A CRITICAL ANALYSIS OF SOUTH AFRICAN ANTI-MONEY LAUNDERING LEGISLATION WITH REGARD TO CRYPTOCURRENCY

Deon Erasmus
B Juris LLB LLD
Professor, Criminal and Procedural Law
Nelson Mandela University

Susan Bowden
LLB LLM
Candidate Attorney
Greyvensteins Incorporated

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. This article discusses concepts of cryptocurrency, its relevance in the financial sector, its associated risks and establishes whether regulatory interference is necessary in order to combat money laundering using cryptocurrency. Currently, cryptocurrencies remain unregulated in South Africa. The article concludes that regulatory intervention is necessary and that cryptocurrencies should be integrated into relevant existing legislation.

1 INTRODUCTION

The online medium of exchange has evolved from Electronic Funds Transfer (EFT), credit cards and PayPal[1] to cryptocurrencies.[2] However, the birth of the Internet has brought with it a new type of criminal – namely,

[1] PayPal is a payment service that 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.

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

cyberlaunderers.[3] Cryptocurrencies are increasingly used by criminals to launder illicit funds obtained through criminal activities. However, cryptocurrency is legal in South Africa, despite its controversial nature. The majority of cryptocurrencies are decentralised and therefore operate without administration or authority by the State or banks. In the case of cryptocurrencies such as Bitcoin,[4] users remain largely anonymous, thereby making transactions difficult to trace back to a particular user. Thus, it is easy to see why cryptocurrencies are used to launder money. Despite these risks, cryptocurrencies remain largely unregulated in South Africa; they also have no legal status.

For the purposes of this article, Bitcoin is used as an example of cryptocurrency; it is referred to throughout, as it has the largest number of contributing computer nodes and has achieved one of the highest market capitalisations.[5] Note that this article focuses on cryptocurrency and not the wider subject of virtual currency. Although Bitcoin is used as a main example of cryptocurrency, the article's scope is not limited to Bitcoin, but to cryptocurrencies as a whole; Bitcoin is merely used as a proxy in order to understand the concepts more easily.

2 MONEY LAUNDERING USING CRYPTOCURRENCY

As the saying goes, "there are two sides to every coin". Where Bitcoin is concerned, two contrasting views have gained popularity: some are of the opinion that cryptocurrencies are the future of payment systems, allowing for fast and effective transactions between users; others believe that cryptocurrencies provide criminals with a very powerful tool to store and move their illegal proceeds, while avoiding law enforcement agencies and other authorities.[6]

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 cryptography. Cryptography is a security measure that circumvents the need for trust, using keys to keep Bitcoin relatively safe.[7]

Bitcoins can either be mined or bought with fiat currency. In order to acquire bitcoins, the user must first have a digital wallet.[8] This wallet

---

3 Leslie *Anti-Cyberlaundering Regulation and Control* (master's dissertation, University of the Western Cape) 2010 1.

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

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

6 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.

7 Small "Bitcoin: The Napster of Currency" 2015 37 *Houston Journal of International Law* 582 588.

8 Small 2015 *Houston Journal of International Law* 588.

contains both a public and a private key. The public key is similar to an email address that users send to each other in order to transfer bitcoins. The private key can be compared to a pin code for a debit card and acts as the user's signature. No other user has access to the private key, and nor can it be replicated. The private key is used to confirm the transfer of bitcoins.[9] Put differently, if the public key of a user works, then it is proof that the message was signed by the private key and that the sender intended to send it. Unlike a signature or credit card number, the keys cannot be forged or faked by a scammer.[10] Bitcoin is said to be pseudo-anonymous as the transfers and public keys of a user are made public, while the personal identity of the user is not disclosed.[11]

Each time bitcoins are transferred, the transaction is recorded on the blockchain. The blockchain is a public ledger that contains the history of each and every bitcoin transaction. In the blockchain, transactions are shared among multiple computers or servers, which are known as the member nodes in the network.[12] The ledger is decentralised, meaning that no person or entity controls or owns the data.[13] 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.[14]

Bitcoin mining has two main functions. First, it creates new bitcoins and secondly, it validates and confirms each transaction on the network. The second function is most important as it creates the tamper-proof system that 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.[15] 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 add these transactions on the digital ledger. This means that the cryptocurrency is essentially "unhackable", and also prevents the problem of double spending.[16] On average, a block is added to the chain every ten to twelve minutes, although the precise interval is unpredictable as the process requires the computers to solve complex mathematical algorithms. Each time a miner's computer solves an algorithm, the miner receives a reward of bitcoins for contributing computing power.[17] The design of the algorithms is such that over time they become increasingly difficult to solve in order to ensure that the blockchain, and the bitcoins, are not created too quickly.[18]

Using the Internet, the blockchain is regularly updated and transferred to all users – hence the term, "peer-to-peer". The validity of the blockchain is

9 *Ibid.*
10 *Ibid.*
11 FATF http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf 6.
12 Small 2015 *Houston Journal of International Law* 589.
13 Ramracheya "The Dawn of Our Tech-Economy: An Introduction to Bitcoin and Cryptocurrency" 2017 *Without Prejudice* 32 33.
14 Ramracheya 2017 *Without Prejudice* 33.
15 Hayes and Tasca "Blockchain and Crypto-Currencies" in Chishti and Barberis *The FinTech Book* (2016) 217.
16 Ramracheya 2017 *Without Prejudice* 33.
17 Small 2015 *Houston Journal of International Law* 589.
18 Small 2015 *Houston Journal of International Law* 590.

secured through hashes. Hashes form part of each block in the blockchain; they represent a mathematical link to the block directly before. Simply put, hashes chain the individual blocks together to create the blockchain.[19] 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 bitcoin sender is an authorised user, the software uses a formula to check the network users.[20]

The transaction is attached to the next block in the blockchain and is credited to the recipient only when a majority of the users on the network confirms the correctness of the transaction. This process is known as the proof-of-work. Only once the block has been added is a new mathematical problem generated for solving. If multiple people solve the mathematical problem roughly at the same time, the network picks one upon which to keep building. This then becomes the longest and most trusted chain.[21]

2 2 What is cryptocurrency?

Simply put, cryptocurrencies refer to mathematically based, decentralised, convertible, virtual currencies that are protected by cryptography. Virtual currencies refer to a digital representation of value that can be traded digitally. Virtual currencies can function as a medium of exchange, units of account as well as a store of value; however, they do not qualify as legal tender within any jurisdiction.[22]

Cryptocurrency refers essentially to the digital asset that forms the foundation of the peer-to-peer electronic cash system, and which uses cryptography as a security measure.

Cryptocurrencies are not illegal *per se* and are often used by consumers as a form of payment owing to its highly secure nature, as well as its fast transferability around the world without third-party costs. Criminals exploit these benefits in order to further their illegal acts, such as money laundering. With this in mind, the reasons that criminals opt for cryptocurrency become obvious.[23]

2 3 How do cryptocurrencies acquire value?

Gold originally acquired its value from the vast amount of time and resources used to try to mine it.[24] The same mining concept applies to Bitcoin. Users spend time and resources building and maintaining a transaction system and get compensated with bitcoins. However, the value of a good is determined

---

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

20 Omlor 2018 *TSAR* 615.

21 *Ibid.*

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

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

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

by the desire for it. Even though time and resources are spent on an object that may prove useful, this does not necessarily mean that the object holds any value.[25] As with all finite resources, the number of bitcoins will eventually run out: only 21 million bitcoins will be produced. Similar to mining in the real world, the last few bitcoins will be the most difficult and expensive to mine.[26]

2 4 Inherent dangers of cryptocurrencies

Although cryptocurrency is used for both legitimate and illegal means, it clearly poses a number of inherent dangers, such as simplifying the money laundering process. This is because the traditional stages of money laundering can easily now be merged into one another with the help of information technology; cryptocurrencies are sent anonymously and directly to a recipient without any need for identification or monitoring of transaction amounts.[27]

One of the mechanisms used to combat traditional money laundering is the "know your customer" policy (KYC).[28] The KYC policy aims to identify the consumers of financial institutions adequately, by requiring legal identification, residency information as well as a valid photograph.[29] By contrast, Bitcoin is known for its high degree of anonymity; the only aspect that identifies a bitcoin user is his or her public key. No other personal information of the user is disclosed. This ensures a high level of protection against identity theft. However, criminals use this mechanism in their favour to circumvent traditional anti-money-laundering mechanisms, such as the KYC policy.[30]

As a result of Bitcoin's decentralised nature, transactions are made directly between users without the need for 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.[31] 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, which poses the risk that criminals may intentionally seek out jurisdictions with inadequate anti-money-laundering mechanisms, thereby enhancing their ability to launder their money or provide a money laundering service to other users.[32]

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, the proceeds of the illegal activity are difficult to

---

25 Zhang https://medium.com/@zmeric5/why-does-bitcoin-has-any-value-520bdc012d46.
26 Nieman "A Few South African Cents' Worth on Bitcoin" 2015 18 *PER* 1979 1987.
27 De Mink 2018 *De Rebus* 33.
28 Bååth *How to Combat Money Laundering in Bitcoin?* (published thesis, Linköpings Universitet) 2016 2.
29 Bååth *How to Combat Money Laundering in Bitcoin?* 7.
30 Bååth *How to Combat Money Laundering in Bitcoin?* 10.
31 De Mink 2018 *De Rebus* 34.
32 *Ibid* .

confiscate.[33] Furthermore, bitcoin transfers are irreversible. Therefore, it becomes almost impossible to recover illegal proceeds once a transfer has been recorded.[34]

The lack of transactional recordkeeping is yet another risk of Bitcoin. During an ordinary money-laundering investigation, following the money trail would be the method used. With Bitcoin, all transactions are made public, but such transactions are only published in computer code. When law enforcement attempts to make a connection between the public key and the user behind it, there is a problem;[35] it is difficult to trace the identities of users without their co-operation.[36]

The final risk factor relates to the jurisdictional issues that arise owing to the fact that there is no internationally accepted regulation or framework regarding cryptocurrency; each jurisdiction individually has the cumbersome task of attempting to regulate cryptocurrency transactions. As discussed above, this becomes a difficult task when such transactions are concluded directly with another user anywhere in the world. According to the Financial Action Task Force (FATF) report on virtual currencies,[37] records linking identification and transactions of users may be kept by different entities within any jurisdiction. However, access by law enforcement agencies and regulators may be hampered or limited in this regard.[38]

2 5 Money laundering using cryptocurrency

For the general public, anonymous browsing has been made available using the Tor-browser, otherwise known as the Onion Router. By routing Internet traffic through multiple Tor nodes, network traffic is encrypted, thereby rendering a user's IP-address[39] 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.[40] The Dark Web is a part of the Internet that 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),[41] to ensure anonymity. The Dark Web can be used for anything, from the purchase of usernames and passwords to hacking

33 *Ibid*.
34 *Ibid*.
35 Brown "Cryptocurrency and Criminality: The Bitcoin Opportunity" 2016 89 *Police Journal: Theory, Practice and Principles* 327 333.
36 De Mink 2018 *De Rebus* 35.
37 FATF http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf 6.
38 De Mink 2018 *De Rebus* 35.
39 An Internet Protocol address is a unique string of numbers that identifies each computer within a network.
40 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* 419 421.
41 A virtual private network is technology that 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).

services and illegal porn.[42] As a result of its anonymous nature, Bitcoin is the main form of currency on the Dark Web.[43]

The blockchain is a public ledger that 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, bitcoin transactions are linked to one another. Simply put, each input is inevitably the output of a previous transaction.[44] 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 bitcoins further in order to assist in bitcoin laundering. There are two aspects to bitcoin laundering. First, there are bitcoin mixers or tumblers,[45] a service that aims to disconnect bitcoins from their illegal source. Secondly, there are bitcoin exchanges, a service that attempts anonymously to convert bitcoins into actual money.[46]

Mixing services break the money trail of bitcoin transactions. 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 an address that is provided by the customer. In order to ensure a higher level of anonymity, the payouts are spread out over time and also introduce an aspect of unpredictability in the division of amounts.[47] 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 transactions, thereby making it difficult to connect the coins with a specific transaction.[48] Once the bitcoin mixing has taken place, it becomes almost impossible to trace it to the illegal source.[49]

The exchange services are used once the bitcoins have been successfully mixed. In terms of this, a exchange agrees to receive bitcoins in exchange for any other currency, thereby allowing users to buy and sell bitcoins online. Output platforms such as Luno[50] are used to ensure that the exchanged currency ends up in the possession of the user.[51] 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

42 Small 2015 *Houston Journal of International Law* 582.
43 *Ibid*.
44 Van Wegberg *et al* 2018 *Journal of Financial Crime* 423.
45 Van Wegberg *et al* 2018 *Journal of Financial Crime* 420.
46 *Ibid.*
47 Van Wegberg *et al* 2018 *Journal of Financial Crime* 423.
48 FATF http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf 6.
49 Van Wegberg *et al* 2018 *Journal of Financial Crime* 424.
50 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.
51 Van Wegberg *et al* 2018 *Journal of Financial Crime* 429; Luno "About Luno" (undated) https://www.luno.com/en/about (accessed 2018-11-27).

suspected criminal activity and to identify the user.[52] However, these accounts are available to be purchased on the Dark Web, thereby creating a mechanism for erasing any connection to criminal users.[53] Criminals can either use the exchange services available on the Dark Web or can exchange currency through a bitcoin ATM, provided that amounts are sufficiently low so as not to raise any suspicion and trigger the requirement of identification verification.[54] It is submitted that in some cases personal or banking information is not required in order to complete a transaction at a bitcoin ATM.[55]

3 REGULATION OF CRYPTOCURRENCY

The general opinion on Bitcoin is that it is unregulated. However, this is both vague and unclear. 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 because the peer-to-peer network is decentralised. Therefore, to say that Bitcoin itself is unregulated is incorrect; Bitcoin is a set of rules that regulates the decentralised digital currency, while the peer-to-peer network ensures that these rules are enforced. Therefore, it is more correct to say that the bitcoin network is self-regulated.[56]

Although cryptocurrency is not expressly mentioned in law or regulation, the use of such new technology may be covered by existing laws.[57] 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.[58] 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.

3 1 Cryptocurrency and the current anti-money-laundering framework within South Africa

Jurisdictions such as Canada, the United States of America (USA) and the European Union (EU) 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 South African Reserve Bank (SARB) has stated its intention to investigate the possibility of the blockchain

---

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

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

54 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.

55 Hyman 2015 *St. Thomas Law Review* 304.

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

57 Hoegner *The Law of Bitcoin* 3.

58 Gruber 2013 *Quinnipiac Law Review* 185.

and has expressed its concerns with the risks involving cryptocurrencies.[59] As the current position stands, South Africa does not regard cryptocurrencies as legal tender, but cryptocurrencies may be used.[60] Given that cryptocurrencies are not regulated by a central authority such as a bank, they fail to meet the definition of legal tender as provided by the South African Reserve Bank Act.[61] 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, which has warned users that there are currently no laws or regulations that address cryptocurrencies. As a result, users have no legal protection or remedies available to them.[62]

The risk-based approach, as applied to the anti-money-laundering framework by the FATF and the EU, emphasised the importance of identifying money-laundering risks associated with payment mechanisms such as cryptocurrencies. One of these risks is 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 them.[63] In general, the legal framework for the financial sector is comprehensive and has kept up with 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.[64]

Compared to other jurisdictions, South Africa has also not completely ignored the matter of cryptocurrencies. SARB's Position Paper on Virtual Currencies, released in 2014, seemed promising with regard to the regulation of cryptocurrencies. However, the Position Paper merely confirms the lack of legal and regulatory framework for cryptocurrencies. SARB emphasises that it does not regulate, supervise or oversee cryptocurrency networks. Therefore, any transaction or activity relating to cryptocurrency is entirely at the risk of the user, who has no recourse to SARB.[65]

Furthermore, SARB recognised that there was no substantial risk to financial stability relating to virtual currencies at the time. However, it reserved the right to change this view according to market developments. Since 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.[66]

---

59 Ramracheya 2017 *Without Prejudice* 33.

60 *Ibid.*

61 90 of 1989.

62 National Treasury "Unregulated in South Africa" in *User Alert: Monitoring of Virtual Currencies* (2014) 2.

63 Mothokoa *Regulating Crypto-Currencies in South Africa* 39.

64 *Ibid.*

65 Nieman 2015 *PER* 1979 1988.

66 Intergovernmental FinTech Working Group "Position Paper on Crypto Assets" (2018) http://www.treasury.gov.za/comm_media/press/2020/20200414%20IFWG%20Position%20Paper%20on%20Crypto%20Assets.pdf (accessed 2020-08-01) 8.

South Africa has been criticised for adopting a "wait and see" approach, as central banks have only published notices and disclaimers stating 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 should be actively involved with cryptocurrencies to understand how they work, and to be able to regulate them effectively.[67] Owing to the decentralised nature of Bitcoin, there is no central organisation upon which money-laundering regulations may be imposed.[68] From a regulatory perspective, anti-money-laundering laws currently in place in South Africa cannot be used. The current framework is based on the assumption that there is a central authority or business that can impose obligations.[69] It thus becomes clear that current anti-money-laundering frameworks need to be developed to include cryptocurrencies, as the current approach is not viable to combat money laundering that uses cryptocurrencies.

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

By comparison, existing legislation in Canada[70] was amended to include cryptocurrencies as well as to authorise the Financial Transactions and Reports Analysis of Canada (FinTRAC) to ensure compliance with existing legislation, by applying the KYC policy to businesses transacting in cryptocurrency and to exchanges. The US and EU applied a different approach by promulgating legislation to regulate cryptocurrencies separately, as well as clarifying the position of the users and businesses that transact with cryptocurrencies.

In 2017, the South African government began working with a blockchain-based solutions provider, Bankymoon, to create a balanced approach to cryptocurrency regulation.[71] Furthermore, SARB released a media statement in February 2018 establishing the Financial Technology (FinTech) programme. The first goal of the FinTech programme was to review the position of SARB regarding cryptocurrencies and to inform an appropriate policy and regulation framework.[72] Although this can be seen as a step in a positive direction, no legislative instruments to regulate cryptocurrencies and combat money laundering have been enacted as yet. One can only remain hopeful that the establishment of the FinTech programme will be the first of

---

67 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.

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

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

70 The Criminal Code was amended to include cryptocurrencies in the definition of money laundering.

71 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).

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

many steps to regulate cryptocurrencies.[73] There is still uncertainty concerning the regulation of cryptocurrencies and enforcement thereof. It is therefore helpful to consider carefully the current legal framework, with particular reference to its purpose, in order to provide some guidelines for the regulation of cryptocurrencies. This framework includes FICA, as well as anti-money-laundering legislation and the KYC policy.[74]

3 2 Challenges in 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 exchange.[75]

Due to the pseudonymous nature of the sender's identity in the bitcoin network, attempting to regulate the sender is unrealistic. When transactions take place, no personal information is exchanged between users. Therefore, being able to identify the bitcoin user is unlikely. 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. A similar result may arise in attempting to regulate receivers or launderers. With no personal information given to link the crime to the user, law enforcement is likely to invest a large amount of time and resources in attempting to trace the user; and the reward of such efforts may be relatively small.[76] Moreover, the regulation of bitcoin miners is also likely to 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 that processes the transaction without user involvement. Thus, it would be illogical to regulate miners when it is the miner's software that processes bitcoin transactions.[77]

It has been argued that an effective solution lies in regulating the bitcoin development team or requiring them to change the software in order to monitor transactions as well as to de-anonymise transfers. However, this fails to recognise that Bitcoin is 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 the development team does not operate as a central authority that controls the operation of the network. It is thus

---

73 *Ibid*.

74 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).

75 Bryans "Bitcoin and Money Laundering: Mining for an Effective Solution" 2014 89 *Indiana Law Journal* 441 469.

76 Bryans 2014 *Indiana Law Journal* 470.

77 *Ibid.*

submitted that regulating the development team would have little to no effect on lessening illegal activity that may occur through Bitcoin.[78]

Lastly, the regulation of bitcoin currency exchanges could be explored. Exchanges generally deal with fiat currencies that are likely to be regulated by money exchange laws. The credibility of exchanges is increased through the user confidence and volume. This means that if the exchange has fewer users who are willing to trade or if the exchange is not trust worthy, the stages of money laundering will not easily occur without attracting the attention of the authorities. Therefore, exchanges are less likely to be decentralised and are easier entities to regulate.[79]

Luno and 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 have stated that they are 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, it employs 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 reporting suspicious transactions. Furthermore, Luno does not provide services when there is good reason to believe that such transactions are associated with money laundering.[80] This illustrates that exchanges can be the site of effective regulation.

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.[81] Bitcoin has been criticised for not providing any beneficial use, and therefore its eradication is justified. However, it is submitted that this is not the case.[82] Attempting to eliminate Bitcoin may be an impossible task as users can remain anonymous by using Tor to prevent having their public keys traced to their personal identities. This means that criminals would continue to operate despite government regulations. It is submitted that this approach would only eradicate the legitimate uses of Bitcoin, leaving criminals unaffected.[83]

Thus, a balanced approach should be implemented. Recognising that Bitcoin has beneficial uses, legislatures should adopt legislation that regulates this use as well as attempts to prevent money laundering. However, legislatures should bear in mind the harsh reality that is the Dark

78 Bryans 2014 *Indiana Law Journal* 471.
79 Bryans 2014 *Indiana Law Journal* 472.
80 Luno https://www.luno.com/en/legal/compliance.
81 Singh "The New Wild West: Preventing Money Laundering in the Bitcoin Network" 2015 13 *Northwestern Journal of Technology and Intellectual Property* 37 49.
82 Singh 2015 *Northwestern Journal of Technology and Intellectual Property* 49.
83 *Ibid.*

Web and understand that, at a certain point, such regulations will not be effective against those users who remain anonymous.[84]

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 or her bitcoins to fiat currency using a bitcoin exchange. This is where the abovementioned jurisdictions regulate Bitcoin, using a risk-based approach. Laws require the exchange to obtain relevant personal information of the user, thus creating a paper trail outside of the bitcoin system for law enforcement to follow. At some point in the process, a criminal user who has exchanged his or her cryptocurrency must launder money in the traditional manner. Doing so will raise suspicion and red flags typically associated with a cash-based money-laundering system.[85]

It is submitted that the need for bitcoin ATMs has spiked in recent years, owing to the increased availability of Bitcoin to the public, especially the underbanked. The need to follow a balanced approach is evident, having regard to the strict requirement of identifying the user and the fact that the underbanked do not usually have the documentation that is traditionally required at a bank. The anonymity of Bitcoin is also a factor to be considered when formulating regulations as many bitcoin users have turned to cryptocurrency in order to protect their personal identity.[86]

Some jurisdictions have put into place regulations that require users to provide identification when transacting for more than 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 installations be required for the operation of bitcoin ATMs: first, a scanner that is able to scan identity or passport barcodes; secondly, software that is able to match the scanned data to a national database; thirdly, a camera to take a real-time photograph of the user; and lastly, facial recognition software that is able to match the identity document to the picture taken and the database.[87]

The scanner helps 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 completed without a valid identification document that matches the national database. For further protection, a real-time photograph is taken, and facial recognition is used in order to verify that the user is indeed using a valid identification document.[88]

However, this approach is not without its sceptics; it could also be a potentially costly operation. What is true, as technology develops, is that governments cannot expect to apply old regulations to an entirely new

---

84 *Ibid.*
85 Singh 2015 *Northwestern Journal of Technology and Intellectual Property* 60.
86 Hyman 2015 *St. Thomas Law Review* 314.
87 *Ibid.*
88 Hyman 2015 *St. Thomas Law Review* 315.

concept. Therefore, there must be developments within the regulatory framework.[89]

3 3 The question of jurisdiction

Due to the Internet being an international phenomenon, the jurisdictional question arises as to where a cyberlaunderer is to be apprehended and prosecuted. This becomes particularly problematic as the cyberlaundering concept is yet to be adequately addressed in either international or national laws.[90] It is submitted that cyberlaundering falls under the category of cyber crimes, and therefore remedies are available in terms of cyber law. This may be a starting point for determining jurisdiction.[91] In terms of the Electronic Communications and Transactions Act,[92] a South African court has jurisdiction over the cyber offences provided for by the Act in terms of the territoriality principle, effects principle or active personality principle.[93]

The activity principle provides that a person who has committed a cyber crime is to be prosecuted in the country where he or she is a national. However, this principle may not be well suited to cyberlaundering as it is difficult to apprehend a cyberlaunderer physically.[94] The effects principle provides that the country seeking jurisdiction must have felt the effects of the crime. However, the effects in question may in reality be difficult to establish owing to the unpredictable nature of cyberlaundering.[95] Therefore, it is submitted that the territoriality principle is the best solution to the question of jurisdiction. In terms of this principle, a court has jurisdiction where the offence is committed, within the territory of the country seeking jurisdiction.[96]

Simply put, in a case of cyberlaundering, the country where a website is registered has jurisdiction to prosecute. This principle is supported by the European Union Convention on Cybercrimes.[97] However, this approach is not without problems, particularly in countries known for a weak anti-money-laundering framework. In addition to this, many websites are not registered, adding yet another problem to many others.[98]

3 4 Approaches to regulating cryptocurrency

It is submitted that cryptocurrency should be clearly defined in legislation. Furthermore, the definition of money laundering in existing legislation should specifically include the use of cryptocurrency for such purposes. While states go back and forth on deciding whether cryptocurrency constitutes

89 *Ibid.*
90 Leslie *Anti-Cyberlaundering Regulation and Control* 1.
91 Leslie *Anti-Cyberlaundering Regulation and Control* 72.
92 S 90 of Act 25 of 2002.
93 Leslie *Anti-Cyberlaundering Regulation and Control* 73.
94 *Ibid.*
95 *Ibid.*
96 *Ibid.*
97 The European Union Convention on Cybercrimes 23. XI. Adopted on 12 April 2001, and came into force on 1 July 2004.
98 Leslie *Anti-Cyberlaundering Regulation and Control* 73.

money, there is no doubt that such currencies have monetary value. That said, the definition of money laundering could be interpreted to imply the inclusion of cryptocurrency laundering – for example, when a user moves bitcoins from an address that is linked to illegal activities to a new address in such a way as to conceal the original source of the proceeds, thus indicating the user's intention to "clean" the bitcoins from their illegal source. This would amount to "bitcoin laundering".[99]

Therefore, financial institutions in all jurisdictions are urged to implement regulations and increase anti-money-laundering enforcement targeting mixers and exchanges. It is 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 by exchanges, which should verify their customers as well as validate the source of their proceeds.[100] In addition, law enforcement agencies should target the Dark Web and websites that offer mixing or exchange services by uncovering their vulnerabilities. Attempting to shut down these websites is merely a temporary solution. Law enforcers should 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.[101]

It is submitted that once regulations begin to form within jurisdictions, such jurisdictions should share these lessons with other states, which can then impose similar regulations. Due to the boundless nature of Bitcoin, states need to cooperate and work together in order to regulate cryptocurrencies on an international level.[102] Given the nature of cryptocurrencies, a coordinated approach at an international level may be important for regulations to be fully effective. This is because these currencies live online, in the virtual world and are not limited by national jurisdictions.[103] Therefore, it is submitted that in order to regulate cryptocurrencies effectively 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.[104] The FATF suggests that national authorities should set up mechanisms to share information in order for countries to fully understand the risks of money laundering within the cryptocurrency network. The FATF also suggests that a risk-based approach be used, whereby authorities target the nodes that are most likely to be used in the money-laundering process. It specifies that exchanges should be targeted and monitored, but requires the exchanges

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

100 Fanusie and Tobinson *Bitcoin Laundering* 11.

101 Fanusie and Tobinson *Bitcoin Laundering* 12.

102 *Ibid.*

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

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

themselves to apply the KYC policy when carrying out transactions or establishing business relations.

Furthermore, it requires exchanges to do so by using reliable and independent documents or information.[105] It suggests that exchanges should identify users using a national identity number or Internet Protocol addresses, as well as conduct online searches for activity information that validates, and is consistent with, customers' transactions.[106]

While it is clear that Bitcoin offers benefits, it also gives rise to a number of risks owing to the malicious use of these benefits by criminals wishing to launder their money. Some countries have attempted to regulate cryptocurrencies by either amending existing laws or adopting new ones. Canada opted for the first approach, whereby existing laws were amended so as to include reference to cryptocurrencies in the definition of money laundering. In addition, businesses that transact with cryptocurrencies, as well as exchange services, are required to be registered. Canadian law requires these entities to be transparent, despite the anonymity of cryptocurrencies. The reason is that disclosure of information reduces the number of illegal exchanges, as authorities are able to identify the exchanges that do not disclose their information as illegal services. Other countries and blocs, such as the US and the 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 that transact using cryptocurrencies, as well as obliging such entities to disclose the required information.

It has been submitted that the best approach to be followed by states is the balanced approach; a balance should be drawn between the benefits of cryptocurrencies and associated risks. Although regulators in many countries have been unwilling to regulate cryptocurrencies owing to their complex nature, 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. South Africa has done nothing more than publish Position Papers that clarify that cryptocurrencies remain unregulated. Furthermore, the position papers fail 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 has expected answers from the FATF in this regard, as opposed to taking progressive steps to regulate cryptocurrencies at a national level. As discussed above, it is not necessary for South Africa to promulgate a single Act for the regulation of cryptocurrencies; rather, it can integrate such regulation into existing laws. By following the steps that Canada has taken, South Africa can incorporate cryptocurrencies into existing legislation in order to offer immediate relief and protection.[107]

There is clearly a need for regulators to be actively involved with cryptocurrencies to understand how they operate, before they can effectively

[105] Campbell-Verduyn 2017 *Crime, Law and Social Change* 12.
[106] *Ibid.*
[107] Mothokoa *Regulating Crypto-Currencies in South Africa* 55.

regulate it.[108] It is strange that despite the growth of Bitcoin giving rise to a number of risks, South Africa, and many other jurisdictions, have not developed any legal or regulatory frameworks in response. To date, South Africa has not promulgated any legislation regarding the regulation of cryptocurrencies in an attempt to combat money laundering.[109] What is clear is that, without national or international laws and regulations, there will be no clear instructions on how to deal with criminals who launder illicit funds using cryptocurrencies, and no clarity on where to prosecute them. Nonetheless, this article has shown that the existing South African legislative framework is capable of embracing cryptocurrency in its legal structure and of addressing the concerns of money laundering using cryptocurrency.

4 CONCLUSION AND 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. Since cryptocurrency is still a relatively new form of currency, it is not yet typically accepted as a form of payment. This means that criminals still need to convert their cryptocurrency into physical cash, thereby using traditional third-party institutions.[110]

Installing and regulating gatekeepers would require registration as well as bringing dealers and exchanges in line with the scope of legislation, such as the Financial Intelligence Centre Act (FICA),[111] which obliges a person to report suspicious transactions. Currently, various downloadable digital wallets, such as Luno, require the user to disclose 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.[112] Cyberlaundering should be a focus for government, law enforcement agencies, legislatures and researchers. The traditional concepts of currency and money laundering, within the current anti-money-laundering framework, need to be expanded and clarified to expressly include cryptocurrencies and cyberlaundering.[113]

In an attempt to strengthen the fight against money laundering, the FATF revised and updated its Recommendations in 2012. One recommendation 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 a country should work together with its authorities and accountable institutions in order to identify, assess and understand the money-laundering risks that the country may face, as well as

[108] Motelle 2017 *Development Finance Agenda* 8 9.
[109] Nieman 2015 *PER* 1999
[110] De Mink 2018 *De Rebus* 35.
[111] 38 of 2001.
[112] De Mink 2018 *De Rebus* 34.
[113] Leslie *Anti-Cyberlaundering Regulation and Control* 79.

adopt any appropriate anti-money-laundering measures.[114] However, in South Africa, the accountable institutions are not compelled by law to apply this risk-based approach to anti-money-laundering techniques.[115]

There is also a need for uniform international regulation of cryptocurrencies. Because of the global and boundless nature of cryptocurrencies, users may abuse weak anti-money-laundering laws of a 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) should devise a model law that governs the regulation of cryptocurrencies at an international level.[116]

The use of cryptocurrencies is gaining popularity in South Africa, but remains unregulated and as such, is 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.[117] In seeking to regulate cryptocurrencies, it is submitted that South African authorities should first ensure that such regulation will be proportional to the risks. Risks within the cryptocurrency system should be identified and dealt with accordingly. Secondly, it is submitted that exchanges should be accredited and regulated. Furthermore, it is suggested that a centralised platform be established where all initial coin offerings (ICO)[118] available to the public should be listed. Registering all ICO with a central body would allow for monitoring of the credibility and quality of the issuers within the network.[119] 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 expressly extended to include cryptocurrencies, rather than developing new legislation, which may quickly become obsolete due to the rapid development of technology.[120]

In short, legislatures have two options: either amend 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, amending existing legislation would require substantial organisation among regulators.[121] Amending existing definitions may also have an effect on the current financial instruments, services or products. If regulators opt for new regulatory legislation targeting cryptocurrencies, it may result in users being

---

114 Williams *An Analysis of the Critical Shortcomings in South Africa's Anti-Money Laundering Legislation* (2017) 42.

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

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

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

118 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 pre-existing digital token. In exchange for their support, investors receive the new cryptocurrency that is specific to the ICO.

119 Intergovernmental FinTech Working Group http://www.treasury.gov.za/comm_media/press/2020/20200414%20IFWG%20Position%20Paper%20on%20Crypto%20Assets.pdf.

120 FinTech *Intergovernmental FinTech Working Group* 10.

121 FinTech *Intergovernmental FinTech Working Group* 13.

subject to more onerous regulations. It is submitted that the existing regulatory framework may adequately regulate the cryptocurrency network.[122] With reference to the approaches taken in the above-mentioned jurisdictions, several recommendations are made.

Currently, the list of "accountable institutions" in terms of FICA has been amended to include any person or category of person used or likely to be used for the purpose of money laundering.[123] It is submitted that this definition should be expressly amended to include institutions that mine, exchange or hold cryptocurrencies.[124] Furthermore, it is recommended that all institutions dealing with cryptocurrencies, such as exchanges and wallet providers, should comply with the provisions of FICA. These institutions will then have the personal identity records of the user, which would make it easier to follow a trail of suspicious transactions related to money laundering.[125] Furthermore, in terms of the Prevention of Organized Crime Act (POCA),[126] it is submitted that cryptocurrencies should be included in the definition of "property". Extending the definition would mean that a person is guilty of the offence of money laundering if he or she launders 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 legislature should focus less on these organisations and more on regulating exchanges and wallet services. Although there is still much uncertainty regarding the regulation of cryptocurrencies and enforcement thereof in South Africa, it may be helpful for the legislature to consider carefully the current legal framework, with particular reference to its purpose, which may provide guidelines in regulating cryptocurrencies. The current framework includes FICA, anti-money-laundering legislation and the 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, and has been shown to be effective. 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.

---

122 *Ibid.*

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

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

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

126 121 of 1998.