA.

⁷⁶ S 105(2) of FSRA.



carries out the business of providing financial products or services or market infrastructures should be licensed in accordance with the applicable financial law.⁷⁷

The Act also establishes the Financial Sector Conduct Authority (FSCA) which is responsible to enhance the efficiency and integrity of financial markets and to protect financial customers.⁷⁸ The FSCA functions as the regulator and supervisor of financial institutions' conduct, as opposed to the Prudential Authority's prudential regulation mandate.⁷⁹ The FSCA has the power to bestow conduct standards on financial institutions aimed at ensuring the efficiency and integrity of financial markets; the fair treatment of financial customers; the provision of financial education to financial customers; and reducing the risk of financial institutions that contributes to financial crime.⁸⁰

In the context of virtual currencies, it is difficult to determine whether virtual currencies should be classified under prudential regulation or conduct regulation. The dynamic fluctuation of the value of virtual currencies and the high level of risk involved in buying, selling and trading in virtual currencies may be subject to prudential regulation in South Africa to ensure safety and soundness of the entire financial system through careful consideration, forethought and prudence. Virtual currencies may also fall within the ambit of the FSCA's regulatory mandate as financial customers may require financial education and fair treatment when trading with virtual currencies and to ensure that the integrity and efficiency of the financial system is not tarnished by an unknown and disruptive technological innovation.

2.3.2.2 Deposit acceptance

The Banks Act⁸¹ describes the 'business of a bank' as any person who accepts deposits from the general public as a regular characteristic of business; solicits or advertises for deposits; accepts money, interest or any other income as a deposit; or grants, loans, acquires investments, or provides finance.⁸² Additionally, if, as a feature of regular business, money is obtained through the sale of an asset in terms of an agreement between a buyer and a seller where the buyer undertakes to purchase the

⁷⁷ S 111(1) of FSRA.

⁷⁸ S 57 of FSRA.

⁷⁹ S 58(1) of FSRA.

⁸⁰ S 106 of FSRA.

⁸¹ Banks Act 94 of 1990 (hereafter Banks Act).

⁸² S 1 of the Banks Act.

asset at a future date, it also meets the requirement of the 'business of a bank'.⁸³ The Act prohibits any person to conduct the 'business of a bank' unless such a person is a public company and is registered under this Act, and failure to adhere to this provision is an offense.⁸⁴

It may be possible that the acceptance of rands and cents in a virtual currency wallet qualifies as the acceptance of deposits. In this case, the operator or owner of a virtual currency wallet will need to have a banking licence in terms of the Banks Act and will have to comply with the provisions of this Act. The wallet will thus be treated as a traditional retail or commercial bank and will be regulated by the SARB.⁸⁵

2.3.2.3 Payment system

The National Payment System Act⁸⁶ defines a payment system as any system that enables payments to be effected and facilitates the circulation of money, while it also includes instruments and procedures that relates to the system.⁸⁷ Additionally, this Act defines a settlement system as a system that discharges payment or a settlement obligation or discharges of payment and settlement obligations between participants.⁸⁸ The SARB has the responsibility to monitor, regulate and supervise the payment, clearing and settlement system.⁸⁹ The SARB has the power to recognise a payment system management body which may determine rules, arrangements, agreements or authorisations of which the SARB is allowed to oversee and withdraw.⁹⁰ The members of a payment system management body includes the SARB, a bank, mutual bank, co-operative bank or a branch of a foreign bank, and a designated clearing system.⁹¹

As mentioned above, virtual currencies can be used for the payment of goods and services and the effecting of transactions. The trading of virtual currencies leads to the circulation of fiat currencies as well as virtual currencies themselves, and the trading of virtual currencies may therefore qualify as a payment system. Virtual currencies can also qualify as a settlement system as the payment with a virtual currency for goods and services or other virtual currencies can lead to the settlement

83 *Ibid.*

84 S 11 of the Banks Act.

85 S 4(1) of the Banks Act.

86 National Payment System Act 78 of 1998 (hereafter NPS Act).

87 S 1 of the NPS Act.

88 *Ibid.*

89 S 10(1)(c)(i) South African Reserve Bank Act.

90 S 3(2) of the NPS Act.

91 S 3(3) of the NPS Act.

of obligations that exist between participants in the decentralised peer-to-peer network. If virtual currencies fall within the ambit of the Act, it will have to comply with the rules, agreements, arrangements and authorisations of the payment system management body as recognised by the SARB and the provisions of the Act.

2.3.2.4 Investment schemes and portfolios

The Collective Investment Scheme Control Act⁹² defines a collective scheme as follows: where the members of the public are solicited or indorsed to invest money or other assets in a portfolio by an association of persons.⁹³ The portfolio should allow two or more investors to contribute money or assets and to hold a particular interest in a portfolio of that scheme or any other participatory portfolio.⁹⁴ An investor shares in the risks and benefits proportionately to their interest in the investment scheme.⁹⁵ Persons that carries out the business of a collective business scheme are required to apply to the Registrar for an association licence if the association of persons represents the interests of the financial industry; the association of persons has sufficient financial resources; the rules of the association complies with the Act; the interest of the public will be served; and the association carries out the business of a collective investment scheme.⁹⁶

In the case where virtual currencies are treated as virtual assets or where members of the public hold a proportion or interest in a virtual currency, it may qualify as a collective investment scheme, since the public is solicited to purchase or invest in a virtual currency. If the definition of a collective investment scheme is broadly interpreted, a person who purchases or invests in a virtual currency or a proportion thereof, shares in the risk and benefit (losses and profit) based on a virtual currency's volatility of value. Since the virtual currency community is based on a peer-to-peer network, it also fulfils the minimum of 'two investor requirement' as stipulated in the Act. An association licence will need to be applied for at the office of the Registrar for the collective investment schemes by the association of persons and that association will need to comply with the provisions in terms of this Act.

⁹² Collective Investment Schemes Control Act 45 of 2002 (CISCA).

⁹³ S 1 of the CISCA.

⁹⁴ *Ibid.*

⁹⁵ *Ibid.*

⁹⁶ S 26 of CISCA.

2.3.2.5 **Foreign currency and securities**

The Currency and Exchanges Act⁹⁷ empowers the Minister of Finance to promulgate Exchange Control Regulations⁹⁸ to control South Africa's foreign currency reserves as well as the spending and accrual thereof, as the foreign currency reserves are vested in the National Treasury.⁹⁹ The Regulations define that an authorised dealer is an authorised person who is permitted by the National Treasury to conduct a transaction in relation to foreign exchange.¹⁰⁰ The Regulations stipulate that a security includes shares, stock, unit certificates and any document that contains evidence of rights in securities.¹⁰¹ The most prominent definition in the Regulations is that of 'foreign currency' which is defined as any currency that is not legal tender in the Republic and includes any instrument for the payment of currency in a currency unit which is not legal tender.¹⁰²

The Regulations restrict the export of securities unless the National Treasury has granted permission or has authorised such a person.¹⁰³ A person who became entitled to the sale or procurement of foreign currency should declare it to the National Treasury or an authorised dealer.¹⁰⁴ Additionally, no person is allowed to acquire or to dispose of a security where the owner is a non-resident without the permission of the National Treasury.¹⁰⁵ Where the Regulations have been contravened, the National Treasury may issue the attachment of any money, goods, and the blocking of accounts in respect of the said contravention,¹⁰⁶ and may forfeit and dispose of money or goods attached of which orders were made.¹⁰⁷

The Regulations aim to control the flow of foreign currency in and out of South Africa. Virtual currencies themselves can qualify as a foreign currency, since it is not legal tender in South Africa and it can also qualify as an 'other instrument' for the payment of conventional foreign currency. It should also be mentioned that securities in terms of the Regulations can also potentially include virtual currencies. A virtual

⁹⁷ Currency and Exchanges Act 9 of 1933 (hereafter CEA).

⁹⁸ Exchange Control Regulations 1961 promulgated by Government Gazette No.1111 (hereafter the ECR).

⁹⁹ S 9 of the CEA.

¹⁰⁰ Regulation 1 of the ECR.

¹⁰¹ *Ibid.*

¹⁰² *Ibid.*

¹⁰³ Regulation 3(1) of the ECR.

¹⁰⁴ Regulation 6 of the ECR.

¹⁰⁵ Regulation 14(1) of the ECR.

¹⁰⁶ Regulation 22A of the ECR.

¹⁰⁷ Regulation 22B of the ECR.



currency user can obtain a share or entitlement to a proportion of a virtual currency, or a user can be entitled to an entire virtual currency.

Therefore, users of virtual currencies are exchanging South African currency for virtual currencies which may be regarded as foreign currency, or users are buying a portion of a virtual currency which may be regarded as a security in terms of the Regulations. Without the authorisation or permission of the National Treasury, the users may be in contravention of the Regulations as the exporting of currency and securities are restricted.

2.3.2.6 Derivatives

The Financial Markets Act¹⁰⁸ will possibly be applicable in cases where a derivative instrument derives its value from virtual currencies. Derivatives fall within the definition of securities in terms of this Act.¹⁰⁹ When trading securities on an exchange, where multiple buyers and sellers bid and offer securities, such an exchange should be licensed with the Registrar of Securities Services, and such an exchange should issue its own directives and rules.¹¹⁰ The same licencing, directives and rules requirements apply to clearing houses (persons responsible for providing infrastructure and the clearing of securities transactions); central securities depositories (persons providing infrastructure to settle securities transactions); and trade depositories (persons responsible for maintaining centralised electronic transaction data).¹¹¹

In the case where derivatives derive their value from virtual currencies, it may qualify as a security and this Act may then be applicable. This means that any virtual exchange where virtual currencies are bought and sold between buyers and sellers; a virtual clearing house which provides the infrastructure to settle; and a virtual central securities depository which stores electronic transaction data, would need to be licenced with the Registrar and the provisions of the Act will apply.

¹⁰⁸ Financial Markets Act 19 of 2012 (hereafter FMA).

¹⁰⁹ S 1 of the FMA.

¹¹⁰ S 1 & 9 of the FMA.

¹¹¹ S 1, 29, 49 & 56 of the FMA.

2.4 Conclusion

As discussed above, the South African regulatory framework rigorously regulates the financial system. The stringent financial regulation enhances the safety and soundness of the highly integrated financial system, promotes the reputation thereof, ensures that it is prudent and has appropriate governance in place. The acceptance of deposits; the formation of an investment scheme; the cross border flow of funds; derivatives trading on exchanges, the settling thereof and the storage of transactional data; and the payment system that effects transactions, all have their own primary legislative requirements and frameworks to enable any person to conduct these activities.

The South African regulatory architecture does not cater directly for the trading, ownership, acquiring, settling, acceptance, payment or cross-border flow of virtual currencies. It can be attempted to create a *nexus* between virtual currencies and the current financial regulatory framework, but it remains unclear which legislation will be applicable. There is also the possibility that multiple financial laws may be applicable to virtual currencies, or that only certain provisions of an act or multiple acts may apply.

It is important to take cognisance of the conceptualisation and categorisation of virtual currencies as it determines which financial regulation law in South Africa might be applicable. The current South African regulatory framework may be regarded as inadequate which can result in a regulatory arbitrage. The uncertainty and regulatory arbitrage of virtual currencies in South Africa can have a major impact and implications on the anti-money laundering and counter terrorism financing regime. Chapter three of this study will demonstrate that there is a connection between the regulatory arbitrage of virtual currencies and money laundering and terrorism financing both internationally and in South Africa.



Chapter 3:

The potential ML/TF risks that virtual currencies pose in South Africa

3.1 Introduction

The lack of an appropriate conceptualisation and classification of virtual currencies has led to a worldwide regulatory arbitrage. It falls almost completely outside the parameters of any financial regulation law. The lack of an appropriate regulatory framework presents potential risks to the interconnected financial system both in South Africa and in the world. The absence of a regulatory and supervisory architecture provides the opportunity for financial malpractice; criminal activity; and the financing of terrorism and the proliferation of weapons of mass destruction.

The anonymity and pseudonymity of virtual currencies have made it difficult to: identify the users, detect their activity, determine the reason for using virtual currencies, or to establish whether illicit merchandise is being purchased. Virtual currencies already pose significant risks to the South African financial sector both from a legal, social and economic perspective. Certain risks have already materialised and present severe implications to the financial system which include: the absence of consumer protection; the avoidance of exchange control; illicit flow of cross border funds; erroneous recording of balance of payments; tax evasion; financial instability; market integrity and reputational trust issues; incorrect monetary policy decisions; and threats to the national payment system. The aforementioned risks are of serious concern but these risks will not be included in this study.

Instead, this study focuses on the money laundering and terrorism financing (ML/TF) risks that virtual currencies pose to the South African anti-money laundering and counter-terrorism financing (AML/CTF) regime. The South African AML/CTF regime currently does not regulate or supervise the use and abuse of virtual currencies. The reason for this can be linked to virtual currencies falling outside the parameters of any other financial law as discussed in chapter two. The South African AML/CTF regime will only be applicable if another financial regulation law is also applicable.

This chapter analyses the current AML/CTF regulatory and supervisory regime by referring to the: promulgation of legislation and regulations which provides the main



requirements; issuance of directives and guidance notes that provide clarity on legislative interpretation; and international best practice and recommendations that assist in enhancing the integrity and reputation of a financial system and that forms the foundation of the South African AML/CTF regime. The first section of this chapter will focus specifically on the risk of ML/TF in relation to virtual currencies. Firstly, this section of the chapter will provide a background of ML/TF and how the formulation of international AML/CTF policy has formed the foundation of the South African regime. Secondly, this section of chapter will allude to the characteristics of virtual currencies that cause the circumvention of the AML/CTF regulatory framework. In the final part of this chapter, I will provide an outline of the current South African AML/CTF regime and how the lack of virtual currency regulation poses risks to this regime.

3.2 AML/CTF regulatory and supervisory regime

3.2.1 Background

3.2.1.1 Money laundering

It is crucial to understand what is meant by money laundering and how it impacts the financial system. Money laundering is the process whereby illegitimate proceeds of crime are made to appear legal in the financial system.¹ Money laundering comprises of a three step process namely: the placement of illegal proceeds of a crime into a legal entity; layering the illegal proceeds with a series of transactions to masquerade the origin thereof; and lastly, integrating the funds into the financial system so that the proceeds appear to be from a legal source.² Once the illegal proceeds are part of the financial system, criminals can use these funds to finance other criminal activities.³ In response to money laundering, countries regarded it as prudent to form an international organisation that is committed to preventing and combating money laundering in the financial system, which organisation is discussed below.⁴

¹ B Yantis, M Attia G Lethouris “Money laundering” (2018) 55 *American Criminal Law Review* 1469- 1496 1469.

² R J Havas, K Boehm & M Kennedy “Money laundering” (2017) 54 *American Criminal Law Review* 1577-1604 1577 (hereafter Havas).

³ Havas *supra* n 2 1578.

⁴ R Urziceanu “Money laundering” (2008) *Agora International Journal of Juridical Sciences* 305-311 310.

3.2.1.2 Terrorism financing

Terrorist organisations comprise of different sizes, complexities, motivations and capabilities, which require financial means to support their voluminous operations to achieve a common goal.⁵ Terrorist organisations require financing to acquire and maintain infrastructure, operations, recruitment, personnel, propaganda, training, compensation and social services.⁶ Terrorism financing is the act where a person wilfully provides or collect funds or other means, directly or indirectly, with an illegitimate objective or the awareness that it will be used partially or wholly for a terrorist act or by a terrorist organisation or a terrorist individual.⁷ The sources of funding for terrorism are mostly received from terrorist organisations, donations (through non-profit organisations), crowdfunding and the proceeds of criminal activities.⁸ Following the terrorist attacks of 11 September 2001 in the United States, a worldwide focus was subsequently placed on terrorism financing and to assist in the prevention and combat of terrorism.⁹

3.2.1.3 Financial Action Task Force

In 1989, the G7 member states (United States, United Kingdom, Germany, France, Italy, Japan and Canada), the European Commission and eight other nations established the Financial Action Task Force (FATF) to combat the criminal abuse of the financial system through the formulation and implementation of countermeasures.¹⁰ The measures involved the adoption of 40 recommendations that provided a comprehensive framework and relevant actions to be taken to prevent ML/TF.¹¹ At the time of this study, the FATF had 37 member states, two regional organisations, 23 observer organisations, and one observer state.¹²

⁵ Financial Action Task Force Report “Emerging terrorist financing risks” (published October 2015) 1-47 9 (hereafter FATF 2015 Report).

⁶ *Ibid.*

⁷ Financial Action Task Force Report Methodology “For assessing technical compliance with the FATF recommendations and the effectiveness of AML/CTF systems” (updated February 2019) 1-176 33.

⁸ FATF 2015 Report “Financing of recruitment for terrorist purposes” (published January 2018) 1-34 8.

⁹ A Ayers “The Financial Action Task Force: the war on terrorism will not be fought on the battlefield” (2002) 18 *New York Law School Journal of Human Rights* 449-459 454.

¹⁰ D E Osborne “The Financial Action Task Force and the legal profession” (2015) 59 *New York Law School Law Review* 421-432 422 (hereafter Osborne).

¹¹ *Ibid.*

¹² FATF Members and Observers (2019) <https://www.fatf-gafi.org/about/membersandobservers/> (accessed 2019-08-17).



The FATF does not have legislative authority but it will rather provide recommendations where member states can take the decision of whether they want to adopt the recommendations in their legislative framework. The FATF is allied with the World Bank and the International Monetary Fund which results in financial implications for FATF non-compliant member states.¹³ The FATF Recommendations¹⁴ aim at achieving a uniform global legislative and regulation framework to combat ML/TF.¹⁵ The FATF conducts assessments on the technical compliance and the effectiveness of a member state's AML/CTF framework within the 40 Recommendations.¹⁶ Member states that prove to be non-compliant and that do not have an action plan to address deficiencies are placed on a black list. The FATF will apply countermeasures on such a country which might result in the member state being ostracised from the global financial system.¹⁷

The FATF Recommendations stipulate that a member state should identify, evaluate, and comprehend its ML/TF risks and should apply appropriate action through the designation of an authority or mechanism to manage actions to evaluate risks, and subsequently apply resources to ensure the mitigation of these risks.¹⁸ The evaluation should be founded on a risk-based approach (RBA) to ensure that procedures avert or mitigate ML/TF risks.¹⁹ The Recommendations require that a member state's financial intelligence unit, policy-makers, supervisors, law enforcement agencies, and other competent agencies formulate and implement policies, share information, and any other measure to enable cooperation with the objective to combat ML/TF and the proliferation of weapons of mass destruction.²⁰

The first major technical compliance element that should be present in a member state's AML/CTF regime is the criminalisation of money laundering and applying it to other serious predicate offences, and the criminalisation of terrorism financing.²¹ Since 2003, South Africa has been a member state of the FATF and was at the time of this

¹³ Osborne n 10 *supra* 423.

¹⁴ Financial Action Task Force Recommendations (adopted February 2012) (updated June 2019) (hereafter FATF R.)

¹⁵ N W Turner "The Financial Action Task Force: international regulatory convergence through soft law" (2015) 59 *New York Law School Law Review* 547-560 556 (hereafter Turner).

¹⁶ Turner n 15 *supra* 554.

¹⁷ Turner n 15 *supra* 555.

¹⁸ FATF R.1.

¹⁹ *Ibid.*

²⁰ FATF R.2.

²¹ FATF R.3 & 5.

study assessed for the fourth time as part of the FATF's mutual evaluation mandate.²² In response to South Africa's FATF membership, the Financial Intelligence Centre Act²³ was promulgated, which lays the foundation for combating ML/TF.²⁴ The Protection of Constitutional Democracy against Terrorist and Related Activities Act²⁵ and the Prevention of Organised Crime Act²⁶ should also be taken cognisance of when ML/TF risks are considered.

3.2.1.4 South Africa

(a) Prevention of Organised Crime Act (POCA)

POCA was promulgated to prevent criminals from using proceeds of crime to facilitate and enable other criminal offences.²⁷ The preamble of POCA introduces organised crime and money laundering as a danger to public order and safety, a threat to economic stability, and a menace against international security.²⁸ The Act provides protection for every person against organised crime, intimidation and physical harm of criminal activities of organised gangs.²⁹ The Act stipulates that any person that knows that property or a part thereof forms part of the proceeds of any unlawful activity that have the effect of concealing or disguising the source, nature, location, disposition or movement of the property, ownership thereof, or interest in the property to commit an offence, avoid prosecution or remove property as a result of committing an offence, will be guilty of an offence.³⁰

POCA directly criminalises money laundering in South Africa in response to fighting the use of property which derives its origin from the commission of a crime through the financial system. Upon conviction of money laundering a person can receive a fine or imprisonment of up to five years in a magistrate's court or a life

²² FATF Countries: South Africa (2019) <http://www.fatf-gafi.org/countries/#South%20Africa> (accessed 2019-08-19).

²³ Financial Intelligence Centre Act 38 of 2001 (hereafter FICA).

²⁴ L De Koker "Client identification and money laundering control: perspectives on the Financial Intelligence Centre Act 38 of 2001" (2004) 4 *The Journal of South African Law* 715-746 716 (hereafter De Koker).

²⁵ Protection of Constitutional Democracy against Terrorist and Related Activities Act 33 of 2004 (hereafter POCDATARA).

²⁶ Prevention of Organised Crime Act 121 of 1998 (hereafter POCA).

²⁷ N C Ndzengu "Legal expenses POCA clauses: a loophole to make crime pay?" (2011) 3 *South African Journal of Criminal Justice* 309-332 310.

²⁸ Preamble of POCA.

²⁹ *Ibid.*

³⁰ S 4 of POCA.

sentence in a high court.³¹ Money laundering was considered a crime in South Africa prior to South Africa becoming a member state of the FATF who explicitly requires the criminalisation thereof.

POCA also criminalises terrorist activities and the financing of activities associated with terrorism.³² The Act describes that a person who wholly or partially, directly, or indirectly acquires, collects, uses, posses, owns, provides, make available, invites persons to make available property; provides, make available or invites persons to make available economic means; or facilitates in the acquisition, collection, use or provision of property or provision of any financial service or economic support, is guilty of an offence.³³ The intention of the property, financial service or economic support should be to commit or facilitate an offence of terrorism or terrorist activities; or for the benefit or at the direction or under the control of an entity who attempts or commits an act of terror or terrorist activities or for the benefit of a person who is listed in terms of POCDATARA,³⁴ will be guilty of an offence.³⁵ The Act also covers arrangements and transactions that are associated directly or indirectly, partially or wholly, with any of the aforementioned properties, financial services or economic support.³⁶

(b) Protection of Constitutional Democracy against Terrorist and Related Activities Act (POCDATARA)

POCDATARA also forms part of the AML/CTF regime specifically to provide for measures to combat and prevent: acts of terror that threaten the constitutional democracy of South Africa, the achievement of violent political aims that are unconstitutional and undermine the values of the Constitution and to promote international cooperation to address terrorism.³⁷ The Act also gives effect to South Africa's membership of the United Nations and the African Union, and to adhere to United Nations' Resolution 1373/2001 and the Organisation of African Unity's Convention on Combating of Terrorism.³⁸ The description of 'the financing of terrorism' and 'related terrorist activities' in POCDATARA are almost identical to POCA's

³¹ S 26 of POCA.

³² S 2 & 4 of POCA.

³³ S 4(1) of POCA.

³⁴ POCDATARA *supra* n 25.

³⁵ *Supra* n 33.

³⁶ S 4(2) & 4(3) of POCA.

³⁷ Preamble of POCDATARA.

³⁸ *Ibid.*

description.³⁹ Nonetheless, POCDATARA also makes provision for the retention or control of terrorist property, converting, concealment or disguising, removing from a jurisdiction, or the transferring of property to a nominee.⁴⁰

(c) Financial Intelligence Centre Act (FICA)

FICA was promulgated to give effect to the POCA money laundering transgressions and it gave rise to comprehensive money laundering control obligations in South Africa.⁴¹ FICA established the Financial Intelligence Centre (FIC) as South Africa's financial intelligence unit, which accepts suspicious and unusual transactions reports that are subsequently shared with intelligence and law enforcement agencies.⁴² The Act also establishes accountable and reporting institutions, which are determined by the Minister of Finance and affords certain obligations on them, requires them to be registered and to report to the FIC.⁴³

FICA identifies business sectors which are susceptible to ML/TF in South Africa and are listed *inter alia* as follows: a person that conducts the business of a bank;⁴⁴ an authorised user of an exchange;⁴⁵ a manager of a collective investment scheme;⁴⁶ a person authorised to deal in foreign exchange;⁴⁷ a person authorised to lend money against a security;⁴⁸ and a person who carries out the business of a money remitter.⁴⁹ Payment and settlement systems⁵⁰ are not listed as accountable institutions in Schedule 1 of the Act, but the FATF requires that South Africa comply with wire transfer Recommendations.⁵¹ The Act also lists other industries (such as life insurers, mutual banks and gaming activities) that should be registered as accountable institutions.⁵² Accountable institutions are required to comply with money laundering control obligations and the sharing of information with the appropriate entities.⁵³

³⁹ See S 4 of POCDATARA; S 4 of POCA.

⁴⁰ S 4(3) of POCDATARA.

⁴¹ De Koker *supra* n 24 717.

⁴² *Ibid*; FATF R.26.

⁴³ S 1, 43B & 73 of FICA.

⁴⁴ Banks Act 94 of 1990.

⁴⁵ Exchange Control Regulations 1961 promulgated by Government Gazette No.1111.

⁴⁶ Collective Investment Schemes Control Act 45 of 2002.

⁴⁷ *Supra* n 45.

⁴⁸ Securities Services Act 36 of 2004.

⁴⁹ *Ibid*.

⁵⁰ National Payment System Act 78 of 1998.

⁵¹ FATF R.16; SARB Directive 1 of 2015.

⁵² *Supra* n 35.

⁵³ D Millard & V Vergano "Hung out to dry? Attorney-client confidentiality and reporting duties imposed by the Financial Intelligence Centre Act" (2013) 389-427 395.



As mentioned above, FICA established the FIC as a juristic person that has the primary mandate to identify: proceeds of crime; combat ML/TF activities; implement United Nations Security Council Resolutions; and to share information with the National Prosecuting Authority, an investigation authority, an intelligence service, South African Revenue Service, South African Police Service, Independent Police Investigative Directorate, Intelligence Division of the National Defence Force, Office of the Public Protector, investigative division of an organ of state, or a supervisory body.⁵⁴ The FIC also implements measures for accountable institutions to freeze assets, exchange information with other similar intelligence units in other countries while it also supervises and ensures compliance with FICA.⁵⁵ The FIC is at the centre of the financial system in relation to the monitoring, analysis, compliance, guidance and identification of ML/TF risks, trends and typologies. The FIC assists law enforcement and other government agencies to combat and prevent ML/TF and other offences as recognised by the South African criminal law regime.

As virtual currencies do not fall within any of the applicable laws as discussed in chapter two of this study, the result is that traders, dealers, buyers, sellers, investors and participants in the virtual currency industry currently circumvent Schedule 1 of FICA as well as the FATF Recommendations. In the event that any of the aforementioned persons do not fall in the ambit of Schedule 1, the consequence is that neither FICA, the Money Laundering and Terrorist Financing Control (MLTFC) Regulations, FIC Guidance Notes, FIC Directives, nor FIC Public Compliance Communications are applicable. Therefore, South African law enforcement agencies, intelligence services, regulators and supervisors will not be able to identify, investigate, report or prosecute the use and abuse of virtual currencies in the financial system for ML/TF purposes. The characteristics of virtual currencies enable ML/TF which will be discussed below and have certain implications for the South African AML/CTF regime.

3.2.2 Characteristics of virtual currencies

3.2.2.1 Anonymity and pseudonymity

The anonymity and pseudonymity of virtual currencies provide users with the opportunity to use and abuse virtual currencies for ML/TF while it also provides for

⁵⁴ S 3(1) & (2) of FICA.
⁵⁵ S 3(2) of FICA.

greater anonymity than traditional currencies.⁵⁶ Virtual currencies allow for anonymous value transfers and funding where users and the source of funds are not adequately identified or not identified at all.⁵⁷ A virtual currency address comprises of a private and a public key which is not registered in the name of the user.⁵⁸ The user is in possession of the private key which provides active control over the balance of the virtual currency.⁵⁹ The transactional history is traceable, but the addresses of users are not easily identified, resulting in transactions being anonymous.⁶⁰ The implication of anonymous transactions makes it difficult for law enforcement agencies to identify, investigate and prosecute ML/TF and predicate offences.⁶¹

The use of virtual currencies leaves no paper trail for law enforcement to identify users.⁶² Each new transaction has its own address which can never be linked to a user's personal information or would be difficult to link an address to a user in the case of pseudonymity.⁶³ In 2018, the European Parliament conducted a study and concluded that anonymity is a major reason for why virtual currencies are used and abused for ML/TF.⁶⁴ Anonymity causes non-face-to-face relationships often in different jurisdictions and it enables cross-border transactions with the absence of an appropriate oversight body.⁶⁵ The absence of an oversight body is caused by the decentralised characteristic of virtual currencies.

3.2.2.2 Decentralised system

Blockchain technology allows for the execution of transactions without the need for an intermediation third party system such as banks, security repositories or brokers.⁶⁶ All transactions are validated against a predefined cryptographic validation method that

⁵⁶ FATF Report "Virtual currencies: key definitions and potential AML/CTF risk" (published June 2014) (hereafter FATF 2014 Report).

⁵⁷ *Ibid.*

⁵⁸ G W Peters, A Chappelle & E Panayi "Opening discussion on banking sector risk exposures and vulnerabilities from virtual currencies: an operational risk perspective" (2016) 17 *Journal of Banking Regulation* 239-272 262 (hereafter Peters).

⁵⁹ *Ibid.*

⁶⁰ *Ibid.*

⁶¹ E G Sanchez "Crypto-Currencies: The 21st century's money laundering and tax havens" (2017) 28 *University of Florida Journal of Law and Public Policy* 167-192 189.

⁶² *Ibid.*

⁶³ L Tennant "Improving the anonymity of the IOTA cryptocurrency" (2017) 1-20 2 (hereafter Tennant).

⁶⁴ European Parliament "Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion" (2018) PE 619.024 1-101 53 (hereafter PE 619.024).

⁶⁵ FATF 2014 Report *supra* n 56 9.

⁶⁶ PE 619.024 *supra* n 64 18.

ensures the correct sequencing of transactions and prevents double-spending.⁶⁷ A decentralised system refers to an open and complex peer-to-peer network which is established by a dedicated computing system with the absence of a central, intermediary body or entity.⁶⁸ In addition to anonymity and pseudonymity, decentralisation of a system makes it difficult for law enforcement agencies to enforce the law, seize assets, monitor and identify suspicious and unusual transaction trends, and to identify a single location or entity that have committed an offence.⁶⁹

3.2.3 The South African AML/CTF regime

In 2016, the FIC published a notice with the intention to amend Schedule 1 of FICA to include *inter alia* virtual currency exchanges as accountable institutions because the business of such exchanges poses high degree of ML/TF risks.⁷⁰ In response hereto, an Intergovernmental FinTech Working Group was established between the National Treasury, South African Reserve Bank (SARB), South African Revenue Service, Financial Sector Conduct Authority, and FIC to study, amongst other issues, the implications of virtual currencies for the AML/CTF regime of South Africa.⁷¹ As mentioned above, virtual currencies do not currently fall within the ambit of FICA, which results in repercussions for the regulatory and supervisory framework. The next part of the study will focus on the different implications that virtual currencies have for the South African AML/CTF regulatory architecture.

3.2.3.1 Customer due diligence

Accountable institutions are prohibited from entering into a business relationship where a prospective client or active client is anonymous or operate under a fictitious name.⁷² Therefore, accountable institutions should conduct customer due diligence (CDD) whereby they can identify and verify the client; understand the nature and purpose of the business relationship; and conduct ongoing due diligence to ensure

⁶⁷ *Ibid.*

⁶⁸ R M Bratspies “Cryptocurrency and the myth of the trustless transaction” (2018) 58 *Michigan Technology Law Review* 1-58 3 (hereafter Bratspies).

⁶⁹ E Howden “The crypto-currency conundrum: regulating an uncertain future” 29 (2015) Emory *International Law Review* 743-798 784.

⁷⁰ FIC notice: amendment of the schedules to the Financial Intelligence Centre Act 38 of 2001 (published 16 September 2016).

⁷¹ Intergovernmental FinTech Working Group: Crypto Assets Regulatory Working Group “Consultation paper on policy proposals for crypto assets” 2018.

⁷² FATF R.5.



that the activities of the client are in line with the client's risk profile.⁷³ Accountable institutions are explicitly prohibited from entering into a business relationship with an unknown person or a person with a fictitious identity.⁷⁴ Accountable institutions are therefore compelled to establish and verify the identity of the client; the person acting on behalf of the client; or the person on whose behalf the client is acting.⁷⁵ The main purpose of CDD, also known as 'know your customer', is for an accountable institution to understand the business that the client is conducting with the institution.⁷⁶

The CDD process functions as a ML/TF risk mitigation measure to enable an accountable institution to understand a client and to determine if it is being exploited for ML/TF purposes.⁷⁷ Prior to the implementation of the FIC Amendment Act (FICAA), accountable institutions were obliged to identify and verify the identity of a client by applying the stringent and rigid MLTFC Regulations.⁷⁸ Post the implementation of FICAA, accountable institutions may apply a flexible approach which provides the institutions a discretion on the manner in which the identity of its clients will be established and verified.⁷⁹

In addition to the CDD requirements, accountable institutions should obtain information to ensure that the client's forthcoming activity is aligned with the client's profile. The information that will provide an indication of whether transactions are in the course of the client's business includes the nature and intended purpose of the business relationship, which is dependent on the product or service that is requested; and the client's source of funds.⁸⁰ Additional information that can be obtained to understand the nature of the business relationship may include: the client's business, profession, employment, anticipated source or origin of funds, and predicted level of activity.⁸¹

The establishment of the identity of the client and the understanding of the business relationship result in the creation of a client profile and any activity that does

⁷³ *Ibid.*

⁷⁴ S 20A of FICA.

⁷⁵ S 21 of FICA.

⁷⁶ W Spruyt "The Financial Intelligence Centre Amendment Act and the application of a risk-based approach" (2017) *Annual Banking Law Update* 19-30 20.

⁷⁷ FIC Guidance Note 7 para 63 (hereafter FIC GN 7).

⁷⁸ FIC GN 7 para 73.

⁷⁹ FIC GN 7 para 74

⁸⁰ S 21A of FICA; FIC GN 7 para 124.

⁸¹ FIC GN 7 para 125.

not fit within the profile gives rise to ML/TF suspicion.⁸² Ongoing due diligence (ODD) should be conducted and includes the identification of an activity that is suspicious and that is not aligned with the client profile can be determined by keeping client information up to date, obtaining the source of funds where transactions are inconsistent, and the monitoring of transactions to identify multifaceted and uncommonly large transactions and patterns of transactions that have no ostensible motive.⁸³

It is unlawful for an accountable institution to establish a business relationship with a client or to conclude a single transaction in the instance where it is unable to comply with CDD measures.⁸⁴ Where client information is inadequate, untruthful or doubtful, the CDD process should be reinstated to ensure that a client's identity is fully established.⁸⁵ In cases where an accountable institution is unable to satisfy CDD measures of an existing client, the business relationship must be terminated.⁸⁶ This is referred to as the 'inability to conduct customer due diligence' and includes inadequate information necessary to: identify and verify the client; understanding the business relationship; and conducting ODD of the accountable institution's existing client base.⁸⁷

3.2.3.2 Enhanced due diligence

(a) Ultimate beneficial ownership

As part of the CDD process, accountable institutions are required to identify and verify the ultimate beneficial owner (UBO) and control structure where a business relationship is concluded with a legal person.⁸⁸ Additional measures to the CDD process should be applied to prevent the use of legal persons or other legal arrangements for ML/TF purposes.⁸⁹ Accountable institutions are required to apply an enhanced due diligence (EDD) process in the case of legal persons, trusts and partnerships.⁹⁰ The EDD process involves the ordinary CDD process as discussed above and additional steps to establish the nature of the client's business as well as

82 FIC GN 7 para 128.

83 S 21C FICA.

84 FATF R.10.

85 S 21D of FICA.

86 *Ibid.*

87 S 21E of FICA.

88 FATF R.10.

89 FATF R.24.

90 S 21B of the FICA.



the client's ownership and control structure.⁹¹ The EDD process should be applied to legal persons and associated legal arrangements because criminals might obscure a corporate vehicle's ownership structure and control information, purpose of the business relationship, and the source and use of funds.⁹²

The identity of the UBO of the client should be established by identifying each natural person who individually or collectively with another natural person has a controlling interest in the legal person.⁹³ In the absence of establishing the identity of a natural person with a controlling interest, the identity of the natural person who exercises control should be established.⁹⁴ In the absence of establishing either the identity of a natural person with a controlling interest or the natural person exercising control, the natural person who exercises control over the management of the legal person should be identified.⁹⁵

Similar requirements are applicable to partnerships, where the partnership; the identity of all the partners (including anonymous and *en commandite*); the person exercising control; the person authorised to conduct a single transaction or conclude a business relationship, should be established and verified.⁹⁶ In the case of a trust arrangement, an accountable institution should establish the identity of the: trust; trust number; address of the Master of the High Court; founder; trustees and beneficiaries.⁹⁷

(b) Prominent persons

An accountable institution should have measures in place to establish whether a client is a foreign prominent public official (FPPO) or domestic prominent influential person (DPIP) or holds a prominent function at an international organisation.⁹⁸ The accountable institution must obtain senior management approval; conduct reasonable steps to establish the source of wealth and source of funds; and ensure enhanced ongoing monitoring of the business relationship.⁹⁹ The aforementioned requirements should also be applied to immediate family members and known close associates of

⁹¹ S 21B(1) of FICA.

⁹² FATF Guidance "Transparency and beneficial ownership" (issued October 2014) paras 8 & 10.

⁹³ S 21B(2)(i) of FICA.

⁹⁴ S 21B(2)(ii) of FICA.

⁹⁵ S 21B(2)(iii) of FICA.

⁹⁶ S 21B(3) of FICA.

⁹⁷ S 21B(4) of FICA.

⁹⁸ FATF R.12; S 21F-G of FICA.

⁹⁹ *Ibid.*

FPPOs and DPIP.s.¹⁰⁰ It is important to take note that DPIP.s include influential persons of both the public and private sector and these persons are always considered to be a higher ML/TF risk.¹⁰¹

3.2.3.3 Duty to keep record

It is mandatory for accountable institutions to maintain client information and transaction records for a period of at least five years, which should be made effortlessly available to the applicable authorities and must be reconstructed in a manner that can be used as evidence in criminal prosecution.¹⁰² The client information that should be kept for a minimum of five years involves all the information necessary to establish and verify the identity of a client during the CDD and EDD process from the date a business relationship was terminated or a single transaction was conducted.¹⁰³

Transaction records that should be kept should include those of all the transactions that a client has effected during the business relationship five years from the date of transaction conclusion.¹⁰⁴ Transaction records should include the: amount; denominated currency; date; parties; nature; business correspondence; and account files where applicable.¹⁰⁵ The production of client information and transaction records are admissible as evidence in a court of law.¹⁰⁶

3.2.3.4 Terrorism financing and weapons of mass destruction

The FATF stipulates that member states are required to implement targeted financial sanctions relating to the prevention and suppression of terrorism and terrorism financing, and the prevention, suppression and disruption of the proliferation of weapons of mass destruction.¹⁰⁷ The President of the Republic is obliged to issue a Proclamation in the Government Gazette whenever the United Nations has identified an organisation that has committed or attempted to commit a terrorist or terrorist related activity.¹⁰⁸ This will also apply where United Nations member states should take action against a specified organisation as identified in an adopted Security

100 FATF R.12; S 21H of FICA.

101 FIC GN 7 para 140.

102 FATF R.11.

103 S 22 & S 23 of FICA.

104 S 22A(1) & S 23 of FICA.

105 S 22A(2) of FICA.

106 S 25 of FICA.

107 FATF R.6 & R.7.

108 S 25 of POCDATARA.

Council Resolution.¹⁰⁹ Upon the Proclamation of an entity in the Government Gazette, an accountable institution is required to determine whether it has a business relationship with the listed person.¹¹⁰ An accountable institution is required to submit a terrorist property report (TPR) if it has any terrorist property in its possession, under its control, or controlled by or on behalf of, to the FIC within five business days.¹¹¹

In the case where the United Nations Security Council has imposed financial sanctions against a person or an entity, the Minister of Finance and the National Director of the FIC should issue a financial sanctions notice in the Government Gazette.¹¹² Upon the issue of such a financial sanctions notification, no person is allowed to: acquire, collect, use possess, own, make available; invite to make available sanctioned property; make available financial or economic support; facilitate the acquisition, collection, issue or provide sanctioned property.¹¹³

The aforementioned prohibitions are also applied to the facilitation of financial sanctions, transactions or entering of any arrangement related to the concealment, disguising, converting and removing sanctioned property.¹¹⁴ Once an accountable institution has identified that it holds a business relationship with a sanctioned individual, the accountable institution should, in addition to reporting such a person to the FIC, freeze the property, account and services, and terminate the business relationship.¹¹⁵ The FIC has implemented a targeted financial list which accountable institutions are expected to use to identify sanctioned persons and entities.¹¹⁶

3.2.3.5 Cash transactions

The FATF provides that financial intelligence units may obtain any additional information from entities in order to undertake its functions, which include transactions of a significant amount above a set threshold.¹¹⁷ An accountable institution is compelled to report cash transactions in excess of the prescribed amount that has been received by or paid to a client, a person acting on behalf of the client, or from a

109 *Ibid.*

110 S 28A(3) of FICA.

111 S 28A(1) of FICA read with the Money Laundering and Terrorist Financing Control Regulations (hereafter MLTFC regulations) Regulation 24(1); FIC GN 6A.

112 S26A (1) & (3) of FICA.

113 S 26B(1) of FICA.

114 S 26B(2) & (3) of FICA.

115 FIC GN 6A paras 13 & 18.

116 FIC media release 9/5/1/3 (released 1 April 2019).

117 FATF R.29 read with Interpretive Note R.29.

person on whose behalf the client is acting, to the FIC as soon as possible or within two days.¹¹⁸ Such a cash threshold report (CTR) or cash aggregated transaction report (CTRA) involves an amount of higher than the prescribed threshold of R24 999.99 or a series of smaller transactions that exceeds the threshold. At the time of this study, the Minister of Finance has published draft regulations which will increase the threshold to R49 999.99.¹¹⁹

3.2.3.6 Suspicious and unusual transactions

In the event that accountable institutions suspect or has reasonable grounds to suspect that funds are the proceeds of crime or related to terrorism financing, it should be reported to the financial intelligence unit of the member state.¹²⁰ The directors, officers and employees of accountable institutions are prohibited from disclosing the report of a suspicious transaction related to the funds that are deemed to be suspicious and they are protected from criminal and civil liability if such a report breaches another law.¹²¹

Section 29 of FICA places an obligation not only on accountable institutions but also on any person that carries on a business, is in charge of or manages a business, or who is employed by a business to report suspicious and unusual transactions (STRs).¹²² Where the person has reasonably suspected that the business has: received the proceeds of crime or funds that are connected to an offence of terrorism; the business has been used for ML/TF purposes; or a transaction that transfers the proceeds of crime or terrorism, has no lawful purpose, avoids a reporting duty under FICA, relates to the financing of terrorism or financial sanctions, or tax evasion, it must report a STR to the FIC.¹²³ The section also makes provision for the reporting of suspicious and unusual activities (SARs) where a person would conduct enquiries on transactions that have not been concluded but will provide reasonable grounds for suspicious behaviour as discussed in this paragraph.¹²⁴

¹¹⁸ S 28 of FICA read with MLTFC regulation 24(4) & FIC GN 5B.

¹¹⁹ Regulation 22B of the Draft Amendments to MLTFC Regulations in terms of FIC Act.

¹²⁰ FATF R.20.

¹²¹ *Ibid.*

¹²² S 29(1) of FICA.

¹²³ S 29(1)(a)-(c) of FICA.

¹²⁴ S 29(2) of FICA.

STRs and SARs should be reported to the FIC as soon as possible after a person became aware of any fact that gave rise to the suspicion within 15 business days.¹²⁵ When a STR or SAR is reported to the FIC, it must contain as much information as possible as listed in the MLTFC Regulations.¹²⁶ The reporting of a STR or SAR is purely based on the subjective mind and a court will draw inferences based on circumstances and the evidence which it has before it.¹²⁷ The circumstances that gave rise to a STR or SAR is based on what a person suspects as opposed to what can be proven by evidence.¹²⁸ A STR/SAR report also includes terrorist financing activity reporting (TFAR) and terrorist financing transaction reporting (TFTR).¹²⁹ The former includes an activity such as where a business transfers property linked to terrorism financing and the latter involves a transaction or a series of transactions that are linked to an offence of terrorism financing.¹³⁰

3.2.3.7 Cash conveyances

Measures should be implemented by FATF member states to detect, restrain and confiscate the physical cross-border transportation of currency and bearer negotiable instruments that are suspected to be involved in ML/TF.¹³¹ A person who intends to convey an amount of cash or a bearer negotiable instrument in excess of a prescribed amount should report it to the authorised person who will report such conveyance to the FIC.¹³² It is important to note that the reporting of cash conveyances was at the time of this study not in force in South Africa and the commencement date still had to be proclaimed.¹³³

3.2.3.8 International and domestic fund transfers

Cross-border and domestic wire transfers should contain basic information of both the originator and the beneficiary to prevent criminals and terrorists from moving funds electronically to commit offences or terrorist activities.¹³⁴ All wire transfers should

¹²⁵ S 29 of FICA read with MLTFC Regulation 24(3).

¹²⁶ MLTFC Regulation 23A.

¹²⁷ FIC GN 04A para 20.

¹²⁸ *Supra* n 127 para 18.

¹²⁹ *Supra* n 127 para 28 & 29.

¹³⁰ *Supra* n 127 para 34.

¹³¹ FATF R.32.

¹³² S 30 of FICA.

¹³³ *Ibid.*

¹³⁴ FATF R.16.

include the: name of the originator; originator account number; originator's address, customer or national identity number, or date and place of birth; name of the beneficiary; and beneficiary account number.¹³⁵ Electronic transfer of funds include any transaction which is carried out by means of a credit, debit or prepaid card; or electronic transactions between accountable institutions.¹³⁶ An accountable institution that sends electronic funds out of the Republic or receives electronic funds from outside the Republic that are in excess of the legal prescribed threshold, should report such a transaction to the FIC.¹³⁷ It is important to note that international fund transfer reporting (IFTR) was at the time of this study not in force and the commencement date must still be proclaimed.¹³⁸

Accountable institutions with authorisation to conclude IFTRs are: Authorised Dealers, Authorised Dealers with Limited Authority, Financial Service Providers with direct reporting dispensation in terms of the Exchange Control Regulations and the Post Office.¹³⁹ The Minister of Finance has published draft regulations that will require that cross-border electronic transfers that are in excess of R4 999.99 should be reported to the FIC.¹⁴⁰ The main purpose of IFTRs is to identify illicit cross-border flows of funds and to enable the FIC to analyse and detect such flows of funds.¹⁴¹ An accountable institution will be required to report an IFTR to the FIC as soon as possible or within three business days once the IFTR provision is in force.¹⁴²

FICA does not make provision for domestic wire transfers as in the instance of IFTR, but accountable institutions that are participants of the clearing system should ensure that any electronic funds transfer complies with FATF Recommendation 16.¹⁴³ In the event that a participant fails to comply with Recommendation 16, it will amount to a contravention of Directive 1 of 2015 and will qualify as an offence under the National Payment Systems Act.¹⁴⁴ Any participant of the Society of Worldwide Interbank Financial Telecommunications; Intermediate Settlement Payment Clearing

¹³⁵ FATF R.16 & Interpretive Note to R.16.

¹³⁶ *Ibid.*

¹³⁷ S 31 of the FIC.

¹³⁸ *Ibid.*

¹³⁹ FIC GN 104 (draft) para 10.

¹⁴⁰ Regulation 23D of the Draft MLTFC Regulations in terms of FIC Act.

¹⁴¹ FIC consultation paper relating to the commencement of section 31 of FICA and Draft MLTFC Regulations.

¹⁴² FIC GN 104 para 28.

¹⁴³ SARB Directive 1 of 2015 para 1.3.1.

¹⁴⁴ *Supra n* 142 para 4.2.



House (PCH); Electronic Funds Transfer Debit (PCH); Electronic Funds Transfer Credit PCH; Real-time Clearing PCH; or any other electronic funds system should ensure full compliance with FATF Recommendation 16.¹⁴⁵

3.2.3.9 Powers of the FIC

As mentioned above, FICA establishes the FIC, which is *inter alia* responsible for the processing, analysing and interpreting of information that it obtains in terms of the Act and to inform certain government and law enforcement agencies where appropriate.¹⁴⁶ FICA has provided a number of specific powers to the FIC to enable it to obtain information to serve its purpose. As discussed above, accountable institutions have numerous reporting obligations in relation to transactions, activities and terrorism financing that they have to fulfil towards the FIC. The FIC is allowed to request information from an accountable institution to establish whether a person is a client; acting on behalf of a client; or a client has acted on behalf of a specified person; whether a specified number was allocated to a client; a person had a business relationship; or the status of a business relationship.¹⁴⁷ The FIC may also request accountable institutions to furnish it with additional information in relation to CTRs/CTRAs, STRs/SARs and IFTRs which includes transactional activity information and supporting documentation.¹⁴⁸ The FIC also has the power to direct an accountable institution to proceed with a CTR or STR.¹⁴⁹

Additionally, the FIC may intervene in the proceeding of a transaction or proposed transaction of an accountable institution if such a transaction is involved in the proceeds of crime or property relating to the financing of terrorism, or property that is owned, controlled by or on behalf of, or at the direction of a person or entity pursuant to a resolution of the United Nations Security Council.¹⁵⁰ Furthermore, if a transaction or a proposed transaction constitutes money laundering or a transaction that relates to the transfer of proceeds of crime, tax evasion, has no lawful purpose, avoid a reporting duty, or relates to financial sanctions or terrorism financing, the FIC may intervene in the proceeding of such transaction.¹⁵¹ The FIC may intervene for a period

¹⁴⁵ *Supra n* 142 para 1.3.7.

¹⁴⁶ S 2(1) & 4 of FICA.

¹⁴⁷ S 27 of FICA.

¹⁴⁸ S 32(1) & (2) of FICA.

¹⁴⁹ S 33 of FICA.

¹⁵⁰ S 34(1)(a) of FICA.

¹⁵¹ S 34(1)(b) of FICA.

of up to ten business days in order to make the necessary investigations and involve investigating agencies or the National Prosecuting Authority.¹⁵² The FIC may apply to a designated judge to issue a monitoring order where an accountable institution will be obliged to report all transactions in respect of an account or specific facility to the FIC on an ongoing basis.¹⁵³

3.3 Analysis of the South African AML/CTF regime and virtual currencies

The characteristics and non-regulation of virtual currencies have created the opportunity for criminals and terrorist organisations to operate outside the conventional South African financial and intermediary system. Virtual currencies present the opportunity to launder money of criminal proceeds and the funding of terrorism without the detection of accountable institutions. This results in the failure to report transactions to the FIC, which has the ultimate consequence of South African law enforcement agencies and intelligence services not being able to investigate and prosecute money laundering, the predicate offences related thereto or the financing of terrorism.

Virtual currencies that derive its value from the proceeds of crime or that are used to finance terrorism or terrorist activities fall within the ambit of POCA and will qualify as an offence.¹⁵⁴ However, the use of virtual currencies disguises the source, nature, location, disposition, ownership and movement of value through the decentralised peer-to-peer network which cannot be traced. The same holds for terrorism financing where the value derived from virtual currencies can be used to provide for property, provision of financial services or economic support for terrorist organisations.

Since FICA, MLTFC Regulations, FIC Guidance Notes and South Africa's FATF obligations are not applicable to virtual currencies, it renders it impossible for the FIC, supervisory bodies, law enforcement agencies and intelligence services to fulfil their objectives as mandated by the AML/CTF regime. The next section will conclude the chapter by demonstrating the implications that virtual currencies have for specific areas of the AML/CTF regulatory framework.

¹⁵² S 34(1)(b)(ii) of FICA.

¹⁵³ S 35(1) of FICA.

¹⁵⁴ See S 4(1) of POCA.

3.3.1 **Customer due diligence and enhanced due diligence**

Virtual currencies do not fit within the CDD process to identify and verify its users, buyers, sellers, investors and traders.¹⁵⁵ The anonymity and pseudonymity of virtual currencies allows for the transfer of value without establishing the identity of the person or to be able to realise that client information is doubtful or veracious, since no client information is obtained.¹⁵⁶ Virtual currencies are only effected through a private and public encrypted key that are not registered to an address.¹⁵⁷ This results in the transfer of value or proceeds between users without linking their personal information.¹⁵⁸ Not only is value transferred through the network without the oversight of a central authority but it enables a non-face-to-face relationship and transaction between participants who are unknown to one another.¹⁵⁹

A business relationship can thus be established or a single transaction can be concluded between buyers and sellers through the virtual community completely – either fictitiously, anonymously or without a risk profile. Not only are the buyer and the seller unknown to one another but the nature of the business is also unknown, which is usually determined through the product or service that the client has taken up.¹⁶⁰ The purpose for buying or selling virtual currencies can be for investment or currency trading purposes, or the purchasing of legal or illegal goods and services. The trading of virtual currencies occurs without any interaction between the buyer and seller and the reason for the trading is not disclosed. The buying of virtual currencies can be derived from the proceeds of crime and the selling thereof can form part of the layering process.¹⁶¹

Another significant consequence of not understanding the nature of the business relationship between the buyer and seller, is that the source of funds cannot be established or verified.¹⁶² The absence of knowledge regarding the sources of funds conceals and disguises the true cradle of the earnings of funds, whether it is legitimate or illegitimate.¹⁶³ There is no evidence of a trail between the proceeds of a crime and the integration of those proceeds either back into the financial intermediary system or

¹⁵⁵ See S 21 of FICA.

¹⁵⁶ FATF 2014 Report *supra* n 56.

¹⁵⁷ Peters *supra* n 58 262.

¹⁵⁸ Tennant *supra* n 63 2.

¹⁵⁹ FATF 2014 Report *supra* 56 9.

¹⁶⁰ FIC GN 7 *supra* n 77 para 124

¹⁶¹ See an explanation of the stages of money laundering in Havas *supra* n 2 1577.

¹⁶² See S 21A of FICA.

¹⁶³ FATF 2014 Report *supra* n 56 9.

kept within the virtual network to fund other criminal activities or terrorist activities. In the absence of establishing a person's identity, source of funds and risk profile, transactions of virtual currencies cannot be monitored.¹⁶⁴ Multifaceted and uncommonly large transactions that have no perceived intention goes unnoticed.¹⁶⁵ The identity, source of wealth, source of funds and business relationship of DPIPs, FPPOs, their family members and known associates present itself as impossible to establish and monitor.¹⁶⁶

Entities such as legal persons, trusts and partnerships can also transact with virtual currencies without the establishment of these entities' identity. The UBO, the significant controller or the person with executive power of the legal entity cannot be identified and all other CDD measures can also not be applied as discussed above.¹⁶⁷ Trusts and partnerships, the trustees and beneficiaries, the partners and persons with significant control, respectively are similarly unidentifiable.¹⁶⁸ Entities are presented with the opportunity to layer the proceeds of crime through the exchange of conventional currency for virtual currency between different entities, between an entity and the virtual network, transferred from the virtual network back to an entity, and the proceeds thereof subsequently diluted between other corporate entities appearing to be legal and integrated into the financial system.¹⁶⁹

3.3.2 Record keeping

The absence of the establishment of the identity and the verification of buyers and sellers of virtual currencies as a result of anonymity and pseudonymity, means that the record keeping requirement becomes inefficacious.¹⁷⁰ There is no CDD or EDD client information that can be kept for a minimum period of five years after the relationship between the buyer and the seller has been established and to be reconstructed in manner to be used as evidence in criminal prosecution.¹⁷¹ Similarly, each new virtual currency transaction has its own address and cannot be linked to any

¹⁶⁴ See S 21C of FICA.

¹⁶⁵ *Ibid.*

¹⁶⁶ See S 21F-G of FICA.

¹⁶⁷ See S 21B(1) of FICA.

¹⁶⁸ See S 21(2)-(3) of FICA.

¹⁶⁹ FATF Report "The misuse of corporate vehicles, including trust and company service providers (published 13 October 2006) 1-67 3.

¹⁷⁰ See S 22 of FICA.

¹⁷¹ *Ibid.*

user, which ultimately means that the transaction is also anonymous.¹⁷² It is also important to take cognisance of the question of who shall be responsible for keeping record of CDD, EDD and transactional information if virtual currency users and transactions were not anonymous, since it operates in a decentralised system.

3.3.3 Terrorism property and sanctions

Virtual currencies can be exploited to: acquire, collect, use, possess, own, make available; invite to make terrorist property available; make financial or economic support available; facilitate the acquisition, collection, issue or provide funding for terrorist organisation and their operations.¹⁷³ The anonymity of users poses the risk that other participants might be trading with a sanctioned individual. The obligation to report terrorist property to the FIC within five days becomes redundant.¹⁷⁴ The terrorist property cannot be linked to a virtual currency and therefore neither the terrorist property nor the virtual currency can be frozen or restricted.¹⁷⁵

3.3.4 Reporting duties

The cash threshold reporting obligation is circumvented as transactions pass through the decentralised peer-to-peer network and traditional cash do not pass through the hands of virtual currency users.¹⁷⁶ The absence of cash transactions results in the failure for the cash threshold obligation to meet its objective. Large value transactions of virtual currencies in excess of the present-day legal cash threshold limit of R24 999.99 if converted, go undetected and therefore will not be reported to the FIC.¹⁷⁷ For the same reason, the cash conveyance reporting objective will not be satisfied.¹⁷⁸

STRs and SARs should be reported by any person who carries out a business, employed by a business or manages a business irrespective of whether or not the person qualifies as an accountable institution in terms of Schedule 1 of the Act.¹⁷⁹ A user of virtual currencies should, when he or she applies his or her mind, report a STR or SAR when he or she has a reasonable suspicion that the proceeds of virtual

¹⁷² Tennant *supra* n 63 2.

¹⁷³ FATF 2015 Report *supra* n 5 report 9-10.

¹⁷⁴ S 26B & S 28A(1) of FICA read with MLTFC Regulation 24(1) & FIC GN 6A paras 12-13.

¹⁷⁵ *Ibid.*

¹⁷⁶ Bratspies *supra* n 68 3.

¹⁷⁷ S 28 of FICA read with MLTFC Regulation 24(4) & FIC GN 5B.

¹⁷⁸ See S 30 of FICA.

¹⁷⁹ See S 29(1) & (2) read with Schedule 1 of FICA.

currencies have been derived from criminal activities, has no legal purpose or is used to fund acts of terrorism, or has inquired on any of the aforementioned.¹⁸⁰ In instances when the user realises through subjective knowledge that virtual currencies are being abused to launder money or finance terrorism, the person will not be able to report a STR or SAR to the FIC as the user does not have access to the information that needs to be reported as required in terms of the MLTFC Regulations.¹⁸¹ The user will have to submit information in relation to the person and the transaction which proves to be anonymous.¹⁸²

When the IFTR reporting requirement commences, all cross-border transactions above the legal threshold of R4 999.99 need to be reported to a designated authority by authorised persons in terms of the Exchange Control Regulations.¹⁸³ The decentralised peer-to-peer network creates the opportunity for virtual currency users to conduct cross-border transactions with other unknown peers and establish a non-face-to-face relationship without a central body overseeing these transactions.¹⁸⁴ This results in the movement of illicit funds going undetected by the designated authority and unreported to the FIC.¹⁸⁵

3.3.5 Wire transfers

As discussed, the FATF requires that wire transfers should include both the originator's and beneficiary's information, and this applies to electronic fund transfers as well.¹⁸⁶ The payment and settling of all electronic domestic and international transactions are therefore required to comply with FATF requirements.¹⁸⁷ In chapter two, this study showed that the trading of virtual currencies can qualify as a payment or settlement system, or a clearing house, or even a central depository.¹⁸⁸ The non-face-to-face relationship between the originator and beneficiary and their unknown identities have the consequence that the aforementioned information cannot be obtained. An originator and beneficiary may know each other or be aware of each

¹⁸⁰ See S 29(1)(a)-(c) of FICA.

¹⁸¹ MLTFC Regulation 23A.

¹⁸² Tennant *supra* n 63 2.

¹⁸³ See S 31 of FICA read with MLTFC Regulations & FIC GN 104 (draft) para 10.

¹⁸⁴ FATF 2014 Report *supra* n 56 9

¹⁸⁵ FIC consultation paper relating to the commencement of section 31 of FICA and Draft MLTFC Regulations.

¹⁸⁶ FATF R.16 read with Interpretive Note to R.16.

¹⁸⁷ SARB Directive 1 of 2015 para 1.3.1.

¹⁸⁸ See National Payment Systems Act 78 of 1998.

other, but the users' addresses cannot be linked to the transactions since transactions are effected through a private and public key through the decentralised network.¹⁸⁹ The objectives of both FATF Recommendation 16 and SARB Directive 1 therefore become expendable.

3.3.6 Powers of the FIC

The FIC will not be able to receive all the legislatively required reports under FICA, namely CTRs and CTRAs, STRs and SARs, TPRs and TARs, cash conveyances and IFTRs, which should be made within their own respective time frames.¹⁹⁰ The FIC will not be able to submit a request for additional information to any person in relation to any of the reporting obligations, as the users of virtual currencies are unknown and no reports have been received.¹⁹¹ The FIC will fail in intervening in transactions of virtual currencies that are proceeds of crime, constitutes money laundering or tax evasion, or that are connected to any terrorist act or linked to a terrorist activity, and will be unable to apply for a monitoring order at a competent judge.¹⁹² The FIC will not be able to serve its purpose of collecting and analysing information, and the sharing of significant information with the appropriate law enforcement agencies, intelligence services and supervisory bodies.¹⁹³ The entire existence of the FIC might become obsolete as a result of virtual currencies.

3.4 Conclusion

As deliberated in chapter two, the absence of conceptualisation and categorisation of virtual currencies has had the consequence that no financial regulation law will be applicable. Chapter three has indicated that the regulatory arbitrage in relation to virtual currencies lead to it circumventing the South African AML/CTF regime, which has attracted the attention of criminal enterprises to launder money off their predicate offences and terrorist entities to finance their terrorist activities. Anonymity, pseudonymity and decentralisation as characteristics of virtual currencies have been taken advantage of by criminals and terrorist organisations. These characteristics

¹⁸⁹ Peters *supra* n 58 262.

¹⁹⁰ See part 3 of chapter 3 of FICA.

¹⁹¹ S 27 of the FIC.

¹⁹² S 34 of FICA.

¹⁹³ S 2 & 4 of FICA.



make it impossible to identify users, their activities, the transactions and the reason for dealing in virtual currencies.

Chapter three focused mainly on setting out the current South African AML/CTF regime and the implications that virtual currencies have therefor. The regime does not apply to virtual currencies and it also does not make provision therefor. This chapter showed that it is impossible to identify persons, legal entities, trusts, partnerships, DPIPs and FPPOs that trade in virtual currencies through the application of the CDD and EDD process. The consequence of this is that no records of personal information or transactions are kept. The CTR, CTRA and cash conveyance reporting obligations in terms of sections 28 and 30 of FICA respectively cannot apply since cash is not utilised in any manner, which results in these two reporting obligations being pointless.

The identification of a sanctioned person and the acquisition, funding and control of terrorist property through virtual currencies cannot be detected, which results in a TPR not being submitted. Users of virtual currencies will not be able to report a STR or SAR in relation to virtual currency transactions that are deemed suspicious and unusual within 15 days as the transactions cannot be linked to a user. The transfer of virtual currencies in and out of South Africa will go undetected and the section 31 IFTR obligation, which has to be submitted to FIC within three days, will fail. It is impossible to give effect to FATF Recommendation 16, since originators and beneficiaries of domestic and international transfer of virtual currencies will not be obtained and they will remain unidentified.

The third chapter has evidenced significant implications for specific areas of the South African AML/CTF regime. This has the possible consequence that the FIC and the regime it administers to become obsolete and redundant. The regime has not kept abreast with new technological innovations that serve the same purpose as traditional fiat currency and the financial intermediary system. This has called for the revision of the current AML/CTF regime to ensure that virtual currencies are regulated and to prevent the ML/TF risks thereof. Chapter four will focus on potential policy recommendations to close the regulatory arbitrage of virtual currencies.



Chapter 4:

Potential AML/CTF policy recommendations for virtual currencies

4.1 Introduction

The absence of the legal classification of virtual currencies has created a regulatory arbitrage which resulted in significant implications for the South African anti-money laundering and counter terrorism financing (AML/CTF) regime. The existing legislation and regulations, directives and guidance notes assist in enhancing the integrity and reputation of the financial system. It forms the foundation of the South African AML/CTF regime, but it does not include virtual currencies or mitigate the money laundering and terrorism financing (ML/TF) risks. This has created the opportunity for criminal enterprises to launder the proceeds of crime and terrorist entities to finance terrorism through the use of virtual currencies.

It is therefore necessary for policy-makers to review the current regulatory and supervisory framework to guarantee that virtual currencies are regulated in a prudent manner and to ensure that ML/TF risks are mitigated. The current regulatory framework can be reviewed by allowing for either self-regulation, government regulation or a combination thereof. All of the aforementioned approaches will broaden the existing regulatory scope.

This chapter will firstly discuss the difficulties that are faced when virtual currency regulation is considered. Secondly, this chapter will analyse the regulation of virtual currencies by alluding to international commitments, regulatory approaches and South Africa's current stance on the regulation thereof. Thirdly, possible regulatory frameworks for virtual currencies will be deliberated and the chapter will conclude by suggesting regulatory action that South African policy-makers can take to ensure the regulation of virtual currencies and the mitigation of ML/TF risks.

4.2 Difficulties of virtual currency regulation

To address the regulatory arbitrage, policy-makers will have to achieve technology-neutral regulation and make a distinction between virtual currency activity from a legal and securities standpoint.¹ Virtual currencies, as discussed in chapter two, can be classified under various functions and it operates across borders.² Regulators need to collaborate to ensure that virtual currencies are treated similarly according to its function and to provide a risk profile.³

Failure to treat virtual currencies in a similar manner causes fragmented regulatory approaches which will lead to a difficulty in deciding on and enforcing the correct regulatory action.⁴ Additionally, the implementation of the correct regulatory approach also has to include the regulation of anonymity and pseudonymity.⁵ In response to the difficulties that are associated with virtual currencies, different jurisdictions have taken different approaches in relation to regulation.

4.3 Virtual currency regulation

4.3.1 *International commitments*

FATF member states are obliged to identify and evaluate the ML/TF risks that are associated with the development of new technologies, which include delivery channels, products and services.⁶ Member states are clearly required to regulate virtual currency service providers (VCSP) from an AML/CTF perspective, have licensing requirements for VCSPs and the necessary operational systems to guarantee compliance.⁷

FATF has stipulated that certain of its adopted Recommendations also apply to the value of virtual currencies and its service providers.⁸ The value of a virtual currency is determined by the supply and demand thereof which will result in economic gains

¹ R Auer & S Claessens “Regulating cryptocurrencies: assessing market reactions” (2018) *BIS Quarterly Review* 1-65 63.

² IFWG “Crypto assets regulatory working group: consultation paper on policy proposals for crypto assets” (published 2018) 1-32 19 (hereafter IFWG).

³ *Ibid.*

⁴ IFWG *supra* n 2.

⁵ IFWG *supra* n 2.

⁶ Financial Action Task Force Recommendation 15 (hereafter FATF R.)

⁷ *Ibid.*

⁸ Financial Action Task Force “Guidance for a risk-based approach: virtual assets and virtual asset service providers” (published 2019) 1-57 19 (hereafter FATF 2019 Report).

or losses for the trader.⁹ In the instance where the value of virtual currencies form part of the proceeds of crime or is used to finance terrorism, it qualifies as a money laundering offense or a terrorism financing offense, respectively.¹⁰ Measures should be applied to confiscate and freeze without delay the value of virtual currencies when it qualifies as the proceeds of crime or is used to finance terrorism, and implement financial sanctions against the value of virtual currencies where it is used for the proliferation of weapons of mass destruction.¹¹

Procedures should be implemented to ensure that the value of virtual currencies is not abused to fund terrorism through non-profit organisations.¹² Government agencies should ensure that they have effective controls in place to identify, trace, freeze, seize and confiscate the value of virtual currencies if there is a suspicion that it is wholly or partly the proceeds of crime.¹³ VCSPs should be compelled to report suspicious and unusual transactions to the relevant authorities.¹⁴ Criminal, civil and administrative sanctions as part of the AML/CTF regime should also apply to VCSPs.¹⁵ In response to the FATF's guidance as discussed above, member states should decide on the appropriate regulation approach to include virtual currencies in their regulatory frameworks.

4.3.2 Regulatory approaches

The broad approach that countries can take is to establish whether virtual currencies can be regulated within the current regime by amending legislation or if an entirely new framework should be designed and implemented.¹⁶ After a jurisdiction has decided which broad regulatory approach to follow, the degree of robustness of the regulation can then be decided on.

Lansky provides different regulatory approaches to virtual currencies which can be divided into six robustness levels namely level zero to level five.¹⁷ The level zero

⁹ See F Wenjun, Y Wang & Z Zhang "Can cryptocurrencies be a safe haven: a tail risk perspective analysis" (2018) 50 *Applied Economics* 1-18.

¹⁰ FATF R.3; FATF R.5; FATF 2019 Report *supra* n 8

¹¹ FATF 2019 report *supra* n 8; FATF R.4, R.6 & R.7.

¹² FATF 2019 report *supra* n 8; FATF R.8.

¹³ FATF 2019 report *supra* n 8; FATF R.30.

¹⁴ FATF 2019 report *supra* n 8; FATF R.33.

¹⁵ FATF 2019 report *supra* n 8; FATF R.35.

¹⁶ European Banking Authority Opinion on Virtual Currencies (published 2014) EBA/Op/2014/08 para 150.

¹⁷ J Lansky "Possible state approaches to cryptocurrencies" (2018) 1 *Journal of Systems Integration* 19-31 22 (hereafter Lansky).

approach shows that authorities do not pay attention to the presence of virtual currencies and have effectively disregarded the phenomenon.¹⁸ The level one approach indicates that authorities have issued a declaration that the presence of virtual currencies is acknowledged and authorities are in the process of monitoring the developments surrounding such currencies.¹⁹ The level two approach involves authorities acknowledging the presence of virtual currencies and provides a regulatory proposal which involves endorsements, caution against risks and the demonstration of advantages.²⁰ The level three approach shows that an authority has issued direction to oversee virtual currencies.²¹ The level four approach establishes predefined legal requirements while authorisation would be granted if the requirements are fulfilled.²² The level five approach entails an embargo on activities that support virtual currencies.²³

4.3.3 South African approach

In 2014, the South African Reserve Bank (SARB) issued a position paper on virtual currencies.²⁴ The SARB indicated in the position paper that no regulatory standards apply to virtual currencies and therefore the SARB did not regulate or oversee virtual currency activities.²⁵ The SARB alluded that it would follow the development of technical innovation and would draft and implement a regulatory framework if it was necessary in the future.²⁶ In the same year, the National Treasury issued a press statement warning the public that there is no virtual regulatory framework in place and virtual currencies are susceptible to abuse leaving users without any legal recourse.²⁷ Virtual currencies are not legal tender and may therefore be refused as a payment instrument.²⁸ Therefore, in the same year, the SARB's and National Treasury's position placed South Africa at a level one regulatory approach.

18 *Ibid.*

19 Lansky *supra* n 17 23.

20 *Ibid.*

21 *Ibid.*

22 Lansky *supra* n 17 24.

23 *Ibid.*

24 National Payment Systems Department "Position paper on virtual currencies" (published 2014) No. 02/2014 (hereafter NPS 02/2014).

25 NPS 02/2014 *supra* n 24 para 5.1.

26 NPS 02/2014 *supra* n 24 para 5.3.

27 National Treasury "User alert: monitoring of virtual currencies" (published 18 September 2014).

28 *Ibid.*



In 2016, the Financial Intelligence Centre (FIC) issued a notice to amend Schedule 1 of the Financial Intelligence Centre Act to potentially include virtual currency exchanges as accountable institutions.²⁹ The Intergovernmental FinTech Working Group between the SARB, National Treasury, Financial Sector Conduct Authority and South African Revenue Service (SARS) issued a consultation paper in 2018 which moved South Africa's position on virtual currencies from a level one to a level two approach.³⁰ Also in 2018, SARS delivered a statement instructing that the Income Tax Act applies to virtual currencies and any gains and losses made from the trading of virtual currencies should be reported as part of a taxpayer's gross income.³¹

Since October 2018, South Africa was required to move to a level three or level four approach as the FATF indicated that the FATF Recommendations also apply to virtual currencies.³² Therefore, in order to adhere to new international requirements, South African regulators will need to provide specific conditions for formal authorisation of VCSPs.³³ Regulators have different types of regulatory frameworks which they can apply to virtual currencies, which will be discussed in the next section.

4.4 Virtual currency regulatory frameworks

4.4.1 Self-regulation

The first possible regulatory framework to consider is self-regulation. It proves to be an effective form of regulation as it is flexible in nature and caters specifically for a multifaceted and dynamic financial services industry.³⁴ It involves an amalgamation of private interests and government oversight.³⁵ The purpose of financial self-regulation is similar to that of government regulation where it aims to preserve market integrity through the reduction of risks and market transparency, and to protect financial

²⁹ FIC notice "Amendment of the schedules to the Financial Intelligence Centre Act, 2001" (published 14 September 2016).

³⁰ IFWG *supra* n 2 22.

³¹ SARS's stance on the tax treatment of cryptocurrencies (issued 6 April 2018) available at <https://www.sars.gov.za/Media/MediaReleases/Pages/6-April-2018---SARS-stance-on-the-tax-treatment-of-cryptocurrencies-.aspx> (accessed on 2019-09-12).

³² Outcomes of FATF Plenary held on 19 October 2018 Paris France para 2; FATF 2019 report *supra* n 8.

³³ IFWG *supra* n 2 22.

³⁴ International Organization of Securities Commissions Report "Model for effective regulation" (published May 2000) 1-14 1&3 (hereafter IOSC Report).

³⁵ *Ibid.*



participants.³⁶ The organisations that form part of the industry establish their own standards and best practices, and emboldens compliance there with.³⁷

The process of self-regulation is founded on a contractual relationship between individuals or entities, and regulatory standards are flexible which can easily be amended.³⁸ Contractual and regulatory standards can be enforced and disputes can be resolved through peer-to-peer arbitration, since government entities are not involved.³⁹ In certain instances, a central non-government authority can be established to ensure the adherence to standards and best practices.

Virtual currencies are already inherently a self-regulated system as it functions in a peer-to-peer network which incessantly progresses in a regulatory free environment.⁴⁰ Virtual currencies are regulated based on mathematical algorithms and formulaic which are used by the users to construct a peer-to-peer network.⁴¹ If self-regulation is not permitted it can leave virtual currencies vulnerable to criminal abuse and may lead users to trade currencies outside the jurisdiction that has the objective to regulate virtual currencies.⁴²

Self-regulation forms part of the new governance paradigm which argues against government regulation as it is a monopolistic command and control structure where information flows top-down and a government does not have the sufficient knowledge to identify challenges and address non-compliance.⁴³ Self-governance removes informational asymmetry and allows for practical regulatory decisions which address risks and issues proactively.⁴⁴ A technological driven financial system needs to be regulated by a dynamic framework and not by stringent and static rules.⁴⁵

³⁶ IOSC Report *supra* n 34 1.

³⁷ IOSC Report *supra* n 34 3.

³⁸ IOSC Report *supra* n 34 5-6.

³⁹ M Abramowicz "Cryptocurrency-based law" (2016) *Arizona Law Review* 58 359-420 405.

⁴⁰ D Sonderegger "A regulatory and economic perplexity: bitcoin needs just a bit of regulation" (2015) 47 *Washington University Journal of Law and Policy* 175-216 204 (hereafter Sonderegger).

⁴¹ Sonderegger *supra* n 40 205.

⁴² Sonderegger *supra* n 40 209.

⁴³ S T Omarova "Rethinking the future of self-regulation in the financial industry" (2010) 35:3 *Brooklyn Journal of International Law* 666-706 672 (hereafter Omarova).

⁴⁴ Omarova *supra* n 43 673.

⁴⁵ Omarova *supra* n 43 678.

4.4.2 Government regulation

The second possible regulatory framework to consider is to establish a new regulator or expand the mandate of an existing regulator. This will involve regulatory reform which is associated with changes in organisational structures of regulators, the forming of new authorities, and accompanied by uncertainties of the role of the central bank.⁴⁶ The complete prohibition of virtual currencies by an appointed regulator is economically insufficient, deprives law-abiding citizens of financial freedom and may lead to the movement of illegal activities to less regulated or less stringent jurisdictions.⁴⁷ Before a government intervenes by drafting and implementing a regulatory framework, the objectives of the regulation need to be established.⁴⁸ Regulation of virtual currencies ought to be technology-neutral and should be aimed at reducing risks, as the technology changes on an ongoing basis.⁴⁹ To achieve the objective of virtual currency regulation it requires sophisticated surveillance tools, data analytics, access to real-time information, additional expertise and target relevant information.⁵⁰

After the establishment of the regulatory objective, a synthesised approach can be adopted whereby virtual currencies are categorised and treated under existing financial regulation laws.⁵¹ Virtual currencies can be treated from a regulatory perspective according to the function thereof.⁵² Once the function has been established, the VCSPs need to be licensed at the appropriate regulator.⁵³

The virtual currency regulatory approaches that have been recommended are as follows: to declare the use of virtual currencies as legal; provide clear AML/CTF obligations guidance; allow VCSPs access to bank accounts; taxation requirements should be amended; and the creation of regulatory sandboxes.⁵⁴ The regulatory framework proposal will thus be a functional approach whereby a VCSP will be subject

⁴⁶ Omarova *supra* n 43 679-670.

⁴⁷ M Orffer "The inclusion of virtual currencies in the calculation of income tax" (2018) *Mini dissertation North-West University* 1-84 45; Sonderegger *supra* n 40 209.

M W Swinehart "Modeling payments regulation and financial changes" (2018) 67 *University of Kansas Law Review* 83-147 90 (hereafter Swinehart)

⁴⁹ Swinehart *supra* n 47 128.

⁵⁰ Swinehart *supra* n 47 146-147.

⁵¹ S Alkadri "Defining and regulating cryptocurrency: fake internet money or legitimate medium of exchange" (2019) 71 *Duke Law and Technology Review* 71-98 87 (hereafter Alkadri).

⁵² *Ibid.*

⁵³ Alkadri *supra* n 51 87-88.

⁵⁴ K Kariyawasam & D Mayes "Regulating cryptocurrencies in New Zealand" (2018) *The Law Foundation of New Zealand* 1-179 126-130.



to different licensing requirements with the appropriate regulators based on the function of the virtual currency.⁵⁵

4.5 South African regulatory action to be taken

4.5.1 General regulation

The South African regulatory regime should find a balance between virtual currencies regulating themselves and applying a hybrid regulatory framework to provide space for both the protection of the financial system and allowing for technological innovation.⁵⁶ South African policy-makers should indicate that all the functions of virtual currencies fall within the definition of regulated activities and this will establish the applicable financial legislation.⁵⁷ In a South African context, virtual currencies can be classified as a function of: deposit taking; cross-border transactions; payment and settlement system; collective investment scheme; and trading in securities.

The South African regulators should instruct VCSPs to apply for authorisation and licensing in terms of the: Banks Act as a deposit taker;⁵⁸ Collective Investment Schemes Control Act⁵⁹ as a collective investment scheme; National Payment System Act⁶⁰ as a payment and clearing system or a clearing house; Security Services Act⁶¹ as a security exchange; or Currency and Exchanges Act⁶² as an authorised dealer or authorised dealer with limited authority. The licensing and regulation will be dependent on the function of the virtual currencies which are traded on the VCSP's platform. It is thus important to note that the regulatory action proposal is that virtual currencies themselves should not be regulated but rather the activity surrounding them.

4.5.2 AML/CTF regulation

In the instance where authorisation is granted to VCSPs and licensed in terms of the appropriate financial regulatory legislation, virtual currency service providers will be

⁵⁵ A D Schmulow "The four methods of the financial system regulation: an international comparative survey" (2015) 26 *Journal of Banking and Financial Law and Practice* 151-172 154.

⁵⁶ M Alvarez "A comparative analysis of cryptocurrency regulation in the United States, Nigeria and China: the potential influence of illicit activities on regulatory evolution" (2018) 25 *ILSA Journal of International and Comparative Law* 34-56 54.

⁵⁷ Sonderegger *supra* n 40 211-213.

⁵⁸ Banks Act 94 of 1990.

⁵⁹ Collective Investment Schemes Act 45 of 2002.

⁶⁰ National Payment System Act 78 of 1990.

⁶¹ Security Services Act 36 of 2004.

⁶² Currency and Exchanges Act 9 of 1933.



automatically required to register as an accountable institution with the FIC.⁶³ The requirement will be enforceable the moment when a VCSP has been granted a license by the appropriate regulator as they will already be listed as an accountable institution.⁶⁴

Should South African financial regulators decide not to authorise and license VCSPs in accordance with the function that virtual currencies are used for, the Minister of Finance can amend the list of accountable institutions to specifically include VCSPs.⁶⁵ These service providers will be required to comply with the entire South African AML/CTF regulatory regime and failure to do so will result in enforcement and sanction actions.⁶⁶

4.6 Conclusion

As discussed above, the current regulatory framework in South Africa needs to be reviewed in order to ensure that virtual currencies are regulated in a prudent manner and to promote the protection against risks which are posed to the financial system. The failure to review the current regulatory architecture will result in further abuse of virtual currencies and continue to pose significant ML/TF risks to the financial system.

Regulatory approaches can be divided into six levels of robustness. The robustness of regulation ranges from zero where virtual currencies are disregarded, up to level six which completely prohibits the use and trading thereof. In 2014, South African regulators and policy-makers stated that they are aware of virtual currencies and are monitoring the development thereof. This has effectively moved South Africa from a level one to a level two regulatory approach which means that regulators and policy-makers acknowledge the presence of virtual currencies, different regulatory possibilities are being explored and caution should be taken against the risks thereof. Regulators and policy-makers have indicated that the South African regulatory regime should move from a level two to a level three or four regulatory robustness level to adequately address the risks that it poses to the South African financial system.

The South African regulatory regime is compelled, at least from an AML/CTF perspective, to regulate virtual currencies and to apply all AML/CTF international

⁶³ Schedule 1 of the Financial Intelligence Centre Act 38 of 2001 (hereafter FICA).

⁶⁴ *Ibid.*

⁶⁵ S 73 of the FICA.

⁶⁶ See chapter 4 of the FICA.



obligations. As South Africa is a member state of the FATF, the AML/CTF regime will need to be reviewed to include virtual currencies. In this chapter I have discussed two possible options to regulate virtual currencies, namely self-regulation and governmental regulation. The former will lead to VCSPs regulating themselves as it already forms part of a virtual peer-to-peer network which is inherently self-regulatory. The latter involves a newly established government entity which oversees all the activities of virtual currencies.

A possible recommendation for the South African regulatory regime is to apply a hybrid approach. Firstly, the approach should involve virtual currencies to remain legal and allow users to use the peer-to-peer network and promote contractual relationships between users and VCSPs. Secondly, the approach should provide VCSPs the ability to apply for licenses at existing regulators, which will depend on the function of the virtual currency. Existing regulators will therefore ensure that the functions of virtual currencies will comply with the suitable prevailing financial regulatory legislation.

The application of existing legislation will have the consequence that VCSPs will qualify as accountable institutions, which will compel them to adhere to all local and international AML/CTF obligations and standards. If policy-makers fail to include the functions of virtual currencies within any of the existing financial regulatory legislation, the Minister of Finance can declare VCSPs as accountable institutions, which will also oblige them to comply with local and international AML/CTF requirements. It is important to take cognisance of the fact that the effective regulation of virtual currencies is dependent on the activity behind the use thereof and not the virtual currency itself.



Chapter 5: Conclusion

This mini-dissertation analysed the significant money laundering and terrorism financing (ML/TF) implications that virtual currencies pose to the prevailing South African anti-money laundering and counter-terrorism financing (AML/CTF) regime. This study showed that virtual currencies are a new dynamic technological innovation that have disrupted the financial system and that it does not currently fall within the ambit of any regulatory or supervisory regime. The failure of the South African financial regulatory regime to regulate virtual currencies has presented the opportunity for criminal and terrorist organisations to abuse the system for ML/TF purposes. The lack of adequate classification and characterisation of virtual currencies has created a number of issues for policy-makers, regulators and law enforcement agencies to address. The existence of regulatory arbitrage is the main problem highlighted by this study.

Chapter one was the introductory chapter which stated the legal problem, and provided the background and context of this study. The chapter afforded the main purpose of this study which was to evidence that the lack of adequate regulation of virtual currencies poses potential ML/TF risks to the current AML/CTF regime in South Africa. The absence of regulation stems from the failure to classify virtual currencies under one or multiple financial regulation laws, which failure has caused the ML/TF risks.

Chapter two showed that the South African financial regulatory framework is rigorous and stringent to enhance the safety and soundness of the financial system. Various financial practices have their own primary financial regulation law that are applicable to each practice which includes *inter alia*: deposit-taking; cross-border transactions; payment and settling systems, and clearing houses; collective investment schemes; and the trading of derivatives and securities on exchanges. This chapter revealed that the South African financial regulatory architecture does not currently cater for virtual currencies in the context of payment, exchange, trading, acquiring, settling, ownership, use, and cross-border transactions.

Therefore, there remains a question of which financial regulation law would be partially or wholly applicable, or whether multiple financial regulation laws would be

relevant. The absence of appropriate conceptualisation and categorisation of virtual currencies has resulted in regulatory arbitrage. As virtual currencies do not fall in the ambits of any of the present financial regulation laws, this demonstrated significant ramifications for specific areas of the South African AML/CTF regime.

Chapter three evidenced that virtual currencies currently circumvent the AML/CTF regulatory regime, which presents opportunities for criminal enterprises and terrorism organisations. The main characteristics of virtual currencies, namely anonymity and pseudonymity, as well as the function thereof on a decentralised peer-to-peer network, have established a foundation for ML/TF. These features of virtual currencies make it impossible to identify the users, activities, transactions and the reason for trading therein.

This chapter demonstrated that the current South African AML/CTF regime does not make provision for virtual currencies. This proved to have a significant impact on various aspects of the AML/CTF regime. The natural persons, legal entities, trusts, partnerships, domestic politically influential persons, foreign politically prominent persons, and their family members and known associations, who use and trade with virtual currencies, cannot be identified. No personal information of the virtual currency users can be obtained and verified, nor can any record thereof be kept. This has resulted in the futility of the customer due diligence, enhanced due diligence processes and record keeping obligation.

The cash threshold reporting, cash threshold aggregated reporting and cash conveyances obligations are potentially meaningless in this context, since the essence of virtual currencies does not involve the handling of cash. The terrorist property reporting obligation would also fail, since sanctioned individuals and property cannot be detected if virtual currencies are used. The suspicious and unusual transactions and activities reporting obligations also prove to be pointless as virtual currency transactions cannot be traced and identified, and it would therefore not be possible to report transactions and activities that are deemed suspicious within fifteen days to the Financial Intelligence Centre (FIC). Virtual currencies allow for funds to be transferred in and out of South Africa without the detection thereof, which could result in the inability to report international fund transfers within three days to the FIC. Beneficiary and originator information of the transfer of funds, both domestically and internationally, can also not be obtained and verified, resulting in wire transfer requirements to be redundant.



The existing South African AML/CTF regime has not keep abreast with new financial technological developments and phenomenon. The current regime only focuses on conventional fiat currency and the traditional financial intermediary system. The purpose and existence of the FIC might become obsolete if virtual currencies are not regulated. It was therefore determined that the current regulatory regime should be reviewed to include the regulation of virtual currencies in order to reduce the ML/TF risks posed by such currencies.

Chapter four indicated that the present-day financial regulatory framework needs to be reviewed to ensure that virtual currencies are regulated in a prudent manner. The chapter set out Lansky's six robustness levels of regulation ranging from level zero, the complete disregard of the existence of virtual currencies, to level five, which outlaws virtual currencies entirely. In 2014, South Africa moved from a level one to a level two regulation severity level after the South African regulators and policy-makers had indicated that it acknowledged the presence thereof and that it was exploring potential regulatory solutions. It was indicated that the South African regulation robustness level should be moved to level three or four.

The South African AML/CTF regime should be amended to bring it in line with the Financial Action Task Force requirements to ensure that virtual currencies are regulated. This chapter explored self-regulation, where virtual currency service providers (VCSP) would regulate themselves and set their own standards, and governmental regulation, where a government would have oversight and directly regulate virtual currencies.

In this study, I recommend that the South African regulatory framework should apply a hybrid approach towards regulation. The use of virtual currencies should remain legal as prohibition thereof would likely prevent significant consequence for the AML/CTF regime. Policy makers should promote self-regulation of peer-to-peer networks through contractual relationships and endorse the establishment of self-arbitration forums. Additionally, VCSPs should have the ability to apply for registration or licencing at prevailing regulators, depending on the activity that the virtual currency is used for. The prevailing regulators would therefore be responsible for regulating the functions of virtual currencies and ensure compliance with existing financial regulation laws.

In conclusion, VCSPs should be required to register as accountable institutions with the FIC as the function of such service providers would fall within the ambits of



an existing financial regulatory law. In the alternative, the Minister of Finance should list VCSPs specifically as accountable institutions which will force them to adhere to all AML/CTF obligations. Thus, in order to address the ML/TF implications of the virtual currency regulatory arbitrage, it is recommended that the functions of virtual currencies be regulated and not the virtual currency itself.



Bibliography

International and foreign guidance

Article 2(2) Payment of Services Directive 2009/110/EC Official Journal of the European Union

Bank for International Settlements Committee on Payments and Market Infrastructures “Central Bank digital currencies” 2018

Department of the Treasury Financial Crimes Enforcement Network Guidance FIN 2013-G001 “Application of FinCEN’s regulations to persons administering, exchanging or using virtual currencies” (issued 18 March 2013)

European Banking Authority Opinion on Virtual Currencies EBA/Op/2014/08 (published 2014)

European Banking Authority Report “EBA opinion of virtual currencies” (2014)

European Central Bank Report “Virtual currencies scheme” (2012)

European Parliament “Virtual currencies and central banks’ monetary policy: challenges ahead” Monetary Dialogue issued July 2018 ECON Committee PE 619.009

European Parliament PE 619.024 1-101 53 “Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion” (2018)

FATF 2015 Report “Financing of recruitment for terrorist purposes” (published January 2018)

FATF Guidance “Transparency and Beneficial Ownership” (issued October 2014)

FATF Report “The misuse of corporate vehicles, including trust and company service providers (published 13 October 2006)

FATF Report “Virtual currencies: key definitions and potential AML/CTF risk” (published June 2014)

Finance and Economics Discussion Series Divisions of Research & Statistics and Monetary Affairs Federal Reserve Board “Bitcoin: Technical Background and Data Analysis” (issued 7 October 2014)

Financial Action Task Force “Guidance for a risk-based approach: virtual assets and virtual asset service providers” (published 2019)

Financial Action Task Force Recommendations (adopted February 2012)



- Financial Action Task Force Report “Emerging terrorist financing risks” (published October 2015)
- Financial Action Task Force Report “Virtual currencies key definitions and potential AML/CFT risks” (2014)
- Financial Action Task Force Report Methodology “For assessing technical compliance with the FATF recommendations and the effectiveness of AML/CTF systems” (updated February 2019)
- Financial Conduct Authority “Guidance on cryptoassets: feedback and final guidance to CP 19/3” (issued July 2019) Policy Statement
- FINMA Guidance 04/2017 “Regulatory treatment of initial coin offerings” (issued 29 September)
- Internal Revenue Service Notice 2014-21 (issued March 2014)
- International Organization of Securities Commissions Report “Model for effective regulation” (published May 2000)
- M Dabrowski & L Janikowski Monetary Dialogue “Virtual currencies and central bank’s monetary policies: challenges ahead” (2018) Request by ECON Committee of the European Parliament
- Outcomes of FATF plenary held on 19 October 2018 Paris France FATF 2019 report

Internet sources

- Bank of England “What is legal tender?” (2019) Available at:
<https://www.bankofengland.co.uk/knowledgebank/what-is-legal-tender>
(accessed 2019-04-27)
- FATF Members and Observers (2019) Available at: <https://www.fatf-gafi.org/about/membersandobservers/> (accessed 2019-08-17)
- FATF Countries: South Africa (2019) Available at: <http://www.fatf-gafi.org/countries/#South%20Africa> (accessed 2019-08-19)
- SARS’s stance on the tax treatment of cryptocurrencies (issued 6 April 2018)
Available at: <https://www.sars.gov.za/Media/MediaReleases/Pages/6-April-2018---SARS-stance-on-the-tax-treatment-of-cryptocurrencies-.aspx> (accessed on 2019-09-12)



Journal articles and dissertations

- Abramowicz M “Cryptocurrency-based law” (2016) 58 *Arizona Law Review*
- Alvarez M “A comparative analysis of cryptocurrency regulation in the United States, Nigeria and China: the potential influence of illicit activities on regulatory evolution” (2018) 25 *ILSA Journal of International and Comparative Law*
- Auer R & Claessens S “Regulating cryptocurrencies: assessing market reactions” (2018) *BIS Quarterly Review*
- Ayers A “The Financial Action Task Force: the war on terrorism will not be fought on the battlefield” (2002) 18 *New York Law School Journal of Human Rights*
- Bayern S “Dynamic common law and technological change: the classification of bitcoin” (2014) 71 *Washington and Lee Law Review*
- Bratspies R M “Cryptocurrency and the myth of the trustless transaction” (2018) 58 *Michigan Technology Law Review*
- Brühl V “Virtual currencies, distributed ledgers and the future of financial services” (2017) 6 *Leibniz Information Centre for Economics*
- Dang D “Macroeconomics and blockchain” (2014) European Business Administration
Metropolia University of Applied Sciences
- De Koker L “Client identification and money laundering control: perspectives on the Financial Intelligence Centre Act 38 of 2001” (2004) 4 *The Journal of South African Law*
- Fusco N “Financial regulation - regulating a new sector: how should regulatory agencies classify and regulate virtual currencies - CFTC v McDonnell” (2018) 4 *Journal of Trial & Appellate Advocacy*
- Goforth C “The lawyer’s cryptionary: a resource for talking to clients about crypto-transactions” (2019) 41 *Campbell Law Review*
- Havas R J, Boehm K & Kennedy M “Money laundering” (2017) 54 *American Criminal Law Review*
- Howden E “The crypto-currency conundrum: regulating an uncertain future” (2019) 29 *Emory International Law Review*
- Hughes S J & Middlebrook S T “Advancing a framework for regulating cryptocurrency payments intermediaries” (2015) 32 *Yale Journal on Regulation*
- Kalbaugh G “Virtual currency, not a currency?” (2016) 16 *Journal of International Business and Law*



- Kariyawasam K & Mayes D “Regulating cryptocurrencies in New Zealand” (2018) *The Law Foundation of New Zealand*
- Lansky J “Possible state approaches to cryptocurrencies” (2018) 1 *Journal of Systems Integration*
- Litwack S “Bitcoin: currency or fool’s gold: a comparative analysis of the legal classification of Bitcoin” (2015) 29 *International and Comparative Law Journal*
- Maume P & Fromberger M “Regulations of Initial Coin Offerings: reconciling U.S. and E.U. Securities Laws” (2019) 19 *Chicago Journal of International Law*
- Mokhtarian E & Lindgren A “Rise of the Crypto hedge fund: operational issues and best practices for an emergent investment industry” (2018) 23 *Stanford Journal of Law, Business and Finance*
- Ndzengu N C “Legal expenses POCA clauses: A loophole to make crime pay?” (2011) 3 *South African Journal of Criminal Justice*
- Nel H A “*Know-Your-Customer measures: mitigating money-laundering risks in mobile banking transactions*” (2017) LLM dissertation University of the North West
- Omarova S T “Rethinking the future of self-regulation in the financial industry” (2010) 35:3 *Brooklyn Journal of International Law*
- Orffer M “The inclusion of virtual currencies in the calculation of income tax” (2018) Mini-dissertation North-West University
- Osborne D E “The Financial Action Task Force and the legal profession” (2015) 59 *New York Law School Law Review*
- Peters G W, Chapelle A & Panayi E “Opening discussion on banking sector risk exposures and vulnerabilities from virtual currencies: an operational risk perspective” (2016) 17 *Journal of Banking Regulation*
- Reddy E & Minnaar A “Cryptocurrency: a tool and target for cybercrime” (2018) 31(3) *Acta Criminologica: Southern African Journal for Criminology*
- Reyes C L “Moving beyond bitcoin to an endogenous theory of decentralized ledger technology regulation: an initial proposal” (2016) 61 *Villanova Law Review*
- Sanchez E G “Crypto-Currencies: The 21st Century's Money Laundering and Tax Havens” (2017) 28 *University of Florida Journal of Law and Public Policy*
- Schmulow A D “The four methods of the financial system regulation: an international comparative survey” (2015) 26 *Journal of Banking and Financial Law and Practice*



- Schulze W G “Smart cards and e-money: new developments bring new problems” (2004) 16 *South African Mercantile Law Journal*
- Sims A, Kariyawasam K & Mayes D “Regulating cryptocurrencies in New Zealand” (2018) *The Law Foundation New Zealand*
- Small S “Bitcoin: the napster or currency” (2015) 37 *Houston Journal of International Law*
- Sonderegger D “A regulatory and economic perplexity: bitcoin needs just a bit of regulation” (2015) 47 *Washington University Journal of Law and Policy*
- Spruyt W “The Financial Intelligence Centre Amendment Act and the application of a risk-based approach” (2017) *Annual Banking Law Update*
- Stankovic A I, Mihajlovic R A & Mihajlovic A R “Crypto-currency and e-financials” (2014) 4 *International Journal for Economics and Law*
- Swinehart M W “Modeling payments regulation and financial changes” (2018) 67 *University of Kansas Law Review*
- Tennant L “Improving the Anonymity of the IOTA Cryptocurrency” (2017)
- Tobin J “Financial innovation and deregulation in perspective” (1985) 635 *Cowles Foundation Papers*
- Tuba M D “The regulation of electronic money institutions in the SADC region: some lessons from the EU” (2014) 17 *Potchefstroom Electronic Law Journal*
- Tuba M D “The technology-neutral approach and electronic money regulation in the EU: identifying the promises and challenges for future regulation in South Africa” *Paper presented at the 10th Annual International Conference on Law, 8–11 July 2013, Athens, Greece*
- Turner N W “The Financial Action Task Force: international regulatory convergence through soft law” (2015) 59 *New York Law School Law Review*
- Urziceanu R “Money Laundering” (2008) *Agora International Journal of Juridical Sciences*
- Wenjun F, Wang Y & Zhang Z “Can cryptocurrencies be a safe haven: a tail risk perspective analysis” (2018) 50 *Applied Economics*
- Yantis B, Attia M & Lethouris G “Money laundering” (2018) 55 *American Criminal Law Review*



Legislation and regulations

Banks Act 94 of 1990

Collective Investment Schemes Control Act 45 of 2002

Consumer Protection Act 68 of 2008

Currency and Exchanges Act 9 of 1933

Draft Regulations Amendments to Money Laundering Terrorism Financing Control
Regulations in terms of the FIC Act

Exchange Control Regulations 1961 promulgated by Government Gazette No.1111

Financial Intelligence Centre Act Act 38 of 2001

Financial Markets Act 19 of 2012

Financial Sector Regulation Act 9 of 2017

National Credit Act 34 of 2005

National Payment System Act 78 of 1998

Prevention of Organised Crime Act 38 of 1998

Protection of Constitutional Democracy against Terrorist and Related Activities Act 33
of 2004

Securities Services Act 36 of 2004

South African Reserve Bank Act 90 of 1989

South African regulatory guidance, directives and position papers

Financial Intelligence Centre consultation paper relating to the commencement of
section 31 of FICA and Draft MLTFC Regulations

Financial Intelligence Centre Guidance Note 04A

Financial Intelligence Centre Guidance Note 5B

Financial Intelligence Centre Guidance Note 6A

Financial Intelligence Centre Guidance Note 7

Financial Intelligence Centre Guidance Note 104A

Financial Intelligence Centre Guidance Note: amendment of the schedules to the
Financial Intelligence Centre Act 38 of 2001 (published 2016)

Intergovernmental FinTech Working Group “Crypto assets regulatory working group:
consultation paper on policy proposals for crypto assets” (published 2018)

National Payment Systems Department “Position paper on electronic money” (2009)
South African Reserve Bank NPS 01/2009

South African Reserve Bank Directive 1 of 2015



South African Reserve Bank National Payment Systems Department “Position paper on virtual currencies” (published 2014) No. 02/2014

Press statements, notifications and speeches

FIC media release 9/5/1/3 (released Wednesday 4 September 2016)

FIC notice “Amendment of the schedules to the Financial Intelligence Centre Act, 2001” (published 14 September 2016)

National Treasury “User alert: monitoring of virtual currencies” (published 18 September 2014)



List of abbreviations

AML/CTF	Anti-money laundering and counter terrorism financing
CDD	Customer due diligence
COFI	Conduct of Financial Institutions
CTR	Cash threshold reporting
CTRA	Cash threshold reporting aggregation
DPIP	Domestic prominent influential person
EBA	European Banking Authority
ECB	European Central Bank
EDD	Enhanced due diligence
FATF	Financial Action Task Force
FCA	Financial Conduct Authority
FIC	Financial Intelligence Centre
FICA	Financial Intelligence Centre Act
FICAA	Financial Intelligence Centre Amendment Act
FinGen	Financial Crime Enforcement Network
FINMA	Financial Market Supervisory Authority
FinTech	Financial technology
FPPO	Foreign politically
FSCA	Financial Sector Conduct Authority
FSRA	Financial Sector Regulation Act
IFTR	International fund transfer reporting
IFWG	Inter-Governmental Fintech Working Group
IRS	Internal Revenue Service
ML/TF	Money laundering and terrorism financing
MLTFC	Money laundering and terrorism financing control
ODD	Ongoing due diligence
PCH	Payment Clearing House
POCA	Prevention of Organised Crime Act
POCDATARA	Protection of Constitutional Democracy against Terrorist and Related Activities Act
SAR	Suspicious and unusual activity reporting



SARB	South African Reserve Bank
SARS	South African Revenue Service
STR	Suspicious and unusual transaction reporting
TFAR	Terrorist financing activity reporting
TFTR	Terrorist financing transaction reporting
TPR	Terrorist property reporting
UBO	Ultimate beneficial ownership