

https://dspace.org/

Cryptocurrencies and the Risks of Money Laundering and Terrorist Financing: Proposals for a Regulatory Regime

Masuku, Owen Jabulani

2023
University of the Witwatersrand, Johannesburg
https://hdl.handle.net/10539/38751
Masuku, Jabulani. (2024). Cryptocurrencies and the Risks of Money Laundering and Terrorist Financing: Proposals for a Regulatory Regime [Master's dissertation, University of the Witwatersrand, Johannesburg]. WireDSpace.https://hdl.handle.net/10539/38751

Downloaded from a DSpace repository. https://dspace.org/

Cryptocurrencies and the Risks of Money Laundering and Terrorist Financing: Proposals for a Regulatory Regime

by

Owen Jabulani Masuku

Submitted in partial fulfilment of the requirements for the degree of

Master of Laws by Coursework and Research Report

at the University of the Witwatersrand, Johannesburg

Under the Supervision of

DR. Herbert Kawadza

DECLARATION

I, ***Owen Jabulani Masuku*****,** state that this Research Paper submitted for the conferment of *Legum Magister* (LLM) in Commercial and Business Law by the Faculty of Law, Commerce and Management of the University of the Witwatersrand, Johannesburg, South Africa is my original work. The Research Paper has never been submitted to this or another educational institution for the award of a degree or other academic qualification.

14 August 2023.

ACKNOWLEDGEMENTS

I would like to extend my most sincere gratitude, love and appreciation for the support, and encouragement shown and showered upon me by my dear wife, Sinqobile. Thank you for tirelessly supporting me and my dreams.

To my sons, Bhekuxolo and Simphiwe, thanks so much for all your interests, endless questions, and engagements during this Research Project. I appreciate you, my boys.

To my good friend and brother, Dr. Eric Nyembezi Makoni, thanks again for the encouragement. Your belief in me is remarkable. It motivated and drove me to complete this Research Paper and my LLM. Indeed, learning, studying is contagious and fashionable!!

To my Supervisor, Dr. Herbert Kawadza, thank you so much for your support and guidance during this period.

ABSTRACT

Rapidly emerging new technology and payment methods are gradually replacing traditional payment methods and sovereign legal tenders as viable substitutes in the global economy. The emergency of cryptocurrencies on the world's economies has brought with it excitement, frustration, and uncertainty in equal measures. Cryptocurrencies are decentralised convertible virtual currencies that rely on the use of blockchain technology and the math-based peer-to-peer reference without the reliance on a central controlling authority to administer, monitor, regulate and exercise oversight control.

Cryptocurrencies offer many potential benefits, such as speed of payment settlement, reduced costs of doing business, speedy cross-jurisdictional reach, and accessibility, as well as the anonymity of the users compared to the traditional payment methods. The integrity of the financial systems is at danger due to these same benefits and advantages. The risks and dangers of money laundering, terrorist financing, fraud, tax evasion, and other unlawful actions are associated with cryptocurrencies.

The first cryptocurrency, Bitcoin, was created in 2008. The internet and globalization have allowed cryptocurrencies to enter South Africa. These currencies are not accepted as legal money in the South African legal system at this time.

The objective of this desk-top research is to consider, amongst others, the following: what cryptocurrencies are, why cryptocurrencies are a Money Laundering and Terror Financing (ML/TF) risk, the red flags in ML/TF through cryptocurrencies transactions, structural and regulatory weaknesses associated with ML/TF through cryptocurrencies and the recommendations for structural and regulatory enhancements and changes to combat the ML/TF risks from cryptocurrencies.

This thesis recommends the need for regulatory intervention in South Africa. It argues that there is a need to regulate cryptocurrencies through the amendments to the relevant legislations such as the Financial Intelligence Centre Act, the Consumer Protection Act, Financial Advisory and Intermediaries Act, amongst others.

Contents

1 INTRODUCTION *7*

2 THE PARTIES IN THE CRYPTOCURRENCY ECOSYSTEM *8*

3 THE INHERENT RISKS OF CRYPTOCURRENCIES *9*

4 CRYPTOCURRENCIES AND A RICH HISTORY OF MONEY LAUNDERING *12*

5 CYPTOCURRENCIES IN MIDST OF STRUCTURAL AND REGULATORY WEAKNESSES *14*

5.1 Structural Weaknesses Resulting in Money Laundering *14*

5.2 A Non-Sovereign and Parallel Monetary System *15*

5.3 Lack of Consumer Protection *16*

5.4 Distortion of Capital Flows and Statistical Information *16*

5.5 Credit Risks and Lack of Guaranteed Timeous Settlement of Payments *17*

5.6 Price Instability and Fluctuations *17*

5.7 Financial Instability *18*

6 TOWARDS REGULATORY REGIMES: COMPARATIVE JURISPRUDENCE *18*

6.1 Japan *19*

6.2 Canada *19*

6.3 The United States of America *20*

6.4 Australia *21*

6.5 The United Kingdom *21*

6.6 The Central Africa Republic *21*

6.7 El Salvador *22*

6.8 Obfuscation and Inadequate Responses *23*

7 RECOMMENDATIONS ON MITIGATING CRYPTCURRENCY ML/TF RISKS *23*

7.1 Applying Risk Based Approach to ML/TF *24*

7.2 Licensing and Registering VASPs *24*

7.3 Obtaining Information on Beneficial Owners and Shareholders of VASPs *25*

7.4 Know Your Clients through Client Due Diligence Measures *25*

7.5 Conducting Enhanced Due Diligence on High-Risk Clients *25*

7.6 Record Keeping Obligations *26*

7.7	*Risk Assessments of New and Enhanced Products*	*26*
7.8	*Sanctions Control and Enforcement*	*26*
7.9	*Reporting Obligations*	*27*
7.10	*Cross-Jurisdictional Co-operation*	*27*
	8 SOUTH AFRICA TRUDGES TOWARDS REGULATING CRYPTOCURRENCIES	***27***
8.1	*CASPs Declared Accountable Institutions in terms of the FICA*	*28*
8.2	*Developing Risk Management Programmes*	*28*
8.3	*Suspicious Transactions Reports and Sanctions Enforcement*	*28*
8.4	*Regulating Cross-Border Financial Flows*	*29*
8.5	*Crypto Assets as Financial Products*	*29*
	9 CONCLUSION.	***29***
	10 BIBLIOGRAPHY	***31***

1 INTRODUCTION

According to the Financial Action Task Force, ('FATF'),[1] cryptocurrency refers to a math-based, decentralised convertible virtual currency protected by cryptography. It is made up of the cryptographic principles that put a distributed, decentralized, secure information economy into place. To transfer value from one person to another using cryptocurrency, public and private keys must be used, and each transfer of value must be cryptographically signed.[2] Cryptocurrencies are a representation of value and a medium of exchange that is capable of being traded digitally. They are part of the decentralised virtual currencies that are distributed[3] in an open-source, math-based peer-to-peer reference with no central administration, monitoring or playing an oversight role. The U.S Government Accountability Office (GAO) has stated that there is no single widely accepted definition for virtual currency and described them as 'a digital unit of exchange that is not backed by a government-issued legal tender. Virtual currencies can be used exclusively within a virtual economy or alternatively in an officially recognized economy to make purchases--.'[4]

Bitcoin was the first major decentralised virtual currency,[5] and the first cryptographical currency launched in 2009. Bitcoins are units of account made of a combination of unique numbers and letters that together make up units of currency and exchange value for the individual users willing to use them for the purchase of goods and service.[6] They are digitally traded between users with a high degree of

[1] The Financial Action Task Force (FATF) is a global, intergovernmental organization that keeps tabs on money laundering and terrorism financing. As an organization that develops policy, FATF seeks to build the political will required to implement national legislative and regulatory reforms to combat money laundering and terrorist financing. To ensure a coordinated international response in the fight against organized crime, corruption, and terrorism, the FATF has created the FATF Guidelines and FATF Standards. The FATF's recommendations and guidelines are binding on South Africa as a member of the organization. Mutual evaluations and jurisdiction-specific findings and recommendations are given to FATF members to implement and comply with.

[2] FATF Report: Virtual Currencies- '*Key Definitions and Potential AML/CFT Risks*" 2014 at 5

[3] Transactions are validated and confirmed by a distributed ledger system are referred to as distributed. An algorithm is used by a network of participants to verify, examine, and preserve the transaction records for each transaction.

[4] Department of Justice press release, "Co-Founder of Liberty Reserve Pleads Guilty to Money Laundering in Manhattan Federal Court" GAO-13-516, Oct.31, 2013, available at http://www.justice.gov/opa/pr/2013/October/13-crm-1163.html (Accessed 12 August 2022).

[5] The European Commission defines a virtual currency as *'a digital representation of value that is accepted as payment by individuals or organizations and that can be moved, stored, or traded electronically but is not issued by a central bank or other governmental entity or required to be paired with a fiat currency.'*
European Commission, Proposal for a directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016PC0450 (Accessed 12 August 2022)

[6] FATF Report Virtual Currencies, *supra* note 2 at 5.

anonymity[7] and can be traded or cashed out into different legal tenders (such as into US dollars, Euros, Rand) or for other virtual currencies as well.[8] Bitcoin was created by Satoshi Nakamoto through the application of the concept of cryptocurrency.[9] In a research paper produced by Nakamoto, Bitcoin is described as a wholly peer-to-peer version of e-money that permits digital payments and trades between parties without the involvement of a central bank or any other financial institution other than peer-to-peer.[10] Nakamoto claims that the purpose of cryptographic currency is to eliminate the need for a third party. Any willing parties could conduct business directly with one another without the involvement of a third party. The sellers and buyers would be protected from fraud because it would be computationally difficult to reverse these transactions.[11]

Other examples of decentralised convertible virtual currencies are Ethereum and LiteCoin.

2 THE PARTIES IN THE CRYPTOCURRENCY ECOSYSTEM

There are various actors in the cryptocurrency world, each playing a particular role for the success of the cryptocurrency ecosystem because cryptocurrencies are a digital representation of value that is neither issued by a central bank nor a public body. An **Exchanger** is a person or organisation that exchanges cryptocurrencies for actual sovereign money, foreign currency, or other digital currencies in exchange for a fee or commission.[12] A variety of payment methods, including cash, wire transfers, credit card payments, and other cryptocurrencies, would be accepted by exchangers. Exchangers also function as an exchange and deposit desk. Individuals involved in cryptocurrency exchanges and transactions will use the Exchangers to deposit and/or withdraw sovereign money from their cryptocurrency wallets/accounts.[13]

An **Administrator** is a person responsible for the issuing, administering, and managing a centralised cryptocurrency platform. The Administrator would establish

---

[7] According to Gaspare Jucan Sicignano, '*bitcoin and cryptocurrencies guarantee absolute anonymity and absolute impermeability, all of which is extraordinarily attractive for those who want to launder money.'* Gaspare Jucan Sicignano, '*Money Laundering using Cryptocurrency: The Case of Bitcoin,'* 2021 Athens Journal of Law 7 (2) 253-264 at 254.
[8] FATF Report Virtual Currencies, *supra* note 2 at 6.
[9] S Nakamoto 'Bitcoin: *A peer-to-peer Electronic Cash System'* http://www.bitcoin.org/bitcoin.pdf (accessed 14 November 2022).
[10] *Ibid*.
[11] *Ibid*.
[12] FATF Report Virtual Currencies, *supra* note 2 at 7.
[13] *Ibid*.

the rules for the use of the cryptocurrency platform and maintain a central payment ledger of the virtual currency.[14]

A User is an individual or legal entity who receives cryptocurrency, spends it on goods and services, and buys more cryptocurrency. Moreover, users can transmit, transfer, or trade cryptocurrencies with others.[15] Users may also elect to hold and store the cryptocurrency as an investment.

A **Miner** is any entity that operates and manages the special software to resolve mathematical equations of the distributed cryptocurrency ledger and validates the transactions of the virtual currency of the ecosystem.[16] Proof of mining is called blockchain, constituting a public ledger with records of every transaction conducted on the network.[17]

A **Cryptocurrency Wallet** refers to a wallet owned by the User for holding, storing, transferring, and receiving cryptocurrency.[18] A Cryptocurrency Wallet is provided by the **Wallet Provider,** an entity that provides a Cryptocurrency Wallet by way of software applications for the holding, storing, transferring, and receiving of cryptocurrency by the User. A wallet stores the user's private keys (or access codes), enabling them to make transactions using the virtual money assigned to the block chain cryptocurrency address.[19] The Wallet Provider facilitates transactions between Users, Exchangers and those merchants who accept cryptocurrencies as a medium of exchange.[20] The Wallet Provider also maintains the User's transaction records and provides security over the transaction conducted in that wallet.

3 THE INHERENT RISKS OF CRYPTOCURRENCIES

The anonymity or pseudo-anonymity provided by cryptocurrency is an advantage towards the protection personal data for the user. In conventional financial institutions, a user`s identity is requested and processed before transactions are processed. In contrast, cryptocurrencies service providers protect the identity of parties to a certain extent. Cryptocurrencies give the users privacy or pseudo-

[14] *Ibid*.
[15] *Ibid*.
[16] *Ibid*.
[17] C Swinton 'A critical analysis of the risks associated with crypto-currencies' unpublished LLM thesis, University of Dundee, 2015 at 16
[18] FATF Report Virtual Currencies, *supra* note 2 at 7
[19] FATF Report Virtual Currencies, *supra* note 2 at 8
[20] *Ibid*.

anonymity, which reduces crimes such as fraud and provided the protection against the identity theft of the participant.[21]

Implementing client due diligence policies (or "CDD") in traditional banks and financial institutions is amongst the strategies used to detect and fight money laundering and terror financing. The CDD policy attempts to identify and verify the clients of the financial institutions by demanding valid identification, information on the client's residence, and a legitimate photo to complete the identification process before a client can transact with the financial institution. CDD is a compulsory requirement in terms of the Financial Intelligence Centre Act.[22] By contrast, conducting transactions through cryptocurrencies ensures clients a high degree of anonymity, with little identification, except for the user's public key. The user's other private and personal identification information is always kept private.[23] This guarantees a high level of identity theft protection. Yet, criminals take use of this anonymity to get around and beyond conventional anti-money-laundering measures like the CDD policy.

Cryptocurrencies function in a decentralized manner, allowing transactions to be conducted directly between users without the involvement of a third-party intermediary. Because to the absence of a third-party intermediaries, the systems typically operate without regulatory oversight. Regulatory jurisdictions with lax anti-money-laundering and countering terrorism financing ('AML/CFT) frameworks may host cryptocurrency-based payment systems. The aim of the AML/CFT framework is to monitor and enforce compliance with AML/CFT regulations. The traditional methods of AML/CFT are difficult to implement in the cryptocurrency network due to the lack of regulatory intermediaries, which increases the risk of criminals purposefully choosing jurisdictions with weak AML/CFT systems.[24]

One of the benefits of cryptocurrencies is that they provide for real time settlement of transactions as well as low transaction fees.[25] Criminals can exploit this real time clearance and settlement advantage. Compared to the traditional means of

[21] Kiel Institute for the World Economy *'Virtual currencies: monetary dialogue July 2018,'* European Union, available online at http://www.europarl.europa.eu/cmsdata/149902/KIEL_pdf (Accessed 23 November 2022)
[22] S21-29 of the Financial Intelligence Center Act, 38 of 2001, as amended by the 2017 Act, require Accountable Institutions to conduct CDD before the commencement of a business relationship or a single transaction.
[23] Deon Erasmus and Susan Bowden '*A Critical Analysis of South African Anti-Money Laundering Legislation with regard to Cryptocurrencies.'* (2020) Obiter, 41(2) 309–327 at 313
[24] Deon Erasmus and Susan Bowden, *supra* note 23 at 310.
[25] J Brito & A Castillo "*Bitcoin: A primer for policymakers"* (2013) Mercatus Centre at George Mason University 10 at 10.

financial transactions, cryptocurrencies provide for real time settlement of financial transacting and financial settlements, thereby bringing a lot of convenience not always available from traditional banking system. Transnational transactions can be settled in real time without the involvement of the government. Transfers frequently happen instantly, and it can be challenging to seize and reverse the proceeds of unlawful conduct even where an illegal transaction has been identified by the authorities. Irreversibility, cross border challenges in confiscating the proceeds of crimes, as well as the anonymity that comes with these currencies add to the layers of challenges that authorities face in attempts to fight money laundering and terror financing, ('ML/TF').[26] Owing to the anonymous nature of these currencies, it will be difficult to employ a solution that resolves the erroneous or fraudulent transactions.[27]

Most of the key players in the cryptocurrencies landscape are unregulated and unsupervised. Users and other players are not afforded any legal protection in this unregulated environment, such as a deposit guarantee or other legal remedies.[28] This exposes client to many risks that would, otherwise, be avoided by the enactment of regulations. Additionally, because there is little information available regarding the parties' legal obligations, clients may be further exposed to unforeseen legal repercussions that could make their transactions invalid or illegal.[29] Such legal consequences may include taxation laws and liability on transacting through cryptocurrencies.

There is no regulatory requirement for transactional record keeping on these cryptocurrencies rendering an ordinary money-laundering investigation difficulty. With cryptocurrencies, computer codes are used to publish all transactions. Due to the difficulty of tracing users' identities without the User's cooperation, law enforcement authorities are likely to run into issues when attempting to link the public key and the User behind it.[30]

Cryptocurrencies are cross-jurisdictional in their creation, use, and storage.[31] Some countries have still not grasped the nature and functioning of these new

[26] Deon Erasmus and Susan Bowden, *supra* note 23 at 314.
[27] European Central Bank '*Virtual currency schemes – a further analysis'* 2015 at 20.
[28] European Central Bank, *supra* note 27 at 21.
[29] Mothokoa, '*Regulating Crypto-Currencies in South Africa: The Need for an Effective Legal Framework to Mitigate the Associated Risks'* (LLM mini-dissertation, University of Pretoria) 2017 at 35.
[30] Deon Erasmus and Susan Bowden, *supra* note 23 at 314.
[31] Deon Erasmus and Susan Bowden, *supra* note 23 at 322.

methods of value storage and transacting. There is presently no internationally recognised structure or regulation for cryptocurrencies. Each territorial jurisdiction has the difficult problem of trying to control cryptocurrency exchanges in an unfamiliar environment and unfamiliar financial product. This becomes a challenging task when such transactions are concluded directly with different participants from anywhere in the world. According to the FATF report on cryptocurrency, that multiple entities in any jurisdiction may keep data connecting user identification and transactions.[32] Due to the cross-jurisdictional nature of the transactions and the participants, access by law enforcement agencies and regulators to the records tying identities and transactions of users may be hindered or constrained by the cross-jurisdictional nature of the transactions.[33]

Cryptocurrency is a complex concept to understand. Although it has been in use since 2009, it is still difficult to comprehend for routine and daily transactions. This is because of the limited information that is available. By their nature, cryptocurrencies have no transparency requirements.[34] This lack of transparency and the complex nature of the information about them, could mislead the clients about the risks associated with their financial value and tradability.[35]

Cryptocurrencies are vulnerable to volatility in their price and exchange with fiat money/legal tender.[36] A financial asset's price volatility and instability relates to how much its value changes over time. The higher the volatility, the riskier it is for the user to hold on to the asset. One of the main issues for cryptocurrency consumers and regulators is their excessive volatility. The value of cryptocurrencies depends on how their users and other stakeholders perceive them at a particular time. There is no monetary policy to regulate the environment in which they operate, and as result, they are always vulnerable to inflation and deflation.[37]

4 CRYPTOCURRENCIES AND A RICH HISTORY OF MONEY LAUNDERING

Cryptocurrencies are a technological and financial innovation with enormous economic potential. However, they are also capable of being utilized for illegal

[32] FATF Report Virtual Currencies, *supra* note 2 at 6.
[33] *Ibid*.
[34] European Central Bank, *supra* note 27 at 22,
[35] *Ibid*.
[36] At its peak in November 2021, Bitcoin was valued at USD$68,000, but is currently trading below USD$17,000 as of 3 December 2022.
[37] Mothokoa, *supra* note 29 at 36.

activities like fraud, money laundering, and the online trading of illegal goods and services.[38] The use of this payment method is speeding up while its use in criminal operations is also expanding.[39] Criminals are using cryptocurrency in increasingly complex ways. As part of intricate money-laundering operations, criminals are increasingly adopting cryptocurrencies as payment methods or as a currency for fraud as well as to disguise the movement of laundered money.[40] Fintech Global described, cryptocurrency as 'a hot commodity for money launderers due to [the then] lack of workable regulatory guidance from the Financial Action Task Force.'[41] Because of its secrecy and anonymity, organized crime rings are honing the technique of digital money laundering. Transactions can take place off-book thanks to anonymous and untraceable transfers between buyers and sellers.[42]

In August 2017, an amount thirty-three billion comprising of South African Rands and United Arab Emirates E-Dinar were exchanged for a cryptocurrency called Localtrade, based and operating from Dubai, United Arab Emirates.[43] Speculation was rife that the transaction was another instance of money laundering by those who are politically connected. What is however evident is that the amounts were swiftly transferred across borders, on real-time clearance and settlement, and bearing to the long-held notion that cryptocurrencies provide uncomplicated means for criminals to export large sums of money without adhering to the correct processes and going unnoticed.[44]

The US Department of Justice demolished the illicit Silk Road network in September 2013. Silk Road was a covert website set-up to allow users to transact covertly in illegal goods and services like drugs, guns, counterfeit items, and identity theft, without the knowledge of law enforcement. The criminal network was charged with drug trafficking, computer hacking, and money laundering crimes. It is claimed to

[38] Gaspare Jucan Sicignano, *supra* note 7 at 254.
[39] Europol Spotlight, '*Cryptocurrencies Tracing the Evolution of Criminal Finances'* https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf (Accessed 25 November 2022).
[40] Europol Spotlight, *supra* note 39.
[41] https://fintech.global/2022/05/03/how-is-cryptocurrency-changing-money-laundering/ (Accessed 25 November 2022).
[42] https://fintech.global/2022/03/05/how-is-cryptocurrency-changing-money-laundering/ (Accessed 25 January 2023)
[43] Biznews ,Update –Mailbox: Curious case of a R33bn trade in a UAE linked cryptocurrency" 2017 http://www.biznews.com/global-investing/2017/08/28/r33bn-transfer-uae-linked-edinar-edr-cryptocurrency/ (Accessed 25 November 2022)
[44] *Ibid*.

have produced revenue for Silk Road of about USD 80 million (more than 600 000 bitcoins) and sales income of about USD 1.2 billion (more than 9.5 million bitcoins). Silk Road operated on a secret network and only accepted bitcoin payments.[45] The use of bitcoins facilitated the Silk Road traders and their clients to hide their identity through the senders and recipients use of the peer-to-peer ('P2P') bitcoin method of trading and transacting,[46] to which no one else can gain access to.

Western Express International was one of the biggest virtual currency exchangers in the United States. It ran a widespread cyber-fraud and identity theft scams. Using phony identities, anonymous email addresses, and anonymous cryptocurrency accounts, members of the cybercrime gang communicated and engaged largely through websites known as "carding" that deal in the trafficking of credit card and other stolen personal information. Using anonymity accounts, they were able to evade detection by law enforcement agencies and regulatory agencies.[47] Through several intricate, complex, and technologically advanced methods, the money-mover was able to transfer more than USD 35 million through different anonymous accounts.[48]

5 CYPTOCURRENCIES IN MIDST OF STRUCTURAL AND REGULATORY WEAKNESSES

In 2014, the South African National Treasury, in a joint initiative with the South African Reserve Bank ('SARB'), the Financial Sector Conduct Authority ('FSCA'), the South African Revenue Service ('SARS') and the Financial Intelligence Centre ('FIC') issued a public statement cautioning people to exercise caution when using crypto assets for investing or transacting purpose and alerting the public of the risks.[49] The cautionary statement was prompted by the fact that no specific legislation or regulations had been promulgated to regulate the use of crypto assets.

5.1 Structural Weaknesses Resulting in Money Laundering

Following the National Treasury's user notice, the SARB published a position paper on cryptocurrency assets in 2014 and issued it through the National Payment System Department ('NPSD').[50] The possibility of cryptocurrency assets being used for money laundering and terrorism financing, ('ML/TF') was emphasized in the position paper. It

[45] FATF Report Virtual Currencies, supra note 2 at 11.
[46] *Ibid*.
[47] FATF Report Virtual Currencies, supra note 2 at 12
[48] *Ibid*.
[49] At the time this statement was issued, the term 'virtual currencies' was used to refer to crypto assets.
[50] The 2014 IFWG Position Paper Virtual Currencies.

was clear that the ecosystem for digital assets lacked a legal and regulatory framework. It did not have consumer protection legislation and made it simple to get around exchange control rules. The position paper mentioned that the SARB did not control, oversee, or supervise the ecosystem of digital asset service providers and their intermediaries. All transactions related to the acquisition, trading, or use of crypto assets were solely done at the users' own and independent risk, with no recourse to the SARB.[51]

Stakeholders in the financial sector could not continue with business as usual and pretend that cryptocurrencies did not exist. The Intergovernmental Fintech Working Group ('IFWG'), which includes representatives from the NT, SARB, FSCA, and FIC, was founded in 2016. In 2019, SARS and the National Credit Regulator (the "NCR") joined the IFWG. The aim of the IFWG is '*to develop a common understanding among regulators and policymakers of financial technology (fintech) developments as well as the regulatory and policy implications for the financial sector and the economy*.'[52] The IFWG produced a position paper recommending for the development of a regulatory and policy position to crypto asset activities in South Africa. According to the position paper, given the variety of innovations seen in the financial services industry, it is necessary to evaluate the existing regulatory framework for appropriateness, effectiveness, and suitability and, where necessary, identify any improvements that may be needed.[53] This is because current regulatory framework was drafted without the new fintech innovations, as such, cryptocurrency risks were not envisaged when the legislature drafted the current laws and regulations.

5.2 A Non-Sovereign and Parallel Monetary System

Cryptocurrencies pose the risk of a separate, independent, dispersed, and non-sovereign monetary system. The cryptocurrency blockchain systems operates outside the central government monetary system. Cryptocurrencies pose risks to the current financial system because they operate independently of the monetary system of the central government. Under the central government system, central banks maintain a reliable system for settling payments as well as carrying out monetary policy by issuing money or sovereign currencies.[54] A persistent increase in cryptocurrency demand and

[51] 2020 Intergovernmental Fintech Working Group 'Position paper on crypto assets' 2020 at 3.
[52] *Ibid*.
[53] *Ibid.*
[54] 2020 Intergovernmental Fintech Working Group, *supra* note 43 at 15.

use could result in the emergence of a parallel, separate, independent, and eventually non-sovereign monetary system within an economy. This is the risk that cryptocurrencies represent to the monetary policy mechanism. The central bank's responsibility for maintaining an effective monetary system could become dwindled and ineffective, leading to the decrease in the use of fiat currency, resulting in cryptocurrency effectively competing with sovereign currencies. This would result in the monetary system being under the control of private entities and individual and serving their own interests.

5.3 Lack of Consumer Protection

Transacting through cryptocurrency does not provide consumers with protection. Cryptocurrencies pose risks to consumers, mostly because of their unregulated character. Liquidity exposures, irreversibility of transactions, anonymity of parties to transactions, failure of the exchanger to hold enough cryptocurrencies to settle the transactions on time, price volatility of cryptocurrencies, lack of transparency and information on price are some of the risks to consumers.

5.4 Distortion of Capital Flows and Statistical Information

The anonymity of the persons behind the transactions is a selling point for those intending to use cryptocurrencies for illicit transactions. Money laundering is defined by the International Monetary Fund as the processing of proceeds from criminal activity to sever the connection between the money and its source.[55] The integrity and stability of the financial sectors and the global economy are negatively impacted by ML/TF.[56] These illegal (ML/TF) operations may deter foreign direct investment, which would skew global capital flows. Due to their decentralised character, cryptocurrencies systems provide anonymity to the parties transacting on the platforms since the addresses or accounts are sometimes not associated with the true names of their users or any form of acceptable identification. Unlike the traditional banks, there is no requirement for CDD before the clients of these digital platforms are on-boarded on the platforms.[57] These platforms are not subjected to any central regulatory and monitoring authorities, and as such the central authority and regulators have no means

[55] International Monetary Fund „The IMF and the Fight Against Money Laundering and the Financing of Terrorism" 2017 http://www.imf.org/en/About/Factsheets/Sheets/2016/08/01/16/31/Fight-Against-Money-Laundering-the-Financing-of-Terrorism (accessed 13 November 2020).
[56] *Ibid*.
[57] Mabunda, S. *'Cryptocurrency: The new face of cyber money laundering.'* 2018 International Conference on Advances in Big Data, Computing and Data Communication Systems, University of the Western Cape Research Repository, at 9.

to identify, and combat ML/TF activities and other suspicious activities conducted through the decentralised systems. New payment channels may present ML/TF threats, according to the US Department of Justice.[58] This as the global reach of cryptocurrencies increases the potential of ML/TF risks.

5.5 Credit Risks and Lack of Guaranteed Timeous Settlement of Payments

The timeous settlement of payments is the engine driving the efficient performance of any economy. The payment system comprises the systems and infrastructures that enables payments to be conducted between different role players that enables and facilitates the circulation of money.[59] A nation's payment systems comprises of the infrastructure, such as financial institutions, the regulators, and the technical support from different partners, all at disposal to facilitate the transfer of monetary value between different parties for different reasons, and at different times. The National Payment System ('NPS') processes transactions and payments of over R576 billion daily,[60] through recognised payment methods such as EFTs, mobile transfers, cash, and debit cards. In terms of the National Payment System Act, cryptocurrencies do not fall under the definition of 'money'[61] and are therefore not paid or transacted through the NPS. This leaves the cryptocurrencies out of the NPS and thus remain unregulated and provide no guarantee of payments to the users of the virtual assets. Owing to the lack of assurance for settlement of current and future financial obligations and transactions, cryptocurrency users face credit risk regarding the settlement of payments and the transfer of value obligations. The NPS is tasked with mitigating the credit and liquidity risks posed by intermediaries who must carry out the payment transaction. A transparent, end-to-end regulatory framework is not available to consumers who use cryptocurrency to pay for products and services to execute and settle the transactions.

5.6 Price Instability and Fluctuations

The impact of cryptocurrency adoption on the stability of the financial system is still unclear. However, it can be argued that cryptocurrencies have the potential to jeopardise financial stability due to the unstable nature of the cryptocurrencies.[62]

---

[58] US Department of Justice, '*Report of the Attorney General's Cyber Digital Task Force'* October 2020.
[59] Section 1 of the National Payment System Act, 78 of 1998.
[60] https://www.resbank.co.za/content/dam/sarb/what-we-do/payments-and-settlements/regulation-oversight/Oversight.pdf (Accessed 21 November 2022)
[61] S1 of the National Payment System, Act 78 of 1998, "money" means a banknote or coin issued by the Reserve Bank in terms of section 10(1)(a)(iii), read with section 14 of the South African Reserve Bank Act.
[62] Mothokoa, *supra* note 29 at 36.

Bitcoins has a history of price fluctuation and instability. The SARB is mandated with monitoring the financial system for potential financial instability and taking corrective measures. Section 221(1) of the Constitution of the Republic of South Africa, 1996 read with section 3 of the SARB Act states that, the protection of the currency's value in the interest of balanced and sustainable economic growth in the Republic is one of the SARB's main objectives. The SARB must identify systemic events in the financial system and take action to stop them from happening to ensure financial stability. When a systemic event has already happened or is about to happen, SARB must take mitigating action to control the systemic event and its impacts on the economy.[63] Cryptocurrencies operate outside of the SARB mandate for stability, and therefore expose the users to price instability and fluctuations, on which SARB cannot implement corrective measures.

5.7 Financial Instability

If cryptocurrency usage, acceptance, and circulation grow significantly, there may be a risk to financial instability. This could result from cryptocurrency developing greater usage and acceptance in the real economy, through the presence of financial institutions that participate in cryptocurrencies in a financial and regulatory framework lacking structural developments and interventions to make cryptocurrencies more stable.[64] An economy must have a strong financial system that can anticipate, avoid, and endure shocks in all kinds of domestic and foreign market conditions if it is to attain financial stability. The establishment of a strong financial regulatory framework, which is comprised of laws, rules, standards, and practices, is necessary to ensure financial stability.[65]

6 TOWARDS REGULATORY REGIMES: COMPARATIVE JURISPRUDENCE

The decentralised nature of cryptocurrencies distances them from the body of laws that govern fiat currency. The unregulated and under-regulated landscape of cryptocurrencies poses numerous risks of financial crimes such as ML/TF activities, tax evasion, and payment of ransoms. There is need for regulatory bodies to keep up with the developments, use and acceptability of cryptocurrencies and embark on regulatory initiatives to protect the clients, cryptocurrency service providers, and the financial systems against ML/TF and inflow of illicit funds. Some countries have moved

[63] Section 15(1) of the Financial Sector Regulation Act 9 of 2017
[64] ECB “Virtual currency schemes – a further analysis” (2015) 26.
[65] Financial Sector Regulation Act, 9 of 2017.

towards regulation and embedment of the cryptocurrencies. This initiative has been informed by a variety of factors and considerations, amongst others, the need to mitigate the risks that emanate from an underworld economy that has its own means of payment and a full unit of payment.

6.1 Japan

Japan is amongst the first countries to introduce regulations on cryptocurrencies. Japan recognises Bitcoin and other digital currencies as having the same function as fiat money in terms of the Payment Services Act. The Japanese government took the initiative and developed a regulatory framework to fully integrate the cryptocurrency into the Japanese banking system. Cryptocurrency are regulated through the Financial Services Agency ('FSA') of Japan, which also regulates the issuing of the Japanese national currency.[66] Exchanges and dealers in cryptocurrencies are required to register with the FSA, which has the authority to inspect these establishments and take the necessary administrative action. The cryptocurrencies exchanges are also compelled to adhere to stringent AML/CFT and cybersecurity requirements.[67]

Accordance to Japanese law, cryptocurrencies have a value equivalent to an asset. Any transactions involving virtual currencies are taxable under the relevant income tax regulations. The profit made by a legal entity from virtual currency is liable to corporate income tax, and any income received by an individual in the form of cryptocurrency is subject to income tax. The Japanese Consumption Tax is applicable to the sale and exchange of cryptocurrencies.[68]

Japan is still a favorable country for cryptocurrencies but growing AML concerns have spurred the FSA to propose new regulations. The FSA stated in December 2021 that it would draft new legislation in 2022 to regulate stablecoin issuers, manage client risks and restrict the usage of stablecoin tokens for ML/TF.[69] The proposed legislation will impose new requirements for crypto service providers to report suspicious activities.

6.2 Canada

Cryptocurrencies are not legal tender in Canada, though they can be used to pay for goods and services from those merchants that accept them. Canada has taken the

[66] Irina Cvetkova, '*Cryptocurrencies Legal Regulation.'* 2018 5 2 BRICS Law Journal 128–153 at 133.
[67] https://complyadvantage.com/insights/cryptocurrency-regulations-around-world/ (Accessed on 20 November 2022)
[68] Irina Cvetkova, *supra* note 66 at 140.
[69] https://complyadvantage.com/insights/cryptocurrency-regulations-around-world/ (Accessed on 20 November 2022)

lead in regulating cryptocurrencies, principally doing so through provincial securities laws.[70] As of 2014, Canada began enforcing the Proceeds of Crime (Money Laundering and Terrorist Financing Act), or 'the PCMLTFA', which regulates businesses that trade in virtual currencies. It is a regulatory requirement for cryptocurrency exchanges to be registered in terms of the FinTRAC as of 1 June 2020. Since 2013, the Canada Revenue Agency levies and taxes the payment for goods or services that have been bought through the cryptocurrency. In the world, Canada comes in second place to the United States in terms of the number of bitcoin ATMs installed,[71] and this has in turn necessitated the proactive approach to regulate the cryptocurrency sphere in Canada.

6.3 The United States of America

The United States of America (the "United States") does not recognize cryptocurrencies as legal tender. Nonetheless, the Internal Revenue Service ('IRS') of the United States issued guidance on the taxation regime applicable to Bitcoin and other cryptocurrency transactions, stating that these digital assets might be classified as money, property, and investment instruments.[72]

Cryptocurrency exchanges are regulated under the Bank Secrecy Act.[73] In terms of this Act, cryptocurrency exchanges are required to register with the Financial Crimes Enforcement Network, ('FinCEN'),[74] implement AML/CFT programs, maintain appropriate transaction records, conduct the necessary CDD requirements on their clients and submit reports to the authorities as and when requested.[75] FINCEN proposed a new law in December 2020 to enforce data collection obligations on cryptocurrency exchanges and wallets.[76] The Justice Department continues to collaborate with the Securities and Exchange Commission ('SEC') and Commodities Futures Trading Commission ('CFTC') on potential cryptocurrency laws to advance efficient consumer protection and more streamlined regulatory oversight.

---

[70] *Ibid*.
[71] Irina Cvetkova, *supra* note 66 at 138.
[72] Increase Popularity for Self-Directed IRA s, According to IRA Financial Group, Cision PRWeb, 25 March 2014 available at http://www.prweb.com/releases/bitcoins-self-directed-/ira-taxproperty-currency/prweb11704323.htm. (Accessed 20 November 2022)
[73] Bank Secrecy Act of 1970 as amended by the USA Patriotic Act 31 U.S.C.
[74] Financial Crimes Enforcement Network, "Application of FinCEN's regulations to persons administering, exchanging, or using virtual currencies" Guidance FIN-2013-G001, available at FIN 2013 G001 (fincen.gov) (Accessed 20 November 2022)
[75] https://complyadvantage.com/insights/cryptocurrency-regulations-around-world/ (Accessed 20 November 2022)
[76] *Ibid*.

6.4 Australia

Australia has been forward-thinking in its adoption of cryptocurrency rules, hence it is legal in Australia to use both exchanges and cryptocurrency. The Australian government announced in 2017 that cryptocurrencies were legal, and that Bitcoin (and cryptocurrencies with similar properties) should be recognized as property, and they should be subjected to Capital Gains Tax. Since 2018, the Australian Transaction Reports and Analysis Centre (also known as "AUSTRAC") has imposed compliance requirements on cryptocurrency exchanges operating in Australia. These compliance requirements include registration and licensing requirements, user identification and verification, record keeping and maintenance, and compliance with AML/CFT reporting requirements. Cryptocurrency exchanges that are not registered are liable to legal action and financial penalties.[77]

In December 2021, the Australian government introduced new licensing framework specifically for cryptocurrency exchanges. The framework positions Australia at the forefront of the global drive to rein in and regulate digital cryptocurrency exchanges and allow consumers to safely buy and sell crypto assets in a regulated environment.[78]

6.5 The United Kingdom

After leaving the European Union in 2020, the UK transposed the cryptocurrency regulation requirements set out in 5th Anti-Money Laundering Directive ('5AMLD') and '6AMLD' into domestic law. In the UK, cryptocurrency exchanges must register with the Financial Conduct Authority (the 'FCA') and adhere to AML/CFT reporting requirements as well as CDD standards. The FCA guidance emphasises that entities involved crypto assets must comply with the ML/TF and Transfer of Funds (Information on the Payer) in terms of 2017 MLRs Regulations).

6.6 The Central Africa Republic

Bitcoin was adopted as legal tender in the Central African Republic ('CAR') in April 2022. According to the publication, '*Bloomberg Crypto,'* as of September 2022 in a country of 4.8 million people, just 11% of the population has internet access and only 14% have electricity.[79] These figures show that there is limited access to bitcoin use by the population that has no access to internet and electricity. It defeats the purpose of recognising bitcoin as legal tender in CAR. According to the CAR authorities, the

[77] *Ibid.*
[78] *Ibid.*
[79] https://www.competitionpolicyinternational.com/central-african-republic-adopts-bitcoin-as-legal-tender/ (Accessed 30 November 2022)

objectives of the country launching bitcoin as legal tender was being able to attract investors to those sectors of the economy that could use it. However, trading and transacting in the currency has been stopped after the CAR's Constitutional Court ruled that the use cryptocurrency to buy land and citizenship through "e-residency" was illegal and unconstitutional.[80]

6.7 El Salvador

El Salvador passed the *Bitcoin Law* in September 2021, making it the first nation in the world to accept bitcoin as legal tender. Article 1 of the *Bitcoin Law*, provides that 'it aims to control the use of Bitcoin as unlimited, unrestricted legal tender that can be used for any transaction and for any purpose that the public, private, natural, or legal persons are required to carry out.'[81] The *Bitcoin Law* also makes bitcoin a unit of account within the country and endows it with value by accepting it as a means of payment for tax purposes and expressing process. According to Article 7 of the *Bitcoin Law*, every economic agent must accept Bitcoin as payment when it is made available for the purchase of goods or services. Within 20 days of starting business, bitcoin service providers and exchanges are required under the *Bitcoin Law* to register with the Central Bank of El Salvador.[82] Service providers are required to implement AML/CFT plans that include measures and controls that are in compliance with the FATF and Salvadoran laws on AML best practices and standards, such as maintaining client accounts and transaction records, implementing cyber-security programs, and maintaining asset, liability, and equity records.[83]

However, there has been misgivings about these developments. The legalization of Bitcoin in El Salvador has raised concerns from numerous financial institutions and governments who fear that it may encourage money launderers and other financial criminals to take advantage of legal loopholes relating to cryptocurrencies.[84] The International Monetary Fund has warned of the risks that El Salvador faces following the adoption of Bitcoin as legal tender.[85] Financial stability is a risk that the country

---

[80] https://www.reuters.com/technology/central-african-republic-top-court-blocks-purchases-with-new-cryptocurrency-2022-08-29/ (Accessed 30 November 2022).
[81] Article 1 of the El Salvador Bitcoin Law 2021.
[82] https://sanctionscanner.com/blog/cryptocurrencies-in-el-salvador-631 (Accessed 30 November 2022).
[83] *Ibid*.
[84] *Ibid*.
[85] https://www.imf.org/en/News/Articles/2022/02/15/cf-el-salvadors-comeback-constrained-by-increased-risks The following were identified by the IMF as risk that El Salvador could face because of the recognition of Bitcoin as legal tender: (i) ***Financial stability***: B Price swings in crypto assets might have a significant impact on banks and other financial institutions. To properly hedge against the volatility of Bitcoin, banks would need to implement new prudential regulations, such as capital and liquidity requirements, or forbid Bitcoin deposits. (ii) ***Financial integrity:*** Due to the anonymity they offer, cryptocurrency assets may make it easier to launder money illegally,

currently faces following the recent downward spiral in the value of the Bitcoin. Banks and other financial institutions could be subjected to significant fluctuations in crypto-asset prices. At its peak in November 2021, Bitcoin was valued at USD$68,000, but is currently trading below USD$17,000, therefore giving credence to the IMF[86] fears and warning on volatility and lack of stability.

6.8 Obfuscation and Inadequate Responses

In some jurisdictions today, the cryptocurrency communities still do not have any single coordinating or regulatory authority. The process of regulating cryptocurrency activity and enabling the creation of conditions that will facilitate the implementation of legal and secure cryptocurrency relations has only just begun in a few progressive countries. Other jurisdictions continue to show a total lack of ability to adapt to the changes in technology and innovation brought by the cryptocurrency wave. However, as decentralised networks and cryptocurrencies proliferate, payment and transaction settlements mechanisms will unavoidably develop, forcing governments to catch up to the cryptocurrency waves affecting their legal and regulatory systems. It is now evident that, in addition to traditional fiat money and e-money, it is required for the authorities to make firm pronouncements on the legal ambit, nature and functions of cryptocurrencies.

7 RECOMMENDATIONS ON MITIGATING CRYPTCURRENCY ML/TF RISKS

Contemporary products, services, and technologies can promote financial inclusion, increase efficiency, and drive innovation in the financial sectors. However, these contemporary inventions can give criminals and terrorists new ways to finance their illicit activities or launder their ill-gotten money. Given the developments of these ML/TF risks, FATF recognized the need to give guidance on managing and mitigating risks resulting from innovative technologies and provided guidance through the FATF 2021 Guidance for RBA to VAs and VASPs,[87] (hereinafter referred to as the 'FATF 2021 VASPs Guidance').

fund terrorism, and evade taxes. There are threats to financial integrity. (iii) ***Contingent fiscal liabilities***: A trust fund managed by the government provides all the funding for the acceptance of Bitcoin as legal cash. The assets in the trust might be quickly exhausted if the price of bitcoin were to fall. The trust would require funding from extra resources or the issuing of debt for the government to continue to guarantee the conversion of Bitcoin to US dollars.

[86] This is the price as of 3 December 2022, as quoted on various Bitcoin trading markets, such as Luno, Coinbase, Crypto.com and others.

[87] FATF (2021), Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers.

7.1 Applying Risk Based Approach to ML/TF

The 2021 VASPs Guideline states that countries should use a risk-based approach (also known as a “RBA") to make sure that the measures they implement to prevent or reduce ML/TF risks are proportionate to the risks that have been identified in their jurisdictions.[88] Under the RBA, countries should provide more resources to those higher-risk situations or activities involving virtual assets (‘VAs’). When assessing the ML/TF risks associated with VAs, the types of VAs, the activities or operations of VA Service Providers, (‘VASPs’),[89] as well determining the distinction between the centralized and decentralized VAs, and whether or not they are issued by a regulated VASP.[90] For effective application of the RBA, the country should perform risk assessments and get some understanding of how different VA products and services fit into, function, and affect the prevailing regulatory framework for AML/CFT purposes, and thereafter apply the commensurate risk mitigation measures.

7.2 Licensing and Registering VASPs

Countries should designate licensing and registering authorities for VASPs. According to the Guidance, in addition to legal incorporation of VASPs, as a minimum, VASPs should also be licensed in the jurisdiction(s) where they are located. To ensure compliance with the licensing and registering requirements, an authority should be appointed with the responsibility for identifying and taking corrective measures, and sanctions on unlicensed or unregistered VASPs.[91] It should be compulsory for registered and/or licensed VASPs to comply with the minimum licensing and registration requirements set by the authorities. The national authorities should be confident that the VASPs in question will be able to adhere to the AML/CTF requirements. To that end, the criteria should mandate that organisations demonstrate, prior to launch, that their AML/CFT programs, including policies, processes, and procedures, are implemented or capable of being implemented once launched, taking into account the characteristics of the VASP's activity (such as the types of VAs and transactions, targeted clients, and distribution channels).[92] Furthermore, VASPs should be obliged to implement AML/CFT compliance prior to

[88] Williams ‘*An Analysis of the Critical Shortcomings in South Africa’s Anti-Money Laundering Legislation’* (2017) 42.
[89] ‘Virtual Asset Service Provider’ are defined by FATF to be any natural or legal person who conducts any of the following activities: i. Exchanges of virtual assets for fiat currencies, and *vice versa;* ii. Exchange one or more virtual assets for other virtual assets; iii. Transfers virtual assets between Users; and iv. Safekeeps and/or administers, manages virtual assets, and maintains control over virtual assets.
[90] FATF 2021 VASPs Guidance, *supra* note 87 at 38.
[91] FATF 2021 VASPs Guidance, *supra* note 87 at 46.
[92] FATF 2021 VASPs Guidance, *supra* note 87 at 45.

the launch and designing or developing a new products or services, as it is far more challenging to do so later. This is in addition to the requirement for AML/CFT programs to be in place.

7.3 Obtaining Information on Beneficial Owners and Shareholders of VASPs

Authorities should implement the necessary legal and regulatory safeguards during the licensing and registration process to prevent criminals from acquiring ownership of or becoming the beneficial owners of VASPs. The measures could include VASPs obtaining prior approval from the authorities for major changes in shareholding structures and changes in business operations. Since different agencies may possess information relating to illegal shareholders or activities, coordination between multiple agencies involved in the regulation and licensing of VASPs is crucial. Authorities in different jurisdictions should also share information about those VASPs that have been previously deregistered in their jurisdiction and have obtained licensing (in a different jurisdictions) and are operating in their counterparties' jurisdictions. Authorities at national level should have appropriate channels for exchanging information and cooperate with one another to identify and penalise unregistered or unlicensed VASPs.[93]

7.4 Know Your Clients through Client Due Diligence Measures

It is recommended by FAFT that the implementation of 'Know Your Clients,' ('KYC') processes could reduce the risk of ML/FT. As part of the KYC processes, VASPs should be obliged to implement CDD processes to meet the FATF Standards and national statutory and regulatory requirements for effective ML/TF risk management. The CDD process should assist VASPs in assessing the ML/TF risks linked to VA activities, business relationships or single transactions above the predetermined threshold.[94] CDD processes should comprise of identifying the client and, the client's beneficial owner, (where applicable), and verifying the client's identity. As part of the CDD process, the VASPs should enquire about and comprehend the nature of the business relationship and obtain further information for those high-risk scenarios as part of their enhanced due diligence.

7.5 Conducting Enhanced Due Diligence on High-Risk Clients

On those clients that have been rated as high risk, the VASPs should consider implementing enhanced due diligence, ('EDD'). EDD measures include obtaining

[93] FATF 2021 VASPs Guidance, *supra* note 87 at 47.
[94] *Ibid*.

more client information and verifying that information against third party independent sources for the VASPs to have comfort on the decision whether to commence or decline a business relationship with the clients. EDD also includes conducting enhanced monitoring of the relationship and transactions conducted by the client.

7.6 Record Keeping Obligations

The countries should mandate through the necessary regulations that VASPs maintain all transaction records and CDD measures in such a way that specific client transactions can be recreated, and that the pertinent records be made available to the requesting authorities upon request as part of the measures to combat ML/TF. The information relating to the identification of the relevant parties, such as the public keys, the addresses of the accounts involved, the nature and date of the transaction, and the amount involved in the transaction should all be kept by VASPs.[95] These records should be retained for a period of at least five years.

7.7 Risk Assessments of New and Enhanced Products

As the cryptocurrencies landscape keeps developing, authorities must identify and assess the ML/TF risks resulting from the invention and enhancement of products, services, and business practices. These new developments could include new delivery methods, the use and embedment of new or enhanced technologies for both new and enhanced products. This will assist the authorities to respond appropriately in managing and mitigating the ML/TF risks before the launching of new or enhance products or enhanced technologies. Authorities should also invest in learning and development so that they can keep-up with the developments and innovations in the cryptocurrencies space.

7.8 Sanctions Control and Enforcement

To ensure that VASPs can adhere to the duties of targeted financial sanctions, authorities should require the implementation of an efficient sanctions control mechanism by the VASPs. Both ordering/sending and beneficiary/recipient VASPs must implement sanctions policies and processes to freeze and prohibit transactions with sanctions designated individuals. At the time of onboarding their clients, the ordering and beneficiary institutions should screen the names of their clients for compliance with targeted financial sanctions requirements. As they carry out the VA transfer, they must again screen the names of both the originator and the recipient of

[95] FATF 2021 VASPs Guidance, *supra* note 87 at 52.

the VA.[96] Sanctions screening and monitoring is part of the wider KYC processes. It means the VASPs would implement processes to 'Know their Clients' and avoid doing any business with those clients who are on designated sanctions lists, as approved by the competent sanctioning authorities such as the United Nations Security Council, OFAC and others. Authorities should require VASPs to have in place effective compliance frameworks to ensure compliance with statutory obligations for enforcing financial sanctions in terms of the national legislation and international conventions. Such measures could include VASPs placing a hold on a wallet until screening is completed and confirmed that there are no concerns raised.

7.9 Reporting Obligations

Authorities should require that all registered VASPs who have good reason to suspect that VA are the proceeds of illegal acts or are connected to ML/FT to immediately report their suspicions to the appropriate authorities. Accordingly, authorities should ensure that VASPs file suspicious transactions reports ('STR') to the authorities without tipping off their clients about the filed STRs. The ability of the authorities to better comprehend and analyse ML/TF operations in the VA ecosystem has been improved thanks to the STRs that reference VAs in their reports.[97]

7.10 Cross-Jurisdictional Co-operation

International co-operation by competent authorities is critical, given the transnational and virtual nature of VA activities and the VASP sector. Countries should implement the necessary regulations that provide for mutual legal assistance, identify proceeds and instrumentalities of crime, and provide for freezing, seizing, and confiscating of the proceeds of crime in the form of VAs and other assets associated with illegal VASP activities. Where criminal acts have been suspected or are being investigated, the authorities should provide effective extradition assistance and co-operation to bring to book those engaged in ML/TF illicit activities.

8 SOUTH AFRICA TRUDGES TOWARDS REGULATING CRYPTOCURRENCIES

The South African Crypto Assets Regulatory (CAR) Working Group of IFWG, ('CAR Working Group of IFWG') agrees that crypto assets cannot remain outside of the South African regulatory framework and recommends that South Africa

[96] *Ibid*.
[97] FATF 2021 VASPs Guidance, *supra* note 87 at 67.

implements a gradual approach to regulate the cryptocurrencies and the CASPs.[98] Though late, this is a bold step towards formulating a regulatory regime as cryptocurrencies cannot be ignored and wished away anymore. To this end, the CAR Working Group of IFWG made various recommendations on the urgent need to regulate crypto assets.

8.1 CASPs Declared Accountable Institutions in terms of the FICA

CASPs are now recognised and categorised as Accountable Institutions under Schedule 1 of the Financial Intelligence Centre Act, 38 of 2001 (FIC Act).[99] Being designated as an Accountable Institution brings with it a host of regulatory obligations on the CASPs. This entails registering with the Financial Intelligence Centre ('FIC'), performing CDD, identifying and verifying clients, maintaining transactional records, continuously monitoring and reporting suspicious and unusual activities to the FIC, and informing the FIC of odd transactions;[100] reporting cash transactions of R50 000.00[101] and above (or the applicable limit at any given time); and reporting the ownership of property that could be connected to terrorist action or terrorist organizations' activities.[102]

8.2 Developing Risk Management Programmes

Now that the CASPs are recognised as Accountable Institutions, they would be required to develop own Risk Management Programmes ('RMCP') in terms of section 42 of the FIC Act. The CASP RMCP must document how the CASPs will, among other obligations, manage and mitigate the ML/TF risk faced by the CASPs.[103] The RMCP should document how the CASPs will develop, document, maintain and implement an RBA in the risk management of ML/TF.

8.3 Suspicious Transactions Reports and Sanctions Enforcement

CASPs as Accountable Institutions are required to report suspicious transactions in terms of section 29 of the FIC Act and are prohibited in terms of section 26B from

[98] These are the equivalent of VASPs, South Africa refers to them as 'CASPs', and for this section of the Paper, and for the Recommendation, the writer will use CASPs as the Recommendation are for the South African jurisdiction.
[99] Government Gazette No. 47596 of 29 November 2022, gazetted CASPs as Accountable Institutions, effective 19 December 2022, and therefore must report all suspicious transactions and provide records to the authorities in terms of the FIC Act. (Item 22(c) of the Government Gazette No. 47596 of 29 November 2022).
[100] Ss 20-29 of the FIC Act.
[101] FIC has changed the Cash Transactions Reportable ('CTR') amount from the initial R25 000, to the new amount of R50 000 effective 14 November 2022.
[102] 2021 Intergovernmental Fintech Working Group '*Position paper on crypto assets'* at 3.
[103] Section 42 of the FIC Act, 38 of 2001, as amended.

dealing with individuals and entities sanctioned by the United Nations Security Council.[104]

8.4 Regulating Cross-Border Financial Flows

The IFWG's CAR Working Group suggests that SARB take on the oversight duties for the supervision of international and cross-border financial transfers and transactions using crypto assets and CASPs. This would necessitate the Finance Minister to make the necessary changes to the definition section of Exchange Control Regulation 10(4) and include crypto assets as in the definition of 'capital.' FinSurv would also have to update the Currency and Exchanges Manual to facilitate the reporting of transactions involving the transfer of foreign currency for the purpose of purchasing cryptocurrency assets crypto asset trading platforms.[105]

8.5 Crypto Assets as Financial Products

CAR Working Group of IFWG also recommended that crypto assets be recognised as a "financial product" through the necessary amendments to the Financial Advisory and Intermediary Services Act 37 of 2002 (the FAIS Act). As a result, CASPs would have to be registered and obtain licenses as financial services intermediaries. This would enable regulatory control and supervision and will provide consumer protection against dishonest CASP entities.[106] In response to this recommendation, the Financial Sector Conduct Authority, through a notice in the Government Gazette, designated and declared crypto assets as financial products in terms of the FAIS Act.[107] Following the proclamation, the Financial Sector Conduct Authority ('FSCA') can now take action against any unauthorised and unlicensed service providers offering "advice" and/or "intermediary services" in relation to crypto assets.

9 CONCLUSION.

The South African regulators have three options when deciding whether to regulate crypto assets: (i) ban, (ii) regulate, or (iii) do nothing. Banning crypto asset would be contrary to the recommendation and guidance of FATF who in 2015 warned against outright banning of cryptocurrency-related activities, because doing so may push such activities underground with little to no regulatory monitoring.[108]

---

[104] S26B of the FIC Act.
[105] 2021 Intergovernmental Fintech Working Group '*Position paper on crypto assets'* at 3.
[106] *Ibid*.
[107] Financial Sector Conduct Authority General Notice No:1350 of 2022.
[108] FATF. (2015). Guidance for a risk-based approach: Virtual currencies. June 2015. Available at https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf (Accessed 25 November 2022).

Authorities in South Africa must take regulatory action to make sure that safeguards are put in place to stop the corrosive effects of cryptocurrencies on the financial industry.[109] South Africa should aim to mitigate and manage the risks posed by cryptocurrencies such as ML/TF and the current lack of consumer protection laws, while at the same time recognising the potential benefits resulting from such financial innovations. An RBA regulatory framework should be applied by South African authorities to control and manage the CASPs in a manner that fairly balances the potential advantages and disadvantages introduced into the financial system by the cryptocurrencies. The authorities must preserve a level playing field by that does not unfairly favor or disadvantage the new fintech entrants or the established role players. To achieve this, CASPs must be effectively managed with appropriate regulations that are proportionate to the risks they pose (i.e., RBA to cryptocurrency regulation must be applied).

The regulators must continue to aggressively follow the market's dynamic developments, especially by staying informed of new global best practices and striving to implement them in the South African market. Lastly, there should be active and aggressive investment by all role players in cryptocurrency literacy that aims to raise the knowledge about cryptocurrencies among the existing and potential users of crypto assets.

[109] Mothokoa, *supra* note 29 at 60.

10 BIBLIOGRAPHY

Books and Journals.

1) Brito, Jerry *et al* "Bitcoin: A primer for policymakers" Mercatus Centre at George Mason University 2013 10.

2) Cvetkova, Irina "Cryptocurrencies Legal Regulation." (2018) Volume 5 Issue 2 BRICS Law Journal Volume 5 Issue 2 2018 128–153.

3) Erasmus, Deon *et al,* "A Critical Analysis of South African Anti-Money Laundering Legislation with regard to Cryptocurrencies*"* (2020) Obiter Volume 2 Issue 41 2020.

4) European Central Bank "Virtual Currency Schemes – a further analysis" 2015 26.

5) Fanusie, Yaya, & Robinson, Tom "Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services." Center on Sanctions and Illicit Finance 2018 11.

6) Itzikowitz, Angela *et al* "South Africa" in J Dewey (ed) "Blockchain & Cryptocurrency Regulation." London: Global Legal Group Ltd 1st ed 2019 432 – 437.

7) Mabunda, Sagwadi "Cryptocurrency: The new face of cyber money laundering." International Conference on Advances in Big Data, Computing and Data Communication Systems, University of the Western Cape Research Repository 2018.

8) Mothokoa, Karabo "Regulating Crypto-Currencies in South Africa: The Need for an Effective Legal Framework to Mitigate the Associated Risks." LLM mini-dissertation, University of Pretoria 2017.

9) Sicignano, Gaspare Jucan "Money Laundering using Cryptocurrency: The Case of Bitcoin." 2021 Athens Journal of Law 7 (2) 253-264.

10) Swinton, Caroline "A critical analysis of the risks associated with crypto-currencies" unpublished LLM thesis, University of Dundee, 2015.

11) Williams, Carol "An Analysis of the Critical Shortcomings in South Africa's Anti-Money Laundering Legislation." LLM mini-dissertation, University of the Western Cape 2017.

12) US Department of Justice, "Report of the Attorney General's Cyber Digital Task Force" October 2020.

Guidance Notes and Position Papers.

1) 2014 FATF Report: Virtual Currencies- 'Key Definitions and Potential AML/CFT Risks.

2) 2018 Kiel Institute for the World Economy “Virtual currencies: monetary dialogue.”
3) 2020 Intergovernmental Fintech Working Group (IFWG) Position Paper on Crypto Assets.
4) 2020 US Department of Justice, “Report of the Attorney General’s Cyber Digital Task Force.’’
5) 2021 FATF Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers.
6) 2022 Intergovernmental Fintech Working Group (IFWG) Position Paper on Crypto Assets

Website Sources

1) S Nakamoto Bitcoin: A Peer-to-Peer Electronic Cash System http://www.bitcoin.org/bitcoin.pdf

2) FATF. (2015). Guidance for a risk-based approach: Virtual currencies. June 2015. Available at https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf

3) Kiel Institute for the World Economy “Virtual currencies: monetary dialogue July 2018” European Union.” http://www.europarl.europa.eu/cmsdata/149902/KIEL_

4) How is Cryptocurrency changing the world? https://fintech.global/2022/05/03/how-is-cryptocurrency-changing-money-laundering/

5) Europol Spotlight, “Cryptocurrencies Tracing the Evolution of Criminal Finances.” https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf

6) International Monetary Fund “The IMF and the Fight Against Money Laundering and the Financing of Terrorism” http://www.imf.org/en/About/Factsheets/Sheets/2016/08/01/16/31/Fight-Against-Money-

7) Oversight of the South African National Payment System https://www.resbank.co.za/content/dam/sarb/what-we-do/payments-and-settlements/regulation-oversight/Oversight.pdf

8) Cryptocurrency Regulations Around the World https://complyadvantage.com/insights/cryptocurrency-regulations-around-world/

9) “Increased Popularity for Self-Directed IRAs” According to IRA Financial Group http://www.prweb.com/releases/bitcoins-self-directed-/ira-taxproperty-currency/prweb11704323.htm

10) Central African Republic Adopts Bitcoin as Legal Tender https://www.competitionpolicyinternational.com/central-african-republic-adopts-bitcoin-as-legal-tender/

11) Central African Republic Top Court Blocks purchase with new Cryptocurrency https://www.reuters.com/technology/central-african-republic-top-court-blocks-purchases-with-new-cryptocurrency-2022-08-29/

12) AML Guide: Cryptocurrency in El Salvador https://sanctionscanner.com/blog/cryptocurrencies-in-el-salvador-631

13) El Salvador’s Comeback Constrained by Increased Risks https://www.imf.org/en/News/Articles/2022/02/15/cf-el-salvadors-comeback-constrained-by-increased-risks

South African Legislation

1) Banks Act 94, of 1990.
2) Constitution of the Republic of South Africa Act 108, of 1996.
3) Consumer Protection Act 28, of 2008.
4) Financial Advisory and Intermediaries Services Act 37, of 2002.
5) Financial Intelligence Centre Act 31, of 2001.
6) Financial Intelligence Centre Amendment Act 1, of 2017.
7) Financial Sector Regulation Act 9, of 2017.
8) National Credit Act 34, of 2005.
9) National Payment System Act 78, of 1998.
10) The South African Reserve Bank Act 90 of, 1989.

South African Government Gazettes and General Notices

1) Exchange Control Regulations, 1961.
2) Government Gazette No. 47596 of 29 November 2022.
3) Financial Sector Conduct Authority General Notice No:1350 of 2022

Foreign Legislation

1) El Salvador Bitcoin Law 2021.
2) UK 5th Anti-Money Laundering Directive (‘5AMLD and 6AMLD).
3) United States of America: Bank Secrecy Act of 1970 as amended by the USA Patriotic Act 31 U.S.C.