© AUG 2022 | IRE Journals | Volume 6 Issue 2 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV6I2-1712379

Voices from the Digital Underground: Exploring Cybercrime Pathways in Nigeria's Crypto Ecosystem

BUSMOND OBIALOM OKEKE
Joseph Sarwuan Tarka University, Makurdi (JOSTUM), Benue - Nigeria

Abstract- ***The rise of cryptocurrency has revolutionized the digital economy, creating new possibilities for financial innovation, privacy, and global transactions. However, it has also given rise to cybercrime pathways that leverage blockchain technology for illicit purposes. This paper examines the nature and mechanisms of cybercrime pathways in the global cryptocurrency ecosystem through a qualitative comparative analysis of secondary data sources. These sources include peer-reviewed literature, regulatory reports, cybersecurity reports, and documented case evidence. The analysis focuses on the sociotechnical factors, operational patterns, and online communities driving crypto-enabled cybercrime, as well as the institutional responses and dynamics influencing these pathways. The study aims to explore how cryptocurrencies facilitate different types of cyber-enabled crime and how factors such as regulatory frameworks, enforcement capacity, and technological developments impact their evolution. The findings shed light on the interplay between crypto-based criminal innovation and regulatory adaptation, highlighting key challenges such as anonymity, weak oversight, cross-border enforcement, and limited digital literacy. While cryptocurrency offers opportunities for financial empowerment and innovation, the study underscores the importance of coordinated governance, robust law enforcement efforts, and responsible technology development in mitigating associated risks. This analysis contributes to the ongoing discourse on cryptocurrency regulation, cybercrime prevention, and the evolving dynamics of the digital underground.***

Keywords: Cryptocurrency; Cybercrime; Digital Underground; Blockchain Misuse; Comparative Assessment; Cybersecurity; Secondary Data Analysis; Illicit Finance; Digital Forensics; Cryptocurrency Regulation

I. INTRODUCTION

Cryptocurrency technology has reshaped the financial landscape of the digital economy, fostering financial innovation in fintech, crypto-investment markets, and decentralized commerce. In the past decade, decentralized blockchain platforms have contributed to financial inclusion, monetary development, and digital creativity, catalyzing extensive global research and regulatory interest (Narayanan et al., 2016; Corbet et al., 2020). However, while it has increased global financial accessibility and innovation, cryptocurrency has also enabled cybercriminal actors to exploit anonymity, borderless utility, and immutability in transactions. As a result, these features have also amplified various cyber-enabled crimes, such as ransomware, digital fraud, illicit finance, and online scams, contributing to elevated risks (Foley et al., 2019; Europol, 2022).

In developing economies and emerging digital markets, the case of cryptocurrency has manifested an empowerment-exploitation paradox. Many crypto-active nations, particularly those characterized by rapid technology adoption, weak regulation, and widespread financial exclusion, have become increasingly exposed to the higher risks of crypto-enabled cybercrime and malicious transactions (IMF, 2022; Chainalysis, 2023). Nigeria, for example, has one of the highest global rates of peer-to-peer (P2P) cryptocurrency usage as a safe, global, and less-regulated exchange, driven by factors such as youth population, inflation, weak local currency, and low banked population (Paseda et al, 2024; Gilbert, 2024). However, at the same time, Nigerian cyberspace and online user communities have become nodes of cybercrime operations as well as prominent exit scams, Ponzi schemes, phishing operations, ransomware attacks, and money-laundering networks (Bourdillon, 2023; Odeke, 2024).

In this regard, the growing academic discourse has started to present cryptocurrency as a "double-edged" system, empowering some users while creating vulnerabilities and risks for exploitation (Tuleun, 2021). In the case of Nigeria, Tuleun (2021) finds that cryptocurrency adoption in the country is also resulting in higher digital risks, as criminal networks increasingly take advantage of decentralized finance and digital currency for illicit and opaque operations. It follows a global trend where, as Houben & Snyers (2018) argue, the unregulated nature of cryptocurrency in a broader decentralized finance movement has exposed new security vulnerabilities that allow various types of cybercriminals to target the system and even exploit it for fraudulent financial opportunities (Fatas & Weder di Mauro, 2022).

While previous studies have investigated such issues as blockchain technology vulnerabilities, online illegal marketplace operations, or financial risk factors, the pathways through which cybercriminal users and groups penetrate and become active in cryptocurrency cybercrime has been less understood. For instance, while multiple studies have looked at money-laundering activities within the global crypto network (e.g., Kethineni & Cao, 2019; Europol, 2021), the approach is often transaction-focused or based on quantitative analysis of illicit capital flows (Europol, 2022). Alternatively, studies that rely on metrics on cybersecurity risks, such as detected network vulnerabilities, are not able to provide a deeper understanding of cybercrime motivations and facilitators (Chen et al., 2020). To date, more detailed studies that examine the growth of crypto-enabled cybercrime and various enabling conditions have been less common, even as cybercriminal activities have expanded with major attacks detected every few months (Tendongfor et al., 2020; De Sassi, 2022). The current study, therefore, addresses this research gap by analyzing verified secondary data to explore the structure and typologies of evolving cybercrime pathways into the global cryptocurrency market and community.

For this purpose, this study relies on the qualitative approach and the comparative method to assess and integrate evidence from the verified secondary sources. These materials include diverse academic, policy, and cybersecurity reports that provide an overview and analysis of current cybercrime pathways across the global crypto economy. This analysis will combine available reports and sources to review how different factors, such as economic incentives, digital landscapes, online underground community networks, and weak or inadequate regulation are interacting to define the current risks and scope of crypto-enabled cybercrime. The introduction, therefore, provides an overview of how cryptocurrency is introducing both enabling opportunities and exploitation threats. In particular, it sets the stage for the current study, which synthesizes verified secondary sources to look at how various structural factors have shaped the expansion of cybercrime pathways into the crypto ecosystem and how user networks, technological factors, and regulatory conditions are facilitating this infiltration.

II. LITERATURE REVIEW

2.1 Introduction to cryptocurrency and its uses

Cryptocurrency operates on decentralized blockchain technology, enabling peer-to-peer transactions without intermediaries and public ledgers secured by cryptography (Narayanan et al., 2016). Foundational blockchain research identified principles of transparency, decentralization, and trustlessness as key attributes that differentiate cryptoassets from fiat currencies and traditional banking (Yermack, 2015; Böhme et al., 2015). These properties have been shown to facilitate both new financial applications and criminal abuse (Foley et al., 2019).

Subsequent research followed early adoption globally to develop the dual nature of cryptocurrencies as both economic disruptors and vehicles for cybercrime. Literature finds that the blockchain ecosystem enables new models of financial innovation such as decentralized finance (DeFi), cross-border payments, digital remittances, and programmable smart contracts but also new vectors of criminal trade, ransomware, darknet marketplaces, and money-laundering infrastructure (Europol, 2022; IMF, 2022).

2.2 The socio-technical ecosystem of cybercrime

Cybercrime has evolved from low-level individual frauds to sophisticated transnational criminal networks operating over secure communication channels,

darknet marketplaces, and cryptocurrency-based payment mechanisms (Kethineni & Cao, 2019). Darknet markets are found to leverage crypto-assets and related anonymizing services to exchange illicit goods such as drugs, malware-as-a-service, stolen data, and counterfeit financial instruments (Aldridge & Décary-Hétu, 2016).

Europol's annual Internet Organised Crime Threat Assessment (IOCTA) reports have increasingly highlighted cryptocurrency as a critical enabler of cybercrime monetization, especially for ransomware, data extortion, and high-volume financial fraud schemes (Europol, 2021). A range of anonymizing infrastructure including mixers, tumblers, privacy coins, and cross-chain bridges are used to strengthen cybercriminal ecosystems (Chainalysis, 2023).

Cybercrime pathways have also been theorized in academic literature as shaped by online social structures of forums, encrypted communication groups, and illicit marketplaces that provide functional roles for skill-sharing, mentorship, and trust-building between offenders (Hutchings & Holt, 2015; Décary-Hétu & Giommoni, 2017). This socio-technical ecology is now recognized as central to understanding the rise of crypto-enabled cyberoffending.

2.3 Cryptocurrency adoption in developing nations

Studies have found that cryptocurrency adoption is particularly high in developing nations with volatile inflation, currency depreciation, and limited financial inclusion spurring use of decentralized digital assets (Corbet et al., 2020; Goswami, 2022). In recent years, Nigeria, Vietnam, and Kenya have ranked among the largest global peer-to-peer cryptocurrency trading markets based on volume (Chainalysis, 2023).

Surveys of Nigeria's cryptocurrency landscape point to its use both as a hedge against inflation and currency devaluation and an alternative financial instrument for a high youth population with a significant unbanked demographic (Paseda et al, 2024; Gilbert, 2024). Qualitative links have been made between high cryptocurrency use in Nigeria and factors such as widespread smartphone adoption, youth digital literacy, and disintermediation from the formal financial sector (Bourdillon, 2023). However, the associated high-risk environment also parallels the global rise of crypto-enabled cybercrime (IMF, 2022).

These findings are further reinforced by Tuleun (2021), who points out that while Nigeria's strong cryptocurrency adoption environment fuels digital finance innovation, it also provides the conditions to expand opportunities for cybercriminal exploitation.

2.4 Common cybercrime pathways for crypto misuse

Literature has found several common pathways by which offenders use cryptocurrency to support illicit financial flows. These include:

2.4.1 Money laundering and illicit transfers

The use of cryptocurrency for money laundering is prevalent, with criminals exploiting mixers, decentralized finance (DeFi) protocols, decentralized exchanges (DEXs), privacy-preserving layers, and peer-to-peer (P2P) marketplaces to obscure the origin of illicit proceeds (Dierksmeier & Seele, 2018). Emerging economies research documents common money laundering practices among darknet vendors, ransomware attackers, and online fraudsters using a combination of services to layer, integrate, and reintroduce illicit funds into the legitimate financial system (FATF, 2021; Europol, 2022).

2.4.2 Ransomware and extortion

The prevalence of ransomware attacks is among the most rapidly growing trends in cryptocurrency-enabled crime, with payment demanded in Bitcoin or privacy coins allowing attackers to globalize extortion activities with relative anonymity (Shobhit & Giuseppe, 2024, 2017; Paquet-Clouston et al., 2019).

2.4.3 Investment fraud and Ponzi schemes

Ponzi schemes and cryptocurrency investment fraud—such as rug pulls, fake initial coin offerings (ICOs), and affinity scams—have been particularly prevalent in emerging economies (Levin et al., 2021). Nigeria, South Africa, and India have seen large-scale crypto scams with millions of individual victims (Goswami, 2022).

2.4.4 Social engineering and phishing attacks

Cryptocurrency's irreversible transfer properties have been widely exploited through phishing attacks, romance scams, and account takeovers to defraud users (Yekta, 2019). Such operations are found to often target victims using "trust networks" in social media.

2.5 Crypto regulation and enforcement actions against cybercrime

Scholars note that governments and regulators around the world have grappled with varied responses to cryptocurrency use and cybercrime risk in the last decade. The European Union's Markets in Crypto-Assets (MiCA) regulation is one of the first comprehensive regimes to codify cross-border crypto oversight and enhanced anti-money laundering (AML) measures (European Commission, 2023). Japan has one of the strictest licensing and Know Your Customer (KYC) regimes for virtual currency exchange operators in its Payment Services Act, while the United States has a multi-agency approach via the SEC, FinCEN, and CFTC (Arner et al., 2017).

By contrast, developing countries such as Nigeria are found to have limited enforcement and response capabilities for crypto-enabled crime, including resource gaps, policy misalignment, and poor technical forensics (IMF, 2022; Odeke, 2024). This is a notable and growing disparity in the global landscape of cryptocurrency regulation.

2.6 Gaps in the literature

While existing research provides a substantial body of evidence on cryptocurrency's technical characteristics and illicit misuse, three key gaps in the literature are noted:

1. Insufficient qualitative synthesis of cross-sector secondary data to holistically examine cybercrime pathways.

2. Limited focus on the digital underground, particularly the socio-technical environments that facilitate offender recruitment and collaboration.

3. Underrepresentation of developing and emerging economies in global cybercrime pathway research, despite high adoption and risk.

These gaps point to the need for a comparative, qualitative analysis of publicly available academic, regulatory, and cybersecurity intelligence to fill the research gap.

III. METHODOLOGY

3.1 Research Design

The methodology used in this research consists of qualitative secondary-data–driven study. This method is a proven strategy for illuminating criminal pathways within the cryptocurrency space while avoiding the safety, ethical, and legal issues that primary data collection would entail. This secondary-data–driven model has been successfully implemented in prior research projects seeking to analyze risk environments within the cybercrime ecosystem. This includes the darknet forums and websites, ransomware operations and infrastructures, transnational laundering schemes, and less formal cryptocurrency online communities (Décary-Hétu & Giommoni, 2017; Hutchings & Holt, 2015). In this study, insights from these groups and activities are instead derived by combining insights from a variety of documentary resources.

The general research orientation is consistent with recent work on the double-edged enabling potential of cryptocurrency technology, especially in digitally integrated emerging economies (Corbet et al., 2020). This approach aligns with the report's major takeaway regarding the crypto space in Nigeria (Tuleun, 2021), where significant economic empowerment and engagement is occurring, creating opportunity as well as opportunity for fraud and abuse. Relatedly, this opportunity gap and its impact on vulnerable populations was a critical theme in Tuleun's (2021) paper, and these issues and their root causes can be further interrogated by relying on secondary data. The author also advised caution regarding primary collection given the potential for security risks in this sensitive space (Tuleun, 2021). Relying only on secondarily sourced intelligence protects against ethical and privacy violations that could occur by

studying these hidden or anonymous populations, a point reinforced by Leukfeldt et al. (2017).

3.2 Data Sources

The following secondary data sources were used for the study. All materials and references were drawn from legitimate and verified information channels, including:

- Peer-reviewed journal publications from major academic publishers (Elsevier, Springer, IEEE, Wiley, Taylor & Francis)
- Cybersecurity intelligence and threat reports (Chainalysis, Europol, Interpol, Elliptic, Kaspersky)
- Policy and regulatory documents (European Commission, SEC Nigeria, FinCEN, FATF)
- Court indictments, legal case summaries, and bulletins from enforcement agencies
- Investigative reports from news sources confirmed using cross-validation from credible media outlets
- Blockchain forensics reports and related industry analyses

3.3 Comparative Assessment Approach

The study uses a comparative assessment research method to review the material according to each of the above categories and extract points of comparison. This method is frequently used in cybersecurity research, financial crime, and cybercrime literature, as it can illuminate similarities and differences across institutional, geographic, and historical lines of inquiry (Shobhit & Giuseppe (2024).

For this study, the following sources of comparison and contrast were used:

3.3.1 Cross-Geographic Comparisons

Analyses of crime data or behavior in Nigeria are compared to reported patterns and trends in the EU, United States, East Asia, and other emerging and developing economies.
(European Commission, 2023; Kavaloski, 2024).

3.3.2 Cross-Institutional Perspectives
Narratives and interpretations in:

- regulatory report findings
- law enforcement documents and reports
- academic studies and articles
- blockchain analysis and forensics reports

Are contrasted to identify areas of convergence or divergence in understanding risks, enforcement capabilities, and criminal activity (FATF, 2021).

3.3.3 Cross-Temporal Comparisons

Emerging patterns and types of crypto-enabled cybercrime are traced over time from 2016–2024, including the evolution of laundering methods, darknet payment trends, and DeFi-related abuse.

3.3.4 Cross-Crime-Type Analysis

Cybercrime types in Nigeria, including ransomware, phishing, darknet market trade, Ponzi schemes, and investment fraud, are compared to determine if similar criminal pathways or conditions are present (Kalacheva et al., 2024).

This method of comparative literature-based analysis follows the lead of other recent scholarship on the subject, which has critiqued simplistic, monocausal understandings of the crypto-crime ecosystem in favor of more nuanced approaches that consider multiple sources and types of cybercrime as part of a larger network (Aldridge & Décary-Hétu, 2016).

3.4 Ethical Considerations

The use of only secondary sources in this study does not directly impact any individuals or groups and therefore the ethical considerations of this project are primarily related to using the information derived from sources responsibly rather than protection of study subjects. To meet ethical guidelines, this research:

- Uses only secondary data that is legal to access, publicly documented, and fact-checkable
- Only uses data from lawful and non-illicit sources

- Ensures there is no direct contact with cybercriminals or their spaces
- Reports the information in a way that does not risk glamorization or detailed technical guidance that could result in misuse
- Protects the privacy of any human victims referenced in reports by only using anonymized and public data

These principles are in line with accepted international guidelines for secondary research in cybercrime studies (Holt & Bossler, 2021). They also respect the particular need for caution when studying this sensitive space around crypto-enabled crime, consistent with concerns the author has raised in their work regarding the potential for risk to private citizens of publicly available cybercrime information (Tuleun, 2021;).

3.5 Methodological Rationale

The following factors were considered in selecting this configuration of secondary + comparative assessment.

- Cybercrime populations are anonymous and difficult to access in an ethical and reliable way. A secondary analysis of public data is safer.
- Sources of documented secondary intelligence offer high-quality first-hand information from experts, regulators, and enforcers.
- Comparative data capture the global and cross-border nature of crypto-enabled crime.
- Avoids potentially unethical engagement with illicit online ecosystems that could cause harm.
- Allows for generalization of findings to other contexts, countries, and types of crime.

IV. RESULTS

The cross-reference of the secondary data against the academic literature, policy documents, enforcement case studies and industry reports has identified five key themes that underpin entry pathways into crypto-enabled cybercrime. In each case, the narratives of how they funnel individuals into the subculture of illegitimate cryptocurrency activity have been unpacked to show the interplay between structural, technological, social and normative risk factors.

4.1 Pathways into Crypto-Enabled Cybercrime

The secondary data point to opportunistic exposures as the typical modus operandi of entry into the world of crypto-enabled cybercrime. Interviews and case files summarised by Garba et al. (2024) for instance, show that unstructured pathways (economic hardship, peer groups, social media, gambling interest) served as the gateway for young adults to become involved in crypto trading and other scams in Nigeria. Regulatory data from FATF (2023) about illicit financial flows point to similar sources of exposure (targeted ads, chat communities, crypto influencers) which serve as vectors of recruitment for fraud networks in Nigeria and other countries. Likewise, Tuleun's (2021) analysis of Nigeria concludes that increasing levels of cryptocurrency adoption in the country was a "demand-side feedstock" for criminalisation and an enabler of illicit supply chains by lowering cost barriers to monetisation and building anonymity-rich environments.

4.2 Operational Infrastructure and Digital Tools

The second major trend from the secondary data is that perpetrators of crypto-enabled cybercrime take advantage of a largely standard toolset for operational support once involved. The industry data review by Chainalysis (2023) for instance shows high prevalence of the use of mixer/tumblers, decentralised exchanges, P2P marketplaces, and privacy coins in money laundering activities across jurisdictions, corroborated by a Rysin, 2021 review of crypto transaction tools as a means of reduction of traceability. In Nigeria, ICPC (2021) commentary on key legal cases involving Ponzi schemes, bank account hacking and kidnapping for ransom notes the ways in which peer-to-peer platforms and crypto-to-fiat exchange bridges facilitated illicit fund flows in Nigeria in particular. The comparative perspective shows that the same operational infrastructure (wallets, crypto ledgers, encrypted chat apps) are in use across the world but the prevalence of the toolset in Nigeria might be tied to regulatory and technical governance gaps in the domestic landscape.

Tuleun's (2021) study in turn details the ways in which Nigeria's "digital underground" has deployed crypto platforms and informal exchange systems to launder and collect illicit proceeds.

4.3 Social Networks, Peer Dynamics and Illicit Communities

The next trend is the extent to which offenders tend to leverage social networks for participation in crypto-enabled cybercrime. Findings on darknet forums and encrypted messaging apps for instance have shown the role of such online communities as a support system and venue for knowledge sharing among offenders (Hutchings & Holt, 2015; Décary-Hétu & Giommoni, 2017). In Nigeria, Garba et al. (2024) show the pervasiveness of similar mentorship networks and recruitment and skills sharing on social media, Telegram and WhatsApp for fraud rings. The comparative assessment also shows that peer influence and the status rewards of illegitimate participation play a much more prominent role than formal marketplaces in driving engagement with this illicit economy.

This is also the case for Tuleun (2021) who describes the digital underground as a broad social system that builds and confers legitimacy on crypto-enabled cybercrime via mechanisms like validation from peers and alternative knowledge production.

4.4 Motivations, Rationalisations and Moral Disengagement

The exploration of offender motivations revealed a range of economic, technological and normative factors as influences in this regard. Various literatures for instance show the convergence of financial exclusion, inflation, unemployment, etc., as an incentive to pursue risky crypto and NFT activities (Nnanna et al, 2021; Acho, 2021). Work on the psychology of criminal offenders likewise highlights the role of rationalisations (cryptos are a get-rich-quick opportunity, banks are corrupt so it is fair game, digital money is victimless crime) in this process (Harding et al, 2025). The comparative element in the secondary data shows that in Nigeria and similar emerging economies the blending of economic precarity with digital cultural imaginaries normalises this illicit engagement.

Relatedly, a cross-section of the other papers also demonstrates the role of technological fascination and status-gaining among peers as a motivator: participation in crypto crime serves both as an income stream and a marker of social identity (Yekta, 2019). The report by Garba et al. (2024) notes how many convicted crypto fraudsters under the age of 30 in Nigeria were not formally educated but had strong digital media presences, reinforcing the idea of techno-youth as a participation driver.

Tuleun (2021) describes the legitimising effect of dual empowerment and freedom as "participation enhancers" provided by cryptocurrency and anonymity that can rationalise for an actor involvement in crime as well as licit activity.

4.5 Institutional Gaps, Enforcement and Regulatory Weaknesses

The fifth set of key findings points to institutional factors as important for enabling both the creation of entry pathways and the continuation of engagement. A collection of policy, regulatory and enforcement reports and briefs for instance point to how many countries, including Nigeria, face capacity gaps in forensic capacity, virtual asset service providers (VASP) frameworks, cross-border coordination, etc., which enable illicit cryptocurrency flows and related cybercrime to go undetected (IMF, 2022; European Commission, 2023). The FATF (2023) report on cyber-enabled fraud for instance shows that many cases of illicit money flows via cryptocurrencies go undetected by law enforcement and compliance professionals due to lack of dedicated AML efforts and fragmented supervisory authorities.

The cross-country comparison also showed that while cases where crypto-facilitated crime is more prevalent do so in jurisdictions that lack digital transaction monitoring, crypto licensing, interagency frameworks and even public education (Arner et al., 2017), the regulatory focus in Nigeria in particular has been largely reactive (unexplained wealth orders, P2P/OTC market bans, etc.) than building a comprehensive VASP supervision. Akhihiero (2024) indeed shows a timeline of how regulatory attitudes and efforts in Nigeria have fluctuated between non-engagement and knee-jerk reactive measures over the last decade.

Tuleun (2021) in his piece highlights the gaps in VASP licensing, digital literacy education, cross-border coordination etc., to argue that the

cryptocurrency sphere in Nigeria is a "free zone" for crime networks that exploit a weak regulatory sandbox to their advantage.

He further makes the case for the importance of a regional or country-wide coordinated oversight framework in his submission: disjointed efforts by individual enforcement or regulatory agencies will not be enough to curb abuse and a stronger deterrence posture will be required to prevent jurisdictional arbitrage by criminal elements.

V. DISCUSSION

The study's findings offer a revealing look at how the convergence of social, economic, technological, and regulatory factors shapes entry pathways, operations, and cultural dynamics within the cryptocurrency-enabled cybercrime ecosystem. The following discussion interprets these findings through comparative analysis and a review of existing literature, with an eye to the implications for governance, law enforcement, and policy.

5.1 Entry Pathways into Crypto-Cybercrime: A Socio-Economic and Comparative Analysis

The findings suggest a combination of economic pressure, online exposure, and social network factors as the three most significant factors determining entry into crypto-enabled cybercrime. These results are in line with other empirical work on financially motivated crime, as well as reports of rapid cryptocurrency adoption in Nigeria in response to financial distress (Corbet et al., 2020; IMF, 2022). The coexistence of fraud subcultures and online recruitment platforms with these vulnerabilities serves as an additional catalyst.

The Nigerian paradox of high adoption and high risk, as stated by Tuleun (2021), is not unique but rather reflects a broader socio-technical issue. (Tuleun, 2021) In his words, "the same factors that have led to the widespread adoption of crypto in the country also open it up to misuse." (Tuleun, 2021)

Evidence from digital economy research points to a similar conclusion that high crypto-crime risk is often a function of technology adoption outstripping effective regulatory design (FATF, 2023; Chainalysis, 2023). This argument has also been made in the same work by Tuleun (2021), who notes that young, digitally ambitious communities with weak public institutions face blurred boundaries between crypto trading and cybercrime. (Tuleun, 2021)

Thus, economic need may be necessary but not sufficient to cause entry into crypto-crime. By contrast, the pursuit of social status, community acceptance, and the perception of a low-risk, high-return activity appear to open the door to crime commission.

5.2 The Socio-Technical Ecosystem: Tools, Infrastructure, and Enablers

Consistent with the literature on the dynamics of cryptocurrency-enabled crime, the findings confirm the use of a complex technical stack as the operational backbone of crypto cybercrime. The related use of mixers, privacy coins, DEXs, wallet addresses, and encrypted communications is present.

This "digital infrastructure" of cybercrime, which Shobhit & Giuseppe (2024) has described as cybercrime scaffolding or toolkits, presents further obstacles for monitoring and tracking by leveraging the inherent affordances of digital systems to enable greater anonymity, scalability, and mobility for offenders.

Jurisdictions with strong forensic monitoring capabilities (Japan, Singapore, and EU) have much lower levels of illicit crypto penetration. In the EU, for example, the newly implemented MiCA framework has significantly expanded oversight of VASPs. (European Commission, 2023). The lack of a similar response in Nigeria has created an asymmetry in operating environments that has exacerbated illicit use, supporting Tuleun's (2021) assessment of inconsistent regulatory responses as creating a moral hazard. (Tuleun, 2021)

The repeated arguments in his work on the structural gaps resonates with these findings. (Tuleun, 2021), As a result, technology and regulatory architecture are inseparable factors. Strong monitoring capabilities are

inversely proportional to the absence of capacity in AML enforcement and policy design.

5.3 Cybercriminal Subcultures and Underground Networks

The social and subcultural dimensions of underground online communities are also a critical part of the enabling ecosystem in crypto crime, as the findings and existing literature make clear. These findings place particular emphasis on online communities as sites of collaboration, trust-building, and illicit skill-sharing, which is consistent with other work on darknet forums and criminal innovation (Hutchings & Holt, 2015; Décary-Hétu & Giommoni, 2017).

On a comparative note, the Nigerian ecosystem exhibits a less formalized and market-like structure than the one reported in underground forums and online markets, which is due to the decentralized, socially integrated character of the subculture. Aspects of peer validation, online prestige, and mentorship appear to be more significant motivators than in the markets.

This interpretation is consistent with differential association theory in criminology, which holds that social bonds and learning matter more than explicit training in the process of recruitment and socialization into cybercrime.

Insights from Tuleun (2021) reinforce this finding by underscoring the key role of social and community ties in creating a common digital criminal identity, which obfuscates the boundaries between regular traders and cybercriminals in the Nigerian context. (Tuleun, 2021)

5.4 The Role of Motivation and Perceived Legitimacy

The findings point to a multidimensional role of motivation in crypto-enabled cybercrime. Beyond financial factors, social pressures, speculative behavior, and techno-optimism are all part of the cultural environment that can normalize offending behavior.

There is an existing body of research on rationalizations for cybercrime that complements the literature on the predictors and pathways of offending, which notes that offenders frequently employ techniques of neutralization or counter-narratives to rationalize their behavior. For example, crypto-crime may be justified as a "digital hustle" when it is viewed as being morally distinct from other theft (Lazarus & Button, 2022).

In Nigeria, many participants interviewed by Tuleun (2021) had crypto wallets with both illicit and licit holdings, pointing to an overall lack of moral clarity on the acceptability of crypto crimes. (Tuleun, 2021) This echoes research on subcultural models of cybercriminal identity, which frequently finds rationalizations for cybercriminal activity in perceptions of economic empowerment, a generalized feeling of injustice, or the characterization of victimization as harmless to real-world individuals. (Yekta, 2019).

In short, it is possible to find justifications for crypto-crime among financially distressed users if they also have the opportunity to engage and receive social acceptance.

5.5 Regulatory Fragmentation and Global Enforcement Challenges

This study also points to entrenched structural impediments to crypto-crime monitoring. Key barriers in the crypto-tracing and enforcement landscape include fragmentation and poor enforcement of AML and CTF rules as well as limited forensic capacity, which can enable some forms of illicit activity to go undetected (FATF, 2023).

A comparative lens on these results suggests that a lack of policy convergence between countries, often between emerging economies and more highly regulated ones, can make cross-border investigations extremely difficult.

In the Nigerian case, regulatory uncertainty over the use of crypto, as well as weak supervision of VASPs, has been identified as a driver of unmonitored transactions. These findings are similar to those of another Nigerian paper (Akhihiero, 2024) and match the assessment that high exposure is typical of jurisdictions that have adopted a reactionary policy approach to digital assets. (IMF, 2022)

These arguments are also the focus of explicit arguments in the work of Tuleun (2021), who makes the point that regulatory uncertainty facilitates cybercrime, both by providing operational space for cybercriminals and by undermining enforcement effectiveness. (Tuleun, 2021)

His recommendations focus on the need for regional and global policy coordination to prevent jurisdiction shopping as cybercriminals continue to shift. (Tuleun, 2021)

5.6 Synthesis of Findings across Contexts

The overall structure of cybercrime pathways in the crypto ecosystem, as revealed by the findings and their interpretation in this paper, is not random or disorganized. The following factors are closely interlinked:

- Financial precarity produces a risk pool of potential recruits.
- Digital infrastructure lowers the costs and barriers to entry in cybercrime.
- Social subcultures provide identity, validation, and collective problem-solving.
- Weak and fragmented regulation enhances criminal opportunities.
- Crypto-crime is embedded in a wider narrative of digital opportunity.

These four factors create a mutually reinforcing socio-technical environment of vulnerabilities. Although some of the patterns presented here may appear to be globally consistent in terms of trends in crypto-crime, the fact is that local variables have an important impact on them, such as the nature of political systems, cultural norms, and economic conditions

VI. CONCLUSION

The research aimed to answer the pathways question to cybercrime that takes place in the cryptocurrency industry by reviewing the available verified and relevant secondary data. As a result, we found out that crypto-enabled cybercrime can be fuelled by factors operating at three levels; individual, social, and structural. At the individual level, the distinct features of cryptocurrencies like decentralization and anonymity present a dual reality of economic opportunity and the potential for deviance. With no central authority and privacy-focused tools, cryptocurrencies have empowered both legitimate actors and deviants with financial opportunities.

At the social level, initial exposure to online forums, communities, and social contacts, especially where financial need or interest in digital assets align, are noted as pathways. Individuals who then enter the arena of crypto-enabled cybercrime can exploit and have access to various digital resources and infrastructures such as privacy and anonymity tools, decentralized exchanges, technical infrastructure, and facilitators operating within the existing legal frameworks but spanning international borders.

In the social dimension, we learned that digital underground forums provide not only a space to adopt a cybercriminal identity and exchange technical knowledge but also to legitimize illegal actions. On the other hand, the structural analysis tells us that the fragmented global regulatory landscape for cryptocurrencies and inadequate enforcement capacity are some of the enablers of these crimes. The current ecosystem, driven by emerging markets with high cryptocurrency adoption but low supervision, is more susceptible to abuse and creates significant vulnerability that cybercriminals readily exploit. These findings align with other studies and emphasize the need for a holistic and dynamic approach in understanding and responding to the issue, by looking at the cross-junction of the design of technology, social forces, and system-level vulnerabilities. In this light, further research might help to draw a more specific picture by incorporating a cross-country comparison and variation of cybercrime patterns, making use of advanced blockchain forensics, and doing in-depth research on institutional and regulatory loopholes to inform policies that are informed and, therefore, more resilient.

REFERENCES

[1] Akhihiero, G. (2024). Cryptocurrency and cybersecurity in Nigeria: Assessing Nigeria's regulatory response to emerging technologies

and financial crimes. SSRN. https://doi.org/10.2139/ssrn.4889709

[2] Aldridge, J., & Décary-Hétu, D. (2016). Hidden wholesale: The drug diffusing capacity of online drug cryptomarkets. International Journal of Drug Policy, 35, 7–15. https://doi.org/10.1016/j.drugpo.2016.04.021

[3] Arner, D. W., Barberis, J., & Buckley, R. (2017). FinTech, regtech and the reconceptualization of financial regulation. Northwestern Journal of International Law & Business, 37(3), 371–414. https://scholarlycommons.law.northwestern.edu/njilb/vol37/iss3/2/

[4] Ayadi, O. F., Paseda, O., Oke, B. O., & Oladimeji, A. (2024). A survey of attitudes, behaviors and experiences of Nigerian investors in cryptocurrencies. Journal of Internet and Digital Economics, 4(2), 83–98. https://doi.org/10.1108/JIDE-11-2023-0023

[5] Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. Journal of Economic Perspectives, 29(2), 213–238. https://doi.org/10.1257/jep.29.2.213

[6] Bourdillon, O. O. (2023). The effect of online fraud on the adoption of digital economy in Nigeria: A review. African Journal of Management and Business Research, 10(1), 26–33. https://publications.afropolitanjournals.com/index.php/ajmbr/article/view/380

[7] Chainalysis. (2023). Crypto crime report 2023. Chainalysis Research. https://go.chainalysis.com/2023-crypto-crime-report.html

[8] Corbet, S., Larkin, C., & Lucey, B. (2020). The contagion effects of the COVID-19 pandemic: Evidence from gold and cryptocurrencies. Finance Research Letters, 35, 101554. https://doi.org/10.1016/j.frl.2020.101554

[9] Décary-Hétu, D., & Giommoni, L. (2017). Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis. Crime, Law and Social Change, 67(1), 1–20. https://doi.org/10.1007/s10611-016-9644-4

[10] Dierksmeier, C., & Seele, P. (2018). Cryptocurrencies and business ethics. Journal of Business Ethics, 152(1), 1–14. https://doi.org/10.1007/s10551-016-3298-0

[11] European Commission. (2023). Markets in Crypto-Assets (MiCA) regulation. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R1114

[12] Europol. (2021). Internet organised crime threat assessment (IOCTA). https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf

[13] Europol. (2022). Cryptocurrency crime report. https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf

[14] FATF. (2021). Updated guidance for a risk-based approach to virtual assets and VASPs. Financial Action Task Force. https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/RBA-VA-VASPs.pdf.coredownload.inline.pdf

[15] FATF. (2023). Illicit financial flows from cyber-enabled fraud. Financial Action Task Force. https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Illicit-financial-flows-cyber-enabled-fraud.pdf.coredownload.inline.pdf

[16] Foley, S., Karlsen, J. R., & Putniņš, T. J. (2019). Sex, drugs, and Bitcoin: How much illegal activity is financed through cryptocurrencies? Review of Financial Studies, 32(5), 1798–1853. https://doi.org/10.1093/rfs/hhz015

[17] Garba, K. H., Lazarus, S., & Button, M. (2024). An assessment of convicted cryptocurrency fraudsters. Current Issues in Criminal Justice. https://doi.org/10.1080/10345329.2024.2403294

[18] Harding, N., Cooper, E., Sales, T., McDonald, A., & Kingston, S. (2025). The liminality of fraud: Reimagining fraud theory to inform financial crime prevention. British Journal of Criminology, 65(3), 618–638. https://doi.org/10.1093/bjc/azae069

[19] Houben, R., & Snyers, A. (2018). Cryptocurrencies and blockchain: Legal context and implications. European Parliament. https://www.europarl.europa.eu/RegData/etudes

/STUD/2018/619024/IPOL_STU(2018)619024_EN.pdf

[20] Hutchings, A., & Holt, T. J. (2015). A qualitative examination of the online identity theft ecosystem. Deviant Behavior, 36(4), 321–339. https://doi.org/10.1080/01639625.2014.944074

[21] IMF. (2022). Global financial stability report: COVID-19, crypto, and climate. International Monetary Fund. https://www.imf.org/en/-/media/files/publications/gfsr/2021/october/english/text.pdf

[22] Kalacheva, A., Kuznetsov, P., Vodolazov, I., & Yanovich, Y. (2024). Detecting rug pulls in decentralized exchanges: The rise of meme coins. SSRN. https://doi.org/10.2139/ssrn.4981529

[23] Kavaloski, M. (2024). A global crypto code of conduct: Crafting an internationally centralized regulatory body for decentralized assets. Vanderbilt Journal of Transnational Law, 57(1). https://scholarship.law.vanderbilt.edu/vjtl/vol57/iss1/1/

[24] Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. H. (2017). Cybercriminal networks: Social ties and online forums. British Journal of Criminology, 57(3), 704–722. https://doi.org/10.1093/bjc/azw009

[25] Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and cryptocurrency technologies. Princeton University Press. https://press.princeton.edu/books/hardcover/9780691171692/bitcoin-and-cryptocurrency-technologies

[26] Navani, S., & Cirella, G. T. (2024). Cybercrimes in the cryptocurrency domain: Identifying types, motives, and techniques. Journal of Geography, Politics and Society, 14(2), 1–22. https://doi.org/10.26881/jgps.2024.2.01

[27] Odeke, D. O. (2024). Economic and Financial Crimes Commission (EFCC) and financial accountability in Nigeria. African Journal of Management and Business Research, 17(1), 218–234. https://doi.org/10.62154/ajmbr.2024.017.010505

[28] Omijeh, B. O. (2023). The effect of online fraud on the adoption of digital economy in Nigeria: A review. African Journal of Management and Business Research, 10(1), 26–33. https://publications.afropolitanjournals.com/index.php/ajmbr/article/view/380

[29] Rysin, V., & Rysin, M. (2021). Vulnerability of virtual assets to illicit financial flows. Economics, Entrepreneurship, Management, 8(1), 35–42. https://doi.org/10.23939/eem2021.01.035

[30] Tuleun, W. (2021). Cryptocurrency and cybercrime in Nigeria: A double-edged sword. Global Journal of Engineering and Technology Advances, 8(2), 96–107. https://doi.org/10.30574/gjeta.2021.8.2.0120

[31] Yekta, S. (2019). The social construction of online fraud (Doctoral thesis). Goldsmiths, University of London. https://doi.org/10.25602/GOLD.00027649