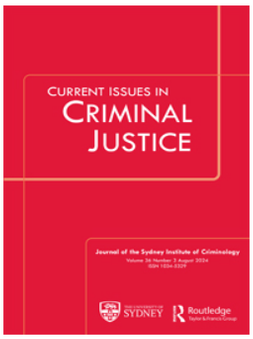

Routledge
Taylor & Francis Group

Current Issues in Criminal Justice

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/rcic20

An assessment of convicted cryptocurrency fraudsters

Kaina Habila Garba, Suleman Lazarus & Mark Button

To cite this article: Kaina Habila Garba, Suleman Lazarus & Mark Button (17 Sep 2024): An assessment of convicted cryptocurrency fraudsters, Current Issues in Criminal Justice, DOI: 10.1080/10345329.2024.2403294

To link to this article: https://doi.org/10.1080/10345329.2024.2403294

Published online: 17 Sep 2024.

CURRENT ISSUES IN CRIMINAL JUSTICE
https://doi.org/10.1080/10345329.2024.2403294

An assessment of convicted cryptocurrency fraudsters

Kaina Habila Garba [a,b], Suleman Lazarus [c,d,e] and Mark Button [e]

[a]Economic and Financial Crimes Commission (EFCC), Abuja, Nigeria; [b]Centre for Cybercrime and Economic Crime, University of Portsmouth, Portsmouth, UK; [c]London School of Economics and Political Science (LSE), London, UK; [d]Centre for Criminology, University of Surrey, Guildford, UK; [e]Centre for Cybercrime and Economic Crime, University of Portsmouth, Portsmouth, UK

ABSTRACT

We examine cryptocurrency fraud cases prosecuted by Nigeria's Economic and Financial Crimes Commission (EFCC). We considered the lens of the Space Transition Theory (STT) in exploring the dynamics of these digital crimes. Our data analysis reveals common types of fraud, including cryptocurrency investment schemes. The results show an exclusive male demographic (100%), with the majority under 30 years old and only a quarter possessing a degree, providing insights into the socio-demographic characteristics of cryptocurrency fraudsters. Additionally, while most fraudsters (55%) targeted victims in the United States, Bitcoin, leveraging blockchain technology, was the most commonly used method (46%) for cryptocurrency fraud. Our examination of the methods and mediums used for cryptocurrency fraud supports some aspects of STT, while others do not. We advocate for a multifaceted strategy that prioritises stringent regulation, implementation, and heightened scrutiny of digital currency ecosystems in Nigeria and beyond. This study contributes to the broader discourse on cybercrime prevention and enforcement by emphasising the novel methodological approach utilised.

ARTICLE HISTORY
Received 3 May 2024
Accepted 8 September 2024

KEYWORDS
Bitcoin; blockchain technology; cryptocurrency scams; Nigeria; online fraud; Western victims; Yahoo boys; convicted cases; West African scammers; Economic and Financial Crimes Commission (EFCC)

Introduction

Nigeria has gained a reputation as the originator of many scams targeting other countries (Ibrahim, 2016; Okosun & Ilo, 2023). This notoriety stems from the activities of scammers based in Nigeria and abroad, commonly known as "Yahoo Boys." Initially centred on advanced fee fraud, also known as 419 scams, and more recently, online romance fraud (Aborisade, 2023; Lazarus et al., 2023a; Lazarus et al., 2023b), their fraudulent activities have evolved in both scope and methods of operation. Cryptocurrency fraud has emerged as a notable variation, utilising increasingly sophisticated digital techniques. While some studies have addressed cryptocurrency fraud (Bartoletti et al., 2021; Corbet, 2021; Krishnan et al., 2024), none have specifically explored

CONTACT Mark Button mark.button@port.ac.uk St Georges Building, 141 High St, Portsmouth, UK
This article has been corrected with minor changes. These changes do not impact the academic content of the article.

the perspectives of Nigerian offenders. This article offers one of the first assessments of this type of fraud using unique access to the case files of convicted fraudsters in Nigeria.

This study examines cryptocurrency fraud cases prosecuted by the Economic and Financial Crimes Commission (EFCC) in Nigeria. Existing literature provides valuable insights into various aspects of cybercrime in Nigeria, such as law enforcement perspectives (Lazarus & Okolorie, 2019), testimonies of cybercriminals within Nigeria (Aransiola & Asindemade, 2011), and outside Nigeria (Lazarus, 2024), as well as public opinion on cybercrime issues (Lazarus et al., 2022). However, no studies have examined cryptocurrency fraud cases originating in Nigeria. Although Nigeria is home to the largest population in Africa and is experiencing rapid economic growth, the surge in digital currency adoption has brought about a myriad of implications (Acho, 2021; Ozili, 2022; Ukwueze, 2021).

Over the past two decades, there has been a significant increase in the adoption of digital currencies in Nigeria, driven by factors such as the pursuit of financial security, remittance activities, and the appeal of cryptocurrencies as a hedge against inflation (Acho, 2021). Digital currencies offer an innovative and efficient mode for conducting secure, quick, and cost-effective transactions (Ukwueze, 2021). This rise in digital currency adoption has led to the proliferation of trading platforms, channels, and wallets in Nigeria, contributing to the expansion of the nation's digital currency market. Globally, the increasing popularity of cryptocurrencies as investment tools and payment methods has coincided with a rise in digital currency fraud, significantly impacting Nigeria. The surge in cryptocurrency transactions, reaching approximately $400 million, positions Nigeria as the third-largest player in Bitcoin transactions globally, following Russia and the United States (Corbet et al., 2019).

The growth of digital cryptocurrencies in Nigeria is closely linked to a desire for financial inclusion. With only 36.8% of Nigerian adults having access to formal banking services, digital currencies provide an alternative to traditional monetary transactions accessible to anyone with a mobile device and internet connection (Agbo & Nwadialor, 2020). However, the expansion of the Nigerian digital currency market has brought new challenges, particularly fraudulent digital currency activities. Ozili (2022) identified various illegal behaviours, including phishing, security breaches, Ponzi-like schemes, and investment scams, which complicate digital currency fraud in Nigeria. For instance, Nigeria has a higher percentage (0.71%) of malicious crypto miners in Africa (Adepetun, 2021), and the EFCC has convicted many offenders, such as Eze Harrison Arinze, who scammed individuals in 13 countries, resulting in victims losing $382,000 worth of Bitcoin (Press Statement, 2023).

The rise of cryptocurrency fraudsters in Nigeria warrants the need for researchers to identify the profiles of these emerging offenders (cf. Childs, 2024; Luchkin et al., 2020). This study aims to understand the demographics of individuals involved in cryptocurrency fraud, providing insights into potential risk factors or patterns. Additionally, it seeks to explore how fraudsters operate, identify common strategies, and highlight potential vulnerabilities in the cryptocurrency industry. By addressing these gaps in the literature, this study contributes to the broader discourse on cybercrime prevention and enforcement.

Literature review

Digital crime in a Nigerian context

In recent decades, cybercrime has had a significant impact on crime and victimisation on an international scale (Cook et al., 2022). Several types of cybercriminal activities differ in their motivations, practices, patterns, and extent of perpetration and victimisation (Ibrahim, 2016; Yar & Steinmetz, 2019). Multiple attempts have been made to classify the diversity of cybercrime and online deviance (e.g., Gordon & Ford, 2006; McGuire & Dowling, 2013; Wall, 2013). Cybercrimes are broadly classified into cyber-enabled and cyber-dependent crimes (see McGuire & Dowling, 2013 for more details). While cyber-enabled crimes involve traditional crimes facilitated by digital technology (e.g., fraud), cyber-dependent crimes require a digital infrastructure to exist (e.g., hacking). Our focus is on 'cyber-enabled crimes' (McGuire & Dowling, 2013, p. 1), also known as 'people-centric cybercrime' (Gordon & Ford, 2006, p. 16). This classification (cyber-enabled crimes), however, complicates the distinction between financially motivated crimes like 'online fraud' and psychologically motivated ones like 'revenge pornography' (Ibrahim, 2016; Lazarus & Okolorie, 2019). We aim to contribute to discussions on cryptocurrency scammers by utilising perspectives sensitive to these motivational differences.

Similar to other academic research reports (Hall & Ziemer, 2023; Hall & Ziemer, 2024; Sarkar & Shukla, 2024), our approach aligns with Ibrahim's (2016) Tripartite Cybercrime Framework (TCF), which groups cybercrime into three motivational categories: psychosocial, socioeconomic, and geopolitical. The rationale for this alignment lies in Ibrahim's (2016) emphasis on the predominance, relevance, and prevalence of cybercrimes with socioeconomic motivations in Nigerian society, as detailed in Table 1, while also acknowledging the psychosocial and geopolitical motivations behind cybercrimes.

Digital crimes in and about Nigeria comprise only principal components: (a) cryptocurrency fraud (Platt et al., 2023), (b) online romance fraud (Lazarus et al., 2023a), and (c) Business Email Compromise (BEC), (Lazarus, 2024; Okpa et al., 2022). Lazarus et al.'s (2023a) systematic review of the empirical literature from 2000 to 2021 defines online romance fraud as exploiting intimate relationships by con artists for financial gain. Conversely, in their investigation into business email compromise (BEC), Okpa et al. (2022)

Table 1. Tripartite Cybercrime Framework (TCF).

Socioeconomic cybercrime	Psychosocial cybercrime	Geopolitical cybercrime
*Hackers and crackers	*Hackers and crackers	*Hackers -'Hacktivist'
Cyber fraud	Child pornography	Cyber spies
Cyber embezzlement	Cyber stalking	Cyber espionage
Cyber piracy	Cyber bullying	**Cyber terrorism
Cyber blackmail	Revenge porn	Cyber Vandalism
Romance scam	Cyber rape	Cyber assault
Online drug trafficking	*Cyber hate speech	*Cyber hate speech
Cyber prostitution	*Cyber extortion	Cyber riot
*Cyber extortion	Obscenity	Cyber sabotage
Illegal online gambling	*Cyber-prostitution	Cyber-colonialism
*Cyber Trespass	*Cyber Trespass	Cyber rebellion
**Cyber terrorism	*Cyber homicide	
***Cryptocurrency fraud	**Cyber terrorism	

Source: Table 1 adopted from the tripartite cybercrime framework (Ibrahim 2016, p. 45).
Notes: * *instances where a specific cybercrime type is listed in more than one column, ***instances where a specific cybercrime type is listed in more than two columns, and *** instances where new cybercrime types are added to the initial list.*

and Lazarus (2024) defined Business Email Compromise as deceptive operations within organisational email exchanges. Our study centres on cryptocurrency fraud, an illicit practice that exploits vulnerabilities in the cryptocurrency ecosystem for monetary gain.

Online offenders in Nigeria

The relationship between cybercrime, university students/graduates/dropouts, and male offenders, often aided by corruption in Nigerian society, has been a common theme in previous research (e.g., Aransiola & Asindemade, 2011). Several academic studies have examined online fraud from various perspectives. These investigations have included interviews with fraudsters (Aransiola & Asindemade, 2011; Ogunleye et al., 2019; Tade, 2013), consultations with law enforcement agents (Lazarus & Okolorie, 2019), perspectives from parents of offenders (Aborisade, 2023), and even analyses of Afrobeats songs (Lazarus et al., 2023b), tweets, and public responses (Lazarus et al., 2022). Despite their diverse approaches, these studies reached similar conclusions to varying degrees. Consistency across these studies strengthens the credibility of empirical research, reinforcing basic insights into the typical traits of online offenders. Moreover, non-empirical studies such as Okosun and Ilo (2023) and Ndubueze (2020) support the empirical literature. The convergence of evidence from various research methodologies validates the importance of these characteristics for understanding the complexities of online fraud and the people involved in these activities.

Cryptocurrency in Nigeria

Some online fraudsters have been implicated in cryptocurrency fraud, as shown in Table 1. While the table does not represent a systematic review of all cases, it provides illustrative examples of cryptocurrency fraud reported in the media and highlights the notable lack of academic studies on this topic within the Nigerian context. Despite the increasing prominence of cryptocurrencies in Nigeria, there remains a noticeable dearth of academic analysis specific to this region. Various studies have explored the role of Bitcoin, particularly its emergence as a viable alternative to the devaluing naira during the 2016 recession (e.g., Ogochukwu & Jarrar, 2018). However, empirical literature addressing cryptocurrencies in Nigeria remains limited, especially from a criminological perspective. For instance, Platt et al. (2023) discovered that individuals who understand Bitcoin's energy consumption are more likely to support environmental initiatives. Eigbe (2018) found that despite widespread discussions, most Nigerians have a limited understanding of Bitcoin, challenging common assumptions. Salawu and Moloi (2018) emphasised the urgent need for dedicated regulations to govern cryptocurrency services, suggesting that professional accountants in Nigeria are hesitant to engage with cryptocurrencies without such regulations. Jimoh and Benjamin (2020) highlighted the significant influence of Bitcoin on Nigerian financial markets, noting its macroeconomic implications. Additionally, Egbo and Ezeaku (2020) warned about the disruptive impact of cryptocurrencies on commercial banks, indicating potential threats to their core operations in Nigeria. While some studies underscore the positive potential of cryptocurrencies for the Nigerian economy, others highlight negative repercussions. Thus, Table 2 provides examples of convicted fraudsters, the amount of cryptocurrency involved, and the locations of their victims, illustrating the geographical reach and financial magnitude of these crimes.

Table 2. Examples of convicted fraudsters and details of their crimes.

Convicted fraudsters	Crypto amount	Location(s) of victim(s)	Sources
Precious Ofure	$256,000	Canada	Daily Post (2021)
Ekwue Joshua Femi	$20,000	United States of America	Daily Post (2023a)
Eze Harrison Arinze	$592,000	Burundi, Cameroon, Costa Rica, Germany, India, Uganda, Rwanda, South Africa, Hungary, Ghana, Singapore, United States of America, Zimbabwe	TRM (2023)
Moses Upkonahusi	$5,576	Australia	Daily Post (2023b)
Benjamin Okenna Ikaa	$120,000	South Africa, Norway, United Kingdom, Barbados	The Eargle (2024)

The ramifications of digital currency fraud are conspicuous, both at the individual level and within the broader economic context. First, Lazarus (2024) investigates the dynamics of cybercriminal networks, explicitly focusing on Business Email Compromise (BEC) scammers, including Nigerians incarcerated in the West. Through interviews with an incarcerated Black Axe leader and the analysis of tapped phone data, Lazarus (2024) uncovers themes such as the impact of Bitcoin. The study highlights how cryptocurrency facilitates anonymous transactions, money laundering, and payments, thereby complicating the tracking and recovery of stolen funds. Second, victims of cryptocurrency scams often face significant financial setbacks, including depletion of life savings, poverty, and emotional distress (Ozili, 2022). Third, a nation's reputation is tarnished by digital currency fraud, discouraging foreign investments and hindering economic growth (Adrian & Mancini-Griffoli, 2021; Alao & Odum, 2019). Scanty empirical data and records make assessing the true scope of digital currency fraud in Nigeria challenging. The limited empirical literature underscores the need for a more in-depth exploration of cryptocurrency dynamics in Nigeria. While there is consensus in the available literature that Bitcoin holds substantial social significance in Nigeria, more empirical studies are needed to have a deeper understanding of its economic, social, and regulatory impacts. We aim to gain a better understanding of cryptocurrency fraud and consider the value of Space Transition Theory.

Theoretical consideration

In examining cryptocurrency fraud cases, we aim to explore their alignment with the theoretical constructs elucidated by the Space Transition Theory (Jaishankar, 2008, 2018), as outlined in Table 3. This theory has been increasingly applied to cybercrime in a variety of contexts, such as Assarut et al. (2019) in Thailand and in West Africa, notable empirical studies include works by Danquah and Longe (2011) in Ghana and Tade (2013) in Nigeria. However, to date, no one has specifically applied the Space Transition Theory to examine cryptocurrency cases. Space Transition Theory is favoured in this study due to its sharpened focus on understanding the interplay between cyberspace and physical space, which is crucial for grasping the full scope of digital criminal behaviour.

Method and materials

While some studies have developed profiles of fraud offenders using a mixture of organisational data or publicly available reports (e.g., Button et al., 2016, 2017), the rise of cryptocurrency fraudsters in Nigeria has prompted researchers to identify the profiles of these

Table 3. Propositions of the space transition theory.

Proposition	Key elements	Descriptions
1. Repressed Criminal Behaviour	Physical Space vs. Cyberspace	Offenders may manifest criminal tendencies in cyberspace due to the status and position they would not exhibit in physical space.
2. Identity Flexibility and Dissociative Anonymity	Cyberspace Characteristics	Offenders are provided with the choice to commit cybercrime due to identity flexibility, dissociative anonymity, and a lack of deterrence factors in cyberspace.
3. Import-Export of Criminal Behaviour	Cyberspace to Physical Space and Vice Versa	Criminal behaviour in cyberspace may influence physical space, and vice versa, emphasising the interconnectedness of these spaces.
4. Intermittent Ventures and Dynamic Spatio-Temporal Nature	Cyberspace Characteristics	Offenders may exploit the dynamic nature of cyberspace and intermittent ventures to escape consequences.
5. Strangers Uniting in Cyberspace	Associates Uniting in Cyberspace	Cross-Space Collaborations
6. Closed Society Influence	Societal Characteristics	Individuals from closed societies are more prone to committing cybercrimes compared to those from open societies, suggesting a societal influence on cyber behaviour.
7. Conflict of Norms and Values	Norms and Values Clash	The clash between norms and values in physical space and cyberspace may lead to cybercrimes, indicating the role of conflicting societal principles.

emerging offenders. To achieve this, we examine cases of cryptocurrency fraud prosecuted by the EFCC. We were granted access to the individual case files of each person involved. The prosecution and trial were conducted on a case-by-case basis, with convictions obtained and sentences imposed on individuals by the court. There were no appeals following the convictions of any of the offenders. The data represents individual case files, with no evidence of collaboration in activities among the persons involved. Notably, the method employed in our study shares similarities with the approach described by Lusthaus et al. (2023) and Leukfeldt et al. (2017) in their research on cybercrime network investigations. These prior studies provide valuable insights into the methodologies and themes relevant to our research.

For instance, our study, like Lusthaus et al. (2023), involved collecting data from law enforcement agencies to analyze criminal activities, albeit in different contexts. While our study analysed cryptocurrency fraudsters using data from Nigeria's EFCC conviction records, Lusthaus et al. (2023) collected data from closed cybercrime investigations, primarily in the UK. Furthermore, both our study and the studies by Lusthaus et al. (2023) and Leukfeldt et al. (2017) utilised primary data sources to gain insights into the characteristics and operations of criminal networks, adapting methodologies to account for the specificity of data collection in their respective contexts. Regarding sample selection, our study focused on convicted individuals implicated in cryptocurrency fraud cases within a specific timeframe and jurisdiction, resulting in a sample size of 22. Similarly, Lusthaus et al. (2023) selected cases based on criteria such as financial motivation and involvement in major cybercrime case types, resulting in a sample of 10 case debriefs.

By drawing parallels with these prior studies, our research methodology gains credibility and situational relevance, allowing for a more robust analysis of cryptocurrency fraud in Nigeria. Convicted offenders may not fully represent all offenders active in this domain, as law enforcement efforts may focus on specific levels and types of

offenders, potentially missing more professional fraudsters who evade detection. Therefore, the data must be viewed as a snapshot of cases in Nigeria, providing insight into a relatively understudied area of criminal activity. This study constitutes a primary analysis of a set of case files produced by the EFCC, acknowledging the inherent limitations of data produced by law enforcement agencies primarily for investigative and prosecutorial purposes rather than research (cf. Adedoyin, 2023). Such data may contain gaps and may be structured to serve the law enforcement process. Despite these limitations, the authors consider this dataset invaluable for understanding the characteristics of this new type of offender (Mosoti et al., 2022).

The dataset was obtained from two regional commands of the Economic and Financial Crimes Commission (EFCC), specifically the Enugu and Lagos Zonal Commands, Nigeria, chosen for their significant caseloads and jurisdiction over financial crimes, including cryptocurrency fraud, within their respective geographical regions. Sample selection prioritised individuals legally convicted of engaging in fraudulent activities related to cryptocurrency from 2021 to June 2023. This timeframe was selected to capture current patterns and advancements in instances of cryptocurrency fraud in Nigeria. Restricting the sample to cryptocurrency fraud convictions ensured the data's relevance to the research inquiry.

The sample size comprised 22 convicted individuals implicated in cryptocurrency fraud cases, determined based on the accessibility of pertinent conviction records within the designated timeframe and jurisdiction. Although the sample size may appear relatively limited, it is essential to recognise that the study focuses on examining comprehensive conviction data obtained from authoritative sources. Each case offers valuable insights into the typology, methodology, financial gains, motivations, and victim locations related to cryptocurrency fraud in Nigeria. Utilising a focused and precise sample selection methodology enhances the overall quality and comprehensiveness of the gathered data (Okeke et al., 2015).

The study did not involve any direct interaction with fraudsters. However, because of the sensitive nature of the private data provided by the EFCC and the fact that one of the authors is an employee of the organisation, the University required the author to obtain ethical clearance from both the University and the EFCC. Both levels of ethical approval were successfully secured, including ethical clearance number 1110 from the University of [redacted] in 2023. The subsequent findings shed light on various aspects of cryptocurrency fraud, contributing to a nuanced understanding of illicit activity.

Findings

Our findings offer insights into the demographics, methods, financial gains, motivations, global reach, and preferred platforms of those involved in cryptocurrency fraud, contributing to a nuanced understanding of illicit activity. The profile of the convicted fraudsters could be described as male (100%), young (nearly two-thirds were under 30), and not well-educated (only a quarter possessed a degree). Table 4 presents core demographics.

Cryptocurrency investment fraud is related to deceiving individuals to invest in fraudulent schemes or projects that promise high returns that never materialise. It is also important to note that fraudsters often use other means to perpetrate fraud. For example, romance fraud might deviate from offering a crypto investment

Table 4. Personal characteristics of offenders.

Characteristic	Number and %
Gender	
Male	22 (100%)
Female	0
Age	
20–24 Age	8 (36.4%)
25–29 Age	7 (31.8%)
30–34 Age	5 (22.7%)
Unspecified Date of Birth	2 (9.09%)
Education	
Senior Sec. Sch Cert	11 (50%)
Degree	6 (27.27%)
Not specified	5 (22.73%)

opportunity. Fraudsters might hack legitimate email accounts and use the contacts in the accounts as targets to encourage participation. They may have created fake websites, luring people to invest in inflated claims. Alternatively, social media may encourage interested parties to invest in a fake product, sometimes with the added dimension of the impersonation of a legitimate actor. Furthermore, Table 5 illustrates how scammers use various platforms and mediums of communication to perpetrate cryptocurrency fraud.

These platforms and mediums of communication frequently have many users, allowing them to reach a wider audience and exploit their victims' trust and lack of awareness of cryptocurrency transactions. Based on the information provided, the study participants used multiple methods to conduct cryptocurrency fraud across the dataset obtained. Facebook was used by 12 participants (27%), making it the most popular method. Due to its widespread popularity and accessibility, false profiles may be created, or interactions with potential victims might be established on the platform. Another popular technique involved using Gmail, as employed by 10 participants (22%) who utilised this email service for fraudulent activities. The extensive use of Gmail, with its robust communication features and user-friendly interface, facilitates scammers' ability to communicate with and deceive victims. The relative ease of creating multiple accounts and the potential for anonymity on Gmail make it a favoured tool among fraudsters. Seven participants (14%) reported using Instagram, making it the third most popular medium of cryptocurrency fraud. The visual appeal of Instagram and its direct messaging features may have attracted scammers to engage with the

Table 5. Medium used for cryptocurrency fraud.

S/N	Platform/Service Used	No of Users	%
1.	Facebook	12	27
2.	Instagram	7	14
3.	Not Specified	6	16
4.	Gmail	10	22
5.	MeetMe	1	2
6.	WhatsApp	5	9
7.	Basetools.tk	1	2
8.	Nextplusapp	1	2
9.	Swapfinder	1	2
10.	Googlevoice	1	2
11.	Hangout	1	2

victims and win their trust. Five participants (9%) used WhatsApp to communicate and implement fraudulent schemes directly. Owing to its extensive instant messaging use, it was probably attractive for short connections with potential victims. Other methods stated in the data included Basetools.tk, Swapfinder, Hangout, NextPlus App, Google Voice, and Meetme. One participant (2% each) employed each of these, indicating that the scammers used different approaches. It is important to note that six participants (16%) did not reveal the method employed to commit cryptocurrency fraud. The lack of specific information regarding their methods highlights the difficulties in gathering comprehensive data on fraudulent operations.

Additionally, the financial gains made by participants in cryptocurrency fraud cases vary. Each value on the list represents the sum of money or cryptocurrencies that a certain participant fraudulently received. Participants in cryptocurrency fraud cases typically make money from relatively lesser amounts, such as $1,000, to significantly larger amounts, like $475,000 and even 1200 BTC (Bitcoin). The data reveal the varying amounts earned through cryptocurrency fraud, reflecting the diverse scale and types of fraudulent activities perpetrated by participants. Specifically, most participants (73%) cited financial gain as their primary motivation for engaging in cryptocurrency fraud. Conversely, six participants (27%) did not explain their involvement in cryptocurrency fraud, leaving their motives undisclosed. Figure 1 sheds light on the pattern of fraudsters' victims across different nations.

Most participants, comprising 12 people (55% of the total), carried out fraudulent activities with victims in the United States. This high percentage shows that the USA was often targeted for cryptocurrency fraud. In other countries, the participants conducted their activities outside the USA. One participant (4%) concentrated on victims in China, whereas another participant (4%) targeted victims in Canada. Furthermore, one participant (5%) performed illicit schemes with victims in Malaysia and the Philippines. Conversely, it is important to note that six individuals (27% of the total) failed to

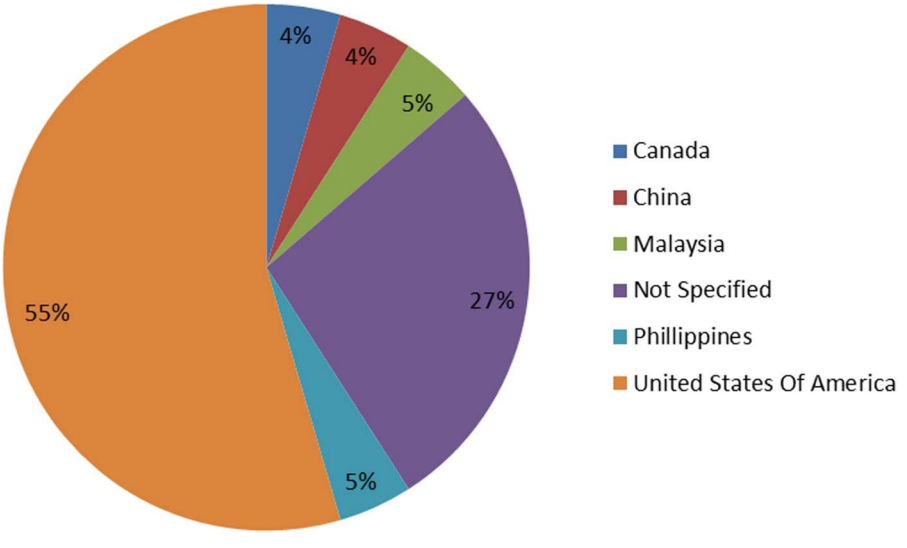

Figure 1. Country and location of victims.

recognise the location or country of their victims. The difficulty of gathering extensive data on cryptocurrency fraud cases is emphasised because of the lack of specific information.

Moreover, describing the types of exchanges and platforms used by participants involved in cryptocurrency fraud is crucial for understanding the methods employed in these activities. Initially, the term 'Blockchain' was used to refer to the most frequently utilised platform in the case files. In this context, 'Blockchain' refers specifically to Bitcoin, which utilises blockchain technology for its transactions and storage.

Bitcoin

Number of Users: 12 (46%)

Description: Bitcoin operates on blockchain technology, a decentralized digital ledger that records cryptocurrency transactions. Its security and anonymity make it a preferred choice for fraudulent activities.

Remitano

Number of Users: 1 (4%)

Description: Remitano is a peer-to-peer trading platform allowing users to buy and sell cryptocurrencies directly. The participant chose Remitano for its convenience in executing fraudulent transactions.

Binance

Number of Users: 3 (7%)

Description: Binance is one of the world's largest and most widely recognized cryptocurrency exchanges. It offers a wide variety of cryptocurrencies and has significant trading volume, which may have influenced participants' decisions to use it for fraud.

Paxful

Number of Users: 2 (8%)

Description: Paxful is a peer-to-peer cryptocurrency trading platform that allows users to buy and sell cryptocurrencies through various payment methods. Its convenience likely made it an appealing choice for fraudsters.

Luno

Number of Users: 1 (4%)

Description: Luno is an international cryptocurrency exchange known for its easy-to-use interface for trading cryptocurrencies. This simplicity may have attracted the participants who used it for fraud.

Localbtc.com

Number of Users: 1 (4%)

Description: Localbtc.com facilitates direct peer-to-peer cryptocurrency transactions. Its straightforward approach makes it another platform chosen for fraudulent activities.

Figure 2. Preferred crypto currencies, exchanges/platforms of offenders.

The reference to 'Blockchain' was intended to denote the use of Bitcoin, leveraging blockchain technology as its ledger for peer-to-peer transactions. It is noteworthy that the confusion stemmed from the language used by the offenders in their written statements, which we sourced as raw data. Their terminology often conflated the broader concept of blockchain technology with specific cryptocurrencies and exchanges. Most fraudsters use Bitcoin due to its decentralised ledger, which provides greater security and anonymity than traditional payments, making it attractive for fraudulent activities. Figure 2 illustrates the preferred crypto currencies, exchanges/platforms of offenders.

The data indicate that a significant proportion of participants (46%) preferred using Bitcoin, facilitated by blockchain technology, for fraudulent activities. Other platforms, including Binance, Paxful, Luno, and Localbtc.com, were also used, but to a lesser extent. This distinction between blockchain as a technology and specific exchange platforms helps to avoid confusion and provides a clearer understanding of the methods used by fraudsters. Monitoring and addressing fraudulent activities on these platforms is crucial for ensuring the security and reliability of cryptocurrency trading. These findings offer valuable insights into the demographics, methods, financial gains, motivations, global reach, and preferred platforms of individuals engaged in cryptocurrency fraud, thereby enhancing our understanding of this illicit activity.

Discussion

Our discussion is centred on core findings that provide insights into the demographics, methods, financial gains, motivations, global reach, and preferred platforms of individuals engaged in cryptocurrency fraud. These insights contribute to a nuanced understanding of this illicit activity, as summarised in Table 6.

Core findings and theoretical implications

A noteworthy pattern emerges in scrutinising the demographic composition of individuals involved in cryptocurrency fraud in Nigeria, revealing that all convicted fraudsters in

Table 6. Summary of findings.

Core findings	Descriptions
Demographic Profile of Fraudsters	Convicted fraudsters in cryptocurrency cases were predominantly male (100%), with almost two-thirds being under 30 years old, and only a quarter possessing a degree.
Methods and Medium Used for Fraud:	Fraudsters employed various means to perpetrate cryptocurrency fraud, with Facebook being the most popular (27%), followed by Gmail (22%), Instagram (14%), and WhatsApp (9%). Other methods such as Basetools.tk, Swapfinder, Hangout, Nextplus App, Google Voice, and MeetMe were also reported.
Financial Gains from Fraud	Participants engaged in cryptocurrency fraud reported varying financial gains, ranging from relatively smaller amounts like $1,000 to substantial sums like $475,000 and even 1200 BTC (Bitcoin).
Motivations for Fraud	The primary motivation for 73% of participants involved in cryptocurrency fraud was financial gain, while 27% did not disclose their motives.
Global Reach of Fraud Activities	Most fraudsters (55%) targeted victims in the United States, emphasising the USA as a frequently targeted country for cryptocurrency fraud. Other countries, such as China, Canada, Malaysia, and the Philippines, were also mentioned, while 27% did not specify the location of their victims.
Preferred Exchanges/Platforms for Fraud:	Bitcoin, leveraging blockchain technology, was the most used platform for cryptocurrency fraud, accounting for 46% of the cases. This was followed by Remitano (4%), Binance (7%), Paxful (8%), Luno (4%), and Localbtc.com (4%).

such cases are exclusively male, constituting a demographic prevalence of 100%. Furthermore, most of these male offenders fell within the age bracket of less than 30 years. This observation not only concurs with antecedent investigations on cybercriminals in Nigeria, drawing from diverse sources such as interviews with offenders (Aransiola & Asindemade, 2011; Lazarus, 2024), insights from law enforcement operatives (Lazarus & Okolorie, 2019), and perspectives of parents with connections to offenders (Aborisade, 2023; Ibrahim, 2017) but also warrants a closer examination through the lens of feminist epistemology of digital crimes.

Gender and cultural dimensions of offending

The socialisation of individuals in West Africa into traditional gender roles reinforces men's dominance in online crime (Lazarus & Okolorie, 2019; cf. Newburn, 2011 on traditional crimes in general). Case files of cryptocurrency scammers exclusively feature men, a pattern consistent with prior research showing men's prominent involvement in online fraud in Nigeria (Aransiola & Asindemade, 2011; Lazarus & Okolorie, 2019; Lazarus et al., 2023b). Ogunleye et al.'s (2019) study, which interviewed 17 female undergraduates claiming to be scammers, highlights that while women participate, they often assume subordinate roles, mentored by men such as boyfriends, brothers, and uncles. In contrast, Cassiman's (2019) study found instances of women independently running scamming businesses in Ghana. However, unlike their male counterparts, these women face greater stigma, demonisation, and negativity, indicating a gendered societal perception in West Africa.

The cultural insights are crucial in understanding why adult men in Nigeria are predominantly linked to cryptocurrency scams. The concept of the 'image of womanhood' refers to societal expectations and views of women at a particular historical moment, shaping femininity (cf. Ibrahim & Komulainen's, 2016 research comparing West African and Scandinavian regions). These perceptions influence women's interactions with men and societal views of women, providing a rich cultural context. Cryptocurrency scamming aligns with traditional masculine traits such as assertiveness and financial provision while deviating from societal expectations of feminine virtues for marriageable women. This study's male domination of cryptocurrency scams aligns with feminist epistemology in digital crime research (Eckert, 2018; Jane, 2018; Lazarus, 2019), highlighting the intersectionality of culture, gender, and crime. Moreover, this study's findings also warrant a closer examination through the lens of the Space Transition Theory proposed by Jaishankar (2008).

Considering the space transition theory

Space Transition Theory posits that offenders can commit cybercrime due to identity flexibility, dissociative anonymity, and a lack of deterrence factors in cyberspace. Our examination of the methods and platforms used for cryptocurrency fraud supports this theory. The study reveals that platforms like Facebook and communication tools like Gmail are crucial in facilitating cryptocurrency fraud. When considering the theoretical implications, Space Transition Theory's focus on identity flexibility and dissociative anonymity is particularly relevant. The study highlights how offenders use these characteristics to their advantage, leveraging the dynamic nature of cyberspace to commit fraud. Platforms like Facebook and Gmail provide the necessary anonymity

and flexibility, demonstrating how fraudsters navigate and exploit the digital landscape to engage in cryptocurrency fraud, thus reinforcing the theory's relevance in understanding cybercrime behaviour.

Similarly, Space Transition Theory asserts that criminal behaviour in cyberspace may influence physical space and vice versa. Our observation of cryptocurrency fraud cases aligns with this aspect of the theory, highlighting the interconnectedness of these spaces. This introduces a nuanced dimension to the discourse on the theory's applicability. Although some demographic findings deviate from Jaishankar's (2008) theory, they underscore the complex interplay between cyberspace and physical space, suggesting that a nuanced dataset and evaluation are required to fully agree or disagree with the theory. However, the Nigerian cybercrime landscape, particularly among men under 30, reveals a pronounced gender imbalance. This gender-specific trend contradicts Jaishankar's (2008) theory, which suggests that individuals may manifest distinct behaviours in cyberspace compared to their conduct in physical space. It posits that those who do not display criminal tendencies in physical space might engage in fraudulent activities in the relatively anonymous cyberspace. Notably, in Nigeria, men exhibit a higher propensity for offending, challenging this theoretical postulation.

Exploring the dimension of financial gains from fraud, Space Transition Theory, while not explicitly addressing financial motivations, accentuates the dynamic nature of cyberspace as a facilitator of criminal activities. Although the theory remains silent on the direct aspect of financial incentives, the study's findings point towards individuals capitalising on the dynamic nature of cyberspace to attain substantial financial gains, aligning with the theory's concept of intermittent ventures. This oversight in Space Transition Theory underscores the significance of the Tripartite Cybercrime Framework (TCF) (Ibrahim, 2016), which offers a nuanced perspective on motivations. The Tripartite Cybercrime Framework (TCF) asserts that the socioeconomic category of cybercrime, as delineated in Table 1, holds paramount relevance and prevalence in Nigerian societies. This assertion is particularly pertinent to citizens operating both within and outside Nigeria, accentuating the need for a comprehensive understanding of the diverse motivations and implications of cybercrime. By shifting the focus to motivations for fraud, the TCF takes a more explicit stance, addressing motivations while acknowledging an individual's choice to engage in cybercrime. The primary motivation uncovered in the study, financial gain, aligns seamlessly with the TCF's socioeconomic classification, reinforcing the framework's utility in comprehensively categorising and understanding the diverse motivations that drive individuals to commit cybercrimes.

Concerning the 'preferred exchanges and platforms for fraudulent activities' finding, while not explicitly delving into specific platforms, the Space Transition Theory accentuates the influence of cyberspace characteristics in shaping criminal behaviour. The usage of blockchain technology, renowned for its decentralised and secure transactions, resonates harmoniously with the tenets of the Space Transition Theory, showcasing a convergence of observed patterns with the theoretical propositions. The diverse array of platforms outlined in this study serves as a testament to the adaptability of fraudsters to navigating and exploiting various cyber environments. This adaptability mirrors the fluid nature of cyberspace, reinforcing Space Transition Theory's emphasis on the dynamic characteristics of the digital realm. Although the core findings generally align with certain aspects of the propositions that the Space Transition Theory put forth, we

acknowledge some disparities. Notwithstanding these nuanced variations, Space Transition Theory remains a valuable and illuminating conceptual framework, offering insights into the intricate dynamics of cryptocurrency fraud activities. Its capacity to explain observed patterns underscores its relevance in comprehending the evolving cybercrime landscape.

Conclusion

This research has underlined the predominance of men in Nigeria, aged 20 to 34, engaging in cryptocurrency-related fraud, primarily targeting North America. These findings are based on an analysis of case files from convicted offenders. The research also highlighted prevalent digital currency fraud typologies in Nigeria, emphasising cryptocurrency investment and its frequent link to romance fraud (46% of the participants employed Bitcoin). Despite acknowledging the potential benefits of digital currencies, such as enhanced financial inclusion and expedited cross-border transactions, this study underscored the challenges associated with anonymity and the lack of regulatory oversight. Striking a balance between nurturing innovation and shielding consumers from fraudulent conduct is paramount in the rapidly evolving digital money ecosystem. The allure of blockchain lies in its decentralisation and tamper-resistant features, which align seamlessly with global trends in leveraging this technology for secure and transparent digital transactions. However, alongside these promising aspects, the study also unveiled the associated criminogenic challenges it brings as offenders embrace these technologies.

Disclosure statement

No potential conflict of interest was reported by the author(s).

ORCID

Kaina Habila Garba http://orcid.org/0009-0008-4074-7332
Suleman Lazarus http://orcid.org/0000-0003-1721-8519
Mark Button http://orcid.org/0000-0002-4169-2619

References

Aborisade, R. A. (2023). Yahoo boys, yahoo parents? An explorative and qualitative study of parents' disposition towards children's involvement in cybercrimes. *Deviant Behavior*, *44*(7), 1102–1120. https://doi.org/10.1080/01639625.2022.2144779

Acho, Y. (2021). Crypto-Currency and the Nigerian economy. *Journal of International Relations Security and Economic Studies*, *1*(3), 43–58. http://journals.rcmss.com/index.php/jirses/article/view/171

Adedoyin, A. D. (2023). *A study of the impact of technology on cybercrime in the public and private sectors in Nigeria* [Doctoral dissertation]. University of Portsmouth.

Adepetun, A. (2021). 0.71% of 1,500 fraudulent attacks aimed at Nigerian crypto investors. The Guardian. https://guardian.ng/business-services/0-71-of-1500-fraudulent-attacks-aimed-at-nigerian-crypto-investors/.

Adrian, T., & Mancini-Griffoli, T. (2021). The rise of digital money. *Annual Review of Financial Economics*, *13*(1), 57–77. https://doi.org/10.1146/annurev-financial-101620-063859

Agbo, E. I., & Nwadialor, E. O. (2020). Cryptocurrency and the African economy. *Economics And Social Sciences Academic Journal*, *2*(6), 84–100.

Alao, B. B., & Odum, A. N. (2019). Fighting fraud in Nigeria banking industry. An examination of the impact of forensic auditing. *Social Science Research Network*.

Aransiola, J. O., & Asindemade, S. O. (2011). Understanding cybercrime perpetrators and the strategies they employ in Nigeria. *Cyberpsychology, Behavior, and Social Networking*, *14*(12), 759–763. https://doi.org/10.1089/cyber.2010.0307

Assarut, N., Bunaramrueang, P., & Kowpatanakit, P. (2019). Clustering cyberspace population and the tendency to commit cyber crime: A quantitative application of space transition theory. *International Journal of Cyber Criminology*, *13*(1), 84–100.

Bartoletti, M., Lande, S., Loddo, A., Pompianu, L., & Serusi, S. (2021). Cryptocurrency scams: Analysis and perspectives. *Ieee Access*, *9*, 148353–148373. https://doi.org/10.1109/ACCESS.2021.3123894

Button, M., Brooks, G., Lewis, C., & Aleem, A. (2017). Just about everybody doing the business? Explaining 'cash-for-crash' insurance fraud in the United Kingdom. *Australian & New Zealand Journal of Criminology*, *50*(2), 176–194. https://doi.org/10.1177/0004865816638910

Button, M., Pakes, F., & Blackbourn, D. (2016). 'All walks of life': A profile of household insurance fraudsters in the United Kingdom. *Security Journal*, *29*(3), 501–519. https://doi.org/10.1057/sj.2013.43

Cassiman, A. (2019). Spiders on the world wide Web: Cyber trickery and gender fraud among youth in an Accra*zongo*. *Social Anthropology*, *27*(3), 486–500. https://doi.org/10.1111/1469-8676.12678

Childs, A. (2024). 'I guess that's the price of decentralisation … ': Understanding scam victimisation experiences in an online cryptocurrency community. *International Review of Victimology*, *30*(3), 441–478. https://doi.org/10.1177/02697580231215840

Cook, S., Giommoni, L., Trajtenberg Pareja, N., Levi, M., & Williams, M. L. (2022). Fear of economic cybercrime across Europe: A multilevel application of routine activity theory. *The British Journal of Criminology*, *63*(2), 384–406. https://doi.org/10.1093/bjc/azac021

Corbet, S. (2021). *Understanding cryptocurrency fraud: The challenges and headwinds to regulate digital currencies* (Vol. 2). Walter de Gruyter GmbH & Co KG.

Corbet, S., Lucey, B. M., Urquhart, A., & Yarovaya, L. (2019). Cryptocurrencies as a financial asset: A systematic analysis. *International Review of Financial Analysis*, *62*, 182–199. https://doi.org/10.1016/j.irfa.2018.09.003

Daily Post. (2021). EFCC arrests Precious Ofure for $200,000 Bitcoin fraud, links suspect to Cubana Group. https://dailypost.ng/2021/11/12/efcc-arrests-precious-ofure-for-200000-bitcoin-fraud-links-suspect-to-cubana-group/.

Daily Post. (2023a). Internet fraudster jailed for defrauding American of $20,000. https://dailypost.ng/2023/11/15/internet-fraudster-jailed-for-defrauding-american-of-20000/.

Daily Post. (2023b). Nigerian convicted for scamming Australian in crypto fraud. https://dailypost.ng/2023/03/31/nigerian-convicted-for-scamming-australian-in-crypto-fraud/.

Danquah, P., & Longe, O. (2011). An empirical test of the space transition theory of cyber criminality: Investigating cyber crime causation factors in Ghana. *African Journal of Computing & ICT*, *2*(1), 37–48.

The Eagle. (2024). Court jails fraudster for $1.6 m cryptocurrency fraud. Retrieved from: https://theeagleonline.com.ng/court-jails-fraudster-for-1-6m-cryptocurrency-fraud/.

Eckert, S. (2018). Fighting for recognition: Online abuse of women bloggers in Germany, Switzerland, the United Kingdom, and the United States. *New Media & Society*, *20*(4), 1282–1302. https://doi.org/10.1177/1461444816688457

Egbo, O. P., & Ezeaku, H. C. (2020). Overview of the intermediary role of banks: The threat of cryptocurrency. *European Journal of Management and Marketing Studies*, *1*(1), 88–101.

Eigbe, O. E. (2018). Investigating the levels of awareness and adoption of digital currency in Nigeria: A case study of bitcoin. *Information Technologist*, *15*(1), 75.

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, *2*(1), 13–20. https://doi.org/10.1007/s11416-006-0015-z

Hall, T., & Ziemer, U. (2023). Cybercrime in commonwealth West Africa and the regional cyber-criminogenic framework. *The Commonwealth Cybercrime Journal*, *5*(7), 1–13.
Hall, T., & Ziemer, U. (2024). Online deviance in post-soviet space: Victimisation, perceptions and social attitudes amongst young people in Armenia. *Digital Geography and Society*.
Ibrahim, S. (2016). Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime and Justice*, *47*, 44–57. https://doi.org/10.1016/j.ijlcj.2016.07.002
Ibrahim, S. (2017). Causes of socioeconomic cybercrime in Nigeria. *Paper presented at IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*. (pp. 1–9). https://doi.org/10.1109/ICCCF.2016.7740439
Ibrahim, S., & Komulainen, S. (2016). Physical punishment in Ghana and Finland: Criminological, sociocultural, human rights and child protection implications. *International Journal of Human Rights and Constitutional Studies*, *4*(1), 54–74. https://doi.org/10.1504/IJHRCS.2016.076060
Jaishankar, K. (2008). Space transition theory of cyber crimes. In F. Schmallager & M. Pittaro (Eds.), *Crimes of the internet* (pp. 283–301). Prentice Hall.
Jaishankar, K. (2018). Cyber criminology as an academic discipline: History, contribution and impact. *International Journal of Cyber Criminology*, *12*(1), 1–8.
Jane, E. A. (2018). Gendered cyberhate as workplace harassment and economic vandalism. *Feminist Media Studies*, *18*(4), 575–591. https://doi.org/10.1080/14680777.2018.1447344
Jimoh, S. O., & Oluwasegun, O. B. (2020). The effect of cryptocurrency returns volatility on stock prices and exchange rate returns volatility in Nigeria. *Acta Universitatis Danubius. OEconomica*, *16*(6).
Krishnan, L. P., Vakilinia, I., Reddivari, S., & Ahuja, S. (2024). Analyzing cryptocurrency social media for price forecasting and scam detection. *2024 12th International Symposium on Digital Forensics and Security (ISDFS)*. (pp. 1–6). IEEE.
Lazarus, S. (2019). Just married: the synergy between feminist criminology and the Tripartite Cybercrime Framework. *International Social Science Journal*, *69*(231), 15-33. https://doi.org/10.1111/issj.12201
Lazarus, S. (2024). Cybercriminal networks and operational dynamics of business email compromise (BEC) scammers: Insights from the "black Axe" confraternity. *Deviant Behavior*, 1–25. https://doi.org/10.1080/01639625.2024.2352049
Lazarus, S., Button, M., & Adogame, A. (2022). Advantageous comparison: Using twitter responses to understand similarities between cybercriminals ("Yahoo boys") and politicians ("Yahoo men"). *Heliyon*, *8*, 1–9. https://doi.org/10.1016/j.heliyon.2022.e11142
Lazarus, S., & Okolorie, G. U. (2019). The bifurcation of the Nigerian cybercriminals: Narratives of the economic and financial crimes commission (EFCC) agents. *Telematics and Informatics*, *40*, 14–26. https://doi.org/10.1016/j.tele.2019.04.009
Lazarus, S., Whittaker, J. M., McGuire, M. R., & Platt, L. (2023a). What Do We know about online romance fraud studies? A systematic review of the empirical literature (2000–2021). *Journal of Economic Criminology*, *2*, 1–17. https://doi.org/10.1016/j.jeconc.2023.100013
Lazarus, S., Olaigbe, O., Adeduntan, A., Dibiana, E. T., & Okolorie, G. U. (2023b). Cheques or dating scams? Online fraud themes in hip-hop songs across popular music apps. *Journal of Economic Criminology*, *2*, 100033. https://doi.org/10.1016/j.jeconc.2023.100033
Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017). Cybercriminal networks, social ties and online forums: Social ties versus digital ties within phishing and malware networks. *The British Journal of Criminology*, *57*(3), 704–722.
Luchkin, A., Lukasheva, O. L., Новикова, НЕ, Melnikov, V., Zyatkova, A. V., & Yarotskaya, E. V. (2020). Cryptocurrencies in the global financial system: Problems and ways to overcome them. *Russian Conference on Digital Economy and Knowledge Management*. (RuDEcK 2020). https://doi.org/10.2991/aebmr.k.200730.077
Lusthaus, J., Kleemans, E., Leukfeldt, R., Levi, M., & Holt, T. (2023). Cybercriminal networks in the UK and beyond: Network structure, criminal cooperation and external interactions. *Trends in Organized Crime*, 1–24.
McGuire, M., & Dowling, S. (2013). Cybercrime: a review of the evidence. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf.

Mosoti, J. M., Wafula, J., & Nyang'au, A. (2022). Effect Of forensic auditing and investigation techniques on the financial performance of deposit-taking microfinance institutions in Kenya. *International Research Journal of Business and Strategic Management*, *4*(3), 186–198.

Ndubueze, P. N. (2020). Cybercrime and legislation in an African context. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 345–364. https://doi.org/10.1007/978-3-319-78440-3_74

Newburn, T. (2011). Policing youth anti-social behaviour and crime: Time for reform? *Journal of Children's Services*, *6*(2), 96–105. https://doi.org/10.1108/17466661111149394

Ogochukwu N. S., & Jarrar, Y. (2018). Online media coverage of BitCoinCrypto-currency in Nigeria: A study of selected online version of leading mainstream newspapers in Nigeria. H-ermes. *Journal of Communication*, *2018*(12), 141-172.

Ogunleye, Y. O., Ojedokun, U. A., & Aderinto, A. A. (2019). Pathways and motivations for cyber fraud involvement among female undergraduates of selected universities in south-west Nigeria. *International Journal of Cyber Criminology*, *13*(2), 309–325.

Okeke, T. C., Ezeh, G. A., & Ugochukwu, N. O. A. (2015). Service quality dimensions and customer satisfaction with online services of Nigerian banks. *The Journal of Internet Banking and Commerce*, *20*(3). https://doi.org/10.4172/1204-5357.1000117

Okosun, O., & Ilo, U. (2023). The evolution of the Nigerian prince scam. *Journal of Financial Crime*, *30*(6), 1653–1663. https://doi.org/10.1108/JFC-08-2022-0185

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

Ozili, P. K. (2022). Central bank digital currency in Nigeria: Opportunities and risks. In *The new digital era: Digitalisation, emerging risks and opportunities* (pp. 125–133). Emerald Publishing Limited. https://doi.org/10.1108/S1569-37592022000109A008

Platt, M., Ojeka, S., Drăgnoiu, A., Ibelegbu, O. E., Pierangeli, F., Sedlmeir, J., & Wang, Z. (2023). Energy demand unawareness and the popularity of bitcoin: Evidence from Nigeria. *Oxford Open Energy*, *2*, 1–18. https://doi.org/10.1093/ooenergy/oiad012

Press statement. (2023). 'How Nigerian fraud suspect allegedly dupes victims in 13 countries -EFCC' [online] Available at: How Nigerian fraud suspect allegedly dupes victims in 13 countries – EFCC (premiumtimesng.com) (Accessed:1st June 2023).

Salawu, M. K., & Moloi, T. (2018). Benefits of legislating cryptocurrencies: Perception of Nigerian professional accountants. *Academy of Accounting and Financial Studies Journal*, *22*(6), 1–17.

Sarkar, G., & Shukla, S. K. (2024). Bi-directional exploitation of human trafficking victims: Both targets and perpetrators in cybercrime. *Journal of Human Trafficking*, 1–22. https://doi.org/10.1080/23322705.2024.2353015

Tade, O. (2013). A spiritual dimension to cybercrime in Nigeria: The 'yahoo plus' phenomenon. *Human Affairs*, *23*(4), 689–705. https://doi.org/10.2478/s13374-013-0158-9

TRM Labs. (2023). Nigerian crypto scammer sentenced to three years for running international pig-butchering scheme. https://www.trmlabs.com/post/nigerian-crypto-scammer-sentenced-to-three-years-for-running-international-pig-butchering-scheme.

Ukwueze, F. (2021). Cryptocurrency: Towards regulating the unruly enigma of fintech in Nigeria and South Africa. *Potchefstroom Electronic Law Journal/Potchefstroomse Elektroniese Regsblad*, *24*(1), 1–38. https://doi.org/10.17159/1727-3781/2021/v24i0a10743

Wall, D. S. (2013). *Cybercrime*. Polity Press.

Yar, M., & Steinmetz, K. F. (2019). *Cybercrime and society*. London: SAGE Publications Limited.