Economic and Financial Crimes Commission and the Fight Against Virtual Currency-Related Crimes in Nigeria

Scholastica Okoronkwo [1], **Joachin Chetachi Uchegbulam** [1], **Sunday E. Egbo** [1], **Chinedu Joseph Igboke** [2], **Oluwadamilola Oluwatoni Odesola** [3], **Ogbonneya Fortunate Chidiebere** [2]

[1] *University of Nigeria, Nsukka*
Nsukka Road, 410001, Nsukka, Enugu State, Nigeria

[2] *Ebonyi State University*
PMB 053, Abakaliki, Nigeria

[3] *Igbinedion University*
Main Campus, Mission Rd, Okada 302111, Edo, Nigeria

DOI: 10.22178/pos.125-7

JEL Classification: K32

Received 06.10.2025
Accepted 28.12.2025
Published online 31.12.2025

Corresponding Author:
Joachin Chetachi Uchegbulam

Abstract. The rise of virtual currencies has given rise to novel forms of financial crime. This study conducted an assessment to determine the effectiveness of the Economic and Financial Crimes Commission (EFCC) in combating virtual currency-related financial crimes, with a focus on phishing scams and Ponzi schemes. The study used secondary sources and employed content analysis as its data collection method. Narrative analysis was used as the method, and the structural-functional theory served as the theoretical framework. The study finds that virtual currency–related phishing scams and Ponzi schemes continue to proliferate unchecked in Nigeria. Despite its efforts, the Economic and Financial Crimes Commission (EFCC) has not effectively mitigated these financial crimes, suggesting that its current strategies and resources are insufficient to address the evolving nature of virtual currency-related financial crimes. In light of these findings, the study recommends that the EFCC invest more funds in acquiring advanced technological capabilities and devote greater effort to enhancing its staff's skills. That will adequately position the EFCC to stay ahead of cybercriminals who adopt sophisticated methods to perpetrate financial crimes.

Keywords: Economic; Financial Crimes; Virtual Currency; EFCC; Nigeria.

INTRODUCTION

Virtual currencies are digital forms of currency that use cryptography to carry out secure transactions and control the creation of new units [1]. Virtual currencies are tokens and cryptocurrencies. The most well-known virtual currency is Bitcoin, which was created in 2009. Bitcoin has experienced a surge in popularity in recent years [2]. However, there are other virtual currencies, such as Ethereum, Ripple, and Litecoin. Each of those currencies has its own unique features and uses, as authors [3] highlight. One of the cardinal features of virtual currencies is that they operate outside the control of a central bank or government; this means they are not subject to the same regulations and oversight as traditional currencies and can be used for a range of transactions, both legal and illegal.

Authors [4] note that a decentralised network of computers usually operates virtual currencies and uses blockchain technology to record and verify transactions. This system provides a high level of security and transparency because it records each transaction in a public ledger that cannot be altered or tampered with. However, the use of virtual currencies also raises concerns about anonymity and the potential for illegal activities, such as money laundering and tax evasion, as noted by [5]. The proliferation of virtual currency has also fundamentally altered the

global financial landscape, offering new opportunities while creating challenges in combating economic crime.

Nigeria, one of the leading economies on the African continent, has not been immune to financial crimes involving virtual currencies. The Economic and Financial Crimes Commission (EFCC) is a key player in the Nigerian government's efforts to tackle financial crimes, including those involving virtual currency. In Nigeria, virtual currencies have seen significant popularity in recent years, as evidenced by the many individuals and businesses that have turned to cryptocurrencies to navigate the country's volatile economic landscape [6]. In addition, virtual currencies offer Nigerians a way to access financial services and make international transactions, bypassing traditional banking systems, which are known to be costly and inaccessible to many [7]. However, the Nigerian government and regulatory authorities have raised concerns about the use of virtual currencies, fearing that criminals could use them for fraud and other illegal activities. In response, the Central Bank of Nigeria has repeatedly issued warnings about the risks of investing in virtual currencies and has taken significant steps to regulate their use [8].

While virtual currency offers numerous benefits, including lower transaction costs and increased financial inclusion, it has also become a means for many forms of financial crime, as [9] highlights. These crimes range from money laundering and fraud, which, together, create many challenges for regulatory and law enforcement agencies worldwide. Nigeria, which has a rapidly growing digital economy and a vibrant, tech-savvy population, has also seen an increase in virtual currency-related financial crimes. The EFCC, established in 2003, is Nigeria's primary anti-corruption agency. The organisation has the mandate to investigate and prosecute the perpetrators of economic and financial crimes. It was established with the primary objective of combating economic and financial crimes in Nigeria. It is empowered by the EFCC Act of 2004 to investigate, prosecute, and prevent various forms of financial malfeasance, including money laundering, advance fee fraud, and other fraudulent practices [10]. The commission is also authorised to collaborate with other law enforcement agencies and international organisations to address the transnational dimension of economic and financial crimes.

In recent years, the EFCC has expanded its focus to include virtual currency-related financial crimes as part of its efforts to adapt to the new economic landscape and the challenges posed by technological advancements [11]. Its role in combating virtual currency-related financial crimes is paramount, given the ever-changing nature of financial crime and the increasing use of virtual currencies by criminal elements to conduct their activities. However, despite the EFCC's efforts, a critical assessment of its effectiveness in addressing these emerging challenges is needed. The gaps in the existing literature regarding the EFCC's capacity to effectively combat virtual currency-related financial crimes, particularly phishing scams and Ponzi schemes, underscore the importance of this study.

Gap in Literature/Study Rationale. A detailed and comprehensive literature review, carried out to ascertain the role Nigeria's EFCC has played in combating financial crimes, yields a wide range of publications. The review found that significant scholarly attention has been devoted to the mandate and objectives of the EFCC. Scholars such as authors [12, 13] extensively examined the legal framework and institutional structure that underpin the EFCC and highlighted its broad scope and focus in combating economic and financial crimes. In addition, a growing body of literature examines the areas where the EFCC has achieved some success in combating financial crimes. Notably, researchers [14, 15] examined specific cases in which the EFCC's interventions led to the successful prosecution of individuals involved in financial crimes, such as money laundering and corruption. Conversely, the EFCC also focuses on issues associated with virtual currencies that it has not adequately addressed. Scholars such as [16] raised concerns about the proliferation of virtual currency-related financial crimes in Nigeria and the challenges the EFCC faces in regulating and monitoring these emerging financial transactions.

The gap in the extant literature lies in the inadequate research attention directed towards studies that explain the role the EFCC plays in combating specific types of financial crimes, such as phishing scams and Ponzi schemes. While there is some research on these types of crimes that captures the Nigerian context, scholars have not investigated in depth the outcomes of the EFCC's efforts to combat virtual currency-related criminal activities.

METHOD

Source of Data. The purpose of this study is to examine the role of the Economic and Financial Crimes Commission (EFCC) in combating virtual currency-related financial crimes in Nigeria. To achieve this, the study relies on secondary sources, including journal articles, news articles, official government reports, reports from independent research organisations, and other credible sources relevant to the research topic.

The primary reason for choosing secondary sources of data is the sensitive, clandestine nature of virtual currency-related financial crimes. Access to primary sources of information, such as official investigations and confidential reports, is often restricted due to the sensitive nature of the subject matter. As such, secondary sources do provide a wealth of relevant information that can be used to get a comprehensive assessment of how the EFCC's efforts have fared in combating phishing scams and Ponzi schemes.

Method of Data Collection. The study adopted content analysis to conduct an in-depth examination and interpret information from various documents, such as reports, legal documents, media coverage, and online communications, to identify and extract relevant information. The researchers scrutinised the gathered information against predefined criteria that they explicitly developed for the study.

Method of Data Analysis. The researchers analysed data from these secondary sources using a qualitative method, specifically a narrative analysis approach. They chose this approach because it provides a nuanced and detailed understanding of the EFCC's activities and their impact on mitigating virtual currency–related financial crimes [17]. The narrative analysis approach allows exploration of the EFCC's actions within the specific context of the complexities and intricacies of the Nigerian economic landscape, as well as the global nature of virtual currency-related financial crimes.

Theoretical Framework of Analysis: The Structural-Functional Theory. The Structural-Functional Theory is a prominent perspective in political science. Its focus is on explaining the interplay between social structures and political institutions. The theory emphasises the role of structures in maintaining order and stability within a society [18]. One of the major proponents of the structural-functional theory is the prominent scholar Talcott Parsons. Parsons made significant contributions to advancing the theory through his writings in the 1950s and 1960s.

The main arguments of the structural-functional theory are summarised as follows:

First, the theory posits that society is made up of interconnected parts that work together to maintain stability and equilibrium. These parts include political institutions, social norms, and cultural values.

Second, the theory argues that the various interconnected parts within society serve specific functions that contribute to society's overall functioning. For example, political institutions help maintain order and regulate conflict, while social norms guide individual behaviour and promote social cohesion.

Third, the theory emphasises the importance of consensus and integration in maintaining social order. Consensus here refers to the shared values and beliefs that bind society together, while integration refers to the processes that connect individuals to larger social systems.

As noted by the author [19], David Easton extended the structural-functional theory to the study of political systems. Easton then argued that political systems can be understood as complex, adaptive structures that respond to both external and internal pressures. He also emphasised the role of feedback mechanisms in maintaining equilibrium within political systems. For example, when a political system encounters a problem or challenge, it generates feedback that prompts the system to make adjustments and restore equilibrium. On the other hand, Robert Merton developed the concepts of manifest and latent functions. Manifest functions are the intended consequences which social structures or institutions aim to have, while latent functions are the unintended or unrecognised consequences, which they do seek to have [20]. Merton's work illustrated the complexity of social systems and highlighted the importance of considering both intended and unintended effects when assessing the effectiveness of social structures.

Theoretical Framework of Analysis: Application of theory. This study argues that the EFCC has failed to adequately mitigate virtual currency-related crimes in Nigeria. Researchers can examine the role of the Economic and Financial Crimes Commission (EFCC) in adequately addressing virtual-currency-related cybercrime in Nigeria through

the lens of structural–functional theory. One of the cardinal propositions of the Structural-functional theory is that social structures are interrelated and contribute to the stability, social order, and functionality of society [21]. In Nigeria, the EFCC's failure to tackle virtual-currency-related cybercrimes is linked to the complex web of social structures, including political, economic, and legal institutions. As highlighted by scholars such as [14], Nigeria's political structure is characterised by a high level of systemic corruption, fuelled by the elevation of vested interests over public interest. This corruption has permeated law enforcement agencies, hindering their effectiveness in combating cybercrime. Others, like authors [22], argued that the economic structures in Nigeria are marked by widespread poverty and inequality, which provide a fertile ground for criminal activities such as phishing scams and Ponzi schemes to thrive.

However, in Nigeria, the EFCC's effectiveness has been hampered by institutional weaknesses, including inadequate funding, limited technical expertise, and political interference. These institutional inadequacies have undermined the EFCC's capacity to address cybercrimes involving virtual currency, thereby contributing to the perpetration of such offences.

Another relevant dimension of the structural-functional theory is the notion of functional prerequisites, which are the essential functions that must be fulfilled for society to operate smoothly [23]. In Nigeria, the EFCC's failure to tackle virtual-currency-related cybercrimes stems from its inability to meet these functional prerequisites. The rise of virtual-currency-related cybercrime has not only enabled but also facilitated fraudulent activities such as phishing scams and Ponzi schemes [24]. Furthermore, the Structural-functional theory also emphasises the need for societal adaptation to maintain equilibrium [25]. However, Nigeria's response to virtual-currency-related cyber crimes has been inadequate, as the EFCC has been unable to adapt to the rapidly evolving landscape of cybercriminal activities. The agency has been slow to develop the technological and investigative capacities needed to address these modern forms of criminality, thereby contributing to its failure to mitigate virtual-currency-related cybercrime effectively.

To improve the EFCC's effectiveness in addressing virtual currency-related crimes in Nigeria, a multifaceted approach is necessary. The EFCC should focus on building its capacity and on strengthening partnerships with international organisations, regulatory bodies, and stakeholders in the crypto industry. It is essential to use proactive strategies, stay updated on technological advancements, and also use digital forensics and data analytics tools [26]. Policymakers need to create clear regulatory frameworks for virtual currencies and ensure proper monitoring, reporting, and oversight. Government agencies and financial regulators should regularly organise public awareness campaigns to educate citizens about the risks associated with virtual currencies, promote a culture of responsible use, and strengthen cybersecurity. In the end, a mix of legislative changes, collaboration, technology integration, and public involvement will help the EFCC effectively combat virtual currency-related crimes.

RESULTS AND DISCUSSION

Phishing Scams. One primary concern regarding virtual currency crimes in Nigeria is phishing scams. Criminals exploit the anonymity and decentralised nature of virtual currencies to defraud unsuspecting individuals [27]. According to [28], Nigeria has experienced a rise in phishing scams targeting virtual currency. Cybercriminals target individuals who want to invest in cryptocurrencies like Bitcoin and Ethereum. These scams are widespread across the country and very sophisticated. They often leave victims facing significant financial losses, as well as emotional distress. The EFCC's ability to investigate and prosecute these complex forms of cybercrime remains limited.

With the popularity of digital currencies like Bitcoin and Ethereum, scammers have found new ways to exploit people and organisations through phishing, leading to significant financial losses and heightened cybersecurity concerns in Nigeria. A recent case highlights this issue. Eze Harrison Arinze, a Nigerian national, was sentenced for defrauding 34 victims across 13 countries. His fraudulent act resulted in losses of about $592,000; this followed a successful investigation and prosecution by Nigeria's Economic and Financial Crimes Commission [29], and also shows the dangers of virtual currency phishing scams [30].

A Central Bank of Nigeria report confirmed that other studies indicate a steady rise in virtual cur-

rency-related phishing scams in the country over the past few years [31]. One report noted that Nigeria has seen a surge in cases of these scams. Data collected by the Nigerian Communications Commission (NCC) also showed that the prevalence of virtual currency-related phishing scams has been increasing consistently [32]. Crypto analysis firms, such as the Israeli blockchain analysis firm Whitestream, have also published detailed reports confirming the rise of cryptocurrency scams in Nigeria, particularly on social media platforms like Instagram. Lagos is the centre for many of these scams [33]. This information highlights the growing threat posed by cybercriminals in Nigeria, who are exploiting the popularity and volatility of cryptocurrencies to target unsuspecting individuals.

Common Modes of Operation. The picture below illustrates what a phishing attack looks like — a pictorial illustration of a Phishing Attack.

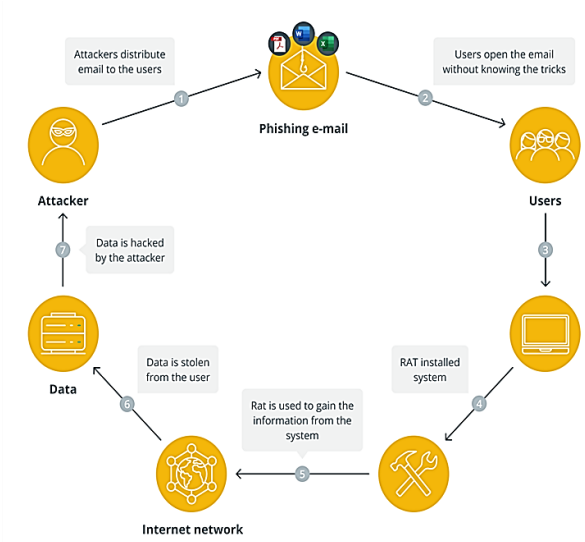

Figure 1 – Diagram representation of a Phishing Attack [34]

Creation of Fake Investment Platforms: One of the most common methods used by cybercriminals in Nigeria for virtual currency-related phishing scams is the creation of fake investment platforms [27]. These platforms often promise high returns in a short amount of time, thereby luring people to deposit their money into bogus accounts. Once the funds are deposited, the scammers vanish, leaving victims with no way to recover their money. In some cases, these fake investment platforms may even use the names of well-known cryptocurrency exchanges or companies to trick victims into thinking they are real, as reported by [35].

Use of Phishing Emails and Websites: Another common tactic is the use of phishing emails and websites to deceive people into sharing their personal information or login credentials [35]. Cybercriminals do send emails that appear to come from legitimate cryptocurrency exchanges or wallets. These emails ask recipients to click on a link and then enter their information. Once the victim provides their details, the scammers can go ahead to access their accounts and steal their funds. Authors [34] note that phishing emails often include convincing graphics and language, thereby making it hard for people to tell they are fake.

Conduct of Social Engineering Attacks: In addition to fake investment platforms and phishing emails, cybercriminals in Nigeria also carry out social engineering attacks to access individuals' cryptocurrency accounts [36]. Social engineering involves tricking people into sharing sensitive information or doing things they usually wouldn't do. For instance, scammers might call individuals and then pretend to be customer service representatives from a cryptocurrency exchange. They may also ask for login details while claiming to help with a technical issue. This tactic exploits people's trust in authority figures and can result in significant financial losses.

Nigeria has one of the highest rates of cryptocurrency adoption in Africa, with millions of citizens actively trading and also using virtual currency [37]. This widespread use has made Nigeria an attractive target for cybercriminals seeking to exploit unsuspecting individuals and businesses through phishing scams. Additionally, the lack of strong regulation and oversight of virtual currency in Nigeria has fostered an environment where fraud can thrive [7]. The decentralised nature of digital currency makes it even harder for law enforcement to track and catch cybercriminals, allowing scammers to act with a sense of freedom [38].

In Nigeria, the regulatory challenges, along with high poverty and unemployment rates, do make citizens more vulnerable to phishing scams [22]. Many people are drawn to the allure of quick, easy money through virtual currency investments, making them easy targets for fraud. Scammers often take advantage of this by pretending to be legitimate cryptocurrency platforms or by promoting unrealistic investment

opportunities. As a result, victims suffer financial losses.

Scholars, including authors [39] and cybersecurity experts, have emphasised the importance of raising awareness and educating people about the risks posed by phishing scams targeting virtual currency in Nigeria. Many individuals and businesses lack the knowledge or skills to recognise and protect themselves from these scams [40]. This situation has prompted calls for government agencies, financial institutions, and cybersecurity groups to work together. They should focus on creating educational programmes and initiatives that help people learn how to avoid becoming victims of phishing scams related to virtual currency.

Ponzi Schemes. These schemes often promise unrealistic returns on investment. They lure unsuspecting people into investing their hard-earned money, only to vanish with their funds, thereby leaving victims in financial ruin. The rise of virtual currency Ponzi schemes in Nigeria is concerning. The anonymity and lack of regulation surrounding virtual currencies like Bitcoin make them popular tools for scammers [41]. Data from the Nigeria Deposit Insurance Corporation (NDIC) shows that reported cases of Ponzi schemes involving virtual currencies have increased in recent years [42]. Another report by the Nigerian Securities and Exchange Commission (SEC) indicates a spike in Ponzi schemes targeting Nigerians, particularly those involving virtual currencies [43]. These schemes often promise quick, high returns on investments and attract unsuspecting people seeking fast profits in the volatile cryptocurrency market. The table below lists Ponzi schemes that have operated in Nigeria from 2016 to 2025.

Table 1 – Ponzi Schemes that have Operated in Nigeria between 2016 & 2025 [44]

2016	2017	2018-2020	2021-2022	2023-2025
MMM Nigeria	NNN Nigeria	Bitclub Advantage	86FB (aka 862)	CALA (Cala Finance)
Ultimate Cycler	MMM Cooperation	Million Money	Eagle Cooperative	6 Dollar Investments
Get Help World Wide (GHW)	Global Crediting Cooperative Hub (GCCH)	Helping Hands International	Royal Q (Nigerian Scam Version)	Sidra Investment (Cloned Scam Version)
Twinkas	Money Riot	DGSOUK	FINAFRICA	Wealth Buddy
ICharity Club	Revo Money	Pennywise	Ovaioza Farm	Compoundly
			Produce Storage	
Crowd Rising	Swiss Golden (Nigeria Version)	Loom	Q Net (Nigeria)	Bitfinance Global
Claritta	Nigeria News Update (NNU)	Crowd 1	Afriq Arbitrage System (AAS)	CBEX
Help2Get	Peer-2-Peer Donation	Lion's Share	MBA Forex	
Loopers Club	Twinkas Reloaded	Inks Nation	Chinmark Group	
Givers Forum	Donation Hub	Banzaza Multipurpose Cooperative	Inksledge	
	My Bonus	Racksterli	Axim Exchange	
	Zarfund			

Many studies, such as the author [41], have noted that the lack of regulations and oversight is a key factor enabling cryptocurrency Ponzi schemes to flourish. The decentralised, largely unregulated nature of virtual currencies allows fraudsters to run Ponzi schemes without fear of being caught or facing legal action. Additionally, the widespread use of social media and other online platforms to promote these schemes helps fraudsters reach more potential victims, thereby worsening the problem [45].

Modes of Operation. The picture below presents five major characteristics of a cryptocurrency Ponzi scheme.

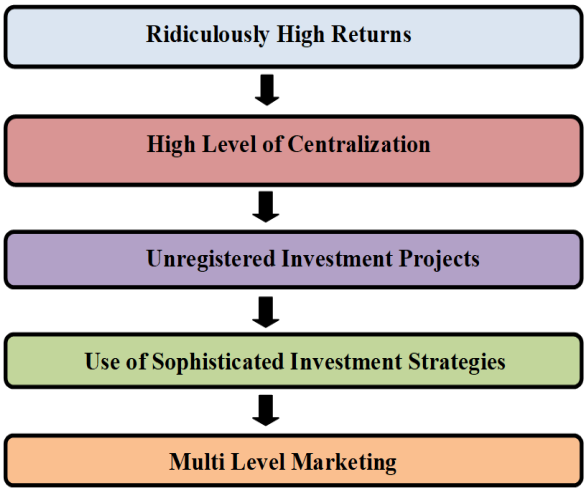

Figure 2 – How to Identify a Cryptocurrency Ponzi Scheme. Source: Adapted from [46]

Promise of Huge Returns on Investments: One standard method used by virtual currency Ponzi

schemes in Nigeria is the promise of huge returns on investments. A report published by authors [46] shows that these Ponzi schemes often offer investors extremely high returns and claim to use special trading algorithms or secret investment strategies that guarantee profits. Victims are lured into investing their money in these schemes with the promise of doubling or even tripling their investments in a short time.

Recruitment of New Investors to Sustain the Scheme: Another common way virtual currency Ponzi schemes operate is by recruiting new investors to sustain the scheme [47]. Participants are encouraged to bring in more investors to earn extra bonuses or commissions, creating a pyramid-like structure in which early investors are paid with funds from new investors. This cycle continues until the scheme falls apart due to a lack of recruits or unsustainable returns, leaving most participants with significant financial losses.

A study by the Nigeria Deposit Insurance Corporation (NDIC) reported that virtual currency-related Ponzi schemes accounted for a large percentage of financial fraud cases in the country [48]. The report emphasised the need for greater awareness and regulatory action to combat the spread of these fraudulent activities in Nigeria's financial sector. In response to the rising threat of virtual currency-related Ponzi schemes, regulatory bodies in Nigeria have begun educating the public about the risks of such scams. The Securities and Exchange Commission (SEC) has warned investors about the dangers of engaging in Ponzi schemes. They have advised individuals to conduct thorough investigations before investing in any scheme that promises high returns [49].

Additionally, the Central Bank of Nigeria (CBN) has introduced stricter rules on cryptocurrency use in the country to curb illegal financial activities and protect investors from scams [31]. These regulatory actions are essential to safeguard Nigerians' economic well-being and prevent further exploitation by Ponzi scheme operators. Despite these efforts, fighting cryptocurrency crimes remains a significant challenge, as shown in the information below.

Table 2 – Records of Ponzi Scams that Occurred in Nigeria Recently [44]

Group	Years of Operation	Platform Type	Promise on Investment Return	Target Group	Year of Collapse	Estimated Loss
CBEX	2020-2025	Crypto Currency Investment	100% Monthly Return on Investment	Youths on Social Media	2025	About 1.3 Trillion Naira
MBA Forex and Capital Investment Limited	2018-2021	Forex Trading	15% Monthly Return on Investment	Professionals and Civil Servants	2021	About 213 Billion Naira
Famzhi Interbiz Limited	2021	Business Investment Platform	Not Specified	General Investors	2021	About 30 Billion Naira
Red King Chinmark Group	2022	Business Investment Platform	Not Specified	General Investors	2022	About 40 Billion Naira
Ovaioza Farm Produce Storage Business	2022	Agricultural Business Investment	Not Specified	General Investors	2022	About 3 Billion Naira

The Economic and Financial Crimes Commission (EFCC) has stepped up its monitoring and other efforts to crack down on fraudulent investment schemes, including those involving virtual currencies. Despite these efforts, the issue of virtual currency-related Ponzi schemes in Nigeria remains a significant problem. Reports from the EFCC indicate that the number of Ponzi scheme cases involving virtual currencies continues to rise. This trend highlights the ongoing threat of fraudulent activity in the virtual currency market [50]. The absence of a robust regulatory framework and the decentralised nature of virtual currencies make it difficult to effectively stop the spread of Ponzi schemes. Fraudsters continue to change their tactics to avoid getting caught.

CONCLUSIONS

Based on the findings, it is clear that Nigeria's EFCC alone cannot tackle the significant challenge of combating financial crimes involving virtual currency. The global nature of these issues underscores the need for stronger international cooperation and the development of specialised skills and resources. These are necessary to address complex, cross-border criminal activities effectively. The shortcomings of Nigeria's EFCC in addressing phishing scams and Ponzi schemes call for policymakers, regulators, and law enforcement to develop robust regulatory frameworks and enforcement mechanisms. These will help reduce the rise of virtual currency-related financial crimes. Only through united and organised efforts can Nigeria hope to face and overcome the threats posed by these new types of crime. Given this context, this study offers the following recommendations on how the EFCC can improve its ability to combat the examined crimes:

1) Strengthen collaboration and information sharing with global financial intelligence units: The EFCC should focus on building strong partnerships with international counterparts; this will help in exchanging intelligence and best practices to combat financial crimes related to virtual currency.

2) Invest in technological capabilities and skill development: The complex nature of virtual-currency-related financial crimes requires the EFCC to invest in technology and also provide its staff with specialised training in the areas of digital forensics, blockchain analysis, and cybersecurity; this will help the agency investigate and prosecute offenders effectively. It will also enable early detection and prevention of crimes in the virtual-currency sector.

3) Enhance public awareness and education campaigns: The EFCC should regularly launch public awareness and education campaigns to inform Nigerians about the risks of virtual-currency transactions. Raising awareness of phishing scams and Ponzi schemes will help individuals protect themselves from fraud and report suspicious activity, thereby strengthening the financial system's overall resilience.

4) Collaborate with financial institutions and also regulatory authorities: To effectively tackle virtual-currency-related financial crimes, the EFCC must work closely with other financial institutions and other regulatory bodies in Nigeria. This collaboration will help monitor and regulate virtual currency transactions. A coordinated approach will be instrumental in improving transparency and accountability in the virtual-currency ecosystem, enabling the detection and disruption of illegal financial flows.

5) Promote legislative reforms and policy development. The EFCC should push for legislative reforms and policy development to fill regulatory gaps in Nigeria's governance that allow virtual-currency-related financial crimes to thrive. Working with policymakers and stakeholders will enable the agency to create a strong legal framework that meets global standards and also addresses the specific challenges posed by virtual-currency crimes in Nigeria.

REFERENCES

1. Mora, H., López, F. A. P., Tello, J. C. M., & Morales, M. R. (2019). Chapter 12 Virtual Currencies in Modern Societies: Challenges and Opportunities. In *book: Politics and Technology in the Post-Truth Era* (pp. 171–185). doi: 10.1108/978-1-78756-983-620191012

2. Wisniewska, A. (2016). Bitcoin is an example of a virtual currency. *Institute of Economic Research Working Papers, 1.*

3. Raskin, M., & Yermack, D. (2018). Digital currencies, decentralised ledgers and the future of central banking. In P. Conti-Brown & R. M. Lastra, *Research Handbook on Central Banking* (chapter 22, pp. 474-486). Edward Elgar Publishing.

4. Yuan, Y., & Wang, F. (2018). Blockchain and cryptocurrencies: model, techniques, and applications. *IEEE Transactions on Systems, Man, and Cybernetics Systems, 48*(9), 1421–1428. doi: 10.1109/tsmc.2018.2854904

5. Choo, K. R. (2015). Cryptocurrency and virtual currency. In *Elsevier eBooks* (pp. 283–307). doi: 10.1016/b978-0-12-802117-0.00015-1

6. Afzal, A. (2019). Cryptocurrencies, Blockchain and Regulation: a review. *The Lahore Journal of Economics, 24*(1), 103–130. doi: 10.35536/lje.2019.v24.i1.a5

7. Opebiyi, F. M. (2022). *Regulating user interactions within the financial technology market: Cryptocurrencies in Nigeria* (Thesis: University of Manchester).

8. Tiwari, N. P. J. T. D. R. (2023). A comparative analysis of cryptocurrency legal frameworks in the United States and the European Union. *Tuijin Jishu/Journal of Propulsion Technology, 44*(4), 4835–4841. doi: 10.52783/tjjpt.v44.i4.1804

9. Hanafi, S. F., & Rahman, S. A. (2019). Regulating Digital Currency: Taming the Unruly. In *Emerging Issues in Islamic Finance Law and Practice in Malaysia* (pp. 265–280). doi: 10.1108/978-1-78973-545-120191021

10. Adeniran, A. O. (2019). Anti-corruption Strategies for Balanced Development. *Advanced Journal of Social Science, 5*(1), 52–64. doi: 10.21467/ajss.5.1.52-64

11. Anichebe, U. (2020). Combating money laundering in an age of technology and innovation. *SSRN Electronic Journal*. doi: 10.2139/ssrn.3627681

12. Umar, I., Samsudin, R. S., & Mohamed, M. (2017). Appraising the effectiveness of the Economic and Financial Crimes Commission (EFCC) in tackling public sector corruption in Nigeria. *Journal of Advanced Research in Business and Management Studies, 7*(2), 1-12.

13. Omoroghomwan, O. B. (2018). An Appraisal of the Activities of Economic and Financial Crime Commission (EFCC) on the Administration of Criminal Justice in Nigeria. *Acta Universitatis Danubius. Relationes Internationales, 11*(2).

14. Bello, M. F., & Cosmas, A. O. (2022). The Role of the Economic and Financial Crime Commission (EFCC) in Combating Corruption in Nigeria. *Musamus Journal of Public Administration, 5*(1).

15. Umar, I., Samsudin, R. S., & Mohamed, M. B. (2016). Understanding the Successes and Challenges of the Anti-Corruption Agency (ACA) in Nigeria: A Case of Economic and Financial Crimes Commission (EFCC). *Asian Journal of Multidisciplinary Studies, 4*(5).

16. Esoimeme, E. (2021). A Critical Analysis of the Effects of the Central Bank of Nigeria's Digital Currency Named ENAIRA on Financial Inclusion and AML/CFT Measures. *SSRN Electronic Journal*. doi: 10.2139/ssrn.3921396

17. Wang, C. C., & Geale, S. K. (2015). The power of story: Narrative inquiry as a methodology in nursing research. *International Journal of Nursing Sciences, 2*(2), 195–198. doi: 10.1016/j.ijnss.2015.04.014

18. De Velazco, F. F., Lara, E. C., & Luna, S. R. (2021). Proposal of a Model from the Perspective of Parsons' Functional-Structural Theory. *Journal of Systemics, Cybernetics, and Informatics, 19*(8), 182–197. doi: 10.54808/jsci.19.08.182

19. Hassan, M. D., & Lukman, A. D. (2019). The Significance of Political Theory in the Contemporary Political Discourse: Exploring the Methodological Hardcore of the Political Science Discipline. *Journal of Humanities and Social Science, 17*(4).

20. Merton, R. (2016). Manifest and latent functions. In W. Longhofer & D. Winchester, *Social theory re-wired* (pp. 68-84). Routledge.

21. Parhanudin, M. A. (2020). Analysis of social structure and power relations in the NW Anjani Community. *Sophist Jurnal Sosial Politik Kajian Islam Dan Tafsir, 2*(1), 1–37. doi: 10.20414/sophist.v2i1.20

22. Akinyetun, T. S. (2021). Poverty, cybercrime and national security in Nigeria. *Journal of Contemporary Sociological Issues, 1*(2), 86. doi: 10.19184/csi.v1i2.24188

23. Adedoyin, A. D. (2023). *A study of the Impact of Technology on Cybercrime in the Public and Private Sectors in Nigeria* (Thesis; University of Portsmouth).

24. Popovych, I. S., Borysiuk, A., Zahrai, L., Fedoruk, O., Nosov, P., Zinchenko, S., & Mateichuk, V. (2020). Constructing a structural-functional model of social expectations of the personality. *Revista Inclusiones, 7.*

25. Izadi, A., Mohammadi, M., Nasekhian, S., & Memar, S. (2020). Structural Functionalism, Social Sustainability and the Historic Environment: A Role for Theory in Urban Regeneration. *The Historic Environment Policy & Practice, 11*(2–3), 158–180. doi: 10.1080/17567505.2020.1723248

26. Monkhouse, A. R. (2021). *The Influence of Emerging Technologies on Financial Crime: An Evaluation of Modified Law Enforcement and Risk Management Practices Used to Combat Financial Crimes* (Thesis; Utica College).

27. Omodunbi, B., Odiase, P., Olaniyan, O., & Esan, A. (2016). Cybercrimes in Nigeria: analysis, detection and prevention. *FUOYE Journal of Engineering and Technology, 1*(1). doi: 10.46792/fuoyejet.v1i1.16

28. Scharfman, J. (2023). *The Cryptocurrency and Digital Asset Fraud Casebook.* doi: 10.1007/978-3-031-23679-2

29. EFCC Nigeria. (2023). EFCC Arraigns Three over Alleged $1.6m Crypto-currency Fraud. Retrieved from https://x.com/officialEFCC/status/1732448203260170324

30. TRM Team. (2023). Nigerian Crypto Scammer Sentenced to Three Years for Running International Pig Butchering Scheme. Retrieved from https://www.trmlabs.com/resources/blog/nigerian-crypto-scammer-sentenced-to-three-years-for-running-international-pig-butchering-scheme

31. Central Bank of Nigeria. (2020). Central Bank of Nigeria Press Release Alert! Beware of COVID-19 Cyber-attacks, Fraud. Retrieved from https://www.cbn.gov.ng/Out/2020/CCD/CBN%20Press%20release%20-%20COVID-19%20-%20Cyber%20Security.pdf

32. Adepetun, A. (2023). Combating telecoms-related electronic fraud in Nigeria. *The Guardian.*

33. Hertig, A. (2021). Blockchain Sleuthing Firm Calls Nigeria 'Focal Point' for Africa's Crypto Scams. Retrieved from https://www.coindesk.com/markets/2021/03/03/blockchain-sleuthing-firm-calls-nigeria-focal-point-for-africas-crypto-scams

34. Nambiampurath, R. (2025). What is a phishing attack in crypto, and how to prevent it? Retrieved from https://cointelegraph.com/learn/articles/what-is-a-phishing-attack-in-crypto-and-how-to-prevent-it

35. Scamwatch Nigeria. (2022). 4 Common Cryptocurrency Scams and How to Avoid Them. Retrieved from https://scamwatch.ng/content/4-common-cryptocurrency-scams-and-how-avoid-them

36. Ibenu, N. (2022). Rise of Remote Work Paves the Way for Social Engineering and Cybercriminals to Infiltrate Businesses. Retrieved from https://businessday.ng/opinion/article/rise-of-remote-work-paves-ways-for-social-engineers-cybercriminals-to-infiltrate-businesses/

37. Agbo, E. I., & Nwadialor, E. O. (2020). Cryptocurrency and the African Economy. *Economics And Social Sciences Academic Journal, 2*(6).

38. Sartori, M., Seher, I., & Prasad, P. W. C. (2023). The illicit use of cryptocurrency on the darknet by cyber criminals to evade authorities. In *Lecture notes in electrical engineering* (pp. 449–459). doi: 10.1007/978-3-031-29078-7_39

39. Mangut, P. N., & Datukun, K. A. (2021). The Current Phishing Techniques–Perspective of the Nigerian Environment. *World Journal of Innovative Research, 10*(1), 34-44.

40. Okpa, J. T., Ajah, B. O., Nzeakor, O. F., Eshiotse, E., & Abang, T. A. (2022). Business email compromise scam, cyber victimisation, and the economic sustainability of corporate organisations in Nigeria. *Security Journal, 36*(2), 350–372. doi: 10.1057/s41284-022-00342-5

41. Kethineni, S., & Cao, Y. (2019). The rise in popularity of cryptocurrency and associated criminal activity. *International Criminal Justice Review, 30*(3), 325–344. doi: 10.1177/1057567719827051

42. Onanuga, P., & Taiwo, R. (2020). Discursive features of Nigerian online Ponzi schemes' narratives. *ELOPE English Language Overseas Perspectives and Enquiries, 17*(2), 61–82. doi: 10.4312/elope.17.2.61-82

43. Jack, J. T. C. B., & Ibekwe, C. C. (2018). Ponzi Schemes: An Analysis of Coping with Economic Recession in Nigeria. *The Nigerian Journal Of Sociology And Anthropology, 16*(1).

44. Amakoromo, W. T., Namo, I. B., & Agwadu, L. (2024). State Regulation and Prevalence of Ponzi Schemes in Nigeria. *Fuwukari Journal of Politics and Development, 8*(1).

45. Mirtaheri, M., Abu-El-Haija, S., Morstatter, F., Steeg, G. V., & Galstyan, A. (2019). Identifying and analysing cryptocurrency manipulations in social media. *arXiv (Cornell University)*. doi: 10.48550/arxiv.1902.03110

46. AMLBot. (2023). How To Identify Whether A Crypto Project Is A Ponzi Scheme. Retrieved from https://www.linkedin.com/pulse/how-identify-whether-crypto-project-ponzi-scheme-amlbot

47. Vasek, M., & Moore, T. (2015). There's no free lunch, even using Bitcoin: Tracking the popularity and profits of virtual currency scams. In *Lecture Notes in Computer Science* (pp. 44–61). doi: 10.1007/978-3-662-47854-7_4

48. NDIC. (2018). Special Notice To Banks, Bank Depositors And The General Public On Digital Currencies. Retrieved from https://ndic.gov.ng/special-notice-to-banks-bank-depositors-and-the-general-public-on-digital-currencies/

49. Akamo, A. (2023). Binance's Operations in Nigeria are Illegal – Nigeria's SEC. Retrieved from https://nairametrics.com/2023/06/10/nigerias-sec-declares-binance-operations-in-the-country-as-illegal/

50. EFCC. (n. d.). Red Alert on Scam. Retrieved from https://www.efcc.gov.ng/images/pdfs/RED_ALERT_ON_SCAM.pdf