The regulation of cryptocurrencies to combat money laundering crimes in South African banking institutions

Princess Thembelihle Ncube
LLB LLM LLD
Lecturer, Department of Mercantile of Law, University of Pretoria

Ruddy Kabwe
LLB LLM
Attorney of the High Court of South Africa
Lecturer, Department of Mercantile Law, University of Pretoria

SUMMARY

Cryptocurrencies have become an increasingly popular means of conducting financial transactions globally, and South African banking institutions have not been immune to this trend. However, the pseudonymous nature of cryptocurrency transactions has made it an attractive tool for money laundering activities. In response, there is a growing need for South African regulators to establish a legal framework to regulate the use of cryptocurrency to combat money laundering crimes by banking institutions. While the recent amendments to the Financial Intelligence Centre Act 38 of 2001 (as amended) regarding cryptocurrencies are commendable, it is not without deficiencies. The purpose of this article is threefold. First, it examines the current state of cryptocurrency regulation in South Africa. Second, it explores the vulnerabilities that expose the banking system to money laundering using cryptocurrencies. Third, it highlights the need for further development and implementation of regulatory measures to address vulnerabilities identified in this article. This article argues that the current lack of a comprehensive regulatory framework for cryptocurrencies in South Africa leaves the banking system open to potential abuse. The article suggests that South African regulators should focus on three key areas to combat money laundering activities related to cryptocurrency. First, regulatory measures should be implemented to identify and verify the identities of cryptocurrency traders and investors. Second, measures should be put in place to monitor the flow of cryptocurrency transactions and detect suspicious activities. Third, the digital wallets of crypto users should be managed by South African banking institutions.

How to cite: Ncube & Kabwe 'The regulation of cryptocurrencies to combat money laundering crimes in South African banking institutions' 2023 *De Jure Law Journal* 354-375
http://dx.doi.org/10.17159/2225-7160/2023/v56a22

1 Introduction

Money laundering refers to any practice in which illicit perpetrators conceal the original ownership and control of their criminal proceeds by making them appear to have come from legitimate sources.[1] According to the Financial Intelligence Centre Act 38 of 2001 (as amended) (FICA), money laundering is illegal in South Africa.[2] However, very few money laundering cases have been settled or prosecuted by the Financial Intelligence Centre (FIC) since FICA's promulgation. Money laundering is a serious issue that has a negative impact on economies, societies, and financial systems.[3] The current laws and regulations in South Africa aim to prevent and combat money laundering activities, but their adequacy is still a matter of debate. On the other hand, cryptocurrencies have emerged as a popular mode of payment and investment across the globe, and South Africa is no exception. The decentralised nature of cryptocurrencies makes them susceptible to money laundering crimes. South African banking institutions have been at the forefront of addressing this issue by implementing regulations to combat money laundering crimes. The regulation of cryptocurrencies in the South African banking sector is a crucial step toward ensuring a transparent and secure financial system.

Cryptocurrencies have become an increasingly popular tool for conducting financial transactions in recent years.[4] However, this popularity has also led to concerns about their use in illegal activities, such as money laundering. In response, many countries, including South Africa, have begun to regulate cryptocurrencies to combat money laundering. South African banking institutions have been particularly

1 Burchell "Organised Crime and Proceeds of Crime Law in South Africa, Albert Kruger: Book Review" 2010 SAJCJ 177. S 1 of the Financial Intelligence Centre Act 38 of 2001 (as amended) (FICA) defines "money laundering" as "an activity which has or is likely to have the effect of concealing or disguising the nature, source, location, disposition or movement of the proceeds of unlawful activities or any interest which anyone has in such proceeds and includes any activity which constitutes an offence in terms of s 64 of this Act or [ss] 4, 5 or 6 of the Prevention Act."

2 S 4 of the Prevention of Organised Crime Act 121 of 1998 (POCA).

3 For example, money laundering negatively impacts the private sector by using front companies to disguise illegal proceeds, leading to a loss of control over economic policy as it affects 2 – 5% of the world's GDP. It also affects the financial system as launderers reinvest in less detectable schemes resulting in the misallocation of resources and monetary instability. Money laundering can cause economic distortion and instability, exposing recipient countries to reputation risk. It also makes tax collection difficult while reducing a country's revenue. See Fundanga "The role of the banking sector in combating money laundering" 2003 https://www.bis.org/review/r030212f.pdf (last accessed 29 March 2023) at 2; Van Jaarsveld *Aspects of money laundering in South African law* (LLD thesis 2011 UNISA) 193-200; McDowell "The consequences of money laundering and financial crime" 2001 *Economic perspectives* 6-8.

4 Erasmus and Bowden "A Critical Analysis of South African Anti-Money Laundering Legislation with Regard to Cryptocurrency" 2020 *OBITER* 310.

concerned about the use of cryptocurrencies in money laundering activities. To address this issue, South African policymakers have implemented several measures, including the registration of cryptocurrency service providers with the FIC and the introduction of the Intergovernmental Fintech Working Group (IFWG) to regulate the cryptocurrency sector. Furthermore, the IFWG has issued guidance on the regulation of cryptocurrencies, outlining the requirements for service providers to ensure they comply with anti-money laundering regulations. This includes measures such as customer due diligence, transaction monitoring, and reporting suspicious activities to the FIC.[5] The regulation of cryptocurrencies in South African banking institutions is an ongoing process, as the sector continues to evolve and adapt. However, these measures demonstrate South Africa's commitment to combat money laundering and to ensure that the financial sector operates in a safe and secure manner.

Cryptocurrency has rapidly gained popularity as a form of digital currency, offering a decentralised and secure method for performing transactions. However, its pseudonymous nature has also made it a tool for criminal activities, such as money laundering.[6] In South Africa, the issue of money laundering has become a growing concern, making it imperative for the government to find effective solutions to regulate the use of cryptocurrency. This article examines the potential benefits of using cryptocurrency to curb money laundering crimes in South Africa, while also exploring the necessary measures to regulate its use in a manner that protects both the users and the state. This article also explores the current regulatory landscape in South Africa and the measures taken by banks to prevent money laundering crimes through cryptocurrency. For purposes of this article, the terms “cryptocurrency” and “crypto asset” are used interchangeably.

2 Overview of the regulation of money laundering crimes in South Africa

2 1 The Prevention of Organised Crime Act 121 of 1998

The Prevention of Organised Crime Act 121 of 1998 (POCA) came into effect in 1999. The POCA was enacted to regulate organised crime in South Africa.[7] In this regard, the POCA prohibits racketeering activities, criminalises money laundering, and requires banks to report certain information.[8] The POCA was also enacted to provide for the recovery of

5 S 21(1) read with s 21A of FICA.
6 Kempen “Investigations: When Criminals Use the Dark Web and Virtual Currency to Hide their Illegal Activities” 2018 *Servamus Community-based Safety and Security Magazine* 54.
7 Ncube *The regulation and use of artificial intelligence to combat money laundering in South African banking institutions* (LLD thesis 2022 NWU) 9-10.
8 Ss 2 and 4 of the POCA.

the proceeds of crime. The POCA also criminalises activities related to benefiting from crime and outlines civil proceedings aimed at forfeiting the benefits of crime to the state.[9]

Money laundering is defined under the POCA and encompasses several offences, including concealing, arranging, acquiring, using, or possessing illegal proceeds.[10] In this regard, under POCA, to be charged with money laundering, a person must know or reasonably should have known that the property involved is derived from illegal activities.[11] Knowledge is a requirement for criminal liability, but the accused can argue that they were unaware of the illegal origin of the property.[12] The authors submit that prosecuting authorities in South Africa find it challenging to prove that money laundering perpetrators knew the property at issue was illegal, which may explain the low number of money laundering cases investigated and convictions obtained.

Furthermore, the POCA provides that a person is guilty of money laundering when he or she performs any act in connection with property that forms part of the proceeds of unlawful activities whether it is performed independently or with another person.[13] For purposes of the POCA, "property" means

> money or any other moveable, immovable, corporeal or incorporeal thing and includes any rights, privileges, claims and securities and any interest therein and all proceeds thereof.[14]

In this regard, a third party should either know or reasonably ought to have known that the money laundering perpetrator obtained the proceeds from illegal activities.[15] Any person who knowingly acquires, possesses, or uses the property that is part of the proceeds of another person's unlawful money laundering activities will be liable for an offence.[16] Assisting and engaging or co-working with a money laundering offender is a money laundering offence whether such offence is committed in South Africa or elsewhere to avoid prosecution or to remove or diminish any property acquired directly, or indirectly, as a result of the commission of an offence.[17]

9 Ss 37 and 48 of the POCA.
10 S 6 of the POCA.
11 Van der Linde "The Overlap between the Common Law and Chapter 4 of the Prevention of Organised Crime Act: Is South Africa's Anti-gang Legislation Enough?" 2020 *SAJCJ* 280.
12 S 4 of the POCA.
13 S 4(b) of the POCA.
14 See definition of "property" in s 1 of the POCA.
15 Ss 5(a)-(b) of the POCA.
16 S 6 of the POCA.
17 S 4(b)(ii) of the POCA.

2 2 The Protection of Constitutional Democracy against Terrorist and Related Activities Act 33 of 2004

South Africa enacted the Protection of Constitutional Democracy against Terrorist and Related Activities Act 33 of 2004 (POCDATARA) to combat terrorism-related activities, and the financing of terrorism and related activities and align government action against money laundering.[18] POCDATARA came into operation in 2005. Furthermore, POCDATARA was enacted to give effect to international instruments dealing with terrorist and related activities in South Africa. Interestingly, POCDATARA does not expressly prohibit money laundering. Instead, POCDATARA prohibits terrorist activities and offences associated with such activities. Consequently, money laundering activities may be outlawed under POCDATARA if used to commit or help offenders to commit terrorism.[19]

Under POCDATARA, any person who engages in money laundering to finance terrorist activities is liable for an offence.[20] Furthermore, if a person suspects that someone intends or has committed terrorism or related offences like money laundering, they must report the suspicion to the police as soon as possible to any police official in South Africa.[21] Failure to report suspicions of such offences is itself a money laundering offence.[22] However, POCDATARA alone is not enough to effectively curb money laundering, as it lacks provisions for customer due diligence, record-keeping obligations, and a risk-based approach to client identification. Regulating money laundering under different statutes can lead to inconsistent enforcement.

2 3 FICA (as amended)

FICA is the principal legislative framework governing anti-money laundering laws in South Africa.[23] FICA was enacted to curb financial crimes, such as money laundering, tax evasion, and terrorist financing activities in South African banking institutions.[24] Furthermore, FICA was enacted to conform to international standards for the regulation of anti-money laundering laws to combat money laundering effectively in South Africa.[25]

18 Nkoane "The Prevention of Organised Crime Act: The Proving of 'Instrumentality' in Cases of Obscured use of Intangible Things" 2016 *Stell LR* 185.
19 S 3 of POCDATARA.
20 Cachalia "Counter-terrorism and International Cooperation against Terrorism – An Elusive Goal: A South African Perspective" 2010 *SAJHR* 512.
21 S 12(1)(a)(b) of POCDATARA.
22 S 12(2) of POCDATARA.
23 De Koker *South African Money Laundering and Terrorist Financing Law* (2014) 32-33.
24 See the preamble of FICA.
25 Duri and Matasane "Regulation of Beneficial Ownership in South Africa and Zimbabwe" 2017 *J Anti-Corruption Law* 178.

2 3 1 The establishment of the FIC

The FIC is South Africa's national centre for gathering, analysing, and disseminating financial intelligence.[26] The FIC was established by FICA to identify proceeds of crime, combat money laundering, and the financing of terrorism in South Africa.[27] The FIC enforces money laundering laws to protect South African banking institutions from illicit money laundering offenders.[28] The FIC is responsible for supervising and enforcing compliance with South African money laundering laws. More about the FIC will be discussed under a different heading in this article.

2 3 2 Money laundering offences under FICA

FICA requires banks to verify a client's identity before conducting any business, to curb money laundering in South Africa's banks.[29] Banks must identify potential clients and require proof of identity and residence, a process known as Know Your Customer (KYC).[30] KYC assists in assessing and monitoring risks associated with clients to detect money laundering practices.[31] Banks must also establish the nature of their client's business to reduce the risk of financial fraud and financing criminal organisations.[32] Failure by banks to identify clients can result in administrative sanctions. [33]

FICA distinguishes between business relationships and single transactions.[34] Transactions below R5000 are not considered single transactions under FICA.[35] Failure to disclose clients' identities and transactions makes banks liable for administrative action.[36] Banks must terminate existing or proposed business relationships and cease all transactions with clients/potential clients if unable to establish and verify their identities to ensure FICA compliance.[37]

---

26 See FIC "Notice 2017 A New Guidance on the Amended Reporting Requirements in terms of the Money Laundering and Terrorist Financing Control Regulations" www.fic.gov.za/media/Pages/General%20Notices.aspx (last accessed 2021-04-17).
27 Ss 2(1)(a)-(c) of FICA.
28 Lutescu and Bucur "Money Laundering – An International Phenomenon" 2008 *AI JJS* 156.
29 See s 21 of FICA.
30 S 21(1) read with s 21A of FICA; see related discussion by Goredema and Monsti "Towards Effective Control of Money Laundering in Southern Africa-Some Practical Dilemmas" 2002 *ASR* 8.
31 S 21 of FICA; see related discussion by De Koker "Client Identification and Money Laundering Control: Perspectives on the Financial Intelligence Centre Act 38 of 2001" 2004 *Tydskrif vir die Suid-Afrikaanse* 716.
32 S 21B(1) of FICA.
33 S 46 of FICA.
34 See s 1 of FICA.
35 S 1A of FICA; see related discussion by Kersop and Du Toit "Anti-Money Laundering Regulations and the Effective Use of Money in South Africa" 2015 *PELJ* 1620.
36 S 46 of FICA.
37 S 21E of FICA.

FICA provides for customer due diligence.[38] The purpose of customer due diligence is for a bank to know who its clients are and to understand their business with them.[39] Put differently, customer due diligence was incorporated into FICA to require South African banking institutions to know their customers and to eliminate the use of anonymous accounts.[40] FICA's efforts to combat money laundering in South African banking institutions are commendable, as it facilitates the identification of illicit money laundering perpetrators.

FICA requires banks to collect and keep information about clients, including name, address, nationality, ID, signature, occupation, and account details.[41] Moreover, banks must also retain copies of documents used to verify identity[42] and, in the case of a business relationship, record the nature and purpose of the relationship and the source of funds.[43] The aim is to identify desirable and undesirable customers and improve transaction monitoring to prevent money laundering in South African banks. Keeping records of all customers goes a long way toward ensuring effective transaction monitoring and curbing money laundering in South African banks. FICA requires banks to keep records of every transaction, whether it is a single transaction or part of a business relationship.[44] The records must reflect the amount, currency, date, parties, nature of the transaction, business correspondence, and identifying particulars of all accounts related to the transaction.[45]

3 Understanding the nature of cryptocurrencies

A cryptocurrency is a form of virtual currency that is a decentralised peer-to-peer network-based medium of exchange.[46] A cryptocurrency incorporates the principles of cryptography to implement a distributed, decentralised, secure information economy.[47] Cryptocurrencies came to

38 Henning and Ebersohn "Insider Trading, Money Laundering and Computer Crime" 2001 Transactions of the Centre for Business Law: Combating Economic Crime 115; see related discussion by Njotini "The Transaction or Activity Monitoring Process: An Analysis of the Customer Due Diligence Systems of the United Kingdom and South Africa" 2000 *Obiter* 566-567.

39 Hugo and Spruyt "Money Laundering, Terrorist Financing and Financial Sanctions: South Africa's Response by Means of the Financial Intelligence Centre" 2018 *JSAL* 235.

40 Cox *Handbook of Anti-Money Laundering* (2014) 315.

41 Ss 21-21H of FICA.

42 S 22(1) of FICA.

43 See ss 22(2)(a)(i)-(iii) of FICA.

44 See s 22A (1) of FICA; see related discussion by De Koker "Money Laundering Control and Suppression of Financing of Terrorism: Some Thoughts on the Impact of Customer Due Diligence Measures on Financial Exclusion" 2006 *Journal of Financial Crime* 352.

45 Ss 22A(2)(a)-(e) of FICA.

46 Comolli and Korver "Surfing the first wave of cryptocurrency money laundering" 2021 *Department of Justice Journal of Federal Law and Practice* 184.

47 Financial Action Task Force (FAFT) *Virtual currencies: key definitions and potential AML/CFT Risks* (2014) 5.

the fore after the events of the 2008 financial crisis. Although there are various types of cryptocurrencies currently in circulation, the most famous of those is bitcoin.[48] Bitcoin is an open and interoperable protocol that is not controlled by a single party.[49] Bitcoin's popularity over other cryptocurrencies stems from the latter's first-mover advantage.[50]

Bitcoin users transact directly with each other on an online network without the need for a third-party actor like a financial intermediary.[51] Rather, actors[52] rely on the architecture of the distributed ledger to process cryptocurrencies. An actor gains access to the distributed ledger using an Internet-enabled computer. Once an actor is connected to the Bitcoin[53] network, they can view all the transactions on the network since its inception. If an actor wants to create new bitcoins, they can achieve this by solving a complex mathematical problem to verify the transactions and information embedded in the blockchain.[54] The blockchain is a series of "blocks" that contain sequential storage of data.

Bitcoin transactions are verified, and double spending is prevented using public and private keys.[55] A private key is akin to a secret password. In theory, no other user should possess another's private key. A public key is an alphanumeric address identifiable to each user. When an actor wants to send bitcoins to another actor, the sender sends a bitcoin transaction that contains the recipient's public key.[56] The sender signs the bitcoin transaction with their private key. In doing so, the sender authorises the transaction.[57] A third-party actor can ascertain the origin of a transaction by verifying that the public key corresponds with the sender's private key, thereby associating the bitcoins with the recipient's address.[58] Once a transaction has been authenticated, it is recorded on the blockchain.[59] The records of the transactions on the Bitcoin network are stored on the blockchain governed by an underlying free and open-source software called the Bitcoin protocol.[60]

48 Other popular cryptocurrencies include Monero, LiteCoin, and Dogecoin.
49 De Filippi and Wright *Blockchain and the Law: The Rule Code* (2018) 21.
50 First mover advantage occurs when a product or company obtains a competitive advantage over rivals by being the first to market a specific product. See Van der Auwera *et al Financial Risk Management for Cryptocurrencies* (2020) 19.
51 Brito *et al The Law of Bitcoin iUniverse* (2015) 7.
52 For purposes of this article, an actor refers to a person or a group of persons that perform transactions using bitcoins (cryptocurrencies).
53 When written with an uppercase "B", Bitcoin refers to a decentralised global payment network. When written with a lowercase "b", bitcoin refers to the bitcoin cryptocurrency. See Brito *et al* (2015) 7.
54 Brito *et al* (2015) 9.
55 Brito *et al* (2015) 7.
56 Brito *et al* (2015) 8.
57 As above.
58 As above.
59 As above.
60 De Filippi and Wright (2018) 21.

An actor uses a wallet to send and receive bitcoins with other users on the network. A wallet is an account that holds a person's bitcoins. Generally, wallets are stored on personal computers or third parties can maintain the wallets by using online applications.[61] For a person to transact on the Bitcoin network, the network must be able to link the inputs and outputs to and from a person's wallet.[62] As such, an actor can use different wallets to transact but a transaction that was orchestrated in the past will always be connected to transactions connected in the present.[63] This can be achieved if law enforcement agencies succeed in tying the wallet address to the transactions.[64] This is also made possible because the Bitcoin ledger is immutable in nature. Basically, the transactions that are processed and stored on the ledger cannot be altered. It is impossible for a single actor to erase transactions stored on the distributed ledger. However, the authors submit that in South Africa, achieving this level of traceability is challenging due to the current lack of technical expertise within the local law enforcement agencies required for tracking and tying transactions on a distributed ledger. Notably, transactions on the Bitcoin network are pseudonymous in nature, meaning the identities of the actors are not known to each other. Actors rely on cryptography to create pseudonymous Bitcoin accounts.[65]

Another important feature of the Bitcoin network is that it is highly transparent. Anyone who has access to a computer and an Internet connection can access the Bitcoin network anywhere around the world. A person can download a full copy of the blockchain to go through all the recorded transactions.[66] Due to the Bitcoin network's open and transparent nature, it is difficult for a single actor to shut down the network. For as long as one copy of the Bitcoin blockchain is stored on another computer, the Bitcoin network will continue to exist.[67]

61 As above.
62 Comolli and Korver 2021 *DJJFLP* 185.
63 Comolli and Korver 2021 *DJJFLP* 185.
64 As above.
65 De Filippi and Wright (2018) 21.
66 De Filippi and Wright (2018) 22.
67 As above.

4 The regulation of cryptocurrencies in South Africa

The regulation of cryptocurrencies in South Africa can be traced to the work done by the IFWG. The IFWG[68] was created in 2016

> to understand the growing role of Financial Technology (FinTech)'s and innovation in the South African financial sector and explore how regulators can proactively assess emerging risks and opportunities in the market.[69]

The IFWG made several recommendations regarding South Africa's approach to regulating cryptocurrencies.[70] For the purposes of this article, the authors limit the discussion to the recommendations pertaining to the crypto asset service providers (CASPs). As the name suggests, CASPs are entities that provide a platform for actors to trade and exchange in cryptocurrencies. The services include: (a) trading, converting, or exchanging cryptocurrencies into other cryptocurrencies; (b) trading, conversion, or exchanging cryptocurrencies into fiat currency; (c) trading, conversion, or exchanging fiat currency into cryptocurrencies; and (d) the buying, selling, or transferring of cryptocurrencies including the use of cryptocurrencies vending machine facilities.[71] According to the IFWG, the objectives of regulating CASPs in South Africa include combating illegitimate cross-border financial flows, money laundering/terrorist financing, and ensuring the efficiency and integrity of financial markets. Additionally, it promotes financial inclusion efforts and the advancement of technological innovation in a responsible and balanced manner.[72]

On 29 November 2022, schedule 1 of FICA was amended to include persons who carry on a business involving cryptocurrencies as accountable institutions.[73] Paragraph 22 of schedule 1 now reads:

> A person who carries on the business of one or more of the following activities or operations for or on behalf of a client: *(a)* Exchanging a crypto asset for a fiat currency or vice versa; *(b)* exchanging one form of crypto asset for another; *(c)* conducting a transaction that transfers a crypto asset from one crypto asset address or account to another; *(d)* safekeeping or administration of a crypto asset or an instrument enabling control over a

68 Currently, the IFWG consists of: National Treasury, the FIC, the Financial Sector Conduct Authority, the National Credit Regulator, the South African Reserve Bank, the South African Revenue Service, and the Competition Commission.

69 See IFWG "About us" 2023 https://www.ifwg.co.za/Pages/About-Us.aspx (last accessed 2023-03-08).

70 See IFWG "Crypto Assets Regulatory Working Group: Position paper on crypto assets" 2021 https://www.treasury.gov.za/comm_media/press/2021/IFWG_CAR%20WG_Position%20paper%20on%20crypto%20assets_Final.pdf (last accessed 2023-03-08) (hereinafter IFWG 2021) at 3.

71 IFWG 2021 at 17.

72 IFWG 2021 at 28-29.

73 National Treasury, GN 2800 in GG 47596 of 22 November 2022 (the commencement date is 19 December 2022).

> crypto asset; and *(e)* participation in and provision of financial services related to an issuer's offer or sale of a crypto asset.[74]

The amendment has profound implications for persons who conduct transactions with cryptocurrencies. For example, a person[75] will be required to comply with legislation requirements regarding anti-money laundering and combating the financing of terrorism (AML/CFT).[76] A cryptocurrency trader is now required to register with FIC, conduct customer identification and verification, perform due diligence, keep records of client and transactional information, monitor suspicious and unusual activity, report cash transactions above the applicable threshold, and report control of property that might be linked to terrorist activity or terrorist organisations.[77] Moreover, a cryptocurrency trader must conduct a risk-based approach to customer identification and verification and they must conduct AML/terrorist financing risk assessment in respect of their institution or business.[78] The approach includes distinguishing different categories of risk and applying enhanced customer due diligence where business with customers is deemed as a higher risk and simplified customer due diligence where business with customers is deemed as a lower risk.[79] Notably, a cryptocurrency trader must obtain, hold, require, and accurate beneficiary information[80] and originator information for every cryptocurrency transaction. This information must be provided to the relevant regulatory or law enforcement authorities when requested to do so.[81]

5 Challenges in regulating cryptocurrencies

5 1 The lack of a uniform definition

One of the challenges with cryptocurrency regulation is the lack of a universally accepted definition.[82] Cryptocurrencies have properties

74 See para 22 of sched 1 of FICA.
75 Although not explicitly stated in FICA, the term person includes natural and juristic persons.
76 IFWG 2021 at 3.
77 As above.
78 IFWG 2021 at 33.
79 As above.
80 S 1 of FICA defines "beneficial owner" as: "(a) means a natural person who directly or indirectly – (i) ultimately owns or exercises effective control of – (aa) a client of an accountable institution; or (bb) a legal person, partnership or trust that owns or exercises effective control of, as the case may be, a client of an accountable institution; or (ii) exercises control of a client of an accountable institution on whose behalf a transaction is being conducted; and (b) includes– (i) in respect of legal persons, each natural person contemplated in s 21B(2)(a); (ii) in respect of a partnership, each natural person contemplated in s 21B(3)(b); and (iii) in respect of a trust, each natural person contemplated in [ss] 21B(4)(c), (d) and (e)."
81 IFWG 2021 at 33-34.
82 See Sotiropoulou and Guegan "Bitcoin and the challenges for financial regulation" 2017 *Capital Markets Law Journal* 471.

similar to fiat money, commodities, and payment systems. This influences their legal and regulatory treatment, particularly in ascertaining which national agencies should regulate them.[83] It is possible for different authorities to classify cryptocurrencies according to their own priorities.[84] For example, the Value-Added Tax Act 89 of 1991 (the VAT Act) classifies cryptocurrencies as a financial service[85] whereas FICA classifies cryptocurrencies as a digital asset that has value.[86] Different approaches are followed in other jurisdictions where a formal classification is not followed, instead, the focus of regulation lies in the nature of the transaction.[87]

5 2 Lack of monitoring capabilities

Cryptocurrencies operate outside the financial system, making it difficult for the relevant authorities to monitor their operations.[88] Authorities cannot determine the identity of the users because of the opaque and pseudonymous nature of Bitcoin transactions.[89] The challenge is compounded when actors use anonymisers on the Bitcoin network. Anonymisers are tools and services such as darknets and mixers designed to obscure the source of Bitcoin transactions and facilitate anonymity.[90] It is also possible for users to transact on the Dark Web (or "darknet"). The Dark Web

> is 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 to ensure anonymity.[91]

Once users access or transact on the darknet, it is almost impossible for law enforcement authorities to identify them.

5 3 The decentralisation of cryptocurrencies

The Bitcoin network is decentralised in nature. Transactions can be orchestrated anywhere around the world. This feature makes it difficult for the relevant authorities to regulate the network and all its transactions.[92] Law authorities cannot enforce national laws if they do not know who the user is and where the transaction took place.

83 He *et al* "Virtual Currencies and Beyond: Initial Considerations" 2016 https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf (last accessed 2023-03-19) (hereinafter He *et al* 2016) at 24; Sotiropoulou and Guegan 2017 *CMLJ* 471.
84 He *et al* 2016 at 24.
85 See s 2 of the VAT Act.
86 See para 22 of sched 1 of FICA.
87 He *et al* 2016 at 24.
88 He *et al* 2016 at 5.
89 He *et al* 2016 at 24; Sotiropoulou and Guegan 2017 *CMLJ* 471.
90 FATF (2014) 6.
91 Erasmus and Bowden 2020 *Obiter* 315.
92 He *et al* 2016 at 25.

Moreover, it is difficult to enforce laws and regulations in an online environment such as the Bitcoin network.[93]

5 4 The lack of a central authority

One of the challenges that is associated with regulating cryptocurrencies is the lack of a central authority. Cryptocurrencies operate on a decentralised network that is capable of transcending borders. As such, no single authority or jurisdiction controls the Bitcoin network. Another important aspect to consider is the fact that cryptocurrencies are mutually incompatible with the current existing frameworks. It is difficult to impose direct regulation on a central authority or a person in a Bitcoin network.[94] Cryptocurrencies operate outside the scope of market infrastructures and financial institutions, making it more difficult for any regulation to take place.[95] Nabilou argues that it is difficult to regulate cryptocurrencies because there is a plethora of active players that play significant roles in the cryptocurrency sphere.[96] Currently, the cryptocurrency sphere consists of users, wallet providers, miners, developers, exchanges, and trading platforms.[97] It can be argued that the most feasible model of regulation consists of focusing on established and known financial institutions or other legal entities.[98] For example, persons who provide platforms for the exchange of cryptocurrencies are considered to be accountable institutions in South Africa.[99] As a result, these persons are required to verify the identities of clients (cryptocurrency actors) and maintain a record of cryptocurrency transactions.[100] This type of regulation ensures that all the difficult aspects relating to cryptocurrencies and the Bitcoin network are left to institutions and other known parties.[101] The regulation imposed on a central authority linked to cryptocurrency users helps to regulate crypto-related transactions.

5 5 High volatility

Cryptocurrencies' value in this global network is determined by what a willing buyer will pay to a willing seller in an open market.[102] This implies that the price of bitcoins is affected by the amount of bitcoins

93 As above.
94 Nabilou "How to regulate bitcoin: decentralized regulation for decentralized cryptocurrency" 2019 *International Journal of Law and Information Technology* 278.
95 Nabilou 2019 *IJLIT* 277-278.
96 Nabilou 2019 *IJLIT* 278.
97 As above.
98 As above.
99 See para 22 of sched 1 of FICA read with GN 2800 in GG 47596 of 22 November 2022.
100 S 21 read with s 22 of FICA.
101 Nabilou 2019 *IJLIT* 278.
102 Brito *et al* (2015) 7.

currently in the market and how much people are willing to buy them.[103] According to Reiff, bitcoin is limited to 21 million coins and prices are likely to climb if the circulating supply approaches the limit.[104] The value of cryptocurrencies is not backed by any government or state.[105] This propels cryptocurrencies to extreme levels of price volatility and unpredictability because the price is easily influenced by external factors. For example, the price of bitcoin can easily be influenced by the amount of "news" it receives.[106] Generally, if the "news" around bitcoin is positive the price increases. If, on the other hand, the "news" is negative, the price of bitcoin is likely to go down.

5 6 Technical difficulties

The technology around the bitcoin network is still in its infancy. It is quite possible that the technology is not fully developed yet. There is a possibility that the Bitcoin network grows as more use cases materialise. As a result, it is difficult for authorities to envisage every possible scenario when regulating cryptocurrencies because of their immaturity. Another challenge that poses a challenge to regulation is the fact that there is little personnel that specialise in cryptography. Cryptography is a key component of the bitcoin network. Cryptography is a technique that disguises and reveals information by using mathematics.[107] Cryptography ensures that the identity of an actor is "hidden" when performing transactions and cryptography ensures that information is secured on the network.[108] Another challenge posed by cryptocurrencies is the issue of scalability. Simply put, cryptocurrency transactions are slower than traditional payment methods. This is partly due to the proof-of-work consensus mechanism. Proof-of-work consumes a vast amount of energy.[109] During the mining process, all nodes are required to validate to ensure that a transaction is accurate before it is added to a new block. This requires a substantial amount of computational power.[110] To resolve this issue, other consensus mechanisms such as proof-of-stake can be used because the latter is more efficient and reduces the amount of energy used.[111]

103 Reiff "Why is Bitcoin volatile?" 2022 https://www.investopedia.com/articles/investing/052014/why-bitcoins-value-so-volatile.asp (last accessed 2023-03-02).
104 As above.
105 Brito *et al* (2015) 7.
106 See Van der Auwera *et al* (2020) 105.
107 Van der Auwera *et al* (2020) 6.
108 As above.
109 Van der Auwera *et al* (2020) 10.
110 Van der Auwera *et al* (2020) 12.
111 Van der Auwera *et al* (2020) 12-13.

6 The impact of cryptocurrencies on money laundering

To understand how the use of cryptocurrencies impacts money laundering, one first needs to understand how money laundering works. Generally, money laundering is divided into three phases: placement, layering, and integration. Placement is the process of getting the proceeds of criminal activities into a financial institution, a money service business, or an informal value transfer.[112] After an actor places the illegal proceeds into an institution, they conduct transactions in order to hide the nature, source, and ownership of the proceeds.[113] Layering involves transferring the proceeds from one person to another by making use of an electronic funds transfer.[114] Integration is the final phase in the money laundering process. During the process, an actor integrates the illegal proceeds into their daily lives. They purchase vehicles or property in order to make detection difficult or impossible.[115]

In the context of cryptocurrencies, placement occurs when an actor acquires bitcoins using fiat money. The person goes to a trading platform or cryptocurrency exchange platform to convert the illegal proceeds to bitcoins. Often the conversion takes place on platforms that do not adhere to anti-money laundering laws or KYC rules, making the laundering seamless because of anonymity.[116] Here, a person can open multiple pseudonymous wallets. It costs almost nothing to open a wallet account and there is a low risk of placing proceeds of illegal activities inside the wallet.[117] The layering process is characterised by making use of anonymisation services such as the dark web to commit money laundering activities. It is difficult for law enforcement authorities such as the FIC to identify and trace these actors because these services protect a person's privacy.[118] Ordinarily, illicit bitcoin transactions could have been traced on the bitcoin blockchain by tracking digital footprints on the network.[119] Law enforcement agencies can, for example, use a wallet address to link an individual to all the transactions stored on the bitcoin blockchain.[120] During the layering process, it is easy for an actor to transfer bitcoins between wallets. Integration occurs when actors develop online firms that accept bitcoin payments to turn "dirty bitcoins" into "clean bitcoins".[121] In doing so, actors hide their sources of income

112 Comolli and Korver 2021 *DJJFLP* 188.
113 As above.
114 Comolli and Korver 2021 *DJJFLP* 188-189.
115 Comolli and Korver 2021 *DJJFLP* 189.
116 Wronka "Cyber-laundering": the change of money laundering in the digital age" 2022 *Journal of Money Laundering Control* 334.
117 Rysin and Rysin "The money laundering risk and regulatory challenges for cryptocurrency markets" in Dziura *et al* (eds) *Restructuring Management: models – changes – development* (2020) 195.
118 Wronka 2022 *JMLC* 334.
119 As above.
120 Comolli and Korver 2021 *DJJFLP* 185.
121 Wronka 2022 *JMLC* 334.

and move the funds across borders without detection.[122] Service providers and other role players accept cryptocurrencies when exchanged for goods and services.[123]

The decentralised nature of the Bitcoin network makes it conducive to the proliferation of money laundering activities. An actor can move funds nationally and internationally without interacting with a central authority like a financial institution or money services business.[124] Moreover, a central authority cannot enforce any rules or regulations if an actor uses cryptocurrencies to launder money.[125] For this reason, a central authority or money service business is not able to identify the actors involved in illegal transactions on a Bitcoin network. An actor can perform transactions without providing identification to a central authority.[126] Moreover, the pseudonymous aspect of cryptocurrencies prevents transactions from being monitored, providing a platform for illegal transactions to take place outside the bounds of the law, and allowing actors to access "clean cash".[127] An actor can swap "clean cash" with cryptocurrencies at a cryptocurrency exchange platform. The challenge is compounded by the lack of rules unveiling the pseudonymity associated with cryptocurrencies. The absence of rules regarding the unveiling of pseudonymity makes it difficult for rules that could have been enforced.[128]

7 Cryptocurrencies and money laundering: where is the source?

Contrary to popular belief, money laundering using cryptocurrencies is not limited to cryptocurrency exchanges or trading platforms. A cryptocurrency exchange is "persons or entities who offer exchange services to cryptocurrency users usually against payment of a certain fee."[129] The exchange platforms allow users to sell cryptocurrencies for fiat money or buy new cryptocurrencies with fiat money.[130] Examples of popular exchanges include Luno, Kraken, Bitfinex, and Coinbase GDAX. Trading platforms are "marketplaces that bring together different cryptocurrency users that are either looking to buy or sell coins, providing them with a platform on which they can directly trade with

122 As above.
123 Rysin and Rysin (2020) 195.
124 Comolli and Korver 2021 *DJJFLP* 185.
125 As above.
126 As above.
127 Houben and Snyers "Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion" 2018 https://repository.uantwerpen.be/docman/irua/80a4a6/152140.pdf (last accessed 2023-03-01) (hereinafter Houben and Snyers 2018) at 53.
128 Houben and Snyers 2018 at 54.
129 Houben and Snyers 2018 at 26.
130 As above.

each other."[131] These platforms are not controlled by a single entity or company that oversees and processes all trades, but are operated by software.[132] These platforms are often referred to as peer-to-peer exchanges (P2P exchanges) because it allows users to directly transact with each other.[133] A popular example is *LocalBitcoins*.[134]

There are other platforms that foster the proliferation of money laundering using cryptocurrencies. The authors suggest that without AML and KYC regulations, platforms facilitating cryptocurrency transactions may be targeted for money laundering. If the platform is located outside South Africa and not subject to AML rules, enforcement becomes difficult, particularly if there is no extraterritorial application. This challenge is compounded if the company is not subject to AML rules in its country of residence or in the country of incorporation.

Generally, banking institutions are the primary target of actors seeking to launder money through criminal means.[135] The proceeds of money laundering enter the banking system through cash, deposits made over the counter (OTC), electronic funds transfer (EFTs), and letters of credit from businesses.[136] The money laundering process is successful once the benefits of crime are presented to a legitimate business in a manner that conceals the nexus to the crime.[137] Contextually, actors involved in money laundering use banking institutions to convert cryptocurrencies into fiat money for safekeeping.[138] In doing so, actors continue to send funds to other locations or use the funds to purchase goods and services.[139]

The first platform that is often overlooked as a money laundering platform is a cryptocurrency kiosk. A cryptocurrency kiosk (crypto asset vending machine facilities) is a physical machine, accessible in locations like shopping malls, where persons purchase and sell cryptocurrencies.[140] A cryptocurrency kiosk operates like an automated teller machine (ATM). A user can use a cryptocurrency kiosk to launder money without detection because the kiosk has no links to a bank account or a cryptocurrency exchange.[141] Cryptocurrency kiosks are run by kiosk companies that often operate without AML and KYC rules.[142] Although cryptocurrency kiosks are not as popular as cryptocurrency

131 Houben and Snyers 2018 at 27.
132 As above.
133 As above.
134 See LocalBitcoins "About LocalBitcoins" 2023 https://localbitcoins.com/about (last accessed 2023-03-20). Note that LocalBitcoins has ceased trading since 9 February 2023.
135 Van Jaarsveld 177-178.
136 As above.
137 Van Jaarsveld 178.
138 Comolli and Korver 2021 *DJJFLP* 210.
139 As above.
140 Comolli and Korver 2021 *DJJFLP* 208.
141 Comolli and Korver 2021 *DJJFLP* 209.
142 As above.

exchange platforms in South Africa, the authors submit that it only takes a kiosk to launder money using cryptocurrencies. One feature of a cryptocurrency kiosk is that they do not require identification to operate but may require a phone number.[143] An actor can even make use of a third party to transact on their behalf. The third-party deposits cash in the cryptocurrency kiosk which the machine converts into cryptocurrencies. If the person does not have a crypto wallet, the cryptocurrency kiosk creates one for them. It is difficult to connect actors to transactions because a receipt of transactions can easily be destroyed.[144]

Second, an actor can use a cryptocurrency gambling website or "casino" to launder money.[145] An actor can launder money through cryptocurrency gambling sites because these sites facilitate betting denominated in bitcoin or other cryptocurrencies.[146] Once on the site, an actor can trade ill-gotten cryptocurrencies with credit or virtual chips.[147] Anyone can operate a cryptocurrency gambling website. In fact, these gambling websites can be operated by a person or entity that is not located in South Africa making it difficult to enforce AML and KYC rules.

Third, and as alluded to above, money laundering can take place on peer-to-peer (P2P) platforms. In a P2P exchange, an exchanger transfers the equivalent amount of bitcoins to a recipient's digital wallet in exchange for the equivalent amount in cash.[148] This method is popular because it does not require an actor to produce identification, nor does it require the use of an intermediary or banking institution. The P2P exchange allows an actor to exchange illegally obtained funds with cryptocurrencies. Thereafter, the "dirty" cryptocurrencies can be used to purchase property or goods from a cryptocurrency payment platform.

Fourth, money can be laundered using cryptocurrency debit cards and payment apps. There are companies that provide software that enables retail merchants to accept cryptocurrencies as a payment method.[149] When a payment is required, a customer loads their app wallet or debit card with cryptocurrencies, then the software processor converts the cryptocurrency into fiat money. The converted funds are sent to the merchant less a commission.[150] Companies also provide debit cards

143 Teichmann and Falker "Money laundering via cryptocurrencies – potential solutions from Liechtenstein" 2021 *Journal of Money Laundering Control* 94.
144 As above.
145 Comolli and Korver 2021 *DJJFLP* 212.
146 Comolli and Korver 2021 *DJJFLP* 212-213.
147 Comolli and Korver 2021 *DJJFLP* 213.
148 Comolli and Korver 2021 *DJJFLP* 203.
149 Comolli and Korver 2021 *DJJFLP* 211.
150 Fanusie "Merchant Crypto Payments: A New National Security Frontier" 2021 https://www.lawfareblog.com/merchant-crypto-payments-new-national-security-frontier (last accessed 2023-03-14); Comolli and Korver 2021 *DJJFLP* 211.

linked to cryptocurrency bank accounts. These cards can be used to pay for goods and services online or in person.[151]

Fifth, cryptocurrencies can be bought OTC from traders.[152] An OTC trade relies on OTC brokers to facilitate negotiations between a willing buyer and a willing seller over a computer or a phone.[153] One of the reasons why OTC trades are so popular is that they provide anonymity. OTC trades are not available to the public, enabling large sums of money to be moved quietly without any interruption.[154] The anonymous nature of the transactions makes it conducive for actors to launder money using cryptocurrencies without fear of being caught by law enforcement agencies.

Sixth, an actor can launder money using cryptocurrencies by making use of mixing services. Mixing services are

> entities that attempt to obfuscate the source or owner of particular units of cryptocurrency by mixing the cryptocurrency of several users prior to delivery of the units to their ultimate destination.[155]

In simple terms, banking institutions provide a hub for actors to send their cryptocurrencies to a single account where funds are mixed and sent to different cryptocurrency wallets. The main component of these operations is money laundering.[156] A mixer can offer their services in exchange for one to three per cent of the amount that is being mixed.[157] A mixer can require an actor to have three separate crypto wallets: one regular wallet ("clean wallet") on the Internet and two other wallets on the dark web.[158] A typical transaction commences when an actor transfers cryptocurrencies in a darknet wallet. The mixer divides the cryptocurrencies into different darknet addresses, making it difficult to link them to the original Bitcoin address or to each other.[159] After the process is complete, the cryptocurrencies are transferred to a darknet wallet before they are transferred back into the original "clean wallet".[160]

151 Comolli and Korver 2021 DJJFLP 211.
152 Medalie "What is OTC cryptocurrency trading?" 2019 https://blog.kaiko.com/what-is-otc-cryptocurrency-trading-66d725c867f (last accessed 2023-03-14) (hereinafter Medalie 2019); Comolli and Korver 2021 *DJJFLP* 202.
153 Medalie 2019.
154 As above.
155 US Department of Justice *Cryptocurrency Enforcement Framework* (2020) 41.
156 Comolli and Korver 2021 *DJJFLP* 207.
157 Teichmann and Falker 2021 *JMLC* 94.
158 As above.
159 As above.
160 As above.

8 The role of South African banking institutions in combating money laundering using cryptocurrencies

The role of South African banking institutions in combating money laundering is critical in ensuring the integrity of the financial system and preventing illicit activities.[161] South African banking institutions play a crucial role in detecting and preventing money laundering activities by implementing effective risk-based compliance programs, conducting customer due diligence, and monitoring transactions for suspicious activities.[162]

To effectively combat money laundering involving cryptocurrencies, there are certain steps that South African banking institutions can undertake. First, banking institutions can provide efficient transaction monitoring.[163] For instance, information technology (IT) systems can be deployed to use algorithms to identify patterns and behaviour that show the occurrence of money laundering.[164]

Second, banking institutions must "strengthen anti-money laundering procedures by focusing those on the interchange between financial institutions and basic crypto exchanges and distinguishing normal customer behaviour from possible money laundering."[165]

Third, global standards of cryptocurrency markets and transaction regulation must be developed to combat money laundering involving cryptocurrencies.[166] The standards can prescribe a worldwide KYC policy to determine how digital wallets can be issued.[167] For example, the management of digital wallets can be placed under the supervision of third-party providers like banking institutions. Additionally, KYC information should be provided to third-party providers before a digital wallet is opened on behalf of a person.

The authors submit that it may be prudent for banking institutions in South Africa to manage the digital wallets of cryptocurrency users. A digital wallet is similar to a bank account. Thus, it can be made a requirement for a digital wallet to be opened subject to KYC rules imposed by a banking institution. The management of a digital wallet by a banking institution can be used as a mechanism to monitor the flow of cryptocurrencies. Banking institutions can also become custodians of

161 Sharrock *Law of Banking and Payment in South Africa* (2016) 100.
162 De Koker "Client Identification and Money Laundering Control: Perspectives on the Financial Intelligence Centre Act 38 of 2001" 2006 *SALJ* 717.
163 Rysin and Rysin (2020) 198.
164 As above.
165 As above.
166 As above.
167 As above.

private keys. Generally, a person in possession of a private key controls a digital wallet. Therefore, and in the context of money laundering using cryptocurrencies, an actor can transfer ownership of a wallet by providing the private key to another person.[168]

When ownership of a wallet takes place, a banking institution can establish the identity of the recipient subject to KYC rules. This way, a financial institution is aware of the identity of the person who has access to the funds in a digital wallet. A banking institution can always detect the origin and destination of cryptocurrencies. Any potential illegal transaction or exchange can be identified and flagged. A banking institution can put a limit on the number of cryptocurrencies that can be exchanged or sent at any given time. A block can be made on an exchange or transaction if a person is not able to provide reasons regarding the nature of the exchange, the origin of the funds, and the destination of the funds.

Fourth, exchange platforms can request their customers to provide a bank account as part of the onboarding process.[169] A bank customer uses the bank account to pay for cryptocurrency purchases and receive the proceeds of cryptocurrency sales.[170] During this process, a bank can determine the activities of its customers. In doing so, the bank can conduct an audit to establish the frequency of the exchanges that relate to cryptocurrency transactions. A bank can then make a risk assessment of all its customers.[171] The use of AI can help detect trends or patterns that point to the likelihood of cryptocurrency money laundering.

9 Conclusion

The regulation of cryptocurrency to combat money laundering crimes in South African banking institutions is a critical step toward promoting transparency, accountability, and trust in the financial system. The government, financial regulators, and the banking industry should work together to establish comprehensive and enforceable regulations that address the unique challenges posed by cryptocurrencies. These regulations should include measures such as mandatory KYC and anti-money laundering checks, real-time monitoring of cryptocurrency transactions, and collaboration with law enforcement agencies to investigate and prosecute financial crimes.

Furthermore, education and awareness campaigns should be implemented to educate the public on the risks associated with cryptocurrencies and the importance of complying with regulatory requirements. While the latest developments to FICA are commendable, the authors submit that the latest amendments to FICA do not address all

168 Comolli and Korver 2021 *DJJFLP* 192.
169 Comolli and Korver 2021 *DJJFLP* 210.
170 As above.
171 As above.

the scenarios pertaining to money laundering using cryptocurrencies. The authors submit that where AML legislation (like FICA) fails to address money laundering using cryptocurrencies, South African banking institutions can play an active role by managing the digital wallets of cryptocurrency users. If these measures are adopted, South Africa can create a more secure and reliable financial system that is better equipped to combat money laundering crimes and protect its citizens. Stakeholders in the financial sector must ensure that cryptocurrencies are not exploited for illegal activities, and they must also ensure that the financial system remains a safe and trusted place for all.