VOL 36 NO 3 2024

SA MERCANTILE LAW JOURNAL

SA TYDSKRIF VIR HANDELSREG

Including
2023 CFML
Conference Papers

SA MERC LJ

2024 VOL 36 NO 3 361 - 572

juta

SA MERCANTILE LAW JOURNAL

EDITOR
DR NZUMBULULO SILAS SIPHUMA
LLB (NWU) LLM LLD (Stell)
GUEST EDITOR
PROF HOWARD CHITIMIRA
LLB, LLM (UFH), LLD (NMMU)
MANAGING EDITOR
MRS ZUENÉ TALJAARD
LLB LLM (Pret)
DEPUTY EDITORS
PROF REHANA CASSIM
BA LLB LLM (Wits) LLD (Unisa)
PROF DOROTHY MMAKGWALE FARISANI
B Proc LLB LLM (Unisa) PhD Law (UKZN)
PROF TUKISHI MANAMELA
B Proc LLB (Unin) LLM LLD (Unisa)
ASSISTANT EDITORS
MR BONGANI KHUMALO
LLB LLM (Unisa)
DR RICHARD M SHAY
LLB LLM LLD (Stell)
PROF ME MANAMELA
B Proc LLB (Unin) LLM LLD (Unisa)
PROF MAPHUTI TUBA
LLB (Wits) LLM LLD (Unisa)
DR VELA MADLELA
LLB LLM (Wits) LLD (Pret)

EDITORIAL ADVISORY BOARD

PROF J KIGGUNDU
University of Botswana
THE HON FR MALAN
Retired Judge of Appeal, Supreme Court of Appeal
Honorary Professor, University of Johannesburg
THE HON D MOSENEKE
Retired Deputy Chief Justice, Constitutional Court
THE HON BM NGOEPE
Retired Judge President, North Gauteng, South Gauteng and Limpopo High Courts
THE HON CME O'REGAN
Retired Justice, Constitutional Court
THE HON R H ZULMAN
Retired Judge of Appeal, Supreme Court of Appeal

EDITORIAL PANEL

PROF JL BRINK
Professor extraordinarius, University of South Africa
Attorney, Johannesburg
PROF DW BUTLER
Professor emeritus, University of Stellenbosch
PROF HJ DELPORT
Professor emeritus, Nelson Mandela Metropolitan University
PROF PA DELPORT
Professor emeritus, University of Pretoria
PROF CJ VISSER
University of South Africa
PROF A ITZIKOWITZ
University of the Witwatersrand
Attorney, Johannesburg
PROF VA LAWACK
Deputy Vice-Chancellor (Academic)
University of the Western Cape
PROF PAK LE ROUX
Professor extraordinarius, University of South Africa
Attorney, Johannesburg
PROF J NEETHLING
Research Fellow, University of the Free State
PROF JT PRETORIUS
Professor emeritus, University of South Africa

This peer reviewed journal is approved by the Department of Higher Education for SAPSE purposes

ISSN: 1015-0099
Typeset by CBT Typesetting & Design
Printed and bound by Insidedata

SUBSCRIPTION — INSKRYWING

Subscriptions taken through agents or bookshops:
R1 528,00 (including VAT but excluding postage and packaging)

Inskrywings deur agente of boekwinkels:
R1 528,00 (BTW ingesluit maar sonder posgeld en verpakking)

Subscriptions taken directly through Juta:
R1 528,00 (including VAT but excluding postage and packaging)

Inskrywings direk deur Juta:
R1 528,00 (BTW ingesluit maar sonder posgeld en verpakking)

Postage and packaging charges per subscription:
South Africa – R335
African States – R662
International – R900
Posgeld en verpakkingskoste per inskrywing:
Suid-Afrika – R335
Afrika State – R662
Internasionaal – R900

Subscriptions should be directed to the publisher:
JUTA Law, PO Box 24299, Lansdowne, 7779, Republic of South Africa
E-mail: cserv@juta.co.za

Inskrywings moet gerig word aan die uitgewer:
JUTA Law, Posbus 24299, Lansdowne, 7779, Republiek van Suid-Afrika
E-pos: cserv@juta.co.za

Exclusive Distributors in North America:
Gaunt, Inc., Gaunt Building, 3011 Gulf Drive, Holmes Beach,
Florida 34217-2199, USA
Telephone: 941-778-5211. Fax: 941-778-5252.
E-mail: info@gaunt.com

Three issues of SA *Merc LJ* will appear annually, published by
Juta Law for the School of Law, University of South Africa

Drie uitgawes van SA *Merc LJ* sal jaarliks verskyn, uitgegee deur
Juta vir die Skool vir Regsgeleerdheid, Universiteit van Suid-Afrika

---

INFORMATION FOR CONTRIBUTORS AND REFEREES

See: <*https://www.jutajournals.co.za/samlj/-style-guide*>

SA MERCANTILE LAW JOURNAL
Vol 36 No 3 2024

Date of publication: April 2025

CONTENTS

Articles

The first six articles in this volume are contributions that were presented at the North West University's Third Annual Internation Conference on Corporate & Financial Markets Law (CFML), held on 25–27 October 2023 in Namibia

Promotion of financial inclusion for low-income earners in South Africa ..... *Jean Chrysostome Kanamugire* 361

Should payment of additional remuneration to business rescue practitioners outside section 143 of the Companies Act be prohibited?
..... *Motseotsile Clement Marumoagae & Kiyasha Thambi* 378

Defining corporate social responsibility, corporate social investment and corporate philanthropy for South Africa
..... *Margaretha J Preston* 398

An overview of the statutory duty to cooperate and collaborate between the South African Reserve Bank and other financial roleplayers under the Financial Sector Regulation Act 9 of 2017..... *Howard Chitimira & Sharon Munedzi* 423

Towards the recognition of financial inclusion as a fundamental socio-economic right in selected SADC countries
..... *Howard Chitimira & Luck Mavhuru* 440

A critical assessment of the regulation of cryptocurrency in Nigeria..... *Isau Ahmed Olatunji* 457

The role, relevance and effect of the strike in the 4IR Age of Auto and Robots: A South African Perspective
..... *Nozipho Gwala & Lux Kwena Kubjana* 482

Putting the unconstitutionality of deemed discharge behind us? A review of recent developments on deemed dismissals ..... *Vuyo Ntsangane Peach* 495

A comparative critical analysis of the effectiveness of Remuneration Committees in the determination of executive remuneration in South Africa ..... *Ophellia Kimbini, Rehana Cassim & Michele Havenga* 516

Franchise termination with particular reference to the petroleum sector: Goodbye and good luck, but who owns the goodwill? ..... *Tanya Woker* 544

A CRITICAL ASSESSMENT OF THE REGULATION OF CRYPTOCURRENCY IN NIGERIA

ISAU AHMED OLATUNJI*
Senior Lecturer, Department of Business and Private Law, Faculty of Law, Kwara State University

Abstract

Over the years, there has been a tremendous increase in the use of cryptocurrency as a virtual means and form of payment worldwide. However, in recent years, there has been a steady increase in the use of cryptocurrency for illicit and criminal activities such as money laundering, financing terrorism and other illegal activities. In addition, the virtual nature of cryptocurrency creates opportunities for tax evasion thereby constituting a serious tax challenge for countries. This makes it necessary for countries to put in place measures to regulate cryptocurrency to prevent its use for illicit and criminal activities. Various countries have established certain measures and legislations to regulate the use of cryptocurrency. The objective of this article is to examine nature of cryptocurrency as well as its regulation in some selected jurisdictions. The paper will also examine how cryptocurrency is currently regulated in Nigeria.

Keywords: cryptocurrency; illicit use; criminal activities; terrorism activities; regulation.

I INTRODUCTION

Advancements in technology have led to the emergence of virtual forms of payment such as 'cryptocurrency'. Cryptocurrency can serve as a means of payment, a store of value, a unit of account and it is an investment product.[1] However, cryptocurrency does not enjoy legal tender status in most countries of the world.[2]

* LLB PhD (Unilorin), LLM (University of London). Associate, Chartered Institute of Taxation of Nigeria (CITN).

[1] Perkins, 'Cryptocurrency: The economics of money and selected policy issues' 2020 available at https://sgp.fas.org/crs/misc/R45427.pdf, accessed on 7 March 2024.

[2] Srokosz, 'Legal and economic analysis of the cryptocurrencies impact on the financial system stability' (2015) 4(2) *Journal of Teaching and Education* 619 at 620.

https://doi.org/10.47348/SAMLJ/v36/i3a6

Over the past few years, there has been a tremendous increase in the use of cryptocurrency as means of payment in Nigeria. For example, a report commissioned by a New York-based blockchain research firm, Chainalysis, stated that the volume of cryptocurrency transactions in Nigeria grew nine per cent year-over-year to US$56.7 billion between July 2022 and June 2023.[3] The growing use of cryptocurrency in the global financial system has profound implications for governments, investors, consumers and businesses as its privacy and anonymity increases the risk of its use for illicit and criminal activities.[4] This makes it necessary for countries to put in place measures to regulate cryptocurrency to prevent its use for illicit and criminal activities.

In this regard, many countries have introduced measures to regulate cryptocurrency within their respective jurisdictions. Developing countries such as Nigeria do not have comprehensive legislative measures to regulate cryptocurrency thereby exposing its use to illicit and criminal activities. This article examines the nature of cryptocurrency transactions, the international best practices for regulating cryptocurrency to prevent its use for illicit and criminal activities and the current regulation of cryptocurrency in Nigeria.

II DEFINITION OF CRYPTOCURRENCY

Cryptocurrency is a cryptographically decentralised digital currency used as a means of exchange.[5] According to the European Commission, cryptocurrency is a digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of payment and can be transferred, stored, or traded electronically.[6]

The above definition of cryptocurrency is suggestive of the fact that the significant and fundamental nature of cryptocurrency is that it is not issued by a central bank, government or public authority thereby rendering it theoretically immune to government interference or

[3] Dzirutwe & Holmes, 'Nigerian central bank lifts ban on crypto trading' 2023, available at https://www.reuters.com/world/africa/nigerian-central-bank-lifts-ban-crypto-trading-2023–12–23, accessed on 7 March 2024.

[4] Gruber, 'Trust, identity and disclosure: Are bitcoin exchanges the next virtual havens for money laundering and tax evasion?' (2013) *Quinnipiac Law Review* 135 at 204.

[5] Cvetkova, 'Cryptocurrencies legal regulation' (2018) 5(2) *Brics Law Journal* 128 at 130.

[6] 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' 2018, available at https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CeleX%3a52016PC0450, accessed 1 March 2024.

https://doi.org/10.47348/SAMLJ/v36/i3a6

manipulation.[7] This is in stark contrast to traditional fiat currencies such as the Nigerian Naira, the United Kingdom Pound Sterling, the South African Rand, the US Dollar, the Euro, the Indian Rupee, the Japanese Yen, the Swiss Franc and the Chinese Yuan, etc., which are usually issued by the government's central bank and are designated as legal tender within the boundary of the issuing country.[8] The issuance by a central authority is one of the basic characteristics which a currency must comply with before it can be legally designated as a means of payment.

It can, therefore, be rightly posited that most countries do not recognise cryptocurrency as their *de facto* currency and as such, it is not legally acknowledged as a means of payment. Therefore, the fact that cryptocurrencies are generally not recognised as 'legal tender' or declared the official currency of a country makes them fundamentally different from traditional fiat currencies.

It can also be deduced from the definition given by the European Commission that cryptocurrency can be accepted by natural or legal persons as a means of payment and can be transferred, stored, or traded electronically. This means that a cryptocurrency transaction is a peer-to-peer (P2P) decentralised form of transaction whereby the buyer and the seller transact and interact directly with each other without intermediation by a third party.

In this regard, when two individuals want to exchange cryptocurrency as a means of payment, they do not have to go through a third party such as a bank acting as an intermediary between them. The advantage of this is that it makes transactions quicker and cheaper as it allows the users of cryptocurrency to avoid paying a hefty transaction fee which may result from steep fees and processing fees usually charged by most banks and lawyers acting as intermediaries.[9]

III NATURE OF CRYPTOCURRENCY TRANSACTIONS

Cryptocurrency transactions are enabled by an online database known as a 'blockchain'.[10] A blockchain is a digital ledger that is used to record transactions between two parties in a verifiable permanent way. One of

[7] Bunjaku, Gjorgieva-Trajkovska & Miteva-Kacarski, 'Cryptocurrencies–advantages and disadvantages' (2017) 27(1) *Journal of Economics* 35 at 39.

[8] Chuen, *Handbook of digital currency: Bitcoin, innovation, financial instruments and big data*' (Elsevier 2015) 320.

[9] Bunjaku, Gjorgieva-Trajkovska & Miteva-Kacarski, (2017) 27(1) *Journal of Economics* 35 at 40.

[10] Cvetkova, (2018) 5(2) *Brics Law Journal* 128 at 132.

https://doi.org/10.47348/SAMLJ/v36/i3a6

the key features of a blockchain is that it is a distributed database which allows different parties to share information without requiring a central administrator. By decentralising its data, a blockchain eliminates the risk of a centralised database which can easily be a lucrative target for hackers.[11]

Another key feature of a blockchain is that each transaction on the blockchain is signed digitally, using public key cryptography. Public key cryptography involves the use of two keys – a public and private key. The public key is used to sign and encrypt the sent message, and anyone can see this key.[12] However, only the recipient of cryptocurrency has the private key. The private key guarantees the privacy and anonymity of the transactions and the parties involved as it is only the recipient of cryptocurrency that can decrypt the transaction. This feature of blockchain ensures an immutable and rapid settlement of transactions without any financial intermediation and the use of pseudonymous addresses and anonymity in cryptocurrency transactions.[13]

The implication of this is that tracking cryptocurrency transactions within blockchain can prove difficult, especially for people who do not have access to the blockchain. This privacy and the anonymity feature of cryptocurrency transactions increases the use of cryptocurrency for criminal and illicit activities.[14]

The above unique features of cryptocurrency, especially its privacy and anonymity features, give it some advantages over traditional fiat currency and make it popular as a new method of payment.[15] It is, therefore, not surprising that it was projected that by the year 2023, the value of cryptocurrency transactions would rise to US$16.16 billion as more businesses accept digital currencies as a means of payment.[16] This represents a 177.3 per cent increase from US$2.20 billion in 2021 and

[11] Donovan, Gantori, Ganesh, DeMichiel Dennean, Trussardi & Klien, 'Cryptocurrencies: Beneath the bubble' 2017, available at https://www.ubs.com/gobal/en/about_ubs/follow_ubs/ubs-economic insights/paul_donovan/2017/10/16/cryptocurrencies-beneath-the-bubble.html, accessed on 9 March 2024.

[12] Bitcoin Exchange Guide, 'An introduction to Blockchain: Distributed ledger technology application benefits' 2016, available at https://www.bitcoinexchangeguide.com/blockchain-distributed-ledger-technology/, accessed on 12 March 2024.

[13] Bitcoin Exchange Guide 2016, available at https://www.bitcoinexchangeguide.com/blockchain-distributed-ledger-technology/, accessed on 12 March 2024.

[14] Andersen Tax, 'Cryptocurrency and taxes: Bridging the digital gap' 2018, available at https://www.andersentax.ng/newsletters/cryptocurrency-and-taxes-bridging-the-digital-gap, accessed on 20 March 2024.

[15] Bunjaku, Gjorgieva-Trajkovska & Miteva-Kacarski, (2017) 27(1) *Journal of Economics* 35 at 41.

[16] Lebow, 'Crypto transaction value crosses $10 billion mark worldwide' 2021, available at https://www.emarketer.com/content/crypto-transaction-value-crosses-10-billion-mark, accessed on 19 March 2024.

https://doi.org/10.47348/SAMLJ/v36/i3a6

the projected cryptocurrency transactions of US$6.10 billion in the year 2022.[17] It is further projected that by the year 2027, the global cryptocurrency market will surpass US$32.4 trillion at a compound annual growth rate (CAGR) of 58.4 per cent between 2022–2027.[18]

The most popular types of cryptocurrencies are Bitcoin, Litecoin, Ethereum, Dash and XYO.[19] Cryptocurrency is not without its own disadvantages. According to Ivaschenko, one of the major disadvantages is that the use of cryptocurrency is susceptible to strong volatility as it is not regulated.[20] Other disadvantages include the risk of money laundering, terrorism and other illegal activity financing and the lack of a central issuer.[21]

IV CRIMINAL AND ILLICIT USE OF CRYPTOCURRENCY

Cryptocurrency also has legitimate uses. However, in recent times, there has been a surge in the use of cryptocurrency for illicit and criminal activities.[22] This has been attributed to its privacy and anonymity features which criminals have found attractive to conceal their illicit and criminal activities.

The unique features of cryptocurrency make it an attractive method for quickly transferring value across international borders without any financial intermediary and sometimes with minimal transaction fees, especially in developing countries without a secure and widely available banking infrastructure.[23] The global nature of blockchain technology also makes digital assets an attractive vehicle for malicious actors to hide their financial transactions and transfer assets in a quick and efficient way outside of traditional regulatory oversight.[24]

Several literatures, such as a report commissioned by the European Union Agency for Law Enforcement Cooperation (Europol), have examined the use of cryptocurrency for criminal and illicit activities.

[17] Lebow, 2021, available at https://www.emarketer.com/content/crypto-transaction-value-crosses-10-billion-mark, accessed on 19 March 2024.

[18] Research and Market, 'Global cryptocurrency market report 2022–2027-Industry to cross a staggering $32.4 trillion by 2027, exploding with a CAGR of 58.4%' 2023, available at https://finance.yahoo.com/news/global-cryptocurrency-market-report-2022–120800380.html, accessed on 4 February 2024.

[19] Cvetkova, (2018) 5(2) *Brics Law Journal* 128 at 132.

[20] Ivaschenko, 'Using cryptocurrency in the activities of Ukrainian small and medium enterprises in order to improve their investment attractiveness' (2016) 3 *Problems of Economy* 267 at 272.

[21] Ivaschenko, (2016) 3 *Problems of Economy* 267 at 272.

[22] Ivaschenko, (2016) 3 *Problems of Economy* 267 at 272.

[23] Ivaschenko, (2016) 3 *Problems of Economy* 267 at 272.

[24] Ivaschenko, (2016) 3 *Problems of Economy* 267 at 272.

https://doi.org/10.47348/SAMLJ/v36/i3a6

According to this report, criminals have resorted to using cryptocurrencies to perpetrate crimes such as money laundering, terrorism, fraud, cybercrime as well as drug trafficking in order to evade detection from security agents.[25] The report further indicated that cryptocurrency is continuously being adopted by criminals as their preferred choice of payment for illicit goods and services such as drugs, child sexual abuse materials and fraudulent cryptocurrency investments and cybercrime.

According to Tom Sadon, cryptocurrency is now regarded as an enabler of a multitude illegal and disreputable purposes such as: money laundering, fraud, drug trafficking, human trafficking, child exploitation, dark marketplace trading, cybercrime, terror funding and so on.[26] Some of the illicit and criminal activities globally recognised and associated with cryptocurrency are considered below:

(a) Money laundering

According to the Europol Report, money laundering constitutes one of the criminal activities associated with the illicit use of cryptocurrency due to its privacy and anonymity features which give opportunities to criminals to launder their illicit proceeds. The Europol's report indicated that the use of cryptocurrencies in money laundering schemes has been on the increase.[27]

According to Chainalysis, the use of cryptocurrency creates a possibility for criminals to move large cash transactions, mitigates the risk of suspicious transactions being frozen, reversed or traced, and prevents banks from notifying governments of suspicious activities.[28] Chainalysis estimated that cybercriminals have laundered over US$33 billion worth of cryptocurrency since 2017. The British Broadcasting Corporation further estimated that criminals laundered US$8.6 billion (£6.4bn) of

[25] Europol, 'Cryptocurrencies: tracing the evolution of criminal finances' 2022, available at https://www.europol.europa.eu/publications-events/publications/cryptocurrencies-tracing-evolution-of-criminal-finances, accessed on 4 March 2024.

[26] Sadon, '5 reasons why criminals & terrorists turn to cryptocurrencies' 2021, available at https://www.cognyte.com/blog/5-reasons-why-criminals-are-turning-to-cryptocurrencies/, accessed on 4 March 2024.

[27] Europol, 2022, available at https://www.europol.europa.eu/publications-events/publications/cryptocurrencies-tracing-evolution-of-criminal-finances, accessed on 4 March 2024.

[28] Chainalysis, 'The 2022 crypto crime report' 2023, available at https://blockbr.com.br/wp-content/uploads/2022/06/2022-crypto-crime-report.pdf, accessed on 4 March 2024.

https://doi.org/10.47348/SAMLJ/v36/i3a6

cryptocurrency in 2021 which represented a 30 per cent increase from 2020.[29]

(b) Terrorism activities

Fundraising through cryptocurrency is a common practice that terrorist organisations use to raise funds for their activities.[30] For example, a report by the United States of America Congress titled 'Survey of Terrorist Groups and Their Means of Financing' stated that Al-Qaida conducted fundraising and campaigns with cryptocurrencies.[31]

The rise in the use of cryptocurrency as a form of fundraising is attributable to its privacy and anonymity which protects the identities of donors who want to support terrorists without being exposed.[32] According to Coinbase, donors are always willing to donate to terrorist organisations using cryptocurrency knowing quite well that their identities will not be exposed.[33]

(c) Ransomware

According to the report by the United States Department of Justice, cryptocurrency has also helped to fuel the rise of ransomware and other digital extortion activities.[34] The report defined a form of malicious code that blocks access to a victim's computer system or data, often by encrypting data or files on computer networks to extort ransom payments from victims in exchange for a decryption key to restore a victim's access to their systems or data. The report indicated that criminals make use of ransomware to infiltrate the victim's data before encrypting it and send a ransom demand that includes a threat to

[29] British Broadcasting Corporation, 'Crypto money laundering rises 30%, report finds' 2022, available at https://www.bbc.com/news/technology-60072195.amp, accessed on 4 May 2023.

[30] Wardhana & Nugroho, 'Abuse of cryptocurrency to funding international terrorism activities' 2023, available at https://prosiding.umy.ac.id/grace/index.php/pgrace/article/view/190, accessed on 13 March 2024.

[31] Bauer, 'Survey of terrorist groups and their means of financing' 2018, available at https://www.washingtoninstitute.org/policy-analysis/survey-terrorist-groups-and-their-means-financing, accessed on 4 March 2024.

[32] Bauer, 2018, available at https://www.washingtoninstitute.org/policy-analysis/survey-terrorist-groups-and-their-means-financing, accessed on 4 March 2024.

[33] Coinbase, 'An overview of the use of cryptocurrency in terrorist financing' 2021, available at https://www.coinbase.com/blog/an-overview-of-the-use-of-cryptocurrencies-in-terrorist-financing, accessed on 4 March 2024.

[34] United States Department of Justice, 'How to strengthen international law enforcement cooperation for detecting, investigating and prosecuting criminal activity related to digital assets' 2022, available at https://www.justice.gov/ag/page/file/1535236/download, accessed on 4 March 2024.

https://doi.org/10.47348/SAMLJ/v36/i3a6

release or publish the victim's data if the ransom is not paid in the form of cryptocurrency.

(d) Fraudulent activities

Criminals make use of cryptocurrency in 'romance scams' to defraud their victims by among other methods, assuming online identities to befriend and persuade victims to purchase digital assets and ultimately transfer those assets to the fraudster or entities under their control.[35] In addition, cryptocurrency has been adopted to commit a variety of fraud, theft and scams such as the theft of investor funds, Ponzi-like schemes, and frauds involving initial coin offerings (ICOs).[36]

Another report indicated that about US$1.7 billion in cryptocurrency was lost to scams, theft and fraud which rose to US$1.2 billion in the first quarter of 2019.[37] Investigation further revealed that since 2019, there has been a tremendous increase in the use of cryptocurrency to commit fraud and theft as it was estimated that more than US$10 billion in cryptocurrency was stolen or scammed from victims in 2021.[38]

(e) Tax evasion

The anonymity of cryptocurrency also creates opportunities for tax evasion. With the advancement in technological payment systems, businesses and consumers became conscious of the fact that cryptocurrency can be used as a means through which tax can be evaded when purchasing or selling goods or services with the intention of obtaining a financial benefit through the decentralised payment networks.[39] Accordingly, due to the anonymity provided by cryptocurrency, there is the potential for individuals to withhold

[35] Mengpi, 'Crypto fuel increase in romance scams' 2022, available at https://www.wsj.com/articles/pandemic-crypto-fuel-increase-in-romance-scams-11644879123, accessed on 4 March 2024.

[36] Federal Bureau of Investigation, 'Internet crime report 2021' 2022, available at https://www.ic3.gov/Media/ PDF/AnnualReport/2021_IC3Report.pdf, accessed on 4 March 2024.

[37] Chavez-Dreyfuss, 'Cryptocurrency thefts, fraud hit US$1.2 billion in first quarter' 2019, available at https://www.reuters.com/article/us-crypto-currency-fraud-idUSKCN1S62P3, accessed on 2 March 2024.

[38] Sigalos, 'Crypto scammers took a record US$14 billion in 2021' 2022, available at https://www.cnbc.com/2022/01/06/crypto-scammers-took-a-record-14-billion-in-2021-chainalysis.html, accessed on 2 March 2024.

[39] Torgler & Murphy, 'Tax morale in Australia: What shapes it and has it changed over time?' (2004) 7 *Journal of Australian Taxation* 298.

https://doi.org/10.47348/SAMLJ/v36/i3a6

reporting cryptocurrency-related income and thus evade taxes.[40]

From the above, there is no doubt that cryptocurrency has simplified the operations of criminals who can adopt it for their illicit and criminal activities without being detected. This makes it necessary for government to put in place measures and mechanisms to regulate cryptocurrency to prevent its use for illicit and criminal activities.

V LEGAL MECHANISMS TO COUNTER THE ILLICIT AND CRIMINAL USE OF CRYPTOCURRENCY

There is no global consensus on the legal mechanisms to be adopted to prevent criminals from using cryptocurrency for illicit and criminal activities. Attitudes and approaches to legal regulation of cryptocurrency in this regard differ per country.[41] However, the risk of money laundering, terrorism financing and other crimes associated with the illicit use of cryptocurrency has over the years gained global notoriety thereby pushing the issue of its regulation to the front burner of international discourse.[42]

At the forefront of leading the global fight against the abuse of cryptocurrency is the Financial Action Task Force (FATF). FATF is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of the proliferation of weapons of mass destruction.[43]

In 2012, the FATF proposed some recommendations for countries to adopt as preventive measures to directly counter and address the money laundering and terrorism financing risks associated with cryptocurrency. These recommendations are contained in the FATF report titled 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation'.[44]

These proposed recommendations provide the international minimum standard that countries are expected to implement in their

[40] Ly, 'Coining bitcoin's legal-bits: Examining the regulatory framework for bitcoin and virtual currencies' (2014) 27 *Harvard Journal of Law and Technology* 587 at 595.

[41] Cherniei, Cherniavskyi, Babanina & Tykhonova, 'Criminal liability for cryptocurrency transactions: Global experience' (2021)10 *European Journal of Sustainable Development* 304 at 316.

[42] Cherniei, Cherniavskyi, Babanina & Tykhonova, (2021)10 *European Journal of Sustainable Development* 304 at 320.

[43] Financial Action Task Force, 'Who we are' 2023, available at https://www.fatf-gafi.org/about/whoweare/, accessed on 2 March 2024.

[44] Financial Action Task Force, 'International standards on combating money laundering and the financing of terrorism & proliferation' 2024, available at www.fatf-gafi.org/en/publications/recommendations.html, accessed on 2 March 2024.

https://doi.org/10.47348/SAMLJ/v36/i3a6

respective jurisdictions to counter the illicit use of cryptocurrency.[45] Some of the recommendations proposed by FATF in the report are considered below.

(a) Licensing or registration obligations

Recognising the money laundering and terrorism financing risks associated with the illicit use of cryptocurrency, the FATF recommended that countries should ensure that persons and/or entities transacting in or operating cryptocurrency exchanges, generally classified as virtual asset service providers (VASP), are licensed, or registered in their respective jurisdictions. This recommendation is to ensure that countries can monitor the activities and operations of VASPs in their respective jurisdictions.

Monitoring the activities and operations of VASPs will allow the countries to take all necessary legal or regulatory measures to prevent criminals or their associates from holding or being the beneficial owner of a significant or controlling interest or holding a management function in a VASP. The FATF recommended that such legal or regulatory measures should include requiring VASPs to seek relevant authority's prior approval for substantive changes in shareholders, business operations, and structures.[46]

(b) Introduction of KYC (Know Your Client) requirements

A significant regulation of cryptocurrency transaction is the introduction of KYC (Know Your Client) requirements. The anonymity feature of cryptocurrency transactions creates room for identity theft and other kinds of illicit and criminal activities. It is in this regard that the KYC requirements were proposed by the FATF to prevent the illicit use of cryptocurrency and to trace transactions that may be indicative of crime.

The KYC requirements involve three steps: (i) identify the customers by collecting their personally identifiable information such as their full name, place of residence, date of birth, and address; (ii) compare the customers' information with the official documentation presented by the individual, such as a passport or state-issued driver's license, as well as proof of residence, such as a utility bill; (iii) run the customer's

[45] Financial Action Task Force, 2024, available at www.fatf-gafi.org/en/publications/recommendations.html, accessed on 2 March 2024.

[46] Financial Action Task Force, 2024, available at www.fatf-gafi.org/en/publications/recommendations.html, accessed on 2 March 2024.

https://doi.org/10.47348/SAMLJ/v36/i3a6

identity through official databases containing data on PEPs and sanctioned individuals.[47]

The FATF also advised financial institutions to follow KYC requirements to identify whether a client is at risk for money laundering and financial crime as a result of using cryptocurrency. If everything is in order, the customer can use a cryptocurrency exchange.[48]

(c) Anti-money laundering/countering the financing of terrorism requirements

Recognising the risks of money laundering and terrorism financing associated with the illicit use of cryptocurrency, the FATF recommended that countries should ensure that VASPs are regulated for Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) purposes by imposing certain AML and CFT compliance requirements on VASPs.[49]

Through this recommendation, countries are expected to put adequate legal and regulatory frameworks in place to supervise or monitor and ensure compliance by VASPs with requirements to combat money laundering and terrorist financing.[50] Such legal and regulatory framework should include the authority to conduct inspections, compel the production of information and impose a range of disciplinary and financial sanctions such as powers to withdraw, restrict or suspend the VASP's license or registration.

It is also recommended that countries criminalise terrorist financing because of the Terrorist Financing Convention which should extend not only to the financing of terrorist acts but also to the financing of terrorist organisations and individual terrorists even in the absence of a link to a specific terrorist act or acts. Countries should ensure that such offences are designated as money laundering predicated offences.[51]

[47] Financial Action Task Force, 2024, available at www.fatf-gafi.org/en/publications/recommendations.html, accessed on 2 March 2024.

[48] Electronic Identification (eID), 'KYC crpyto: meaning, requirements and why it is important', available at https://www.electronicid.eu/en/blog/post/crypto-exchanges-compliance/en accessed on 28 February 2024.

[49] Financial Action Task Force, 2024, available at www.fatf-gafi.org/en/publications/recommendations.html, accessed on 2 March 2024.

[50] Financial Action Task Force, 2024, available at www.fatf-gafi.org/en/publications/recommendations.html, accessed on 2 March 2024.

[51] Financial Action Task Force, 2024, available at www.fatf-gafi.org/en/publications/recommendations.html, accessed on 2 March 2024.

https://doi.org/10.47348/SAMLJ/v36/i3a6

(d) Introduction of sanctions

It is recommended that countries introduce a wide range of effective, proportionate, and dissuasive sanctions, whether criminal, civil or administrative, to deal with VASPs that fail to comply with AML/CFT compliance requirements or any other requirement. The sanctions can include the power to withdraw, restrict or suspend the VASP's license or registration, where applicable. Such sanctions should be applicable not only to VASPs, but also to their directors and senior management.[52]

(e) Introduction of guidelines

The FATF's report also recommends that countries should provide guidelines in the form of advisories to assist VASPs' compliance with AML and CFT requirements. It is further recommended in the report that countries should endeavour to introduce measures to combat money laundering and terrorist financing and measures to assist them in detecting and reporting suspicious transactions.[53] The essence of this is to create a culture of compliance and ensure certainty concerning the legal framework of treatment of cryptocurrency. Countries may consider emphasising AML/CFT requirements to VASPs through public communication and events such as education campaigns, seminars, workshops and so on. [54]

(f) Introduction of travel rule

The FATF's report recommended that countries should impose a rule known as 'travel rule obligation' on VASPs.[55] By this rule, VASPs are required to obtain and hold accurate originator information and beneficiary information on cryptocurrency transfers. Such information is to be made available on request to the appropriate authorities. The objective of this rule is to prevent terrorists and other criminals from having unfettered access to electronically facilitated funds transfers for moving their funds and for detecting such misuse when it occurs. This

[52] Financial Action Task Force, 2024, available at www.fatf-gafi.org/en/publications/recommendations.html, accessed on 2 March 2024.

[53] Financial Action Task Force, 2024, available at www.fatf-gafi.org/en/publications/recommendations.html, accessed on 2 March 2024.

[54] Financial Action Task Force, 2024, available at www.fatf-gafi.org/en/publications/recommendations.html, accessed on 2 March 2024.

[55] Financial Action Task Force, 2024, available at www.fatf-gafi.org/en/publications/recommendations.html, accessed on 2 March 2024.

https://doi.org/10.47348/SAMLJ/v36/i3a6

rule is applicable to VASPs that provide services or engage in cryptocurrency transactions.[56]

(g) International cooperation

Given the cross-border and mobile nature of cryptocurrency transactions, it is recommended that countries engage in a wide range of international cooperation with other countries to counter the illicit use of cryptocurrency for money laundering and terrorist financing.[57] In particular, it is advised that countries should have a legal basis for exchanging information with their foreign counterparts on issues relating to cryptocurrency transfer. In this regard, it is recommended that countries have in place the tools necessary to co-operate with one another, provide mutual legal assistance; help identify, freeze, seize, and confiscate the proceeds and instruments of crime arising from cryptocurrency transactions and provide effective extradition assistance in the context of cryptocurrency-related crimes or illicit actors who engage in illicit activities among other international capabilities.

(h) Information exchange

Countries are advised to encourage information exchange between the public and private sectors as a strategy for combating the illicit use of cryptocurrency. It is recommended that public authorities should share risk information, where possible, to better help inform the risk assessments of VASPs. Such information exchange will go a long way to assist VASPs with their compliance obligations to enable them to provide more accurate and specific information to the relevant authority. Domestic co-operation and information exchange is also encouraged between the banking, securities, commodities, and derivatives sectors, law enforcement and financial intelligence units (FIU) which is also vital for the effective monitoring, supervision, and regulations of VASPs.

The above recommendations of the FATF are minimum international standards to regulate cryptocurrency but do not prevent any country from coming up with its own regulation. The FATF advise

[56] Financial Action Task Force, 2024, available at www.fatf-gafi.org/en/publications/recommendations.html, accessed on 2 March 2024.

[57] Financial Action Task Force, 2024, available at www.fatf-gafi.org/en/publications/recommendations.html, accessed on 2 March 2024.

https://doi.org/10.47348/SAMLJ/v36/i3a6

countries to implement these recommendations in a manner consistent with their national legislative and institutional systems.[58]

VI REGULATION OF CRYPTOCURRENCY IN SOME SELECTED JURISDICTIONS

The increased use of cryptocurrency for illicit and criminal activities has spurred many countries to put into place measures and mechanisms to regulate cryptocurrency within their respective jurisdiction. This article will consider the regulation of cryptocurrency in some selected jurisdictions.

The European Union through its Parliament passed a landmark cryptocurrency regulation, known as the Markets in Crypto-Assets Regulation (MiCA) on 20 April, 2023.[59] This regulation includes provisions for consumer and investor protection, addresses financial stability and monetary policy risks as well as measures against market manipulation, money laundering, terrorist financing and criminal activity.[60]

In Canada, the government has been proactive in regulating cryptocurrency. Government enacted the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) as early as 2014 to regulate cryptocurrency.[61] The objective of this Act is to implement specific measures to detect and deter the use of cryptocurrency for money laundering and for financing terrorist activities.[62] In August 2017, the Canadian Securities Administrators (CSA) issued a notice on the applicability of existing securities laws on cryptocurrencies, and in January 2018, the Head of Canada's Central Bank characterised them 'technically' as securities.[63] The Canada Revenue Agency has taxed cryptocurrencies since 2013 and Canadian tax laws apply to cryptocurrency transactions.[64]

[58] Financial Action Task Force, 2024, available at www.fatf-gafi.org/en/publications/recommendations.html, accessed on 2 March 2024.

[59] Williams, 'Europe passes landmark crypto regulation' 2023, available at https://www.verdict.co.uk/europe-passes-landmark-crypto-regulation/, accessed on 9 March 2024.

[60] Williams, 2023, available at https://www.verdict.co.uk/europe-passes-landmark-crypto-regulation/, accessed on 9 March 2024.

[61] Comply Advantage, 'Cryptocurrency regulations around the world' 2022, available at https://complyadvantage.com/insights/cryptocurrency-regulations-around-world/, accessed on 11 March 2024.

[62] Proceeds of Crime (Money Laundering) and Terrorist Financing Act 2000.

[63] Comply Advantage, 2022, available at https://complyadvantage.com/insights/cryptocurrency-regulations-around-world/, accessed on 11 March 2024.

[64] Comply Advantage, 2022, available at https://complyadvantage.com/insights/cryptocurrency-regulations-around-world/, accessed on 11 March 2024.

https://doi.org/10.47348/SAMLJ/v36/i3a6

In the United States of America, entities dealing in cryptocurrency and Digital asset firms are generally required to register with the Financial Crimes Enforcement Network (FinCEN) and comply with AML and sanction requirements.[65] Both FinCEN and the Office of Foreign Assets Control (OFAC), the primary US sanctions regulator, have released guidance and taken enforcement actions for violations of the requirements. Guidance from both regulators as well as the New York State Department of Financial Services has placed emphasis on using blockchain analytics to augment know your customer (KYC), transaction monitoring and sanctions screening programmes. New York has implemented a transaction monitoring and filtering regulation, requiring covered entities to affirmatively certify compliance with the regulation on an annual basis.[66]

Cryptocurrency regulation is fairly advanced in Australia. Entities dealing with Cryptocurrency are mandated to register with and gain approval from the Australian Transaction Reports and Analysis Centre (AUSTRAC).[67] AUSTRAC has the task of preventing, detecting, and responding to criminal abuse of the financial system, including cryptocurrency markets. Entities are required to adhere to strict AML and CFT regulations and reporting obligations. The Australian Securities and Investments Commission (ASIC) has also provided extensive regulatory guidance for businesses handling crypto assets.[68]

In the United Kingdom, entities dealing with cryptocurrency are required to register with the UK Financial Conduct Authority (FCA). Certain reporting obligations are imposed on cryptocurrency exchange providers. In this regard, such providers must comply with the reporting obligations implemented by the Office of Financial Sanctions Implementation (OFSI).[69] This requires providers to notify the OFSI as soon as possible if they know or

[65] PriceWaterCoopers, 'Global crypto regulation report' 2023, available at https://www.pwc.com/gx/en/new-ventures/cryptocurrency-assets/pwc-global-crypto-regulation-report-2023.pdf, accessed on 11 March 2024

[66] PriceWaterCoopers, 2023, available at https://www.pwc.com/gx/en/new-ventures/cryptocurrency-assets/pwc-global-crypto-regulation-report-2023.pdf, accessed on 11 March 2024.

[67] Reeds Solicitors, 'International crypto regulation–around the world' 2023, available at https://www.reeds.co.uk/insight/international-crypto-regulation-around-the-world/, accessed on 11 March 2024.

[68] Reeds Solicitors, 2023, available at https://www.reeds.co.uk/insight/international-crypto-regulation-around-the-world/, accessed on 11 March 2024.

[69] Bryan Cave Leighton Paisner, 'New sanctions reporting obligations on crypto asset providers' 2023, available at https://www.bclplaw.com/en-US/events-insights-news/new-sanctions-reporting-obligations-on-cryptoasset-providers.html, accessed on 9 March 2024.

https://doi.org/10.47348/SAMLJ/v36/i3a6

have reasonable suspicion that a person is subject to sanctions or has committed a financial sanctions offence.[70]

In Japan, crypto exchanges must register with the Financial Services Agency (FSA) and comply with AML/CFT obligations.[71] Also in South Korea, cryptocurrency exchanges and other virtual asset service providers must register with the Korea Financial Intelligence Unit (KFIU), a division of the Financial Services Commission (FSC).[72]

In South Africa, the Prudential Authority (PA) issued a guidance note for Banks on AML/CFT controls in relation to crypto assets and crypto asset service providers (CASP) in August 2022.[73] The note highlights the requirement for a risk-based approach to managing risks, instead of adopting a blanket de-risking policy. In October 2022, the Financial Services Conduct Authority (FSCA) declared crypto assets a 'financial product', under the Financial Advisory and Intermediary Services Act of 2002.[74] In November 2022, the definition of an 'Accountable Institution' in the Financial Intelligence Centre Act of 2001 was amended to include persons who carry on the business of exchanging crypto assets or crypto currency to a fiat currency or vice versa and persons conducting a transaction that transfers a crypto asset from one crypto asset address or account to another. This regulation will require such persons to comply with additional governance, risk, and compliance requirements under the Act, including specific obligations in relation to AML, CFT and sanctions controls. These requirements came into effect on 19 December 2022.[75]

VII REGULATION OF CRYPTOCURRENCY IN NIGERIA

The Nigerian government is quite aware of the criminal and illicit activities associated with cryptocurrency. In this regard, government has

[70] Bryan Cave Leighton Paisner, 2023, available at https://www.bclplaw.com/en-US/events-insights-news/new-sanctions-reporting-obligations-on-cryptoasset-providers.html accessed on 9 March 2024.

[71] Comply Advantage, 2022, available at https://complyadvantage.com/insights/cryptocurrency-regulations-around-world/, accessed on 11 March 2024.

[72] Comply Advantage, 2022, available at https://complyadvantage.com/insights/cryptocurrency-regulations-around-world/, accessed on 11 March 2024.

[73] PriceWaterCoopers, 2023, available at https://www.pwc.com/gx/en/new-ventures/cryptocurrency-assets/pwc-global-crypto-regulation-report-2023.pdf, accessed on 11 March 2024.

[74] PriceWaterCoopers, 2023, available at https://www.pwc.com/gx/en/new-ventures/cryptocurrency-assets/pwc-global-crypto-regulation-report-2023.pdf, accessed on 11 March 2024.

[75] PriceWaterCoopers, 2023, available at https://www.pwc.com/gx/en/new-ventures/cryptocurrency-assets/pwc-global-crypto-regulation-report-2023.pdf, accessed on 11 March 2024.

https://doi.org/10.47348/SAMLJ/v36/i3a6

been proactive in issuing notices about the pitfalls of investing in the cryptocurrency markets. For example, in February 2017, the Central Bank of Nigeria (CBN) banned commercial banks from engaging in any cryptocurrency transactions.[76] This was meant to protect citizens from black market criminal and fraudulent crypto activities.[77] In addition, the CBN also issued another circular dated 28 February 2018 warning Nigerians on the inherent risks of engaging in cryptocurrency transactions on the basis that cryptocurrencies are not regulated all over the world.[78]

On 5 February 2021, the Central Bank of Nigeria (CBN) released a letter addressed to Banks and other Financial Institutions which stated that dealing in cryptocurrencies and facilitating payment for cryptocurrency exchanges are prohibited.[79] The CBN further instructed all Banks and other Financial Institutions to identify individuals or entities who transact in cryptocurrency or operate cryptocurrency exchanges and close the accounts of such persons or entities.[80]

Despite the ban on cryptocurrency, its popularity continued to soar in Nigeria.[81] According to a 2022 report by CoinGecko, Nigeria ranks highest as the country most interested in cryptocurrency since the market crash in April 2022 and the most crypto-curious nation.[82] Another report by Chainalysis in 2023 ranked Nigeria second among the top 20 countries in the Global Crypto Adoption Index.[83] The

[76] Central Bank of Nigeria (CBN), 'Circular to banks and other financial institutions on virtual currency operations in Nigeria' 2017, available at https://www.cbn.gov.ng/out/2017/fprd/aml%20january%202017%20circular%20to%20fis%20on%20virtual%20currency.pdf, accessed on 15 March 2024.

[77] Securities Exchange Commission 'Public notice on investments in cryptocurrencies and other virtual or digital currencies' 2017, available at http://www.sex.gov.ng/public-notice-on-investments-in-cryptocurrencies-and-other-virtual-or-digital-currencies/, accessed on 15 March 2024.

[78] Central Bank of Nigeria (CBN), 'Again, CBN warns on virtual currencies' 2018, available at https://www.cbn.gov.ng/FeaturedArticles/2018/articles/CBN_VirtualCurrencies.asp, accessed on 15 March 2024.

[79] Alex-Adedipe & Atanda, 'Nigeria: prohibition of cryptocurrency transactions by the central bank of Nigeria' 2021, available at https://www.mondaq.com/nigeria/fin-tech/1036556/prohibition-of-cryptocurrency-transactions-by-the-central-bank-of-nigeria, accessed on 15 March 2024.

[80] Alex-Adedipe & Atanda, 2021, available at https://www.mondaq.com/nigeria/fin-tech/1036556/prohibition-of-cryptocurrency-transactions-by-the-central-bank-of-nigeria, accessed on 15 March 2024.

[81] Cointelegraph, 'An overview of cryptocurrency regulations in Nigeria' 2023, available at https://cointelegraph.com/learn/crypto-regulations-in-nigeria, accessed on 11 March 2024.

[82] CoinGecko, 'Top 15 countries most curious about cryptocurrency' 2023, available at https://www.coingecko.com/research/publications/top-15-countries-most-curious-about-cryptocurrency, accessed on 11 March 2024.

[83] Chainalysis, 'The 2023 global crypto adoption index top 20' 2024, available at https://www.chainalysis.com/blog/2023-global-crypto-adoption-index/, accessed on 11 March 2024.

https://doi.org/10.47348/SAMLJ/v36/i3a6

growth of cryptocurrency transactions in Nigeria is attributable to the inadequate financial services, high inflation, the depreciation of Nigeria's fiat currency (the Naira) and a young demographic (53.7 per cent of Nigeria's population aged 15–65) yearning for new opportunities for work, investment and financial independence.[84]

Amid the growing popularity of cryptocurrencies in the country, the Nigerian Financial Intelligence Unit (NFIU) in 2021 released advisory guidance on the application of the relevant FATF recommendations regarding cryptocurrency.[85] The purpose of the advisory guidance is to explain the application of the risk-based approach to AML/CFT measures in the virtual currency context, identify the entities involved in Virtual Currency payment products and services in Nigeria and clarify the application of the relevant FATF recommendations to convertible virtual currency exchangers.[86]

This guidance is also intended to educate the regulators, law enforcement officers, digital currency operators, financial institutions and designated non-financial institutions authorities to understand and potentially develop regulatory responses including the need to amend the law in order to address the potential ML/TF risks of Virtual Currency payment products and services.[87] This advisory is further intended to help the private sector better understand the relevant AML/CFT obligations on Virtual Currency and how they can effectively comply with relevant requirements. Importantly, the advisory incorporates the conceptual framework and key terms adopted by the FATF in its June 2014 Virtual Currency Report.[88]

In applying specific FATF recommendations to the regulation of Cryptocurrency in Nigeria, the NFIU recommended the following in its Advisory Guidance:

(i) Financial institutions and designated non-financial businesses and professions should be required to comply with customer identification, verification and transaction monitoring

[84] Cointelegraph, 2023, available at https://cointelegraph.com/learn/crypto-regulations-in-nigeria, accessed on 11 March 2024.

[85] Nigerian Financial Intelligence Unit, 'NFIU advisory on potential money laundering and terrorism financing risks of virtual currency' 2021, available at https://www.nfiu.gov.ng/Home/AdvisoryGuidance, accessed on 11 March 2024.

[86] Nigerian Financial Intelligence Unit, 2021, available at https://www.nfiu.gov.ng/Home/AdvisoryGuidance, accessed on 11 March 2024.

[87] Nigerian Financial Intelligence Unit, 2021, available at https://www.nfiu.gov.ng/Home/AdvisoryGuidance, accessed on 11 March 2024.

[88] Nigerian Financial Intelligence Unit, 2021, available at https://www.nfiu.gov.ng/Home/AdvisoryGuidance, accessed on 11 March 2024.

https://doi.org/10.47348/SAMLJ/v36/i3a6

requirements for decentralised convertible virtual currency using the most effective and efficient means available, as soon as such products/services are offered.

(ii) Financial institutions, designated non-financial businesses and professions, developers, investors, and other actors in the virtual currency space should seek to develop technology-based solutions that will improve compliance.

(iii) Financial institutions and designated non-financial businesses and professions are advised to explore developing business models to facilitate customer identification/verification, transaction monitoring, and compliance with other relevant Anti-money Laundering (AML) measures, countering the financing of terrorism (CFT).

(iv) To reduce the money laundering (ML) and terrorist financing (TF) risks associated with cryptocurrency, it was recommended that new virtual currency technologies, such as application programming interfaces (APIs) should be developed to provide customer identification information or allow financial institutions to limit transaction size and velocity or establish a variety of conditions that must be satisfied before a virtual currency transaction can be sent to the recipient/beneficiary.

(v) It was further recommended that a third-party digital identity system may also be developed to facilitate AML/CFT compliance requirements.

Following the NFIU's Advisory Guidance, the Securities and Exchange Commission (SEC) of Nigeria took on the task of framing cryptocurrency regulation.[89] The SEC, in May 2022, published a comprehensive 54-page document titled 'New Rules on Issuance, Offering Platforms and Custody of Digital Assets' on its website.[90] These New Rules open doors for cryptocurrency service providers in Nigeria and details a guideline for banking and financial institutions of the country on how they may interact with digital assets.[91]

The rules also clarified and defined digital assets in Nigeria and iterated that all digital assets token offerings, initial coin offerings and

[89] Cointelegraph, 2023, available at https://cointelegraph.com/learn/crypto-regulations-in-nigeria, accessed on 11 March 2024.

[90] Securities and Exchange Commission of Nigeria, 'Rules on issuance, offering platforms and custody of digital assets' 2022, available at https://sec.gov.ng/wp-content/uploads/2022/05/Rules-on-Issuance-Offering-and-Custody-of-Digital-Assets.pdf, accessed on 11 March 2024.

[91] Cointelegraph, 2023, available at https://cointelegraph.com/learn/crypto-regulations-in-nigeria, accessed on 11 March 2024.
(2023).

https://doi.org/10.47348/SAMLJ/v36/i3a6

any other blockchain-based offerings within Nigeria or by Nigerian issuers or foreign issuers engaging Nigerian citizens will be regulated by the Nigerian SEC.[92]

The SEC guidelines were not seen as providing clarity and certainty on the regulation of cryptocurrency in Nigeria.[93] This was due to the fact that the objective and purpose of the SEC guidelines was to provide rules on the issuance of digital assets as securities, Registration Requirements for Digital Assets Offering Platforms (DAOPs), rules on Registration Requirements for Digital Asset Custodians (DACs) offering Platforms and Custody of Digital Assets, rules on Virtual Assets Service Providers (VASPs) and rules on Digital Assets Exchange.

On 22 December 2023, the Central Bank of Nigeria (CBN), which had earlier banned cryptocurrency in 2021, overturned its ban on financial institutions dealing in cryptocurrency and opened the door for a regulated digital currency market.[94] According to the CBN, the reason for lifting the ban on cryptocurrency was due to the fact that current global trends have shown that there is a need to regulate the activities of virtual assets' service providers which include cryptocurrencies and crypto assets.[95] The implication of this is that bank accounts and transactions linked to cryptocurrency trading are no longer subjected to the previous restrictions, ensuring smoother financial operations.[96]

Accordingly, the CBN released guidelines for the regulation and operation of Cryptocurrency and Virtual Assets Service Providers (VASPs) in Nigeria.[97] Unlike the SEC guidelines, the new CBN guidelines provided the much-needed clarity, guidance and certainty in the regulation of cryptocurrency in Nigeria as it reflected the 2022

[92] Cointelegraph, 2023, available at https://cointelegraph.com/learn/crypto-regulations-in-nigeria, accessed on 11 March 2024.
2023).

[93] Law Allianz, 'Framework for the regulation of the Nigerian crypto assets market' 2023, available at https://lawallianz.com/articles/framework-for-the-regulation-of-the-nigerian-crypto-assets-market/, accessed on 11 March 2024.

[94] Credit Coin, 'Nigeria's crypto laws & regulation in 2024' 2024, available at https://creditcoin.org/blog/nigerias-crypto-laws-regulation/the-current-crypto-law-regulation-in-nigeria-as-of-2024, accessed on 11 March 2024.

[95] Central Bank of Nigeria, 'Guidelines on operation of bank accounts for virtual assets service providers (VASPs)' 2024, available at https://www.cbn.gov.ng/Out/2024/FPRD/GUIDELINES%20ON%20OPERATIONS%20OF%20BANK%20ACCOUNTS%20FOR%20VIRTUAL%20Asset%20Providers.pdf, accessed on 11 March 2024.

[96] Cointelegraph, 2023, available at https://cointelegraph.com/learn/crypto-regulations-in-nigeria, accessed on 11 March 2024.

[97] Central Bank of Nigeria, 2024, available at https://www.cbn.gov.ng/Out/2024/FPRD/GUIDELINES%20ON%20OPERATIONS%20OF%20BANK%20ACCOUNTS%20FOR%20VIRTUAL%20Asset%20Providers.pdf, accessed on 11 March 2024.

https://doi.org/10.47348/SAMLJ/v36/i3a6

recommendations from the Financial Action Task Force (FATF) and some of the guidelines in the SEC guidelines.[98]

Under the new CBN guidelines, Banks and Financial Institutions are still prohibited from holding, trading, or transacting in virtual currencies on their accounts, and cash withdrawals are not allowed. The guidelines also bar clearing third-party cheques through crypto accounts and limit withdrawals to two per quarter. However, institutions are now allowed to facilitate cryptocurrency transactions for customers, provided they adhere to strict customer KYC (Know Your Customer) and anti-money laundering (AML) checks. These new regulations stipulate that entities such as cryptocurrency exchanges and digital asset brokers must operate naira-denominated bank accounts exclusively. This move aims to integrate cryptocurrency transactions within the framework of the Nigerian banking system while maintaining a level of control over the operations.[99]

Under the CBN guidelines, entities dealing in cryptocurrency and Virtual Assets Service Providers (VASPs) in Nigeria are required to obtain a license from the SEC and register with the Corporate Affairs Commission (CAC), maintain a minimum paid-up capital of =N=500,000,000,00 million Naira, collect the Bank Verification Number (BVN) of cryptocurrency company owners, verify the identities of their customers and report suspicious transactions to comply with Know Your Customer (KYC) and anti-money laundering (AML) measures and submit a white paper to the SEC for approval if issuing tokens. Entities dealing in cryptocurrency and VASPs which wish to operate in Nigeria are also required to have a physical presence in the country to ensure that exchanges are within the regulatory purview of Nigerian authorities and to help support the local economy and create jobs.[100]

These new regulations place heavy emphasis on privacy and data protection. Thus, entities dealing in cryptocurrency and VASPs are under obligation to secure user data adequately and report any data breaches comprehensively, within stipulated periods. They're also obliged to

[98] Cointelegraph, 2023, available at https://cointelegraph.com/learn/crypto-regulations-in-nigeria, accessed on 11 March 2024.

[99] Cointelegraph, 2023, available at https://cointelegraph.com/learn/crypto-regulations-in-nigeria, accessed on 11 March 2024.

[100] Central Bank of Nigeria, 2024, available at https://www.cbn.gov.ng/Out/2024/FPRD/GUIDELINES%20ON%20OPERATIONS%20OF%20BANK%20ACCOUNTS%20FOR%20VIRTUAL%20Asset%20Providers.pdf, accessed on 11 March 2024.

https://doi.org/10.47348/SAMLJ/v36/i3a6

maintain records of all transactions for a minimum of five years to aid in any future investigations or audits by regulatory bodies.[101]

By virtue of these guidelines, financial institutions are mandated to establish appropriate risk management systems to determine whether a designated account opened for trading cryptocurrency is being used or is likely to be used for ML, TF and PF. Financial institutions are required to take reasonable measures to establish the beneficial ownership, source of wealth and the source of funds of a designated account.[102]

The CBN guidelines also mandated financial institutions to conduct customer due diligence (CDD) when a transaction of significant value takes place; customer information/documentation changes substantially; there is a material change in the way that the account is being operated; or the institution becomes aware that it lacks sufficient information about an existing customer. Financial institutions shall apply enhanced due diligence (EDD) requirements to all designated accounts opened in accordance with the guidelines on the basis of materiality and risk and continue to conduct due diligence on such existing relationships at appropriate times.[103]

The guideline also requires financial institutions to independently validate the address and documentation requirement of customers and where this information is discovered to be incorrect or invalid, the account shall be placed on 'Post-No-Debit' and the customer shall be asked to update their record, and a suspicious transaction report (STR) shall be rendered to the NFIU if necessary.[104]

Furthermore, financial institutions shall maintain all necessary records of transactions of a designated account for at least five years after completion of the transaction or such longer period as may be required by the CBN. The components of records of transactions to be maintained by a financial institution include the records of customers and beneficial owners obtained through customer due diligence measures including copies of records of official identification documents like passports,

[101] Central Bank of Nigeria, 2024, available at https://www.cbn.gov.ng/Out/2024/FPRD/GUIDELINES%20ON%20OPERATIONS%20OF%20BANK%20ACCOUNTS%20FOR%20VIRTUAL%20Asset%20Providers.pdf, accessed on 11 March 2024.

[102] Central Bank of Nigeria, 2024, available at https://www.cbn.gov.ng/Out/2024/FPRD/GUIDELINES%20ON%20OPERATIONS%20OF%20BANK%20ACCOUNTS%20FOR%20VIRTUAL%20Asset%20Providers.pdf, accessed on 11 March 2024.

[103] Central Bank of Nigeria, 2024, available at https://www.cbn.gov.ng/Out/2024/FPRD/GUIDELINES%20ON%20OPERATIONS%20OF%20BANK%20ACCOUNTS%20FOR%20VIRTUAL%20Asset%20Providers.pdf, accessed on 11 March 2024.

[104] Central Bank of Nigeria, 2024, available at https://www.cbn.gov.ng/Out/2024/FPRD/GUIDELINES%20ON%20OPERATIONS%20OF%20BANK%20ACCOUNTS%20FOR%20VIRTUAL%20Asset%20Providers.pdf, accessed on 11 March 2024.

https://doi.org/10.47348/SAMLJ/v36/i3a6

identity cards, driver's licenses or allied documents and beneficiary's names, addresses or other identifying, information normally recorded by the intermediary; nature and date of the transaction; type and amount involved; type and identifying number of any account involved in the transaction; and results of any analysis including inquiries to establish the background and purpose of complex unusually large transactions. Financial institutions are also under obligation to ensure that all customer-transaction records and information are available on request to the CBN on a timely basis, not later than 24 hours from the time of receipt of such request. Records of the supporting evidence and methods used to verify identity shall be retained by the financial institutions for a minimum period of five years after the account is closed or the business relationship has ended.[105]

The CBN guidelines also impose obligations on financial institutions to institute appropriate know-your-customer procedures to reasonably/promptly identify all individuals/entities offering cryptocurrency services on their books and ensure they immediately adhere to the guidelines. Financial institutions are also responsible for monitoring and supervising all activities in designated accounts and shall be held responsible for the misapplication of any account. Financial institutions are expected to have information on the volume and value of transactions carried out for each designated account and are to monitor effective compliance with set limits for each designated account. Financial institutions must take all other measures including onsite visits to ensure that the account is being operated as per the guidelines and other extant laws and regulations. Financial institutions must pay special attention to all complex, unusually large transactions or unusual patterns of transactions that have no visible economic or lawful purpose. They must investigate suspicious transactions and report their findings to the NFIU immediately, in compliance with the relevant provisions of any law or regulations being in force. They must keep records of investigations of reviewed unusual transactions where the transactions were not reported as suspicious transactions to the NFIU.[106]

The CBN guidelines impose a duty on financial institutions to ensure that appropriate consumer protection systems against risks of fraud are established and to provide a channel for the communication of

[105] Central Bank of Nigeria, 2024, available at https://www.cbn.gov.ng/Out/2024/FPRD/GUIDELINES%20ON%20OPERATIONS%20OF%20BANK%20ACCOUNTS%20FOR%20VIRTUAL%20Asset%20Providers.pdf, accessed on 11 March 2024.

[106] Central Bank of Nigeria, 2024, available at https://www.cbn.gov.ng/Out/2024/FPRD/GUIDELINES%20ON%20 OPERATIONS%20OF%20BANK%20ACCOUNTS%20FOR%20VIRTUAL%20Asset%20Providers.pdf, accessed on 11 March 2024.

https://doi.org/10.47348/SAMLJ/v36/i3a6

customer complaints against designated account holders. In addition, they must establish a complaints redress mechanism and ensure proper communication of this mechanism to the general public.[107]

They are mandated to ensure strict adherence to these CBN guidelines. This means that adherence and compliance with the new guidelines is mandatory. The guidelines empower the CBN to sanction any financial institution that fails to comply with the guidelines. Sanctions in this regard include prohibition from opening any further designated account; monetary penalty not below the sum of =N=2,000,000.00 (two million Naira) against the financial institutions, members of its board, senior management, and any staff, for any infraction and suspension of operating licence of a financial institution.[108]

The CBN guidelines provide much-needed legal clarity regarding the regulation of cryptocurrency in Nigeria by defining the roles and responsibilities of all stakeholders within the cryptocurrency ecosystem.[109] The guidelines offer more security to Nigerians participating in cryptocurrency trading by mandating compliance with KYC, AML and CFT protocols. The guidelines can also contribute to the growth of the Nigerian economy by fostering innovation in the fintech sector, attracting investments, and facilitating trade.[110]

Nonetheless, while the guidelines protect the citizens of the country from fraud and diminish the risk of financial crimes, they remove the privacy and anonymity features of cryptocurrency which makes cryptocurrency attractive in the first instance.[111] The effectiveness and success of the new guidelines will be investigated in the nearest future.

VIII CONCLUSION AND RECOMMENDATION

This paper examined the nature of cryptocurrency transactions. It revealed that the unique features of cryptocurrency, such as privacy and anonymity features, make it attractive for criminals to carry out various kinds of illicit and criminal activities such as money laundering,

[107] Central Bank of Nigeria, 2024, available at https://www.cbn.gov.ng/Out/2024/FPRD/GUIDELINES%20ON%20OPERATIONS%20OF%20BANK%20ACCOUNTS%20FOR%20VIRTUAL%20Asset%20Providers.pdf, accessed on 11 March 2024.

[108] Central Bank of Nigeria, 2024, available at https://www.cbn.gov.ng/Out/2024/FPRD/GUIDELINES%20ON%20OPERATIONS%20OF%20BANK%20ACCOUNTS%20FOR%20VIRTUAL%20Asset%20Providers.pdf, accessed on 11 March 2024.

[109] Cointelegraph, 2023, available at https://cointelegraph.com/learn/crypto-regulations-in-nigeria, accessed on 11 March 2024.

[110] Cointelegraph, 2023, available at https://cointelegraph.com/learn/crypto-regulations-in-nigeria, accessed on 11 March 2024.

[111] Cointelegraph, 2023, available at https://cointelegraph.com/learn/crypto-regulations-in-nigeria, accessed on 11 March 2024.

https://doi.org/10.47348/SAMLJ/v36/i3a6

terrorism, fraud, cybercrime, drug trafficking, as well as tax evasion. The susceptibility of cryptocurrency to illicit and criminal activities makes it necessary for the governments to put in place regulatory frameworks for cryptocurrency in order to prevent its abuse.

This article found that the FATF proposed some recommendations for countries to adopt as preventive measures to directly counter and address the abusive use of cryptocurrency. The proposed recommendations include: licensing or registration obligations, anti-money laundering, countering the financing of terrorism requirements, introduction of sanctions, introduction of guidelines, introduction of travel rule, international cooperation and information exchange.

The regulation of cryptocurrency in some selected jurisdictions such as the European Union, Canada, the United States of America, the United Kingdom, Australia, Japan, South Korea and South Africa was considered. The article further considered the regulation of cryptocurrency in Nigeria. Both the CBN and the SEC have released guidelines for the regulation of cryptocurrency in Nigeria. It is now left to be seen if these guidelines will be effective in regulating cryptocurrency in Nigeria. It is submitted that further research will be required to investigate the effectiveness and success of these guidelines in the near future.

It is recommended that policy makers in Nigeria should endeavour to keep pace with new international developments in the regulation of cryptocurrency which can be adopted to further strengthen the regulation of cryptocurrency in the country.

https://doi.org/10.47348/SAMLJ/v36/i3a6