A Critical Analysis of South African Anti-Money Laundering Legislation Regarding Cryptocurrency

Susan E Bowden

2019

A CRITICAL ANALYSIS OF SOUTH AFRICAN ANTI-MONEY LAUNDERING LEGISLATION REGARDING CRYPTOCURRENCY

by

Susan E Bowden

214015343

Submitted in Partial Fulfilment of the Requirements for the Degree of Master of Laws (LLM)

In the Faculty of Law

at the

Nelson Mandela University (NMU)

South Campus

December 2019

Supervisor:

Prof D Erasmus

DECLARATION

I, Susan Bowden student number 214015343, hereby declare that “A Critical Analysis of South African Anti-Money Laundering Legislation regarding Cryptocurrency” for LLM (Criminal Justice) is my own work and that it has not previously been submitted for assessment or completion of any postgraduate qualification to another University for another qualification.

Susan Bowden

TABLE OF CONTENTS

SUMMARY

Cryptocurrencies are decentralised virtual currencies, using blockchain technology to process peer-to-peer electronic payments. In 2009, the first successful cryptocurrency, Bitcoin, was established. As a result of the Internet, cryptocurrencies had soon made their way into South Africa. As such, cryptocurrencies are currently not included under the definition of a legal tender and therefore remain unregulated by the legal framework. This issue is examined within this research project.

The objectives were to understand the concepts of cryptocurrency, the relevance in the financial sector, the associated risks and to establish whether regulatory interference is necessary for the operation of cryptocurrency. The legal and regulatory framework of cryptocurrencies within Canada, the United States of America and the European Union were compared to that of South Africa.

The research explained that cryptocurrencies are decentralised convertible currencies which are secured by cryptography. It highlighted the risks associated with cryptocurrencies, some of which are detrimental due to the wide use of cryptocurrencies. One of the risks included using cryptocurrencies to launder money.

In order to mitigate these risks, jurisdictions such as Canada, the United States of America and the European Union have begun to regulate cryptocurrencies by establishing a legal framework for its operation. However, no such legal framework existed in South Africa for the regulation of cryptocurrencies. As a result, the South African Reserve Bank and National Treasury released position papers, which warn consumers of the associated risks.

Therefore, the conclusion was made that regulatory intervention is necessary in South Africa. Following this, the recommendation was made to integrate cryptocurrencies into relevant existing legislation. It was recommended that regulation is the most effective method of combatting money laundering using cryptocurrencies.

KEY WORDS

Anti-money laundering

Bitcoin

Cryptocurrency

Cybercrime

Financial Action Task Force

Financial Intelligence Centre

Money laundering

ACKNOWLEDGEMENTS

I am thankful to a number of people who have all played an important role, either directly or indirectly, in the preparation of this treatise. First and foremost, I wish to express my sincere gratitude to my supervisor, Professor Deon Erasmus, for his dedication and guiding me throughout the entire process of writing this treatise. His constructive criticism and continuous support helped me to improve the quality of this research project.

Furthermore, I would like to thank Mr Cullen Gilfillan for providing extensive knowledge in technical areas during his spare time. This was much needed to grasp the concept of networking. I would also like to thank him for inspiring me to choose this particular topic.

Finally, I would like to thank my parents, Mr Neville Bowden and Dr Sandra Basson-Bowden, for the motivation, encouragement and understanding during the process of completing this treatise. Their sacrifices have not gone unnoticed. A very special acknowledgement to my grandfather, Judge Johannes Jacobus Basson, who has been a role model and inspiration during my studies.

I would therefore like to dedicate this treatise to my friends, family and all those who have supported me during this period of hard work towards this treatise.

LIST OF ABBREVIATIONS

4AMLD	4th Anti-Money Laundering Directive
ATM	Automated Teller Machine
BSA	Bank Secrecy Act
EFT	Electronic Funds Transfer
EU	European Union
FATF	Financial Action Task Force
FIC	Financial Intelligence Centre
FICA	Financial Intelligence Centre Act
FinCEN	Financial Crimes Enforcement Network
FinTRAC	Financial Transactions and Reports Analysis of Canada
FIU	Financial Intelligence Unit
ICO	Initial Coin Offering
KYC	Know Your Customer
MSBs	Money Services Businesses
NCCTs	Non-Cooperative Countries and Territories
OECD	Organisation for Economic Co-operation and Development
PCA	Proceeds of Crime and Terrorist Financing Act
PEPs	Politically Exposed Persons
POCA	Prevention of Organised Crime Act
SA	South Africa
SARB	South African Reserve Bank
SARS	South African Revenue Services

ULC	Uniform Law Commission
UN	United Nations
UNCAC	United Nations Convention against Corruption
UNCITRAL	United Nations Commission on International Trade Law
UNCTOC	United Nations Convention against Transnational Organised Crime
US	United States of America
VPN	Virtual Private Network

CHAPTER 1: INTRODUCTION

1 1 Background to Study

The State has a sovereign right to make and supply its own currency. In terms of the South African Reserve Bank Act,[1] the South African Reserve Bank (SARB) has been given this right. However, due to the growth of cryptocurrencies, the State now shares its sovereign right with the technology responsible for creating these cryptocurrencies.[2]

The rapid development of technology and the Internet creates an opportunity to improve the user's daily life, by developing innovative ways to pay for goods and services. The online medium of exchange has evolved from Electronic Funds Transfer (EFT), credit cards and PayPal[3] to cryptocurrencies.[4] However, such development is accompanied by many challenges, of which the legislature ought to be aware. Consequently, the birth of the Internet has brought with it a new type of criminal, namely cyberlaunderers.[5]

Cryptocurrencies are a fast and pseudonymous digital payment method, which is increasingly being used by criminals to launder their illicit funds that are obtained through criminal activities. In short, cryptocurrency is legal in South Africa, despite its controversial nature. Currently, South African legislation such as the Electronic Communications and Transactions Act[6] and the National Payment System Act[7] regulate e-money and other Internet-based payment methods. However, no such legislation regulates cryptocurrencies within South Africa.[8]

---

1 S10 of Act 90 of 1989.

2 Mothokoa *Regulating Crypto-Currencies in South Africa: The Need for an Effective Legal Framework to Mitigate the Associated Risks* (Masters Mini-dissertation, University of Pretoria) 2017 1.

3 PayPal is a payment service which enables the user to accept payments more securely as well as pay for goods and services. The user's information is protected by encryption methods. Thus, PayPal is a safe and easy way to pay and receive online payments.

4 Mothokoa *Regulating Crypto-Currencies in South Africa* 1.

5 Leslie Anti-*Cyberlaundering Regulation and Control* (Masters dissertation, University of the Western Cape) 2010 1.

6 25 of 2002.

7 78 of 1998.

8 Mothokoa *Regulating Crypto-Currencies in South Africa* 2.

The majority of cryptocurrencies are decentralized and therefore operate without administration or authority of the State or banks. In terms of cryptocurrencies, such as Bitcoin,[9] users remain largely anonymous, thereby making transactions difficult to trace back to a particular user. Thus, it becomes clear to see why cryptocurrencies are used to launder money. Despite these risks, cryptocurrencies remain largely unregulated in South Africa as well as having no legal status.

For the purpose of this research, Bitcoin will be used as the example of cryptocurrency and will be referred to throughout. The example of Bitcoin is used as it has the largest number of contributing computer nodes, as well achieving one of the highest market capitalisations.[10] It is noteworthy that the focus of this research is on cryptocurrency and not the wider subject of virtual currency. Although Bitcoin is used as a main example of cryptocurrency, the research is not only limited to Bitcoin, but to cryptocurrencies as a whole. Therefore, Bitcoin is merely used as a proxy in order to easily understand the concepts.

1 2 Research Problem

Ideally, South Africa would be proactive in adopting legislation to regulate cryptocurrencies before criminals have the opportunity to launder their illicit funds. This would put law enforcement one step ahead of criminals. In addition to this, it would be easier to identify cryptocurrency users and report suspicious activity if transactions were not anonymous.

However, this is not the case. At present, South Africa does not have any legislation in place regulating cryptocurrency. Therefore, no steps have been taken to combat money laundering in this regard. The reality can be described as a typical cat and mouse game. In order to remain one step ahead of the authorities, criminals use new technology and advanced money laundering techniques, which are unbeknownst to law enforcement.

---

9 Bitcoin is a type of digital currency which uses encryption methods to regulate the production of the units of currency as well as to verify transactions. Bitcoin operates independently from a central bank.

10 Gipp, Meuschke and Gernandt "Decentralized Trusted Timestamping using the Crypto Currency Bitcoin" 2015 *Proceedings of the iConference* 1 1.

Money laundering is a moving target, with new techniques and methods being developed daily. Although, financial crimes are not violent in nature, the consequences of such crimes will inevitably have an effect on the economy. In addition to this, money laundering threatens the values which society attempts to protect such as democracy, human rights and the rule of law.[11]

In terms of the traditional money laundering methods, "dirty" money is made "clean" with the use of a cash front business. However, with cryptocurrencies like Bitcoin, it eliminates the need for the cash front business. Furthermore, the fact that cryptocurrencies are unregulated makes the act of money laundering, for cyberlaunderers, even easier.

Initially, Bitcoin was created in order to allow people to transact in a quick, cheap and anonymous manner without relying on a trusted third party. This decentralised, digital currency has a self-regulatory framework, which is an appealing feature to the average, law-abiding Bitcoin user. However, these features are even more attractive to the cyberlaunderer, who intends to conceal the true origin of his criminal proceeds.[12]

Cryptocurrencies operate within an area which can only be described as a grey area of law, due to the fact that there is no regulatory framework which governs its use. The growth of cryptocurrencies has sparked an international interest, thereby resulting in countries and organisations seeking to develop a legal framework in order to regulate it.[13]

In terms of the South African Reserve Bank Act,[14] cryptocurrencies are not included under the definition of a legal tender. Therefore, legislation which regulates fiat currencies, e-money and other forms of internet-based payment systems, do not regulate cryptocurrencies. The lack of any regulatory framework gives rise to a number

---

11 Williams *An Analysis of the Critical Shortcomings in South Africa's Anti-Money Laundering Legislation* (Master's Thesis, University of the Western Cape) 2017 2.

12 Bååth *How to Combat Money Laundering in Bitcoin?* (Published thesis, Linköpings Universitet) 2016 2.

13 Mothokoa *Regulating Crypto-Currencies in South Africa* 2.

14 90 of 1989.

of risks which include loss, theft via security breach and fraud.[15] Thus, no recourse is available to those who suffer any loss or theft of cryptocurrencies.

It is clear that South Africa does not have a legal framework in place to diminish these risks. Therefore, the overall aim of this research is to bring light to this grey area of the law, namely the South African anti-money laundering legislation regarding cryptocurrency. Although the focus of this research is specifically aimed at money laundering using cryptocurrency, the traditional concept of money laundering is discussed in order to understand the foundation on which cyberlaundering is built.

1 3 Research Question

This research seeks to answer the following two questions: Firstly, can cryptocurrency be used to launder money? Secondly, does South Africa's anti-money laundering legislation cover money laundering using cryptocurrency?

1 4 Treatise Statement

Despite its popularity in many countries around the world, cryptocurrencies are relatively new to South Africa. Thus, its potential growth may bring about benefits as well as a number of risks. Considering this, this treatise will argue that there is a need for regulatory intervention by the legislature, to develop a comprehensive framework for the regulation of cryptocurrencies in order to mitigate the associated risks which currently accompany the unregulated cryptocurrencies within South Africa.

1 5 Aims and Objectives

The aims and objectives of this research are to address money laundering using cryptocurrency, more specifically, Bitcoin. Furthermore, to determine to what extent the South African anti-money laundering framework regulates this issue.

---

15 Mothokoa *Regulating Crypto-Currencies in South Africa* 3.

1 6 Research Methodology

In this treatise, both primary and secondary sources will be consulted. The primary sources include: South African anti-money laundering laws, the Financial Action Task Force (FATF) Recommendations, case law and treaties. Secondary sources include: books, journal articles and websites. The approach is to determine whether South African laws regulate money laundering using cryptocurrency. Any shortcomings in this regard will be identified and critically analysed. Furthermore, the research uses a comparative approach to draw distinctions between the regulatory frameworks of Canada, the United States of America (US) and the European Union (EU) and compare it to that of South Africa.

1 7 Literature Review

National laws only apply to a particular jurisdiction. However, cryptocurrencies have no national boundaries. As such, research has mainly focussed on the international intervention rather than States regulating cryptocurrencies within their national laws. Thus, only limited resources on the topic of cryptocurrency regulation within South Africa are available.

In June 2018, The Law Library of Congress released a report[16] surveying the legal and policy background regarding the regulation of cryptocurrencies around the world. The report is comprehensive in its discussion, by covering 130 countries and regional organisations, which have adapted their laws or policies to regulate cryptocurrencies.[17] The report identified a common action amongst the surveyed countries, were government-issued notices, which emphasised the risks of investing in cryptocurrencies.

These notices were developed in order to educate the public on the differences between state-issued currencies and cryptocurrencies. Most notices warn the public

---

16 The Law Library of Congress "Comparative Summary" in *Regulation of Cryptocurrency Around the World* (2018) 1.

17 The Law Library of Congress *Regulation of Cryptocurrency Around the World* 1.

that by investing in cryptocurrencies, they do so at their own risk and that no legal recourse is available to them in the event of theft or loss.[18]

The report highlights that some countries, such as Canada, go beyond a simple warning and have adapted their anti-money laundering laws to include cryptocurrencies. Other countries have gone a step further to ban any activity involving cryptocurrencies. The report states that countries, such as South Africa, have not only issued warnings to the public regarding the risks of investing in cryptocurrencies, but have also determined that the cryptocurrency market is too small to cause enough concern to warrant regulation or a ban on cryptocurrencies.[19]

In 2014, the SARB released a Position Paper[20] which discussed the categories of risks associated with cryptocurrencies. Furthermore, a South African article[21] highlighted the fact that SARB had reserved the right to change its position on the regulation of virtual currencies, but warns that the legislature should enact a regulatory framework on cryptocurrencies bearing in mind the value which is being moved and stored in the cryptocurrency network.[22]

This research discusses the abovementioned approaches on the regulation of cryptocurrencies within South Africa. Moreover, it will attempt to determine how South Africa can regulate cryptocurrencies in order to combat cyberlaundering, while still encouraging the lawful use of the technology.

---

18 *Ibid.*

19 *Ibid.*

20 South African Reserve Bank "Position Paper on Virtual Currencies" (03 December 2014) https://www.resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/Legal/Documents/Position%20Paper/Virtual%20Currencies%20Position%20Paper%20%20Final_02of2014.pdf (accessed 2018-11-13) 5.

21 Khosa and Visser "Blockchain Revolution and Financial Regulation in South Africa" (05 September 2016) http://www.tech4law.co.za/news-in-brief/59-law/2233-blockchain-revolution-and-financial-regulation-in-south-africa (accessed 2018-11-13).

22 Khosa and Visser http://www.tech4law.co.za/news-in-brief/59-law/2233-blockchain-revolution-and-financial-regulation-in-south-africa .

1 8 Outline of Chapters

This treatise consists of five chapters in total. This chapter introduces the background information to the study as well as discussing the problems which this research aims to address.

The second chapter will define money laundering and include a brief history on the topic. The chapter includes a detailed discussion on the process, effects and legislative framework of money laundering within South Africa. In addition to this, international responses to money laundering have been included within this chapter. This chapter is necessary in order to understand the anti-money laundering framework in South Africa and will be used to determine if cryptocurrencies, which are discussed in the next chapter, are able to fit in this framework.

The third chapter deals with cryptocurrency and its use in money laundering. The chapter starts by defining and explaining basic terms and concepts, as well as the use of cryptocurrency in general. The chapter analyses the inherent dangers of cryptocurrencies and how cryptocurrencies, like Bitcoin, can be used to launder money.

The fourth chapter discusses the regulation of cryptocurrencies. South Africa's legislation will be examined in order to determine whether, and to what extent, it regulates cryptocurrencies and what steps are being taken to prevent money laundering using cryptocurrency. A comparative analysis between South Africa's regulation of cryptocurrencies and that of other jurisdictions will be included.

The last chapter concludes and provides recommendations based on the research provided in previous chapters. South Africa's anti-money laundering legislation is critically analysed in order to determine what improvements can be made to any shortcomings which were identified regarding the regulation of cryptocurrency. Based on the comparisons between jurisdictions, recommendations are made to determine if South Africa could learn from other States when developing the anti-money laundering legislation to cover cryptocurrencies.

CHAPTER 2: UNDERSTANDING MONEY LAUNDERING

2 1 Introduction

Over the years, South Africa has enacted various laws whereby the ultimate goal is to combat money laundering.[23] The term "money laundering" is a relatively new concept, which has been defined as the processing of criminal earnings in order to hide and conceal the illegal source, from which it has initially originated.[24]

The process is of great importance to the perpetrators as it allows them to enjoy the illegal profits without exposing the origin. For a number of obvious reasons, financial institutions are more than just hesitant to handle the profits of a crime. Therefore, criminals must erase the link between these proceeds and the criminal origin as these financial institutions will not hesitate to handle an honest earning. Failure to remove this link means that the criminal proceeds will be fairly useless to the criminals.[25]

Criminal activities such as drug trafficking, smuggling and prostitution are just a few examples generating a huge illegal profit. This means that the criminals involved must find a way to control this money without exposing the illegal source or persons involved. Criminals do this by concealing their sources, altering the form or moving the money to a location which is less likely to draw attention. Governments attempt to confiscate these profits in the hope that it will discourage these activities. However, confiscation alone is not an effective deterrent.[26]

2 2 The Development of Money Laundering

It is submitted that the process of money laundering dates back to 2000BC when merchants would attempt to hide their money and trade from the Chinese rulers, who had outlawed many of the commercial trades. During this time, the merchants would attempt to move their profits by investing it in businesses located outside China. The

---

23 De Koker *Money Laundering in South Africa* (Research Project, RAU University) 2002 3.
24 Sujee *A Study of the Anti-Money Laundering Framework in South Africa and the United Kingdom* (Master's thesis, University of Pretoria) 2016 1.
25 Heymans "What is Money Laundering?" in *Money Laundering* (2002) 5.
26 Heymans *Money Laundering* 5.

reasoning behind this was that the merchants would not be arrested and charged for hiding their illegal sources if the authorities were unable to trace the sources of the benefits.[27]

Modern day money laundering was introduced during the 1920's "Prohibition era" in the US. The US federal constitution had prohibited the transportation, retail and manufacturing of any alcohol exceeding the prescribed alcoholic percentage. This created an illegal market for alcohol, run by gangs, utilising cash orientated businesses in order to hide their criminal proceeds. The purpose was to merge the criminal proceeds with the legitimate money and to declare the total amount as the earnings from these cover businesses.[28]

Money laundering was first used in a legal context in the case of *United States v $4,255,625.39.*[29] The court had upheld a penalty of money, which had been deposited into a US bank account by a Columbian citizen in the name of a fabricated entity. *In casu*, the court had concluded that this conduct is "more likely than not, a money laundering process".[30] It was only in 2001, after the 9/11 terrorist attacks, where international efforts to combat money laundering began to surface. 9/11 had emphasised the importance of tracking of the movement of money within the financial networks, worldwide.[31]

2 3 Process of Money Laundering

Due to recent developments in online technology and payment systems, money may be transferred internationally in an effortless manner. Therefore, the methods used to launder money is essentially limitless.[32] Ultimately, the goal of any money launderer is to avoid having their illegal income confiscated, as well as to evade the relevant tax

---

27 Tuba "Prosecuting Money Laundering the FATF way: An Analysis of Gaps and Challenges in South African Legislation from a Comparative Perspective" 2012 2 *CRIMSA* 103 104.
28 Tuba 2012 *CRIMSA* 104.
29 (1982) 551 F Supp. 314.
30 Tuba 2012 *CRIMSA* 104.
31 *Ibid*.
32 Sujee *A Study of the Anti-Money Laundering Framework in SA and the UK* 2.

authorities.[33] In order to stay one step ahead of authorities, perpetrators are always creating new techniques to launder their criminal proceeds.[34]

In short, the process of money laundering is described as the conversion of money, acquired by illegal means, into money which appears to be legitimate.[35] The process of conversion is done in such a way that it cannot be traced back to the illegal source.[36] By successfully concealing the true origin, the launders retain control of the criminal proceeds, thereby allowing them to enjoy the benefits of the crime.[37]

Essentially, the money laundering process has been divided up into three steps or stages, namely: placement, layering and integration.[38] The stages usually follow after one another successively. However, in some cases, the stages may apply simultaneously with or independently from one another.[39]

The money laundering process is initiated by the placement of the "dirty" money into the legitimate financial system. At this stage, the perpetrator attempts to conceal the illegal earnings by either depositing the money into a bank account, by means of smurfing or purchasing expensive property. Smurfing is the process whereby a number of anonymous people are used in order to divide a large sum of money into smaller transactions. The launderer deposits a small portion into each anonymous person's account in an attempt to avoiding any unwanted attention or raising suspicion. The transfer of large sums of money, which exceed the legal limit, are to be avoided as it may result in being reported as a suspicious transaction. It is submitted that during the placement stage, the perpetrator is said to be at his most vulnerable.[40]

---

33 *Ibid.*

34 Van Jaarsveld *Aspects of Money Laundering in South African Law* (Doctoral Thesis, University of South Africa) 2011 620.

35 Williams *An Analysis of the Critical Shortcomings in South Africa's Anti-Money Laundering Legislation* 3.

36 Naicker *Money Laundering: Fiscal & Economic Implications and the Potential Impact of the Financial Intelligence Centre Act (FICA)* (master's Dissertation, University of KZN) 2004 5.

37 Naicker *Money Laundering* 5.

38 Williams *An Analysis of the Critical Shortcomings in South Africa's Anti-Money Laundering Legislation* 33.

39 Tuba 2012 *CRIMSA* 105.

40 Williams *An Analysis of the Critical Shortcomings in South Africa's Anti-Money Laundering Legislation* 34.

This step is followed by the layering stage. In order to hide the true source of the criminal proceeds, the perpetrator must layer the money. This is done by creating various layers of transactions with the intention of interrupting any audit trail. In terms of this, the money is moved between various accounts and used to purchase property or legitimate businesses. The more layers which are created, the more difficult it becomes to follow the money trail and to prove the source thereof.[41] The purpose of the layering stage is to distance the "dirty" money from the illegal source, as well as to destroy any link which connect the two.[42]

The money laundering process is concluded by the integration stage. At this stage of the process, the perpetrator integrates the money into the economy by using instruments such as cheques, securities and letters of credit. Following this, it is almost impossible to prove the illegal source of the money.[43]

Although academics have categorised the process into three stages, a fourth stage has been identified. This is known as the legitimisation stage, which takes place after integration and is intended to make the laundered money available for use. This stage provides the perpetrators with proof that the money laundering process has been successfully completed.[44] Thus, the illegal profit appears to be a legitimate income, thereby allowing the perpetrator to enjoy the profits of the crime.[45]

2 4 Effects of Money Laundering

The general opinion is that money laundering is not followed by a great consequence. This view stems from the fact that money laundering does not directly impact victims and that the economy may, in some circumstances, benefit as the profits for the financial sector increases. Thereby, resulting in a larger credit being available.[46]

---

41 Williams *An Analysis of the Critical Shortcomings in South Africa's Anti-Money Laundering Legislation* 35.
42 Naicker *Money Laundering* 7.
43 Williams *An Analysis of the Critical Shortcomings in South Africa's Anti-Money Laundering Legislation* 35.
44 Van Jaarsveld *Aspects of Money Laundering in South African Law* 621.
45 Naicker *Money Laundering* 8.
46 Williams *An Analysis of the Critical Shortcomings in South Africa's Anti-Money Laundering Legislation* 2.

It can be argued that money, which has been laundered, is not damaging to developing countries but could be beneficial due to the fact that money remains money, regardless of whether the proceeds were due to crime or honestly earned. However, these so-called "benefits" are short term, as crime will ultimately adversely affect the community in the long term, since money laundering encourages corruption, as well as damaging the financial sector institutions.[47]

One of the consequences of money laundering is the risks to the financial sector. Money laundering poses a risk to the confidence in both the financial system and institutions. This may result in the loss of the public's trust, if financial institutions are seen laundering money. This is likely to result in the decline of business as clients may move elsewhere.[48]

The presence of money laundering in an economy will not only affect the public's confidence in the country's financial institutions but, in addition to this, will undermine the confidence of foreign investors.[49] Financial institutions rely greatly on the public's opinion of the institution's integrity. Consequently, money laundering impairs the integrity of the institution, thereby impeding on the financial institutions ability to conduct business. Therefore, in order to ensure continuous economic growth, it is imperative that the State combats money laundering in order to maintain the foreign investors' confidence in the country's financial institution.[50] In addition to this, money laundering leads to economic instability of the state. Furthermore, it results in the inequality within the distribution of wealth.[51]

Money laundering, organised crime and economic crimes are often linked with one another. Criminal organisations often use their profits to obtain control over legitimate businesses and to bribe individuals or government. The effects of this may be detrimental to the moral and ethical standards of a society, together with damaging the principles which underlie a democratic country.[52]

---

47 *Ibid*.
48 Heymans *Money Laundering* 16.
49 Williams *An Analysis of the Critical Shortcomings in South Africa's Anti-Money Laundering Legislation* 4.
50 *Ibid.*
51 *Ibid.*
52 Van Jaarsveld *Aspects of Money Laundering in South African Law* 193.

It is submitted that there are essentially five reasons for combatting money laundering, which are summarised as follows: Firstly, if crime is to be reduced then money laundering, which is a by-product of crime, is to be combatted. Secondly, money laundering undermines the financial markets. Thirdly, money laundering has the effect of corrupting professionals. Fourthly, it damages the banking industry and lastly, it adds costs to the banks as additional costs are required to implement anti-money laundering measures.[53]

In order to eliminate threats to the economy caused by money laundering, anti-money laundering legislation should be put in place in order to combat money laundering. In order to ensure that money laundering is being combatted effectively within South Africa, the anti-money laundering framework is to be discussed.[54]

2 5 Anti-Money Laundering Framework in South Africa

South Africa became a member of the FATF in 2003 and is therefore required to fulfil the Recommendations. This means that South Africa is required to criminalise and adopt laws in order to combat and prosecute money laundering.[55]

This ultimately led to the promulgation of the Prevention of Organised Crime Act (POCA)[56] as well as the Financial Intelligence Centre Act (FICA).[57] Both Acts are closely connected to one another, whereby POCA deals with substantive money laundering offences and FICA dealing with the necessary administration.[58] In 2005, FICA was amended to incorporate the combatting of the financing of terrorism by the Protection of Constitutional Democracy against Terrorist and Related Activities Act (POCDATARA).[59] However, the mere existence of the anti-money laundering

53 Van Jaarsveld *Aspects of Money Laundering in South African Law* 194.
54 Williams *An Analysis of the Critical Shortcomings in South Africa's Anti-Money Laundering Legislation* 4.
55 Williams *An Analysis of the Critical Shortcomings in South Africa's Anti-Money Laundering Legislation* 6.
56 121 of 1998.
57 38 of 2001.
58 Sujee *A Study of the Anti-Money Laundering Framework in SA and the UK* 5.
59 33 of 2004.

legislation in South Africa does not guarantee the effectiveness or adequacy of such legislation.[60]

The Financial Intelligence Centre (FIC) is established and regulated by FICA and is the Financial Intelligence Unit of South Africa.[61] In order to regulate the access to information and obligations for money laundering control, FICA had established the Counter-Money Laundering Advisory Council. The aim of the FIC is to assist in identifying criminal proceeds and to follow up on money laundering activities, financing terrorism and any other activity in this regard.[62]

In addition to this, the FIC is required to provide any authority, responsible for regulating money laundering, with the information it collects as well as exchanging information with these similar anti-money laundering bodies in order to enforce compliance with FICA.[63] FIC only provides this information to intelligence services, any investigative authorities and to the South African Revenue Services (SARS).[64]

The FATF is an intergovernmental body which was established in order to combat money laundering and terrorist financing.[65] In order to achieve this goal, the FATF established a list of Recommendations, which comprised of a set of international anti-money laundering standards. States are required to implement these Recommendations into their respective jurisdictions in order to bring them in line with the international standards.[66] The main focus of the Recommendations is to improve the anti-money laundering legal system of states, in addition to improving the international co-operation of states in combating money laundering.[67]

---

60 Sujee *A Study of the Anti-Money Laundering Framework in SA and the UK* 19.
61 Williams *An Analysis of the Critical Shortcomings in South Africa's Anti-Money Laundering Legislation* 30.
62 Williams *An Analysis of the Critical Shortcomings in South Africa's Anti-Money Laundering Legislation* 31.
63 *Ibid.*
64 *Ibid.*
65 Williams *An Analysis of the Critical Shortcomings in South Africa's Anti-Money Laundering Legislation* 5.
66 *Ibid.*
67 *Ibid.*

The Recommendations are regarded as soft law. These are laws that are not legally binding but are rather considered to be guidelines, which set a standard. These Recommendations have been subject to much criticism due to the fact that they lack binding effect on member countries and are regarded as nothing more than recommendations.[68]

The Recommendations are imposed through the FATF by way of conducting mutual evaluations. The FATF continues to monitor the compliance of member countries. In addition to this, the FATF evaluates non-member countries regardless of whether these countries have consented. This is done in terms of the Non-Cooperative Countries and Territories (NCCTs) program.[69] Once evaluations are complete, the FATF publishes its findings in a report.[70]

Alternatively, in an attempt to enforce the Recommendations, the FATF may publish a list which "name and shame" the countries who refuse to comply with the Recommendations, within their jurisdictions. These countries are then placed on the "FATF Blacklist" and are categorised as NCCTs.[71] The reasoning for the list is to apply pressure onto these countries, who do not comply with the Recommendations, in order to bring about compliance and amend their legislation so as to meet international standards.[72]

In turn, this negative publicity has consequences for the blacklisted countries. Therefore, it is clear to see why countries should comply with the Recommendations and stand together in the fight against money laundering in order to avoid the consequences which may follow.[73]

---

68 Tuba 2012 *CRIMSA* 106.
69 *Ibid*.
70 Williams *An Analysis of the Critical Shortcomings in South Africa's Anti-Money Laundering Legislation* 5.
71 *Ibid.*
72 Tuba 2012 *CRIMSA* 107.
73 Williams *An Analysis of the Critical Shortcomings in South Africa's Anti-Money Laundering Legislation* 5.

2 5 1 Money Laundering Offences in South Africa

Generally, money laundering offences are committed when certain acts, regarding the proceeds of unlawful activities, are performed. In terms of POCA, the definition is clear that such proceeds could have originated, either directly or indirectly, in South Africa or elsewhere, at any time before or after the commencement of POCA and includes property which represents such property.[74]

The term "property" is defined wide enough to include money as well as any other movable, immovable, corporeal or incorporeal thing. Furthermore, it includes any right, privileges, claims, securities and any other interest in, as well as the proceeds of such property.[75] "Unlawful activity" includes any activity which amounts to a crime or which contravenes any law, regardless of whether such conduct occurred before or after the commencement of POCA or whether or not it occurred in South Africa.[76]

Three main money laundering offences are created by POCA. The first offence arises when a person knows or ought reasonably to have known that the property is or forms a part of the earnings of the illegal activities. Such person commits an offence in terms of section 4 of POCA when they enter into an agreement, transaction or arrangement, regardless whether it is enforceable, which is in connection with such property. Furthermore, such person also commits an offence when they perform any act in connection with such property which is likely to have the effect of either concealing or hiding the nature, source, location, disposition or movement of such property; or is likely to have the effect of assisting any person who had committed such offence, to avoid prosecution in this regard.[77]

Put differently, a person will be guilty of money laundering when he or she knows or reasonably ought to have known that the property forms part of the criminal proceeds and such person continues to commit acts linked to such property, which is likely to have two consequences: firstly, it amounts to the concealment of the nature, location,

---

74 De Koker *Money Laundering in South Africa* 4.
75 De Koker *Money Laundering in South Africa* 5.
76 *Ibid.*
77 *Ibid.*

movement, ownership or interest a person may have with regard to such property. Secondly, it may result in the assistance of a person who has committed crimes in South Africa, with the intention of avoiding prosecution or to eliminate any property acquired by the criminal activities.[78] Here, the perpetrator commits a predicate offence. These are criminal offences which will inevitably give rise to money laundering due to the fact that the predicate offences produce the illegal proceeds, which will lead to money needing to be laundered.[79]

In terms of the second offence, a third party will be guilty of money laundering, in terms of section 5 of POCA, when he or she knew or ought reasonably to have known that the perpetrator had obtained the proceeds from criminal activities and enters into any transaction, agreement or arrangement with anyone in order to control, retain or make illegal funds available to the perpetrator or to benefit them in any way.[80]

The last offence provides that a person commits an offence under section 6 of POCA, when they acquire, use or possess property, while knowing or reasonably ought to have known that such property is or forms part of the proceeds of the unlawful activity of another person.[81] It is noteworthy that sections 5 and 6 deals with money laundering by a third party, whereas section 4 deals with both self and third-party money laundering.[82]

A person is said to have knowledge if such person actually knew the fact or if the court is of the opinion that such person believed that there was a reasonable possibility of such fact existing and such person had failed to acquire further information to confirm or negate the fact.[83]

---

78 Williams *An Analysis of the Critical Shortcomings in South Africa's Anti-Money Laundering Legislation* 26; *S v De Vries* 2012 (1) SA 186 (SCA).

79 Williams *An Analysis of the Critical Shortcomings in South Africa's Anti-Money Laundering Legislation* 26.

80 Williams *An Analysis of the Critical Shortcomings in South Africa's Anti-Money Laundering Legislation* 27.

81 De Koker *Money Laundering in South Africa* 5.

82 Williams *An Analysis of the Critical Shortcomings in South Africa's Anti-Money Laundering Legislation* 28.

83 De Koker *Money Laundering in South Africa* 5.

A person will act negligently when they fail to recognise or suspect a fact, which a reasonable person would have been reasonably expected to recognise or suspect.[84] The test for knowledge was set out in the case of *Frankel Pollak Vinderine Inc v Santon NO*[85] as:

> "Where a person has a real suspicion and deliberately refrains from making enquiries to determine whether it is harmless, where he or she sees red (perhaps amber) lights flashing but chooses to ignore them, it cannot be said that there is an absence of knowledge of what is suspected or warned against."[86]

A person who is convicted of money laundering in terms of section 4, 5 or 6 is liable to a fine of R100 million or to a period of imprisonment not exceeding 30 years.[87]

2 6 International Responses to Money Laundering

South Africa has ratified the UN Convention against Transnational Organised Crime[88] (UNCTOC or the Palermo Convention), United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances[89] (the Vienna Convention), the United Nations Convention against Corruption[90] (UNCAC or Merida Convention) as well as the African Union Convention on Preventing and Combating Corruption[91] (the AU Convention). Therefore, South Africa is required to adopt and implement these anti-money laundering standards into its national legislation.[92]

---

84 De Koker *Money Laundering in South Africa* 6.

85 2000 (1) SA 425 (W).

86 *Frankel Pollak Vinderine Inc v Santon NO* 2000 (1) SA 425 (W).

87 De Koker *Money Laundering in South Africa* 6.

88 UN General Assembly, *United Nations Convention against Transnational Organized Crime: resolution / adopted by the General Assembly*, 8 January 2001, A/RES/55/25, available at: http://www.refworld.org/docid/3b00f55b0.html [accessed 9 July 2018].

89 UN Economic and Social Council (ECOSOC), *United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances*, 19 December 1988, available at: http://www.refworld.org/docid/49997af90.html [accessed 9 July 2018].

90 UN General Assembly, *United Nations Convention Against Corruption*, 31 October 2003, A/58/422, available at: http://www.refworld.org/docid/4374b9524.html [accessed 9 July 2018].

91 African Union, *African Union Convention on Preventing and Combating Corruption*, 11 July 2003, available at: https://www.refworld.org/docid/493fe36a2.html [accessed 26 November 2018].

92 Hamman *The Impact of Anti-Money Laundering Legislation on the Legal Profession in South Africa* (Doctoral thesis, University of the Western Cape) 2015 33.

Article 3 of the Vienna Convention deals with money laundering and drug trafficking. It imposes an obligation on all member States to criminalise laundering the proceeds of the illegal drug trade.[93] The offence involves knowledge as a requirement in that the accused must know that the property in question had originated from illegal activity. Therefore, it is an offence if a person conceals the illegal source of the property in an attempt to avoid the law and is assisted by another person to do so.[94] The term "money laundering" is not expressly mentioned in the Vienna Convention, however it is the effect of money laundering which had been criminalised.[95]

Unlike the Vienna Convention, money laundering as an offence has been expressly included in the UNCTOC. The purpose of the UNCTOC is to promote the co-operation in order to prevent, as well as to combat transnational organised crimes. The UNCTOC created specific crimes which included: participation in organised crime groups, money laundering, corruption and obstruction of justice.[96]

State parties to the UNCTOC are compelled to co-operate in the tracking of persons who are suspected to be involved in money laundering, as well as tracing the benefits of the crime.[97] Article 7 stresses the importance of the "know-your-customer" (KYC) standard, as an effective tool to combat money laundering. In addition to this, the Convention creates an obligation to report any suspicious transactions.[98]

2 7 Conclusion

Money laundering is the process whereby criminals ensure that the proceeds of the crime appear legal. In doing so, the criminals will hide and conceal these illegal proceeds. Money laundering is a serious international problem as it is estimated that

---

93 Hamman *The Impact of Anti-Money Laundering Legislation on the Legal Profession in South Africa* 34.

94 *Ibid.*

95 Hamman *The Impact of Anti-Money Laundering Legislation on the Legal Profession in South Africa* 36.

96 Hamman *The Impact of Anti-Money Laundering Legislation on the Legal Profession in South Africa* 38.

97 Hamman *The Impact of Anti-Money Laundering Legislation on the Legal Profession in South Africa* 39.

98 *Ibid.*

billions are laundered every year.[99] As discussed above, the effects of money laundering are devastating and can seriously impair the development of a country as well as affecting the way in which foreign investors view such countries.

This chapter focused on the process, effects, as well as the national and international responses to money laundering. A lot can be done to fight against money laundering and it is clear that anti-money laundering legislation has already been put into place in South Africa. In addition to this, many governments have established anti-money laundering regimes with the aim of increasing awareness and to provide authorities with the necessary legal tools in order to combat money laundering.[100]

The tools which have already been set into place include: making money laundering a criminal offence, providing investigative agencies with the authority to trace, seize and to confiscate the criminal proceeds and to establish a necessary framework in order for agencies to exchange information.[101]

It is important that government listen to all the relevant authorities when developing a national anti-money laundering framework. Money launderers have been known to be imaginative when designing new ways to launder money and thereby circumventing the governments countermeasures. In today's day and age, money launderers have access to the most advanced technology. Therefore, it is critical that the national framework is to be adaptable and flexible enough in order to identify and respond to any new money laundering techniques.[102] Once anti-money laundering authorities identify the new money laundering schemes with a degree of success, there should be a decrease in crime as the money laundering will no longer hold value to the launderers.[103]

It becomes apparent that national government should work together with other jurisdictions to safeguard against launderers continuing to launder their money, simply

---

99 Ahlers *The South African Anti-Money Laundering Regulatory Framework Relevant to Politically Exposed Persons* (Master's Thesis, University of Pretoria) 2013 95.

100 Heymans *Money Laundering* 50.

101 *Ibid*

102 *Ibid.*

103 Van Jaarsveld *Aspects of Money Laundering in South African Law* 202.

by moving to another jurisdiction where money laundering may be tolerated due to weaker anti-money laundering laws.[104]

It is clear that South Africa's anti-money laundering framework is a relatively strong one. POCA was implemented to ensure that money laundering amounted to a crime. Furthermore, FICA was promulgated as a control measure to detect and to examine cases of money laundering. Therefore, an effective anti-money laundering framework is not only necessary, but it is also crucial in order for South Africa to combat money laundering.

104 Heymans *Money Laundering* 50.

CHAPTER 3: MONEY LAUNDERING USING CRYPTOCURRENCY

3 1 Introduction

As the saying goes: "there are two sides to every coin", particularly Bitcoin, having gained two popular opinions. Some are of the opinion that cryptocurrencies are the future of payment systems, allowing for fast and effective transactions between users. Others are of the opinion that cryptocurrencies provide criminals with a very powerful tool to store and move their illegal proceeds, while avoiding law enforcement agencies and other authorities.[105]

Digital payment methods are becoming increasingly popular amongst criminals to launder money, originally acquired through cybercrime.[106] The Internet relies heavily on financial institutions, functioning as a trusted third party, to process electronic payments.[107] Generally speaking, the system works well for most transactions. However, the trust-based model remains its inherent weakness. The inclusion of a third party means that completely non-reversible transactions are not always possible as the financial institutions cannot avoid mediating transactions. Therefore, the cost of mediation increases the cost of a transaction. Furthermore, the need for trust increases when there is a possibility of reversal.[108]

This led to the development of Bitcoin, an open source and peer-to-peer digital currency, which sought to eliminate the traditional trust-based model by removing any trusted central authority and introducing cryptography. By doing so, transactions are immediate, pseudo-anonymous and have low transaction fees.[109]

---

105 FATF "Virtual Currencies: Key Definitions and Potential AML/CFT Risks" (June 2014) http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf (accessed 2018-08-08) 3.

106 Van Wegberg, Oerlemans and Van Deventer "Bitcoin Money Laundering: Mixed Results? An Explorative Study on Money Laundering of Cybercrime Proceeds using Bitcoin" 2018 25 *Journal of Financial Crime* 419 419.

107 Nakamoto "Bitcoin: A Peer-to-Peer Electronic Cash System" 2009 *Cryptography Mailing List* 1 1.

108 Nakamoto 2009 *Cryptography Mailing List* 1.

109 Sarawat, Chauhan and Faujdar "Analysis on Crypto-Currency" 2017 9 *International Journal of Latest Trends in Engineering and Technology* 185 186.

Currently, fiat currency is the most dominant form of currency, with the use of cryptocurrency growing rapidly.[110] It goes without saying that technology develops at a rapid pace, a fact which criminals recognise and use in their favour in order to advance their laundering techniques.[111]

One such use is known as the Dark Web. The Dark Web is a part of the Internet which is not indexed by search engines and should only be accessed through the use of an anonymising browser or encryption software, such as Tor and a virtual private network (VPN),[112] to ensure anonymity. The Dark Web can be used for anything, from the purchase of usernames and passwords to hacking services and illegal porn.[113] As a result of its anonymous nature, Bitcoin is the main form of currency on the Dark Web. Due to the link between Bitcoin and illegal transactions on the Dark Web, countries have attempted to regulate Bitcoin in order to combat these concerns.[114]

3 2 Cryptocurrency

In order to understand the impact that the cryptocurrency system has had on the South African economy, it is first necessary to understand the cryptocurrency system, the concept of cryptocurrency, as well as the potential risks which may accompany these technological advancements.[115]

3 2 1 How Does Cryptocurrency Work?

Before one can understand the term “cryptocurrencies”, it is first necessary to discuss how the system works. Bitcoin would not exist without a whole network of users and

---

110 Sarawat *et al* 2017 *International Journal of Latest Trends in Engineering and Technology* 185.

111 Bryans “Bitcoin and Money Laundering: Mining for an Effective Solution” 2014 89 *Indiana Law Journal* 441 441.

112 A virtual private network is a technology which creates an encrypted and safe connection over a less secure network, such as the Internet; Burke “Virtual Private Network (VPN)” (September 2018) https://searchnetworking.techtarget.com/definition/virtual-private-network (accessed 2018-12-04).

113 Small “Bitcoin: The Napster of Currency” 2015 37 *Houston Journal of International Law* 582 582.

114 Small 2015 *Houston Journal of International Law* 582.

115 Ramracheya “The Dawn of our Tech-economy: An Introduction to Bitcoin and Cryptocurrency” 2017 *Without Prejudice* 32 32.

cryptography. Cryptography is a security measure which circumvents the need for trust, thereby keeping Bitcoin relatively safe with the use of keys.[116]

Bitcoins can either be mined or bought with fiat currency. In order to acquire Bitcoins, the user must first have a digital wallet.[117] This wallet contains both a public and private key. The public key is similar to that of an email address which users will send to each other in order to transfer Bitcoin. The private key can be described as a pin code for a debit card, which acts as a signature of the user. Furthermore, no other user will have access to the private key, nor can it be replicated. The private key is used to confirm the transfer of Bitcoins.[118]

Put differently, if the public key of a user works, then it is proof that the message was signed by the private key and it is something which the sender had intended to send. Unlike a signature or credit card number, the keys cannot be forged or faked by a scammer.[119] Bitcoin is said to be pseudo-anonymous as the transfers and public keys of the user are made public, however, the personal identities of such user are not disclosed.[120]

Each time there is a transfer of Bitcoins, the transaction is recorded on the blockchain. The blockchain is a public ledger which contains the history of each and every transaction of Bitcoin. In the blockchain, transactions are shared amongst multiple computers or servers, which are known as the member nodes in the network.[121] The ledger is decentralised, meaning that no person or entity controls or owns the data.[122] It is important to note that any attempt to change or manipulate the information in the blockchain can be traced back to the individual member node.[123]

Bitcoin mining has two main functions. Firstly, it creates new bitcoins and secondly, validates and confirms each transaction on the network. The second function is most

116 Small 2015 *Houston Journal of International Law* 588.
117 *Ibid.*
118 *Ibid.*
119 *Ibid.*
120 FATF http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf 6.
121 Small 2015 *Houston Journal of International Law* 589.
122 Ramracheya 2017 *Without Prejudice* 33.
123 *Ibid.*

important as it creates a tamper-proof system, which forms the basis of the blockchain. The process of mining is recorded in a ledger, which is a list of blocks making up the blockchain.[124] Put differently, users on the network are able to "mine" the cryptocurrency using algorithms in the form of mathematical equations in order to verify the transactions and to add these transactions on the digital ledger. This means that the cryptocurrency is essentially "unhackable" as well as preventing the problem of double spending.[125]

On average, a block is added to the chain every ten to twelve minutes, however, precise time is unpredictable as the process requires the computers to solve complex mathematical algorithms. Each time a miner's computer solves an algorithm, the miner will receive a reward of Bitcoins for contributing computing power.[126] The design of the algorithms is such, that they become increasingly difficult over time in order to ensure that the blockchain, as well as the Bitcoins, are not created too quickly.[127]

The blockchain is regularly updated and transferred by the use of the Internet to all users, hence the name given "peer-to-peer". The validity of the blockchain is secured through hashes. Hashes are the parts of each block in the blockchain, representing a mathematical link to the block directly before. Simply put, it chains the individual blocks together to create the blockchain.[128]

These individual hashes continue to build on one another to ensure that complete and constant control of the validity is possible. In order to ensure that a sender of Bitcoin is an authorised user, the software uses a formula to check the network users.[129] The transaction will be attached to the next block in the blockchain and will be credited to the recipient, only when the majority of the users on the network confirm the correctness of the transaction. This process is known as the proof-of-work. Only once the block has been added, a new mathematical problem will be generated to be

---

124 Hayes and Tasca "How Does Digital Currency Work?" in *Blockchain and Crypto-currencies* (2016) 217.

125 Ramracheya "The Dawn of our Tech-economy: An Introduction to Bitcoin and Cryptocurrency" 2017 *Without Prejudice* 32 33.

126 Small 2015 *Houston Journal of International Law* 589.

127 Small 2015 *Houston Journal of International Law* 590.

128 Omlor "Digitalization of Money and Currency Under German and EU Law" 2018 3 *TSAR* 613 615.

129 Omlor 2018 *TSAR* 615.

solved. If multiple people solve the mathematical problem roughly at the same time, the network will pick one to keep building upon. This then becomes the longest and most trusted chain.[130]

3 2 2 What is Cryptocurrency?

Simply put, cryptocurrencies refer to the mathematical-based, decentralised convertible virtual currency, which is protected by cryptography. Virtual currencies refer to the digital representation of value, which can be traded digitally. These currencies can function as a medium of exchange, units of account as well as a store of value, however, does not qualify as a legal tender within any jurisdiction.[131]

Therefore, cryptocurrency refers to the digital asset that forms the foundation of the peer-to-peer electronic cash system, which uses cryptography as a security measure. Cryptocurrencies are not illegal *per se* and are often used by consumers as a form of payment due to its highly secure nature as well as the fast transfer around the world, without incurring any third-party costs. Criminals exploit these benefits in order to further their legal acts, such as money laundering. With this in mind, it becomes obvious as to why criminals opt for cryptocurrency.[132]

3 2 3 How do Cryptocurrencies have Value?

Having regard to the above discussion, one cannot help but wonder how Bitcoin has any value. To understand this, it is necessary to look at the development and origin of money. Initially, there was the barter system where animals were exchanged for a service rendered. The number of animals depended on the amount of services rendered. Over time, people began using gold, as the exchange of livestock became inconvenient. When gold became widely accepted as a medium of exchange, it

130 *Ibid.*

131 FATF http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf 26.

132 De Mink "Dangers Inherent in Bitcoin and Other Cryptocurrencies" 2018 33 *De Rebus.*

became currency. Gold originally got its value due to the vast amount of time spent, as well as the amount of resources used to try to mine it.[133]

The same mining concept applies to Bitcoin. Users spend time and resources to build and maintain a transaction system and get compensated with Bitcoin. However, the value of a good is determined for the desire for it. Even though time and resources are spent on an object, which may prove to be useful, it does not necessarily mean that such object holds any value.[134]

As with all finite resources, the number of Bitcoins will eventually run out, as only 21 million Bitcoins will be produced. Similar to the mining in the real world, the last few Bitcoins will be the most difficult and expensive to mine[135]

3 2 4 Inherent Dangers of Cryptocurrencies

Although cryptocurrencies are used for both legitimate and illegal means, it clearly poses a number of inherent dangers. These include risks such as the ease of process. This is due to the fact that the traditional stages of money laundering can now be merged easily into one another with the help of information technology. During the placement stage, the cryptocurrencies are able to be sent anonymously and directly to a recipient without any need of identification or monitoring of transaction amounts.[136]

One of the mechanisms used to combat traditional money laundering, is one which has proved to be an effective tool, known as "know your customer" policy (KYC).[137] The KYC policy aims to adequately identify the consumers of financial institutions, by requiring legal identification, residency information as well as a valid photograph.[138] However, Bitcoin is known for its high degree of anonymity as the only aspect which

---

133 Zhang "Why Does Bitcoin Have Any Value?" (25 November 2017) https://medium.com/@zmeric5/why-does-bitcoin-has-any-value-520bdc012d46 (assessed 2018-08-07).

134 Zhang https://medium.com/@zmeric5/why-does-bitcoin-has-any-value-520bdc012d46 .

135 Nieman "A Few South African Cents' Worth on Bitcoin" 2015 18 *PER* 1979 1987.

136 De Mink "Dangers Inherent in Bitcoin and Other Cryptocurrencies" 2018 33 *De Rebus.*

137 Bååth *How to Combat Money Laundering in Bitcoin?* (Published thesis, Linköpings Universitet) 2016 2.

138 Bååth *How to Combat Money Laundering in Bitcoin?* 7.

identifies the Bitcoin user is their public key. No other personal information of the user is disclosed. This was to ensure a great level of protection against identity theft, however, criminals use this mechanism in their favour to circumvent the traditional anti-money laundering mechanisms, such as the KYC policy.[139]

As a result of Bitcoin's decentralised nature, transactions can be made directly to users without the need of a third-party intermediary. This means that the cryptocurrency-based payment system may operate or may be located in any jurisdiction with weak anti-money laundering frameworks.[140] The aim of the traditional anti-money laundering directive was to monitor the intermediaries, however, the lack of intermediaries in the Bitcoin network makes this traditional approach impossible to apply. This poses the risk that criminals may intentionally seek jurisdictions with inadequate anti-money laundering mechanisms. Thereby enhancing their ability to launder their money or provide a money laundering service to other users.[141]

Another inherent danger of cryptocurrencies is that transfers can be made across national borders without government interference. Transfers take place at high speeds and sometimes instantaneously, meaning that even if a transaction is detected, such proceeds of the illegal activity are difficult to confiscate.[142] Furthermore, Bitcoin transfers are irreversible. Therefore, it becomes almost impossible to recover illegal proceeds once the transfer has been recorded.[143]

The lack of transactional record keeping is yet another risk of Bitcoin. During an ordinary money laundering investigation, the method used would be to follow the money trail. With Bitcoin, all transactions made are made public, however, such transactions are only published in computer code. The problem comes in when law enforcement attempts to make a connection between the public key and the user

139 Bååth *How to Combat Money Laundering in Bitcoin?* 10.
140 De Mink "Dangers Inherent in Bitcoin and Other Cryptocurrencies" 2018 33 *De Rebus.*
141 *Ibid.*
142 *Ibid.*
143 *Ibid.*

behind it.[144] Therefore, it becomes difficult to trace back the identities of such individuals without their co-operation.[145]

Lastly, are the jurisdictional issues which arise due to the fact that there is no internationally accepted regulation or framework regarding cryptocurrency. This means that each jurisdiction is left with the cumbersome task of attempting to regulate cryptocurrencies. However, as discussed above, this becomes a difficult task when such transactions can be made directly to another user anywhere in the world. According to the FATF report on virtual currencies,[146] records linking identification and transactions of users may be kept by different entities within any jurisdiction. Therefore, access by law enforcement agencies and regulators may be hampered or limited in this regard.[147]

3 3 Money Laundering using Cryptocurrency

It is clear from the above discussion that Bitcoin is vastly different from any other traditional type of currency, which is presently regulated by law. Although it is apparent that Bitcoin has its advantages, recent developments have shown that Bitcoin has played a large role in illegal activities, such as money laundering.[148] Due to the decentralized nature of Bitcoin, users remain pseudonymous. Although every transaction is available and tracible on the public ledger, it is not connected to any user's personal identity.[149]

For the general public, anonymous browsing has been made available using the Tor-browser, otherwise known as the Onion Router. By routing the internet traffic to multiple Tor nodes, the network traffic is encrypted. Thereby rendering the users IP-

144 Brown "Cryptocurrency and Criminality: The Bitcoin Opportunity" 2016 89 *Police Journal: Theory, Practice and Principles* 327 333.
145 De Mink "Dangers Inherent in Bitcoin and Other Cryptocurrencies" 2018 33 *De Rebus.*
146 FATF http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf 6.
147 De Mink "Dangers Inherent in Bitcoin and Other Cryptocurrencies" 2018 33 *De Rebus.*
148 Troeller "Developments in Banking Law" 2017 36 *Review of Banking & Financial Law* 159 159.
149 Troeller 2017 *Review of Banking & Financial Law* 162.

address[150] untraceable and unidentifiable. Put differently, it allows Tor users to browse the Internet without disclosing the originating IP-address. This system allows the user to browse the Dark Web, while remaining anonymous.[151]

The anonymous nature of Bitcoin makes it an attractive form of currency for a criminal, but for one disadvantage to criminals. The blockchain is a public ledger which makes all previous transactions and Bitcoin addresses available to all users, which is favourable to the law enforcement authorities. As a result of the blockchain design, the Bitcoin transactions are linked to one another. Simply put, each input is inevitably an output of a previous transaction.[152]

For cybercriminals, this poses a risk as their transactions are linked and may be traced back to the illegal source. The Dark Web offers services to anonymise Bitcoin even further in order to assist in Bitcoin laundering. There are two aspects of Bitcoin laundering. Firstly, there is Bitcoin mixers or tumblers,[153] a service which intends to disconnect the Bitcoin from its illegal source. Secondly, there is Bitcoin exchanges, a service which attempt to anonymously exchange Bitcoin into actual money.[154]

Mixing services break the money trail of Bitcoin transactions. In terms of this, the customer is given a newly generated Bitcoin address in order to make a deposit. Once a mixing fee has been deducted, the mixing service pays out Bitcoins from its reserve to the address which is provided by the customer. In order to ensure a higher level of anonymity, the pay-outs are spread out over time as well as introducing an aspect of unpredictability in the division of amounts.[155]

To clarify, a mixer is a type of anonymiser disguising the chain of transactions in the blockchain by connecting all the transactions in the same Bitcoin address and sending these transactions together, in such a way, that it appears to have been sent from another address. The mixer sends the transactions through a complex series of fake

---

150 An Internet Protocol address is a unique string of numbers which identifies each computer within a network.
151 Van Wegberg *et al* 2018 *Journal of Financial Crime* 421.
152 Van Wegberg *et al* 2018 *Journal of Financial Crime* 423.
153 Van Wegberg *et al* 2018 *Journal of Financial Crime* 420.
154 *Ibid.*
155 Van Wegberg *et al* 2018 *Journal of Financial Crime* 423.

transactions, thereby making it difficult to connect the coins with a specific transaction.[156]

Once the Bitcoin mixing has taken place, it becomes almost impossible to trace it back to the illegal source. In other words, there will be no connection between the Bitcoins which have been deposited and those which have been received.[157] Thereafter, the consumer is given a returning customer number. The purpose of this number is to ensure that a returning customer is not accidently paid out the same previously tainted Bitcoins from the mixers reserve.[158]

The exchange services are used once the Bitcoin has been successfully mixed. In terms of this, a supplier agrees to receive Bitcoin in exchange for any currency. Thereby allowing users to buy and sell Bitcoin online. Output platforms such as Luno[159] are used to ensure that the exchanged currency ends up in the possession of the user.[160] Generally, these output platforms require a valid and active account in order to be used as a cash-out strategy. This provides an added layer of protection to identify and trace suspected criminal activity and identify the user.[161] However, these accounts are available to be purchased on the Dark Web, thereby erasing any connection to the criminal.[162]

Criminals can either use the exchange services available on the Dark Web or an exchange through a Bitcoin ATM, provided that the amounts are low enough as not to raise any suspicion and trigger the requirement of identification verification.[163] It is submitted that in some cases personal or banking information is not required in order

---

156 FATF http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf 6.

157 Van Wegberg *et al* 2018 *Journal of Financial Crime* 423.

158 Van Wegberg *et al* 2018 *Journal of Financial Crime* 424.

159 Luno is a bitcoin related company, with its headquarters in the UK. It facilitates Bitcoin storage and transactions, including buying, selling and paying through the Bitcoin wallet services. It also operates exchanges between fiat currencies and Bitcoin.

160 Van Wegberg *et al* 2018 *Journal of Financial Crime* 429; Luno "About Luno" (undated) https://www.luno.com/en/about (accessed 2018-11-27).

161 Hyman "Bitcoin ATM: A Criminal's Laundromat for Cleaning Money" 2015 27 *St. Thomas Law Review* 296 303.

162 Van Wegberg *et al* 2018 *Journal of Financial Crime* 429.

163 Gruber "Trust, Identity, and Disclosure: Are Bitcoin Exchanges the Next Virtual Havens for Money Laundering and Tax Evasion?" 2013 32 *Quinnipiac Law Review* 135 139.

to complete a transaction at a Bitcoin ATM.[164] In addition to this, Bitcoin users now have the option to buy and sell Bitcoin in person using cash. Some Bitcoin users even use pre-paid or gift cards to launder their money. This is because certain websites allow users to convert Bitcoin for cash.[165]

A well-known platform, providing for various exchange service, was Silk Road[166] which operated with Bitcoin. It was a platform used by criminals to launder their money. A user could acquire an account anonymously by using a fake name. Thereafter, such a user could participate in an illegal transaction and exchange the Bitcoins obtained from the transaction for "clean" fiat currency.[167] The US Department of Justice had shut down Silk Road, however, it was just days later that Silk Road 2.0 was launched. This is a typical example that, without a proper legal framework in place, there will always be a demand for these types of platforms.[168]

3 4 Conclusion

This chapter discussed the concept of cryptocurrency, how it works as well as its inherent dangers. The chapter focussed on one inherent danger in particular, namely money laundering using cryptocurrencies. It became clear from the above discussion that the Dark Web was utilised as the provider for mixing and exchange services.

The use of cryptocurrencies has experienced a rapid growth over the past number of years. As technology develops, laws and regulations should be regularly updated in order to effectively regulate these new developments. Bitcoin is popular as it has a number of benefits including being unhackable, having low transaction costs, as well as being a safe and fast payment method. Bitcoin is also decentralised, meaning that it is not attached to a state or government and there is no regulatory body or central issuing authority.

---

164 Hyman 2015 *St. Thomas Law Review* 304.
165 Brown 2016 *Police Journal: Theory, Practice and Principles* 333.
166 Silk Road was the first modern Dark Web market. It was best known for selling illegal drugs.
167 Mothokoa *Regulating Crypto-Currencies in South Africa: The Need for an Effective Legal Framework to Mitigate the Associated Risks* (Masters Mini-dissertation, University of Pretoria) 2017 27.
168 Mothokoa *Regulating Crypto-Currencies in South Africa* 28.

However, Bitcoin has its fair share of risks and dangers. One main disadvantage to Bitcoin is that it simplifies the money laundering process. It is submitted that Bitcoin does not create a new crime but rather can be seen as a virtual version of the traditional money laundering process. Therefore, it may be difficult to apply the traditional anti-money laundering mechanisms, such as the KYC policy, monitoring intermediaries and following the paper trail. This is due to the fact that the true identity of a user is never fully known.

There is no doubt that Bitcoin can be categorised as a disruptive financial technology, in which many anti-money laundering laws are not prepared to deal with. Virtual currencies have broken the norm on physical paper currencies, yet there has been no universal standard or regulation in this regard. This does not mean that cryptocurrencies should be deemed illegal or should be heavily regulated in order to offset the initial lack of oversight.[169] However, the failure to regulate cryptocurrencies may lead to consequences such as money laundering. The regulation of cryptocurrencies is to be discussed, in detail, in the next chapter.

169 Bryans 2014 *Indiana Law Journal* 472.

CHAPTER 4: REGULATION OF CRYPTOCURRENCY

4 1 Introduction

The Internet provides a perfect opportunity to defraud those who are unfamiliar with technology.[170] It is a facilitator, meaning that it does not create any new schemes to launder money, which does not already exist. However, the Internet does provide more opportunities to the user, to lauder their money. Thereby making money laundering easier and faster for the user.[171]

The largest problem with the Internet is that users are able to remain anonymous. For some, this may be seen as a blessing, for others a curse. Although some users may disclose a name, the true identity of the user is not known. Thus, it becomes clear to see that regulation of the Internet will not stop its abuse. This is due to the fact that national laws only apply to a particular jurisdiction, however, the Internet has no boundaries and therefore has no jurisdiction.[172]

It is submitted that general opinion of Bitcoin, is that it is unregulated. However, it is unclear as to which aspect is being referred to in this regard, as it could mean that the peer-to-peer network, technology or individual is unregulated. It may be more accurate to say that the peer-to-peer network and technology are unregulated. In fact, these two aspects cannot be regulated. This is due to the peer-to-peer network being decentralised. Therefore, saying Bitcoin itself is unregulated, is incorrect. Furthermore, it is important to note that Bitcoin is a set of rules which regulate the decentralised digital currency, while the peer-to-peer network ensures that these rules are enforced. Therefore, the Bitcoin network is self-regulated.[173]

It is submitted that a typical reaction when one hears that Bitcoin is unregulated, is to assume that government has not yet taken any action to regulate the digital

---

170 Morris-Cotterill "Use and Abuse of the Internet in Fraud and Money Laundering" 1999 13 *International Review of Law Computers & Technology* 211 211.
171 Morris-Cotterill 1999 *International Review of Law Computers & Technology* 219.
172 Morris-Cotterill 1999 *International Review of Law Computers & Technology* 218.
173 Hoegner *The Law of Bitcoin* (2015) 2.

currency.[174] However, this is not the case. Although the cryptocurrency is not expressly mentioned in law or regulation, the use of such new technology may be covered by existing laws.[175] In fact, regulation may occur without any laws. It is submitted that Bitcoin is already well regulated, not by laws set in place by legislatures, banks or payment processors, but by the mathematical algorithms and consensus of the users in the globally accessible system. Furthermore, should a user in the Bitcoin network not follow the rules and regulations, programmed by the network, they are identified as irrelevant and easily ignored by other users.[176] Therefore, it is submitted that it would be more accurate to say that Bitcoin is unregulated by laws and frameworks in the majority of jurisdictions.

4 2 International Regulations

Some countries have been successful in incorporating cryptocurrencies into their existing national laws. Therefore, in some jurisdiction's cryptocurrencies are to some extent regulated.[177] What is to follow is a discussion on the legislative instruments which have been put into place by Canada, US and EU in order to regulate cryptocurrency.

4 2 1 Canada

It is noteworthy that Canada was the first country to pass a law aimed at regulating cryptocurrencies. In terms of Canadian law, the anti-money laundering legislation is mainly found in the Criminal Code,[178] Proceeds of Crime and Terrorist Financing Act (PCA)[179] as well as the Proceeds of Crime and Terrorist Financing Regulations (PCA Regulations).[180]

---

174 Hoegner *The Law of Bitcoin* 2.
175 Hoegner *The Law of Bitcoin* 3.
176 Gruber 2013 *Quinnipiac Law Review* 185.
177 Mothokoa *Regulating Crypto-Currencies in South Africa* 43.
178 *Canada: Criminal Code* [Canada], C-46, 1985, available at: http://www.refworld.org/docid/4cf52bb32.html [accessed 13 August 2018].
179 *Canada: Proceeds of Crime (Money Laundering) and Terrorist Financing Act* [Canada], S.C. 2000, c. 17, 29 June 2000, available at: http://www.refworld.org/docid/5417f4a44.html [accessed 13 August 2018].
180 Mothokoa *Regulating Crypto-Currencies in South Africa* 44.

In terms of the Criminal Code, the definition of money laundering includes money laundering using cryptocurrencies. In terms of the definition, there must be an intention to launder the proceeds. In addition to this, the person must have been aware that the cryptocurrency was illegally obtained.[181]

The PCA had established the Financial Transactions and Reports Analysis of Canada (FinTRAC). FinTRAC analyses financial transaction reports and ensures compliance with both the PCA as well as the PCA Regulations in order to prevent money laundering and terrorist financing. Money Services Businesses (MSBs) are required to register and report to FinTRAC, keep records and acquire information about their customers.[182] The definition of MSB now includes entities which transact in virtual currencies. Following this, cryptocurrency businesses and exchanges must comply with the MSB requirements as provided for by the PCA.[183]

This means that exchanges are now required to register with FinTRAC as well as to disclose information regarding their operations. As discussed above, not all exchange services operate a legal business. Therefore, it is submitted that by disclosing the relevant information to FinTRAC, it would reduce the number of illegal exchanges. In addition to this, exchanges must comply with the PCA Regulations by keeping records, verifying the identity of the consumer, report transactions which raise suspicion as well as to protect the financial system. This disposes of the anonymity feature of cryptocurrencies as the identities of users, wishing to launder their money, will no longer be hidden.[184]

4 2 2 The United States of America

In 2017 the Uniform Law Commission (ULC) had concluded legislation, which regulated cryptocurrencies. The Bank Secrecy Act (BSA)[185] regulates financial institutions and applies to all entities which are categorised as MSBs. The BSA

181 *Ibid.*
182 *Ibid.*
183 Mothokoa *Regulating Crypto-Currencies in South Africa* 45.
184 *Ibid.*
185 Financial Recordkeeping and Reporting of Currency and Foreign Transactions Act of 1970 (31 U.S.C. 5311 et seq.).

requires these financial institutions to put record keeping instruments in place as well as authorising the Financial Crimes Enforcement Network (FinCEN) to combat money laundering. FinCEN requires MSBs to report any suspicious activity, to keep records and report currency transactions.[186] Furthermore, FinCEN published guidelines stating that persons who acquire and use cryptocurrencies as a payment method, do not fall under the definition of MSBs. However, exchanges and administrators of cryptocurrencies are classified as MSBs due to the fact that they are transmitting money.[187]

In addition to this, FinCEN clarified the positions of miners and the software used in cryptocurrency. Miners are classified as users and therefore do not fall within the definition of MSBs and need not be registered as such. Businesses which created and distributed cryptocurrency software, which facilitated the sale of cryptocurrencies, were also excluded from the definition of MSBs.[188]

Furthermore, the new Uniform Regulation of Virtual Currency Businesses Act[189] requires businesses operating with cryptocurrencies to comply with anti-money laundering rules. Businesses or exchanges which deal with cryptocurrencies are to create and maintain policies and procedures in an attempt to prevent money laundering. These policies must identify, as well as to assess the material risks of the cryptocurrency business. [190]

One could also apply the FinCEN approach to mixers, which include mixers into the definition of exchanges. This is because mixers are businesses which exchange virtual currency for another virtual currency. Mixers are required to be registered with FinCEN. Failure to do so makes it an unlicensed MSB, which is subject to a fine or imprisonment. In theory, this approach should work. However, there are a number of factors which make these mixer regulations impossible.[191] This is due to the fact that the mixer makes it difficult to trace the Bitcoin transaction history. Furthermore, it

---

186 Mothokoa *Regulating Crypto-Currencies in South Africa* 48.
187 Mothokoa *Regulating Crypto-Currencies in South Africa* 49.
188 *Ibid.*
189 Uniform Regulation of Virtual Currency Business Act of 2017.
190 Mothokoa *Regulating Crypto-Currencies in South Africa* 50.
191 Singh "The New Wild West: Preventing Money Laundering in the Bitcoin Network" 2015 13 *Northwestern Journal of Technology and Intellectual Property* 37 62.

comes as no surprise that many mixers use Tor, which makes tracing the owner of the mixing service an impossible task. Mixers, together with the use of Tor, handle Bitcoins in their virtual operations. This makes enforcement impossible as the conduct of a mixer stays online and never leaves the Bitcoin network.[192]

However, it has been argued that the battle is not lost. The same tool used by criminals to remain anonymous may be used by law enforcements. Many argue that law enforcements will find a way to determine the identities of mixer owners by using Tor, as seen in Silk Road. However, the Silk Road case is by no means a yardstick to determine the identities of mixer owners, as the owner of Silk Road had made numerous errors which individuals today will be sure to avoid.[193] Therefore, to use the same method utilised in Silk Road means that law enforcements would be relying solely on the hope that mixer owners would make similar mistakes.[194]

With this being said, one cannot say that Tor will forever be out of the reach of law enforcement. There are many agencies which are attempting to develop methods for tracking transactions. It may be possible that in the future, government agencies will devise a similar strategy. As for now, these possibilities are just hopeful solutions. Furthermore, the application of law as it stands is powerless against these secretive organisations. Therefore, legislatures should focus less on these organisations and more on regulating the Bitcoin exchanges and businesses.[195]

4 2 3 The European Union

In 2016 the European Commission had presented a legislative proposal to amend the 4th Anti-Money Laundering Directive. The aim was to incorporate cryptocurrency wallet providers and exchanges into the EU's anti-money laundering framework, with the primary focus of combatting money laundering and financing terrorists.[196] In April 2018 the European Parliament adopted the text in plenary session.

---

192 Singh 2015 *Northwestern Journal of Technology and Intellectual Property* 62.
193 *Ibid.*
194 Singh 2015 *Northwestern Journal of Technology and Intellectual Property* 63.
195 *Ibid.*
196 Mothokoa *Regulating Crypto-Currencies in South Africa* 52.

Initially, the Financial Intelligence Units (FIUs) were allowed to access information, only after a suspicious transaction had occurred. However, the new legislation provides that such information be available, on request, to the FIUs. This means that a request for information may be made before a suspicious transaction occurs. It is submitted that the faster the FIUs are able to acquire the information, the faster they will be able to identify suspicious transactions which may be connected to money laundering.[197]

The new legislation, otherwise known as the 5th Anti-Money Laundering Directive, covers two types of cryptocurrency businesses, namely the exchanges and wallet services. Under the new legislation, these businesses will become obliged entities, which is similar to the traditional financial institutions. These businesses are obliged to adopt measures in order to combat money laundering and financing terrorism.[198]

These measures include the adoption of the KYC policy, monitoring transactions, reporting any suspicious transactions and maintaining comprehensive records. It is submitted that in the EU majority of cryptocurrency businesses have already adopted these control measures. The new legislation merely formalises the requirements in order to safeguard against the operation of any illegal businesses.[199]

4 3 Cryptocurrency and the Current Anti-Money Laundering Framework within South Africa

It is clear from the above discussion that some jurisdictions have taken steps in order to regulate cryptocurrencies in an effort to combat money laundering. However, South Africa has not been so quick to enact such regulations.

The SARB has stated its intention to investigate the possibility of the blockchain and has expressed its concerns with the risks involving cryptocurrencies.[200] As the current

197 Mothokoa *Regulating Crypto-Currencies in South Africa* 53.
198 Robinson "5th AML Directive: EU Regulation Of Cryptocurrency Businesses" (1 May 2018) https://www.elliptic.co/our-thinking/5th-aml-directive-eu-regulation-cryptocurrency (accessed 2018-08-17).
199 Robinson https://www.elliptic.co/our-thinking/5th-aml-directive-eu-regulation-cryptocurrency .
200 Ramracheya 2017 *Without Prejudice* 33.

position stands, South Africa does not regard cryptocurrencies as a legal tender, however, cryptocurrencies may be used.[201] Given the fact that cryptocurrencies are not regulated by a central authority, such as a bank, it fails to meet the definition of a legal tender as provided by the South African Reserve Bank Act.[202] This means that any supplier may refuse cryptocurrencies as a form of payment, without being in breach of the law. This was confirmed by the National Treasury, who warned users that there are currently no laws or regulations which address cryptocurrencies. As a result, users have no legal protection or remedies available to them.[203]

The risk-based approach applied to the anti-money laundering framework by the FATF and EU emphasised the importance of identifying money laundering risks associated with payment mechanisms, such as cryptocurrencies. One of these risks, are due to the high degree of anonymity of cryptocurrencies and their ability to bypass anti-money laundering systems. Although these risks are apparent, South Africa has failed to take steps to combat the risks.[204]

In general, the legal framework regarding the financial sector is comprehensive and has kept up with the international standards. Moreover, South Africa has been regarded as a jurisdiction with relatively strong anti-money laundering laws. However, the same cannot be said for the regulation of cryptocurrencies, which can be used for money laundering.[205]

Compared to other jurisdictions, South Africa has not been completely ignorant on the matter of cryptocurrencies. The SARB's Position Paper on Virtual Currencies, released in 2014, seemed promising on the regulation of cryptocurrencies. However, the Position Paper merely confirms the lack of legal and regulatory framework on cryptocurrencies. SARB emphasises that it does not regulate, supervise or oversee the cryptocurrencies network. Therefore, any transaction or activity relating to cryptocurrency is entirely at the risk of the user and will have no recourse to SARB.[206]

---

201 *Ibid.*
202 90 of 1989.
203 National Treasury "Unregulated in South Africa" in *User Alert: Monitoring of Virtual Currencies* (2014) 2.
204 Mothokoa *Regulating Crypto-Currencies in South Africa* 39.
205 *Ibid.*
206 Nieman "A Few South African Cents' Worth on Bitcoin" 2015 18 *PER* 1979 1988.

Furthermore, SARB recognised that there was no substantial risk to the financial stability relating to virtual currencies at the time. However, SARB had reserved the right to change this view as market developments change. Due to the fact that cryptocurrencies are not defined as a payment instrument or financial product, cryptocurrencies also fall outside the ambit of regulation by the Prudential Authority, forming part of SARB, and the Financial Sector Conduct Authority.[207]

It is submitted that one cannot help but wonder why a country, such as South Africa, with such strong anti-money laundering regulations and frameworks has not yet effectively attempted to regulate the issue of cryptocurrencies and the danger of money laundering attached thereto. There is no doubt that cryptocurrencies are growing at a rapid pace and it becomes evident that if South Africa does not wish to have a gap in its anti-money laundering framework, it should take all necessary steps to regulate cryptocurrencies.

Jurisdictions need to ensure effective financial regulation in order for there to be harmony between the economy and the financial sector. As cryptocurrencies have an impact on the economy, it is advisable that South Africa regulate it.[208] Due to the fact that South Africa's current anti-money laundering legislation is relatively comprehensive, it is submitted that it is not necessary to promulgate a single Act regulating cryptocurrencies but rather to follow the approach taken by Canada to amend existing legislation to include cryptocurrencies.

South Africa has been criticised for adopting the "wait and see" approach, as central banks have only published notices and disclaimers which state that users hold cryptocurrencies at their own risk. This is not an effective method to combat money laundering using cryptocurrencies. It is submitted that regulators must be actively involved with cryptocurrencies to understand how cryptocurrencies work, in order to be able to effectively regulate it.[209]

---

207 FinTech "Private Cryptocurrencies" in *Intergovernmental FinTech Working Group* (2018) 8.

208 Mothokoa *Regulating Crypto-Currencies in South Africa* 55.

209 Motelle "The Race of Innovation in Financial Services and the Regulatory Chase: Some Thoughts on the Regulation of Crypto-Currencies" 2017 3 *Development Finance Agenda* 8 9.

Due to the decentralised nature of Bitcoin, there is no central organisation upon which money laundering regulations may be imposed.[210] From a regulatory perspective, anti-money laundering laws currently in place in South Africa, cannot be used. Consequently, the current framework is based on the assumption that there is a central authority or business which can impose obligations.[211] Therefore, it becomes clear to see why current anti-money laundering frameworks need to be developed to include cryptocurrencies, as the current approach is not a viable option to combat money laundering using cryptocurrencies.

Currently, the anti-money laundering framework for traditional money laundering techniques is strong. However, it is weak for money laundering using cryptocurrencies. This is due to the failure to amend existing legislation. The existing legislation does not define cryptocurrencies, nor does it provide any regulation for businesses which trade in cryptocurrencies. In addition to this, there is no mention of miners or users.

To compare this with the Canadian position, the existing legislation was amended to include cryptocurrencies as well as to authorise the FinTRAC to ensure compliance with the existing legislation, by applying the KYC policy to businesses transacting in cryptocurrency and exchanges. The US and EU applied different approaches by promulgating separate legislation to regulate cryptocurrencies, as well as clarifying the position of users and businesses who transact with cryptocurrencies.

In 2017, the South African government began working with a blockchain-based solutions provider, Bankymoon, to create a balanced approach for the cryptocurrency regulation.[212] Furthermore, the SARB released a media statement in February 2018 which established the Financial Technology (FinTech) programme. The first goal of FinTech would be reviewing the position of the SARB regarding cryptocurrencies and to inform an appropriate policy and regulation framework.[213] Although this can be seen as a step in the positive direction, no legislative instruments have been enacted as

---

210 Stokes "Virtual Money Laundering: The Case of Bitcoin and the Linden Dollar" 2012 21 *Information & Communications Technology Law* 221 230.

211 Stokes 2012 *Information & Communications Technology Law* 230.

212 Nelson "Cryptocurrency Regulation in 2018: Where the World Stands Right Now" (1 February 2018) https://bitcoinmagazine.com/articles/cryptocurrency-regulation-2018-where-world-stands-right-now/ (accessed 2018-08-08).

213 Retief "Accounting for Cryptocurrency" 2018 *Business & Economy* 10 11.

yet, in order to regulate cryptocurrencies in an attempt to combat money laundering. It is submitted that one can only remain hopeful that the establishment of FinTech will be the first of many steps in the regulation of cryptocurrencies.[214]

There is still uncertainty concerning the regulations and enforcement of cryptocurrencies. Therefore, it becomes helpful to carefully consider the current legal framework, with particular reference to its purpose, which may provide some guidelines in regulating cryptocurrencies. This includes FICA, as well as anti-money laundering legislation and KYC policy.[215]

4 3 1 Challenges of Cryptocurrency Regulation

Due to the complex and decentralised nature of Bitcoin, regulation becomes challenging. The most effective approach is to analyse each Bitcoin transaction entity individually and determine an appropriate and effective way to regulate it, as opposed to regulating the Bitcoin network as a whole. These entities include: sender, launderer, miner, Bitcoin development team and currency exchanges.[216]

Due to the pseudonymous nature of the sender's identity in the Bitcoin network, attempting to regulate the sender will be unrealistic. When transactions take place, no personal information is exchanged between users. Therefore, it is not likely that one would be able to identify the Bitcoin user. It is submitted that by attempting to regulate this, a greater distrust and dissatisfaction towards government is likely to arise. Furthermore, this could lead to increased anonymisation. The similar result may arise in regulating receivers or launderers. Thus, if no personal information is given in order to link the crime to the user, law enforcement will dedicate a large amount of time and resources attempting to trace the user. Furthermore, the reward of such efforts may be relatively small.[217]

---

214 *Ibid.*

215 Bothma "Bitcoin, Blockchain, Cryptocurrencies and ICO's: Legal Enigmas for Start-up's Operating on the Future Frontier" (undated) https://dommisseattorneys.co.za/blog/bitcoin-blockchain-cryptocurrencies-icos-legal-enigmas-start-ups-operating-future-frontier/ (accessed 2018-09-15).

216 Bryans 2014 *Indiana Law Journal* 469.

217 Bryans 2014 *Indiana Law Journal* 470.

Moreover, the regulation of Bitcoin miners would also prove difficult. Essentially, miners replace the position of the payment processor. However, the miner is still a user on the network and the same problem, as above, arises with users being anonymous. Furthermore, it is the mining software which processes the transaction without user involvement. Thus, it would seem illogical to regulate miners when it is the miner's software which processes Bitcoin transactions.[218]

It has been argued that regulating the Bitcoin development team or requiring them to change the software in order to monitor transactions as well as to de-anonymise transfers, would be an effective solution. However, this fails to recognise the fact that Bitcoin is an open-source software that is developed generally by the network. Putting a stop to the development team would not stop the distribution of code, as it does not operate as a central authority that controls the operation of the network. Thus, it is submitted, that regulating the development team would have little to no effect in lessening the illegal activity which may occur through Bitcoin.[219]

Lastly, is the regulation of Bitcoin currency exchanges. Exchanges generally deal with fiat currencies, which is likely to be regulated by money exchange laws. Furthermore, if an exchange is not trustworthy, completing the stages of money laundering becomes increasingly difficult without attracting attention of the authorities. Thus, exchanges are less decentralised and are easier entities to regulate.[220]

Luno, together with IceCubed are two well established Bitcoin exchanges in South Africa. Although there are no regulations currently in place within South Africa, exchanges such as Luno, has stated that it is committed to implementing and maintaining a high standard of KYC and anti-money laundering compliance, by way of a risk-based approach. This is to assist in the detection, prevention and reporting of any money laundering activities. Luno implements the KYC policy by requiring the user to submit evidence of their identity. Thereafter, use effective procedures to verify the authenticity of the information. Put differently, Luno implements procedures for customer identification, record keeping, retention of transaction documents as well as

218 *Ibid.*
219 Bryans 2014 *Indiana Law Journal* 471.
220 Bryans 2014 *Indiana Law Journal* 472.

reporting suspicious transactions. Furthermore, Luno does not provide services when there is good reason to believe that such transactions are associated with money laundering.[221] This illustrates that exchanges can be effectively regulated.

A different approach is to regulate cryptocurrencies out of existence, which has been an approach in many jurisdictions. This approach is supported by the view that Bitcoin is primarily used by criminals and should be banned in order to prevent it from being used for illegal purposes.[222] Bitcoin has been criticised as it does not provide any beneficial use, therefore its eradication is justified. However, it is submitted that this is not the case. [223]

Bitcoin has many advantages and benefits, which many countries recognise and therefore attempt to regulate. Attempting to eliminate Bitcoin may be an impossible task as Bitcoin users can remain anonymous by using Tor, to prevent having their public keys traced back to their personal identities. This means that the criminals will continue to operate despite government regulations. It is submitted that this approach will only eradicate the legitimate uses of Bitcoin, thereby leaving the criminals unaffected.[224]

Thus, it has been submitted that a balanced approach be implemented in this regard. By recognising that Bitcoin has beneficial uses, legislatures should adopt legislation which regulates this use as well as attempt to prevent money laundering. However, legislatures should bear in mind the harsh reality that is the Dark Web and understand that at a certain point, such regulations will not be affective against those users who remain anonymous.[225]

The anonymity poses a number of challenges for law enforcement, however, money laundering using Bitcoin will eventually come out of the virtual network. This occurs when the user converts his Bitcoins to fiat currency, using a Bitcoin exchange. This is

---

221 Luno https://www.luno.com/en/legal/compliance .

222 Singh "The New Wild West: Preventing Money Laundering in the Bitcoin Network" 2015 13 *Northwestern Journal of Technology and Intellectual Property* 37 49.

223 Singh 2015 *Northwestern Journal of Technology and Intellectual Property* 49.

224 *Ibid.*

225 *Ibid.*

where the abovementioned jurisdictions regulate Bitcoin, using a risk-based approach. Laws require the exchange to obtain relevant personal information of the user, thus leaving a paper trail outside of the Bitcoin system for law enforcements to follow. At some point in the process the user, who has exchanged his currency, must launder his money in the traditional manner. By doing so will raise suspicion and red flags which are typically associated with the cash-based money laundering system.[226]

It is submitted that the need for Bitcoin ATMs have spiked in recent years, due to the increased availability of Bitcoin to the public, especially the underbanked. This brings about the need to follow a balanced approach, having regard to the strict requirement of identifying the user and the fact that the underbanked do not usually have the necessary documentation, which is traditionally required at a bank. The anonymity of Bitcoin is also a factor to be considered when formulating regulations as many Bitcoin users turned to cryptocurrency in order to protect their personal identity.[227]

Some jurisdictions have put regulations into place, which require users to provide identification when transacting over a certain amount. This requirement can easily be avoided by using a fake or stolen identification in order to complete the transaction. To resolve this issue, it has been suggested that the following requirements be implemented for Bitcoin ATMs: Firstly, a scanner which is able to scan identity or passport barcodes. Secondly, software which is able to match the scanned data to a national database. Thirdly, a camera is to be installed in order to take a real time picture of the user and lastly, facial recognition which is able to match the identity document to the picture taken and the database.[228]

The scanner will help to verify the authenticity of the identification document as currently anyone can use a Bitcoin ATM using a fake identification document to complete the transaction. By using this technology, a transaction cannot be complete unless a valid identification document can be produced, matching the national

226 Singh 2015 *Northwestern Journal of Technology and Intellectual Property* 60.
227 Hyman 2015 *St. Thomas Law Review* 314.
228 *Ibid.*

database. For further protection, a real time photo is taken, and facial recognition is used in order to verify that the user is indeed using his valid identification document.[229] However, this approach is not without its scepticism, as well as being a potentially costly operation. What is true, as technology develops, governments cannot expect to apply old regulations to an entirely new concept. Therefore, there must be developments within the regulatory framework.[230]

I The Question of Jurisdiction

Due to the Internet being an international phenomenon, the jurisdictional question arises as to where the cyberlaunderer is to be apprehended and prosecuted. This becomes particularly problematic as the cyberlaundering concept is yet to be adequately addressed in both international and national laws.[231]

It is submitted that cyberlaundering falls under the category of cybercrimes, therefore, one must have remedies available in terms of cyber law. This may be a starting point to determine jurisdiction.[232] In terms of the Electronic Communications and Transactions Act[233] a South African court would have jurisdiction over the cyber offences as provided for by the Act, in terms of the territoriality principle, effects principle or active personality principle.[234]

The activity principle provides that a person, who has committed a cybercrime, is to be prosecuted in the country where he or she is a national. However, this principle may not be quite well suited for cyberlaundering as it is difficult to physically apprehend a cyberlaunderer.[235] The effects principle provides that the country seeking jurisdiction must have felt the effects of the crime. However, the actual effects in question may be difficult to establish due to the unpredictable nature of cyberlaundering.[236]

---

229 Hyman 2015 *St. Thomas Law Review* 315.
230 *Ibid.*
231 Leslie Anti-*Cyberlaundering Regulation and Control* (Masters dissertation, University of the Western Cape) 2010 1.
232 Leslie Anti-*Cyberlaundering Regulation and Control* 72.
233 S90 of Act 25 of 2002.
234 Leslie Anti-*Cyberlaundering Regulation and Control* 73.
235 *Ibid.*
236 *Ibid.*

Therefore, it is submitted that the territoriality principle would be the best solution to solve the question of jurisdiction. In terms of this principle, the court is to exercise jurisdiction where the offence is committed, within the territory of the country seeking jurisdiction.[237] Simply put, in a case of cyberlaundering, the country where a website is registered is to have jurisdiction to prosecute. This principle is supported by the European Union Convention on Cybercrimes.[238] However, this is not without problems, particularly in countries which are known for their weak anti-money laundering framework. In addition to this, many websites are not registered adding yet another problem to the matter.[239]

4 4 Approaches to Regulating Cryptocurrency

As discussed above, various jurisdictions have used different approaches when regulating cryptocurrencies within their national framework. Although there are no hard and fast rules on its regulation, a number of different approaches have been suggested in order to regulate cryptocurrencies.

It is submitted that cryptocurrency should be clearly defined in legislation. Furthermore, it is submitted that it be included into existing legislation under the definition of money laundering. While States go back and forth to decide if cryptocurrency constitutes money, there is no doubt that such currencies have monetary value. With this being said, the definition of money laundering can include cryptocurrencies by implying that when a user moves their Bitcoins from an address, which is linked with illegal activities, to a new address, in such a way as to conceal the original source of the proceeds. This indicates that the user has the intention to "clean" the Bitcoin from their illegal source. This would amount to "Bitcoin Laundering".[240]

Therefore, financial institutions in all jurisdictions are urged to implement regulations and increase anti-money laundering enforcement on mixers and exchanges. It is

---

237 *Ibid.*

238 The European Union Convention on Cybercrimes 23. XI. Adopted on 12 April 2001, and came into force on 1 July 2004.

239 Leslie Anti-*Cyberlaundering Regulation and Control* 73.

240 Fanusie and Tobinson "Recommendations" in *Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services* (2018) 11.

submitted that most mixers and exchanges, which are used online, conceal their location in an attempt to evade regulations that have been put in place to promote transparency. It is for this reason that law enforcement agencies should target these services. Regulations should be put into place to enforce stronger anti-money laundering practices of exchanges, which verify their customers as well as to validate the source of the proceeds.[241]

In addition to this, law enforcement agencies should target the Dark Web and websites which offer mixing or exchange services, by uncovering their vulnerabilities. It is noteworthy that attempting to shut down these websites is merely just a temporary solution. As seen in Silk Road, when one website gets shut down, it is not long after where a new one arises. Moreover, law enforcements may use the Dark Web to interact with users, while remaining completely anonymous. Although some users may be confident using the Dark Web, the idea that law enforcement is lurking on the Dark Web may discourage those users.[242]

It is submitted that once regulations begin to form within jurisdictions, such jurisdictions should share these lessons with other States in order to impose similar regulations. Due to the boundless nature of Bitcoin, States will need to cooperate and work together in order to regulate cryptocurrencies on an international level.[243]

Given the nature of cryptocurrencies, a coordinated approach at an international level may be important for regulations to be fully effective. This is due to the fact that these currencies live online, in the virtual world and is not limited to national jurisdictions.[244] Therefore, it is submitted that in order to effectively regulate cryptocurrencies at an international level, there needs to be cooperation and assistance between States. Moreover, the Recommendations of the FATF and its risk-based approach should be applied to the regulation of cryptocurrencies.[245]

---

241 Fanusie and Tobinson *Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services* 11.

242 Fanusie and Tobinson *Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services* 12.

243 *Ibid.*

244 Campbell-Verduyn "Bitcoin, Crypto-Coins, and Global Anti-Money Laundering Governance" 2017 *Crime, Law and Social Change* 1 10.

245 Campbell-Verduyn 2017 *Crime, Law and Social Change* 11.

The FATF suggest that national authorities should set up mechanisms in which information can be shared, in order for countries to fully understand the risks in money laundering within the cryptocurrency network. The FATF also suggests that a risk-based approach be used, whereby authorities should target the nodes which are most likely used in the money laundering process. It specifies that exchanges should be targeted and monitored, however, requires the exchanges themselves to undertake the KYC policy when carrying out transactions or establishing business relations.

Furthermore, it requires the exchanges to do so by using reliable and independent documents or information.[246] It suggests that exchanges should identify users using a national identity number or Internet Protocol addresses, as well as to conduct online searches for activity information which validates, and is consistent with, the customers transactions.[247]

4 5 Conclusion

While it is clear that Bitcoin offers benefits, it also gives rise to a number of risks due to the malicious use of these benefits by the criminals wishing to launder their money. Some countries have attempted to regulate the cryptocurrencies by either amending existing laws or adopting new ones. Canada had opted for the first approach, whereby the existing laws were amended to include cryptocurrencies into the definition of money laundering.

In addition to this, businesses which transact with cryptocurrencies as well as exchange services are required to be registered. The Canadian law requires these entities to be transparent, despite the anonymity of cryptocurrencies. The reasoning being that such disclosure of information, would reduce the number of illegal exchanges as authorities would be able to identify the exchanges who do not disclose their information, as being an illegal service.

246 Campbell-Verduyn 2017 *Crime, Law and Social Change* 12.
247 *Ibid.*

Other countries, such as the US and EU have opted for the second approach. These jurisdictions have created new legislation to regulate cryptocurrencies. However, they fundamentally follow the same approach as Canada, by regulating the businesses which transact using cryptocurrencies, as well as obliging such entities to disclose the required information.

Some countries have outlawed cryptocurrencies. However, it is submitted that a total ban is not likely to be effective and that the regulation of cryptocurrencies is the favourable option.[248] As previously discussed, a complete ban would only eradicate the legitimate users and leave the criminals unaffected. It is for this reason that countries ought to be aware of the existence of the Dark Web. For the most part, regulations are not likely to effect Tor users. It has been submitted that the Dark Web is not completely out of reach from law enforcement, however, countries should shift their focus to regulating exchanges and businesses trading in cryptocurrencies. Thereafter, such jurisdictions can attempt to target the services of the Dark Web by exposing its vulnerabilities.

It has been submitted that the best approach to be followed by States, is the balanced approach. In terms of this, a balance is drawn between the benefits of cryptocurrencies and the risks associated with it. However, regulators in many countries have been unwilling to regulate cryptocurrencies due to their complex nature. Thus, there is a need for financial regulation in order to ensure harmony between the economy and financial sector. Therefore, it is submitted that in order to combat money laundering using cryptocurrencies, countries need to regulate cryptocurrencies.

However, South Africa has done nothing more than publish Position Papers, which merely clarify that cryptocurrencies remain unregulated. Furthermore, it fails to give an indication on how cryptocurrencies would be regulated in the future. This can be seen as South Africa's downfall in the anti-money laundering framework. It is submitted that South Africa searches for answers from the FATF in this regard, as opposed to taking progressive steps to regulate cryptocurrencies at a national level.

248 De Mink "Dangers Inherent in Bitcoin and Other Cryptocurrencies" 2018 33 *De Rebus.*

As discussed above, it is not necessary that South Africa promulgate a single Act for the regulation of cryptocurrencies, but rather integrate it into existing laws. By following the steps which Canada have taken, South Africa can incorporate cryptocurrencies into existing legislation in order to offer immediate relief and protection.[249] Instead, many jurisdictions including South Africa, have adopted the "wait and see" approach. However, it is submitted that this approach is far from adequate.

There is clearly a need for regulators to be actively involved with cryptocurrencies to understand how it operates, in order to be able to effectively regulate it.[250] It is strange that the growth of Bitcoin has brought about a number of risks associated with it, yet South Africa and many other jurisdictions have not developed any legal or regulatory frameworks in response to it. To date, South Africa has not promulgated any legislation regarding the regulation of cryptocurrencies in an attempt to combat money laundering.[251]

What is clear, is that without national or international laws and regulations, there will be no clear instructions on how to deal with the criminals who launder their illicit funds using cryptocurrencies, as well as where to prosecute them. Furthermore, it was shown that the South African legislative framework is sufficient to bring cryptocurrency in line with the legal structure and to address the concerns of money laundering using cryptocurrency.

249 Mothokoa *Regulating Crypto-Currencies in South Africa* 55.
250 Motelle "The Race of Innovation in Financial Services and the Regulatory Chase: Some Thoughts on the Regulation of Crypto-Currencies" 2017 3 *Development Finance Agenda* 8 9.
251 Nieman 2015 *PER* 1999.

CHAPTER 5: CONCLUSION AND RECOMMENDATIONS

5 1 Background

2009 was a big year for virtual currencies, particularly the introduction of the cryptocurrency, Bitcoin. Bitcoin was the first convertible decentralised virtual currency, which inspired other developers to create cryptocurrencies of their own. To date there are many different types of cryptocurrencies worldwide. Although some businesses in South Africa do accept cryptocurrencies as a form of payment, legally cryptocurrencies do not qualify as a legal tender. Therefore, businesses may refuse to accept cryptocurrencies as a form of payment, without being in breach of the law.

The research questions, which this treatise sought to address, was how cryptocurrencies are used in money laundering and whether South Africa's anti-money laundering legislation effectively covers this issue. The findings of these questions will be discussed in the section below.

The objectives of this treatise were to understand the traditional methods of money laundering and the anti-money laundering framework, which South Africa currently has in place. Thereafter, it became important to determine how cryptocurrencies work, the risks associated with it, the various ways in which money can be laundered using cryptocurrencies as well as to determine whether South Africa's current anti-money laundering framework is effective in combatting money laundering using cryptocurrencies.

What is to follow is a discussion on the findings of this research.

5 2 Findings

In order to address the research questions regarding how cryptocurrencies are used in money laundering as well as South Africa's regulation of cryptocurrencies, it was first necessary that the traditional concept of money laundering be understood.

Chapter 2 discussed the concept of money laundering, including the traditional stages of money laundering and highlighted the effects that money laundering has on the economy. In terms of this, it was found that the act of money laundering does not directly impact victims and that in some cases, could be beneficial to the economy. These benefits could be seen when the profits for the financial sector increases and results in more credit being available.

However, money laundering would not be regarded as a crime if it were beneficial to a country's economy. The chapter further explains that these "benefits" are short lived for any developing country. The long-term effects ultimately encourage corruption, which has a damaging effect on the financial sector institutions. This is due to the fact that money laundering undermines the confidence of foreign investors as well as the confidence of the public in their financial institutions.

Upon further discussion, it was found that the anti-money laundering framework in South Africa is a relatively strong one. South Africa is compliant with the majority of the FATF Recommendations, as well as enacting its own legislation, such as FICA, POCA and POCDATARA to combat money laundering. Therefore, it is evident that South Africa had taken steps to combat money laundering within its jurisdiction. Although having a strong anti-money laundering framework, the biggest shortcoming was its failure to address cryptocurrencies and its inherent danger of being used for money laundering. This "gap" in the framework is further discussed in chapter 4.

Chapter 3 addressed the issue of cryptocurrencies and its role in money laundering. However, before the issue of money laundering could be addressed, it was first necessary to discuss the concept of cryptocurrency. To summarise, cryptocurrencies refer to the mathematical-based, decentralised convertible digital currency, which is protected by cryptography. Due to its decentralised nature, there is no central monitoring authority. Therefore, Bitcoin is self-regulating. Essentially, being regulated by all the users on the network, hence the term "peer-to-peer" network.

Bitcoin uses blockchain technology which records every single transaction made on the blockchain network. This establishes a public ledger. Although the ledger itself is

public, the Bitcoin system is pseudo-anonymous. This means that although the public key of a user is displayed, it is not connected to the personal identification of the user.

It was clear that the development of Bitcoin showed many benefits, however, it came with its fair share of risks. The chapter further highlights the inherent risks of cryptocurrencies, as a result of its high degree of anonymity and fast transactions. With this being said, it became apparent that cryptocurrencies could be used to launder illegal proceeds. As a result of its anonymous nature, the transaction on the blockchain could not be traced back to a specific user. Furthermore, the only aspect identifying the Bitcoin user is their public key, no other personal information of the user is disclosed. Therefore, it becomes difficult to link a transaction to a particular user.

Furthermore, the different methods on how to launder money using cryptocurrencies were discussed. In order to fully grasp this issue, it was necessary to understand how the Dark Web operates. This was important as users use the Tor protocol to remain completely anonymous, as well as using services available on the Dark Web such as mixers and exchanges to launder their funds.

Chapter 4 emphasised the importance of regulation by comparing the regulations set by different jurisdictions around the world. The position of cryptocurrencies in the US, EU and Canada were discussed. It was found that Canada had amended existing legislation in order to include cryptocurrencies within the existing anti-money laundering framework. The US and EU had followed different approaches. Each jurisdiction had amended existing legislation, as well as enacting separate legislation in order to effectively regulate cryptocurrencies, in an attempt to combat money laundering.

It was found that the abovementioned jurisdictions had fundamentally followed the same approach by regulating businesses, which transact in cryptocurrencies, as well as requiring such entities to disclose the required information. Therefore, regulations required these entities to be transparent. Furthermore, it was found that a total ban on cryptocurrencies was not an effective approach and that regulation was more favourable.

The challenges which may accompany such regulation were further discussed. Due to the existence of the Dark Web, regulations were unlikely to affect Tor users. However, it was found that countries should shift their focus on regulating exchanges and businesses trading in cryptocurrencies. Thereafter, such countries could attempt to target the services on the Dark Web by exposing its vulnerabilities. This could be done by exploring the possibility of law enforcements using the Tor protocol on the Dark Web. The effect of this could potentially be a deterrent for Tor users. It was found that the best approach to follow was the balanced approach to regulation. Thus, a balance is to be struck between the benefits of cryptocurrencies and the risks associated with it.

The legal position of cryptocurrencies in South Africa was also discussed and it was found that cryptocurrencies are not regulated, however, the SARB stated it was open to the idea of regulating cryptocurrencies. To date, no legislative instruments regulating cryptocurrencies in South Africa have been enacted.

5 3 Conclusion

Cryptocurrencies contain many different features, which may make them attractive form of payment. Virtual currencies refer to the digital representation of value which can be traded digitally. This research focused on cryptocurrencies, a decentralised convertible virtual currency, and not the wider topic of virtual currencies.

Cryptocurrencies work on a peer-to-peer network, based on algorithms in order to verify the transactions and add these transactions to the digital ledger. The network is protected by cryptography. Users are able to acquire Bitcoins by either buying them with fiat money or by mining them. The Bitcoin network eliminates the need for a trusted third party, therefore there is low transaction costs.

Transactions are published on the digital ledger, known as the blockchain. However, the information which is disclosed on the blockchain is only the public key of the user and not the personal identity of the individual. This makes the system pseudo-anonymous. This gives rise to many dangers, such as cyberlaundering.

In addressing the first research question of this treatise, regarding the role of cryptocurrency in money laundering, it is submitted that this is not a new crime but rather a virtual version of the traditional money laundering. Due to the decentralised nature of the Bitcoin network, users remain anonymous. Although every transaction is available and tracible on the public ledger, it is not connected to the user's personal identity. Cyberlaunderers have used this to their advantage.

Users who wish to launder their money using Bitcoin, would tend to use mixing and exchange services offered on the Dark Web. Both of these services break the money trail, essentially making it difficult or impossible to trace back to the source. Once the money trail has been destroyed, the cryptocurrency appears to have originated from a legitimate source, as not to raise any suspicion.

In turning to the second question of whether South Africa's anti-money laundering legislation regulates cryptocurrencies, it was found that currently South Africa does not regulate cryptocurrencies, thereby allowing criminals to take advantage of the money laundering aspect. It is submitted that the risks associated with cryptocurrencies may be reduced through the enactment of a comprehensive legal framework.

The South African National Treasury and the SARB have merely published Position Papers, warning users of the risks associated with cryptocurrencies, as well as emphasising that South Africa does not regulate cryptocurrencies. This research makes it clear that cryptocurrencies are not regarded as a legal tender and that the risk remains with the user. Essentially, users have no remedies available to them when transacting with cryptocurrencies. Furthermore, the SARB has expressed that it would consider regulating cryptocurrencies. However, no legislative instruments have yet been enacted.

Countries such as Canada, have amended existing laws to include cryptocurrencies as to provide for immediate relief and protection to users. Therefore, it is not necessary for countries to create new legislation in order to regulate cryptocurrencies. It is submitted that South Africa already has a strong anti-money laundering framework in place. Therefore, the best approach would be to extend existing legislation to include

cryptocurrencies. Furthermore, by introducing cryptocurrencies into the current framework, all anti-money laundering laws and regulations would apply to cryptocurrencies. This would provide an immediate response to some of the risks.

Although cyberlaundering using cryptocurrencies is merely just a virtual version of the traditional money laundering process, it may be difficult to apply the traditional anti-money laundering mechanisms, such as KYC policy, monitoring intermediaries and following the paper trial. This is due to the fact that the true identity of the user is never fully known.

Furthermore, there is no central authority on which to confer these laws. However, the EU passed legislation which covers exchanges and wallet services. Thus, these businesses are obliged to adopt measures such as KYC policy, monitoring transactions, reporting suspicious activity and maintaining comprehensive records. Therefore, the approach is to regulate exchanges and wallet services and not the Bitcoin network as a whole.

In conclusion, the two main issues which this research sough to answer, have been addressed and comprehensively discussed. Cryptocurrencies have revolutionised the financial system. It is submitted that as technology develops, laws and regulations should too. The South African regulatory bodies can take lessons from jurisdictions such as Canada, in integrating cryptocurrencies into their existing legislation. However, it must be emphasised that these regulations should not hinder the growth of cryptocurrencies but rather be used to regulate and improve the current system. Thereby, ensuring a safe and effective use of this new payment system.

In the next section, recommendations will be given on how South Africa can improve its anti-money laundering legislation to include cryptocurrencies as well as to regulate them.

5 4 Recommendations

In order to ensure an effective prevention and prosecution strategy against money laundering using cryptocurrencies, jurisdictions should not ignore the traditional

methods of detection and investigation. Due to the fact that cryptocurrency is still a relatively new form of currency, it is not yet accepted as a well-known form of payment. This means that criminals will still need to convert their cryptocurrency into physical cash and thereby using the traditional third-party institutions.[252]

The public nature of the transactions is also to be preserved. As discussed above, Bitcoin is pseudonymous as all transactions are recorded chronologically on the blockchain. These blocks in the blockchain act like bank statements which can be used to identify crucial details such as the amount transferred as well as the origins of each Bitcoin address.[253]

By installing and regulating gatekeepers, it would require registration as well as bringing dealers and exchanges in line with the scope of legislation, such as FICA, which obliges a person to report suspicious transactions. Currently, various downloadable digital wallets, such as Luno, require the user to disclose their personal information in order to ensure verification. It is submitted that this promotes transparency and could be an effective way to combat money laundering using cryptocurrency as each user needs a digital wallet.[254]

Cyberlaundering should be the focus for government, law enforcement agencies, legislatures and researches. The traditional concepts of currency and money laundering, within the current anti-money laundering framework, is to be expanded and clarified to expressly include cryptocurrencies and cyberlaundering. [255]

In an attempt to strengthen the fight against money laundering, the FATF revised and updated its Recommendations in 2012. One of these changes included an increased emphasis on the risk-based approach, which is now regarded as the foundation of any country's anti-money laundering system. The risk-based approach means that the country will work together with their authorities and accountable institutions in order to identify, assess and understand the money laundering risks which that country may

252 De Mink "Dangers Inherent in Bitcoin and Other Cryptocurrencies" 2018 33 *De Rebus.*
253 *Ibid.*
254 *Ibid.*
255 Leslie Anti-*Cyberlaundering Regulation and Control* 79.

face, as well as to adopt any appropriate anti-money laundering measures.[256] However, in South Africa the accountable institutions are not compelled by law to apply this risk-based approach to anti-money laundering techniques.[257]

Furthermore, there is a need for uniform international regulation of cryptocurrencies. Due to the global and boundless nature of cryptocurrencies, users may abuse weak anti-money laundering laws of another jurisdiction. Therefore, it has been submitted that the United Nations Commission on International Trade Law (UNCITRAL) or the Organisation for Economic Co-operation and Development (OECD) devise a model law which governs the regulation of cryptocurrencies on an international level.[258]

5 4 1 Regulating Cryptocurrencies within the South African Framework

Unfortunately, there is no hard and fast rule on the regulation of cryptocurrencies. Furthermore, due to the decentralised nature of Bitcoin, it is impossible to implement legislation which is to regulate the Bitcoin network. In short, the Bitcoin network is self-regulating and cannot be regulated by legislation.[259] Therefore, by enacting new legislation regulating Bitcoin would have no effect, as the Bitcoin technology cannot be regulated. However, exchanges and businesses trading in cryptocurrencies, such as wallet services, may be regulated.

The use of cryptocurrencies is gaining popularity in South Africa, however, remain unregulated. As such, they are vulnerable to misuse. Thus, there is a need for regulatory intervention within South Africa to ensure that measures are implemented to prevent corrosion of the financial sector by cryptocurrencies.[260] This would be the most effective method of combatting money laundering using cryptocurrencies.

---

256 Williams *An Analysis of the Critical Shortcomings in South Africa's Anti-Money Laundering Legislation* 42.

257 Williams *An Analysis of the Critical Shortcomings in South Africa's Anti-Money Laundering Legislation* 43.

258 Mothokoa *Regulating Crypto-Currencies in South Africa* 61.

259 Shcherbak "How Should Bitcoin be Regulated" 2014 7 *European Journal of Legal Studies* 42 82.

260 Mothokoa *Regulating Crypto-Currencies in South Africa* 60.

It is submitted that South Africa should consider the following when regulating cryptocurrencies: Firstly, the regulations of cryptocurrencies should be proportional to the risks. Risks within the cryptocurrency system should be identified and dealt with accordingly. Secondly, it is submitted that exchanges be accredited and regulated. Furthermore, it is suggested that a centralised platform where all initial coin offerings (ICO),[261] available for the public, be listed. By registering all ICO with a central body will allow for monitoring of the credibility and quality of the issuers within the network.[262]

Lastly, the way in which cryptocurrencies are to be defined is an important aspect when applying a regulation. It is submitted that the scope of existing legislation should be extended to expressly include cryptocurrencies, as developing new legislation may result in it becoming quickly obsolete due to the rapid development in technology.[263]

In short, legislatures have two options available: either amending existing legislation by expanding definitions to include cryptocurrencies or create new legislation. As discussed above, South Africa has a well-developed legal framework regulating the financial services industry. As such, by amending the existing legislation would require substantial organisation among regulators.[264] However, amending existing definitions may have an effect on the current financial instruments, services or products.

Should the regulators opt for a new regulatory legislation regarding cryptocurrencies, it may result in users being subject to more onerous regulations. It is submitted that existing regulatory framework may adequately regulate the cryptocurrency network.[265]

In applying the approaches from the above-mentioned jurisdictions, the following recommendations are made: Currently, the list of "accountable institutions" in terms of

---

261 Initial Coin Offering acts similar to a fundraiser. A company looking to create a new type of coin will launch an ICO. Investors buy into the offering with fiat currency or a preexisting digital token. In exchange for their support, the investors receive the new cryptocurrency which is specific to the ICO.

262 FinTech *Intergovernmental FinTech Working Group* 12.

263 FinTech *Intergovernmental FinTech Working Group* 10.

264 FinTech *Intergovernmental FinTech Working Group* 13.

265 *Ibid.*

FICA has been amended to include any person or category of persons used or likely to be used for the purpose of money laundering.[266]

It is submitted that this definition should be amended to expressly include institutions which mine, exchange or hold cryptocurrencies.[267] Furthermore, it is recommended that all institutions, such as exchanges and wallet providers, dealing with cryptocurrencies must comply with the provisions of FICA. By complying to FICA, these institutions will have the records of the personal identity of the user and suspicious transactions which would make it easier to follow the trail of transactions related to money laundering.[268]

Furthermore, in terms of POCA, it is submitted that cryptocurrencies should be included under the definition of "property". By extending the definition would mean that a person will be guilty of the offence of money laundering if they launder their money using cryptocurrencies.

It is evident that the application of the South African anti-money laundering legislation, as it stands, is powerless against secretive organisations as provided for on the Dark Web. Therefore, it is submitted that the legislatures should focus less on these organisations and more on regulating exchanges and wallet services. Although there is still a lot of uncertainty regarding the regulations and enforcement of cryptocurrencies in South Africa, it may be helpful for the legislature to carefully consider the current legal framework, with particular reference to its purpose, which may provide guidelines in regulating cryptocurrencies. This includes FICA, anti-money laundering legislation and KYC policy.

Bankymoon has expressed its intention to create a balanced approach to regulation. This approach is particularly favoured for the regulation of Bitcoin ATMs. However, the risk-based approach has been favoured for the regulation of exchanges, such as Luno, which have illustrated to be effective.

---

266 Mothokoa *Regulating Crypto-Currencies in South Africa* 60.

267 Itzikowitz, Meiring and Gunning "South Africa" in *Blockchain & Cryptocurrency Regulation* (2019) 432.

268 Mothokoa *Regulating Crypto-Currencies in South Africa* 60.

Technology is developing and changing at a rapid pace. Thus, the risks and growth of cryptocurrencies must be supervised. As such, government cannot expect to apply old regulations to an entirely new concept. Therefore, there must be developments within the regulatory framework.

Word count [17 379]

TABLE OF STATUTES

1 Legislation

Canada: Criminal Code [Canada], C-46, 1985, available at: http://www.refworld.org/docid/4cf52bb32.html [accessed 13 August 2018].

Canada: Proceeds of Crime (Money Laundering) and Terrorist Financing Act [Canada], S.C. 2000, c. 17, 29 June 2000, available at: http://www.refworld.org/docid/5417f4a44.html [accessed 13 August 2018].

Electronic Communications and Transactions Act 25 of 2002.

Financial Intelligence Centre Act 38 of 2001.

Financial Recordkeeping and Reporting of Currency and Foreign Transactions Act of 1970 (31 U.S.C. 5311 et seq.).

National Payment System Act 78 of 1998.

Prevention of Organised Crime Act 121 of 1998.

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

South African Reserve Bank Act 90 of 1989.

The European Union Convention on Cybercrimes 23. XI. Adopted on 12 April 2001 and came into force on 1 July 2004.

Uniform Regulation of Virtual Currency Business Act of 2017.

2 International Instruments

African Union, *African Union Convention on Preventing and Combating Corruption*, 11 July 2003, available at: https://www.refworld.org/docid/493fe36a2.html [accessed 26 November 2018].

UN Economic and Social Council (ECOSOC), *United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances*, 19 December

1988, available at: http://www.refworld.org/docid/49997af90.html [accessed 9 July 2018].

UN General Assembly, *United Nations Convention Against Corruption*, 31 October 2003, A/58/422, available at: http://www.refworld.org/docid/4374b9524.html [accessed 9 July 2018].

UN General Assembly, *United Nations Convention against Transnational Organized Crime: resolution / adopted by the General Assembly*, 8 January 2001, A/RES/55/25, available at: http://www.refworld.org/docid/3b00f55b0.html [accessed 9 July 2018].

TABLE OF CASES

BIBLIOGRAPHY

1 Articles

Brown “Cryptocurrency and Criminality: The Bitcoin Opportunity” 2016 89 *Police Journal: Theory, Practice and Principles* 327.

Bryans “Bitcoin and Money Laundering: Mining for an Effective Solution” 2014 89 *Indiana Law Journal* 441.

Campbell-Verduyn “Bitcoin, Crypto-Coins, and Global Anti-Money Laundering Governance” 2017 *Crime, Law and Social Change* 1.

De Mink “Dangers Inherent in Bitcoin and Other Cryptocurrencies” 2018 33 *De Rebus.*

Gipp, Meuschke and Gernandt “Decentralized Trusted Timestamping using the Crypto Currency Bitcoin” 2015 *Proceedings of the iConference* 1.

Gruber “Trust, Identity, and Disclosure: Are Bitcoin Exchanges the Next Virtual Havens for Money Laundering and Tax Evasion?” 2013 32 *Quinnipiac Law Review* 135.

Hyman “Bitcoin ATM: A Criminal’s Laundromat for Cleaning Money” 2015 27 *St. Thomas Law Review* 296.

Morris-Cotterill “Use and Abuse of the Internet in Fraud and Money Laundering” 1999 13 *International Review of Law Computers & Technology* 211.

Motelle “The Race of Innovation in Financial Services and the Regulatory Chase: Some Thoughts on the Regulation of Crypto-Currencies” 2017 3 *Development Finance Agenda* 8.

Nakamoto “Bitcoin: A Peer-to-Peer Electronic Cash System” 2009 *Cryptography Mailing List* 1.

Nieman “A Few South African Cents’ Worth on Bitcoin” 2015 18 *PER* 1979 1988.

Omlor “Digitalization of Money and Currency Under German and EU Law” 2018 3 *TSAR* 613.

Ramracheya “The Dawn of our Tech-economy: An Introduction to Bitcoin and Cryptocurrency” 2017 *Without Prejudice* 32.

Retief “Accounting for Cryptocurrency” 2018 *Business & Economy* 10 11.

Sarawat, Chauhan and Faujdar “Analysis on Crypto-Currency” 2017 9 *International Journal of Latest Trends in Engineering and Technology* 185.

Shcherbak “How Should Bitcoin be Regulated” 2014 7 *European Journal of Legal Studies* 42.

Singh “The New Wild West: Preventing Money Laundering in the Bitcoin Network” 2015 13 *Northwestern Journal of Technology and Intellectual Property* 37.

Small “Bitcoin: The Napster of Currency” 2015 37 *Houston Journal of International Law* 582.

Stokes “Virtual Money Laundering: The Case of Bitcoin and the Linden Dollar” 2012 21 *Information & Communications Technology Law* 221.

Troeller “Developments in Banking Law” 2017 36 *Review of Banking & Financial Law* 159.

Tuba “Prosecuting Money Laundering the FATF way: An Analysis of Gaps and Challenges in South African Legislation from a Comparative Perspective” 2012 2 *CRIMSA* 103.

Van Wegberg, Oerlemans and Van Deventer “Bitcoin Money Laundering: Mixed Results? An Explorative Study on Money Laundering of Cybercrime Proceeds using Bitcoin” 2018 25 *Journal of Financial Crime* 419.

2 Books

Hoegner *The Law of Bitcoin* (2015) 2.

3 Loose-leaf Publications

Fanusie and Tobinson “Recommendations” in *Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services* (2018).

FinTech “Private Cryptocurrencies” in *Intergovernmental FinTech Working Group* (2018).

Hayes and Tasca “How Does Digital Currency Work?” in *Blockchain and Crypto-currencies* (2016).

Heymans “What is Money Laundering?” in *Money Laundering* (2002).

Itzikowitz, Meiring and Gunning “South Africa” in *Blockchain & Cryptocurrency Regulation* (2019).

National Treasury “Unregulated in South Africa” in *User Alert: Monitoring of Virtual Currencies* (2014).

The Law Library of Congress “Comparative Summary” in *Regulation of Cryptocurrency Around the World* (2018).

4 Thesis

Ahlers *The South African Anti-Money Laundering Regulatory Framework Relevant to Politically Exposed Persons* (Master’s Thesis, University of Pretoria) 2013.

Bååth *How to Combat Money Laundering in Bitcoin?* (Published thesis, Linköpings Universitet) 2016 2.

De Koker *Money Laundering in South Africa* (Research Project, RAU University) 2002.

Hamman *The Impact of Anti-Money Laundering Legislation on the Legal Profession in South Africa* (Doctoral thesis, University of the Western Cape) 2015.

Leslie *Anti-Cyberlaundering Regulation and Control* (Masters dissertation, University of the Western Cape) 2010.

Mothokoa *Regulating Crypto-Currencies in South Africa: The Need for an Effective Legal Framework to Mitigate the Associated Risks* (Masters Mini-dissertation, University of Pretoria) 2017.

Naicker *Money Laundering: Fiscal & Economic Implications and the Potential Impact of the Financial Intelligence Centre Act (FICA)* (master’s Dissertation, University of KZN) 2004.

Sujee *A Study of the Anti-Money Laundering Framework in South Africa and the United Kingdom* (Master's thesis, University of Pretoria) 2016.

Van Jaarsveld *Aspects of Money Laundering in South African Law* (Doctoral Thesis, University of South Africa) 2011.

Williams *An Analysis of the Critical Shortcomings in South Africa's Anti-Money Laundering Legislation* (Master's Thesis, University of the Western Cape) 2017.

5 Websites

Burke "Virtual Private Network (VPN)" (September 2018) https://searchnetworking.techtarget.com/definition/virtual-private-network (accessed 2018-12-04).

FATF "Virtual Currencies: Key Definitions and Potential AML/CFT Risks" (June 2014) http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf (accessed 2018-08-08).

Khosa and Visser "Blockchain Revolution and Financial Regulation in South Africa" (05 September 2016) http://www.tech4law.co.za/news-in-brief/59-law/2233-blockchain-revolution-and-financial-regulation-in-south-africa (accessed 2018-11-13).

Luno "About Luno" (undated) https://www.luno.com/en/about (accessed 2018-11-27).

Nelson "Cryptocurrency Regulation in 2018: Where the World Stands Right Now" (1 February 2018) https://bitcoinmagazine.com/articles/cryptocurrency-regulation-2018-where-world-stands-right-now/ (accessed 2018-08-08).

Robinson "5th AML Directive: EU Regulation Of Cryptocurrency Businesses" (1 May 2018) https://www.elliptic.co/our-thinking/5th-aml-directive-eu-regulation-cryptocurrency (accessed 2018-08-17).

South African Reserve Bank "Position Paper on Virtual Currencies" (03 December 2014) https://www.resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/Legal/Documents/Position%20Paper/Virtual%20Currencies%20Position%20Paper%20%20Final_02of2014.pdf (accessed 2018-11-13) .

Zhang “Why Does Bitcoin Have Any Value?” (25 November 2017) https://medium.com/@zmeric5/why-does-bitcoin-has-any-value-520bdc012d46 (assessed 2018-08-07).