Journal of Contemporary International Relations and Diplomacy (JCIRD)
Vol. 6, No. 2, 2025, pages 46-59, Doi: https://doi.org/10.53982/jcird.2025.0602.04-j

Published by the Department of International Relations and Diplomacy, Afe Babalola University, Ado-Ekiti (ABUAD), Nigeria
E-mail: *jcirdabuad@gmail.com*

ISSN: 2714-3414
E-ISSN: 2971-6470

The Dark Web of Cryptocurrency: Unpacking the Nexus between Digital Currencies, Cybercrime, and Global Governance

Abdulmalik Olalekan OLADIPUPO

Abstract

This study explores the intersection of cryptocurrency, cybercrime, and global governance. It focuses on identifying criminal techniques, analyzing forensic and regulatory countermeasures, and evaluating the broader governance dilemmas that arise. A qualitative desk-based approach was employed, synthesizing secondary data from peer-reviewed studies, institutional policy papers (FATF, IMF, Europol), and industry reports (Chainalysis, Elliptic, TRM Labs). Thematic content analysis was used to trace patterns in illicit cryptocurrency use, law enforcement responses, and regulatory innovations. The findings indicate that while advances in blockchain forensics and policy coordination have strengthened oversight, criminals increasingly exploit decentralized finance platforms, cross-chain laundering, privacy coins, and mixers to evade detection. Enforcement remains uneven, hindered by fragmented regulations and gaps in cross-border cooperation. Overall, the study concludes that cryptocurrency-enabled cybercrime remains a resilient and evolving threat that challenges the stability of the global financial system and exposes weaknesses in governance frameworks. Without stronger coordination, adaptive regulation, and robust technological capabilities, the risks of illicit finance will continue to outpace control efforts. To mitigate these risks, the study recommends enhancing cross-border collaboration, investing in advanced blockchain forensic tools, and adopting flexible, multi-stakeholder governance models that balance innovation with accountability.

Keywords: Cryptocurrency, Cybercrime, Dark Web, Blockchain Forensics, Global Governance, Regulation, Financial Crime

Oladipupo Abdulmalik holds a Ph.D. in International Politics and Diplomacy from the Department of Politics and International Relations at Lead City University, Ibadan. He is currently a Lecturer in the same department, where he specializes in the intersection of global politics and innovative technologies. Oladipupo's research focuses on Blockchain Technology and Cryptocurrency. ORCID Number: 0000-0001-5441-7062

Introduction

The spread of cryptocurrencies worldwide has created a long-term paradox that both researchers and politicians still find difficult to resolve. On the one hand, digital currencies represent the potential of financial innovation, inclusion, and decentralisation, where individuals and businesses can get greater freedom than they ever had under centralised banking regulations. Alternatively, the same technological affordances have provided a ready platform into the hands of cybercriminals who use the pseudonymity, portability, and borderless quality of cryptocurrencies to promote ransomware attacks, drug dealing, fraud, and money laundering in the dark web. It is this duality: cryptocurrency as an emancipatory technology and cryptocurrency as an enabler of illicit finance that is the main puzzle on which the current paper attempts to dismantle. The dilemma to consider is not whether cryptocurrencies are good or bad, but how technological and institutional attributes create incompatibilities in innovation and crime, and what form of governance can be organised to switch between one or the other.

Scholarly discourse on cryptocurrencies has reached maturity within ten years, but it still has a strongly divided stalemate. Cryptocurrencies are viewed, by one of the most influential angles, developed by criminologists and cyber-security experts, as tools of cybercrimes. According to Chainalysis (2024), the number of ransomware payments was above USD 1 billion in 2023, which shows the growth of the dependence of organised cybercriminal groups on digital currencies. According to Elliptic (2022), there have been numerous cases of laundering using decentralised exchanges and mixers, whereas according to Europol (2023) there have always been active cases of legislation in the darknet market where cryptocurrency becomes the key form of exchange. It is through this perspective that cryptocurrencies can never exist without illegal markets and that they present existential risks to financial integrity and security. It is based on the evidence of increasing ransomware syndicates, the durability of black markets and high-level sophistication of laundering typologies, indicating that cryptocurrencies have become a structural facilitator of global cybercrime.

Conversely, there is a different body of literature that focuses on the valid roles and disruptive capabilities of cryptocurrencies. The International Monetary Fund (Bains et al., 2022), maintains that unbacked crypto assets are dangerous, but they can make cross-border transactions quicker, enhance remittance flows and advance payment methods. The World Economic Forum (2023) also points out opportunities for achieving balanced regulation by supporting innovation and reducing risk. In a similar manner, academic literature emphasizes that most cryptocurrency activity is not unlawful, and only less than 1 percent of the total amount of transactions represents illegal transactions (Chainalysis, 2024). The idea of this counter-argument is that the crypto-crime nexus is being overemphasised; and that over-regulation risks inhibiting innovation, or depriving developing economies of the freedom to experiment with finance, and pushing it even further underground.

The contradiction between the two indicates a more profound intellectual dilemma: how are the participants of global governance able to reconcile the dual-use character of cryptocurrencies in a manner that maintains a legitimate innovation and lessens their misuse on the dark web? The

dark web complicates this by adding a new layer onto this discussion, having formed an ecosystem of anonymity, decentralisation and illegal commerce. According to Europol (2023), when designed to combat darknet markets, a response is quickly developed by shifting to new platforms and/or implementing frameworks that are privacy-enabled, thereby pushing markets to others. The United Nations Office on Drugs and Crime (2023) also demonstrates the fact that more and more dark web sellers are turning to encrypted communications, crypto payments and whose conventional means of law enforcement do not work effectively. In such a way, discussion cannot turn upon whether crypto is structurally criminal or radical; instead, it should consider the dynamic interaction process of cybercriminal modification and governance response in a fragmented global system.

The available scholarship has achieved significant gains, but there are still gaps. First, a significant amount of criminological literature is dedicated to technical elements of the illicit use of cryptocurrencies, including mixing services, ransomware attack vectors or even darknet market volumes, without adequately situating these practices within more general inquiries of global governance. On the contrary, the regulatory heterogeneity and regulatory standard setting (e.g., FATF guidance) are frequently the focus of governance studies without necessarily considering the adaptive mechanisms towards cybercriminals on the dark web. Very little literature combines the two lenses to examine the manner in which the interplay between technological affordances, illicit practices, and systems of governance generates cycles of adaptation and enforcement. Second, although the body of empirical evidence on illicit cryptotransactions has continued to grow considerably since 2020, few efforts have been made to synthesise such data and situate it in regard to general theoretical discussions. The aim of this paper is to fill these gaps by putting the two realms of criminological and governance perspectives into conversation, as well as putting the recent findings of empirical studies in a wider theoretical context.

The predominant powers of this debate demonstrate that it is multi-dimensional. Persistent crypto-enabled crimes are reported by law enforcement agencies like Europol and the U.S. Federal Bureau of Investigation, which pose the problem as a security challenge. Financial authorities like the IMF, FATF and central banks are treating it like a financial stability and compliance issue. The presence of industry participants, such as blockchain analytics companies, such as Chainalysis and Elliptic, provides both risk and non-risk analyses based on data. Researchers within the field are divided over those who attribute the causes of cybercrime to routine activity theory and its situational crime prevention (Yar, 2021) and those who focus on regulatory pluralism and situational failure of governance (Leiser, 2022). Through active interaction with these sources, this paper shall find itself in an interdisciplinary discussion that cuts across criminology, finance, international relations and studies in technology.

This study can be applied in three aspects. This analysis first synthesizes results, including industry and institutional reports, to paint a current portrait of the crypto dark web nexus. Second, it advocates a theoretical perspective of integrating Routine Activity Theory and a global governance model to develop a perspective on how affordances provided by technology aspects define the potential to commit cybercrime, whereas enforcement due to audits is dictated by

institutional factors. Third, it conflicts with the binary conceptualization of cryptocurrencies as innovation or crime by showing how the two forms of cybercriminalization have evolved in a mutually reinforcing relationship. The significance of this new approach is that it predicts the systemic nature of the problem: crime and governance do not act independently and good policy needs to consider their interplay.

The general intellectual problem that informs this study is that what mechanisms of global governance can effectively negotiate between the opposing realities of cryptocurrency, as a legitimate innovation, on the one hand, and, as a facilitator of dark web cybercrime, on the other? In the act of providing this answer, the study not only informs the ongoing debates surrounding issues concerning cybercrime, financial regulations, and international collaboration, but it also provides relevant information on policy debates over the future of digital currencies. In methodological terms, the study adopts a qualitative desk-based approach, drawing on secondary data from industry reports, institutional publications, and academic literature published since 2020. A thematic content analysis is applied to extract recurring patterns in cybercriminal tactics, forensic countermeasures, and regulatory responses. Triangulation across multiple data sources enhances validity and ensures a comprehensive account of the nexus between cryptocurrencies, the dark web, and global governance.

The research problem is to determine how cryptocurrencies' technological affordances and global governance arrangements jointly shape the emergence, persistence, and evolution of crypto-facilitated cybercrime on the dark web. Rather than presuming either innovation benefits or criminal risks to be dominant, the study interrogates when, through what pathways, and for whom pseudonymity, programmability, and borderless transfer translate into illicit opportunity or are neutralised by oversight. It probes the conditions under which regulatory coordination, forensic analytics, and law-enforcement cooperation interrupt adaptive criminal tactics, or inadvertently displace them. Clarifying these mechanisms can indicate governance designs that preserve legitimate innovation while constraining dark-web exploitation dynamics. Accordingly, this study pursues three interrelated objectives: (i) to analyse how the technological affordances of cryptocurrencies enable cybercriminal activities on the dark web; (ii) to examine how global and national governance frameworks have responded to crypto-enabled crime, and why enforcement remains fragmented and reactive; and (iii) to illuminate the adaptive cycle between cybercriminal innovation and regulatory countermeasures.

Literature Review

Cryptocurrencies and Illicit Trade on the Dark Web

The dark web has become a central hub for illicit trade, and cryptocurrencies are integral to its operations. Unlike traditional financial systems that rely on centralised authorities, cryptocurrencies enable pseudonymous transactions that are difficult to trace, thereby making them particularly attractive to cybercriminals. Bitcoin remains the most widely used currency on these platforms, though privacy-focused alternatives such as Monero and Zcash have grown in popularity due to their enhanced anonymity features (Europol, 2022). These attributes facilitate a

thriving market for illegal commodities, including narcotics, counterfeit documents, stolen identities, malware and hacking tools. Empirical studies confirm that cryptocurrencies are the financial backbone of dark web marketplaces. The Silk Road pioneered the integration of Bitcoin into illicit trade, and successor markets such as AlphaBay and Hydra expanded this model into billion-dollar ecosystems before being dismantled by law enforcement (TRM Labs, 2022). The resilience of these markets, even after high-profile takedowns, demonstrates how deeply embedded cryptocurrencies have become within the cybercriminal economy. They provide not only a medium of exchange but also a mechanism for sustaining trust among anonymous actors who might otherwise be deterred by the risks of fraud or exposure.

More recent evidence highlights the diversification of cryptocurrency use in dark web campaigns. A study by Xia et al. (2024) documents how cybercriminals deploy a wide range of tokens in scams, ransomware schemes and money laundering operations. Similarly, forensic investigations into cryptocurrency wallet applications reveal the sophisticated methods employed to hide illicit flows and maintain operational security in digital underground markets (Chang et al., 2022). These findings illustrate that cryptocurrencies are no longer peripheral but have become the infrastructural lifeline of dark web commerce, enabling its expansion and globalisation despite regulatory and enforcement efforts. However, much of the existing scholarship focuses on documenting criminal techniques and market trends without explaining how these practices interact with evolving global governance responses. While studies successfully establish the centrality of cryptocurrencies to illicit digital economies, fewer analyses examine the conditions under which enforcement disrupts or reshapes these markets, or how cybercriminals adapt to new regulatory pressures. This absence of explanatory work leaves an unresolved gap concerning the dynamic relationship between technological affordances, illicit practices and regulatory counter-measures, which the present study seeks to address.

Cryptocurrencies and the Cybercrime Economy

The cybercrime economy has expanded significantly in recent years, with cryptocurrencies playing a central role in its growth and sustainability. Unlike traditional payment systems that are heavily regulated and traceable, cryptocurrencies such as Bitcoin and Monero provide cybercriminals with a relatively anonymous, borderless medium of exchange. This characteristic has made them indispensable in ransomware operations, one of the fastest-growing forms of cybercrime. In such attacks, malicious actors encrypt the data of individuals, corporations or even government agencies, demanding ransom payments in digital currencies to unlock access. Evidence from recent global incidents suggests that Bitcoin remains the most commonly demanded currency due to its wide adoption, while privacy-focused coins like Monero are increasingly preferred for their enhanced anonymity (Chainalysis, 2023).

Cryptocurrencies also underpin large-scale money laundering operations within the cybercrime economy. Criminal networks use mixing services, tumblers and decentralised exchanges to obscure the origins of illicit funds. These tools fragment and redistribute cryptocurrency transactions in ways that make it difficult for regulators and blockchain analysts to trace the flow of funds (Möser et al., 2021). Moreover, the advent of decentralised finance (DeFi)

platforms has added a new layer of complexity, as criminals exploit smart contracts, liquidity pools and cross-chain bridges to launder proceeds from fraud, trafficking and ransomware. This highlights how technological innovation often outpaces regulatory capacity, giving cybercriminals a strategic advantage. Concerns have also been raised about the potential use of cryptocurrencies for terrorism financing. While empirical evidence indicates that such use remains limited compared to other financing methods, the borderless and pseudonymous nature of cryptocurrencies presents vulnerabilities that extremist groups may exploit (Irwin & Turner, 2023). Collectively, these dynamics illustrate how cryptocurrencies have become deeply embedded in the cybercrime economy, reinforcing its resilience and posing profound challenges for governance at national and international levels. However, existing research predominantly documents cybercriminal techniques and technological vulnerabilities, with less attention devoted to explaining how cybercriminal activity evolves in response to regulatory interventions, forensic innovation or international cooperation. The literature provides strong descriptive evidence of laundering methods, ransomware models and DeFi exploitation, yet it does not adequately explain when enforcement becomes effective, why certain governance responses fail or how criminals strategically adapt to them. This gap limits understanding of the dynamic, reciprocal relationship between crime and governance, an issue this study seeks to clarify.

Governance and Regulatory Challenges

The decentralised architecture of cryptocurrencies fundamentally disrupts conventional approaches to financial governance. Unlike traditional banking systems, which operate under state supervision and rely on intermediaries such as commercial banks, cryptocurrencies function through distributed ledgers that bypass central authority. This decentralisation presents profound challenges for both states and international organisations that rely on existing regulatory models anchored in jurisdictional control. Peer-to-peer transactions, often pseudonymous, limit the capacity of regulators to monitor, verify and enforce compliance effectively (Irwin & Turner, 2023). Global institutions have attempted to address these governance gaps, most notably through the Financial Action Task Force (FATF). The FATF's introduction of the "travel rule" in 2019, which obliges virtual asset service providers to collect and share transaction information on the originator and beneficiary, represents an effort to align cryptocurrency transactions with anti-money laundering (AML) and counter-terrorism financing (CTF) standards (FATF, 2021). Nevertheless, enforcement remains uneven.

Advanced economies such as the United States and the European Union have made progress in integrating these standards into domestic law, compelling exchanges to implement robust know-your-customer (KYC) and transaction-monitoring frameworks. By contrast, regulatory capacity in many developing states is weak, resulting in gaps that cybercriminals exploit to conduct cross-border operations with minimal oversight (Okorie & Lin, 2021). This fragmented landscape creates opportunities for regulatory arbitrage, where illicit actors migrate to jurisdictions with weaker enforcement mechanisms. The lack of harmonisation further complicates international cooperation, as disparities in legal definitions, compliance standards and enforcement priorities hinder collective responses. Moreover, excessive regulatory rigidity risks stifling innovation,

while insufficient oversight threatens financial stability and security. Recent scholarship argues for a coordinated, multi-stakeholder approach that integrates national regulators, international organisations, private sector actors and technology developers to ensure both innovation and resilience against criminal exploitation (Scott et al., 2023). In essence, governance and regulatory challenges surrounding cryptocurrencies highlight the tension between decentralised technologies and state-based financial oversight, underscoring the urgent need for globally consistent regulatory frameworks. However, while the literature identifies fragmentation, arbitrage and weak enforcement as persistent challenges, fewer studies examine how regulatory shifts shape the adaptive behaviour of cybercriminals, or how governance interventions interact with the technological affordances of cryptocurrencies on the dark web. Most discussions focus on normative claims about what regulation should achieve, rather than empirical analysis of when regulation succeeds, fails or produces unintended consequences. This leaves a gap in explaining the dynamic feedback loop between governance and cybercriminal innovation — a gap this study seeks to address.

Ethical and Political Dilemmas of Regulation

The regulation of cryptocurrencies presents a profound ethical and political dilemma that lies at the intersection of innovation, governance, and security. On the one hand, digital assets are hailed for their potential to promote financial inclusion, particularly in regions where large segments of the population remain unbanked. By providing decentralised alternatives to traditional banking, cryptocurrencies reduce transaction costs, expand access to global financial systems, and offer opportunities for empowerment in fragile economies (Ozili, 2025). In this regard, heavy-handed regulation risks undermining innovation and excluding those who stand to benefit most from financial democratisation. On the other hand, insufficient or fragmented regulation creates a fertile ground for criminal exploitation. Cryptocurrencies are increasingly utilised in illicit practices such as ransomware, money laundering, and dark web transactions, exploiting their pseudonymous and borderless nature (Gonzálvez-Gallego & Pérez-Cárceles, 2021). Weak oversight allows actors to engage in regulatory arbitrage, operating in jurisdictions with minimal enforcement and undermining global financial stability. This dilemma reflects the broader political tension between state sovereignty and the decentralised ethos underpinning blockchain technologies (Ma et al., 2023).

Scholars have emphasised the need for innovative regulatory approaches that avoid the extremes of either suppressing innovation or allowing criminality to flourish. Reflexive law approaches, which emphasise adaptive, dialogue-based regulation rather than rigid rules, have been proposed as a means to balance flexibility with accountability (Motsi-Omoijiade, 2022). Moreover, the growing discourse on multi-stakeholder governance stresses the importance of cooperation among states, industry actors, civil society, and international organisations to manage the transnational challenges of digital currencies (Rau, Wardrop, & Zingales, 2021). Ultimately, the ethical and political dilemmas surrounding cryptocurrency regulation underscore the difficulty of reconciling technological innovation with the imperatives of security and governance. The

debate points to the urgent need for coherent, globally coordinated frameworks that foster innovation while curbing criminal misuse (Korpas et al., 2023). While this literature articulates the ethical and political trade-offs of regulation and advances promising frameworks (e.g., reflexive and multi-stakeholder governance), it seldom specifies *when* particular regulatory designs protect inclusion without amplifying criminal displacement, or *how* ethical commitments (e.g., privacy, autonomy, financial access) are operationalised in concrete supervisory choices. Empirical studies rarely trace the downstream, unintended effects of measures (such as travel-rule implementation or DeFi oversight) on vulnerable populations and on cybercriminal adaptation. This leaves a gap in linking normative regulatory models to observable outcomes across jurisdictions—an analytical space this study addresses.

Theoretical Underpinning

This study is anchored on the cyber-adaptation of Routine Activity Theory (RAT), which provides a robust situational framework for understanding how cryptocurrencies intersect with cybercrime within the dark web environment. Originally developed to explain crime occurrence in physical settings, RAT posits that crime results from the convergence of three elements: a motivated offender, a suitable target, and the absence of capable guardianship. Applied to cyberspace, these constructs take on new meanings as digital routines and technological infrastructures reshape opportunities for criminal behaviour. In the online environment, cryptocurrencies reduce the effectiveness of traditional guardianship mechanisms by offering pseudonymity and decentralisation. Motivated offenders exploit these affordances to conduct illicit transactions on dark web markets, while suitable targets range from vulnerable individuals to institutions exposed to ransomware and fraud. Guardianship is weakened because the borderless and encrypted nature of blockchain-based exchanges complicates tracing, interdiction, and enforcement (Yar & Steinmetz, 2019). Recent empirical studies highlight that RAT remains a valuable framework for explaining variations in cyber victimisation and offence opportunities, particularly in contexts where technological innovations expand anonymity and reduce oversight (Holt & Bossler, 2021).

By adopting RAT, this paper situates cryptocurrency-enabled cybercrime within a broader criminological perspective that emphasises situational opportunities rather than offender pathology. The dark web exemplifies a convergence space where these opportunity structures thrive, while the absence of robust global guardianship further facilitates criminal exploitation. Understanding this nexus through RAT thus clarifies how cryptocurrencies are not inherently criminogenic, but rather create new situational dynamics that motivated offenders can exploit. This theoretical lens, therefore, provides a systematic explanation of the conditions under which cryptocurrency becomes embedded in cybercrime and highlights the governance challenges that arise from weakened guardianship in digital environments.

Research Methodology

This study adopted a qualitative desk-based design that relied exclusively on secondary data to explore the intersection of cryptocurrency, cybercrime, and governance. The evidence base was drawn from three categories of materials. First, industry and forensic reports, particularly from Chainalysis and Elliptic, provided transaction statistics and typologies of illicit cryptocurrency use. Second, policy papers and institutional guidance issued by organisations such as the Financial Action Task Force (FATF), the International Monetary Fund (IMF), and regional regulatory bodies were reviewed to capture evolving governance responses. Third, peer-reviewed academic and technical studies published between 2020 and 2024 offered analytical insights into dark web markets, mixers, money laundering practices, and counter-forensic tools. Document selection was conducted through targeted searches of academic databases, institutional repositories, and organisational websites. To ensure quality and relevance, only sources published from 2020 onwards and directly addressing the dark web, cryptocurrency, or illicit finance were included. Thematic content analysis was employed to identify recurring patterns relating to criminal tactics, market adaptation, forensic innovations, and regulatory strategies.

To strengthen validity beyond secondary sources, the design incorporates primary qualitative evidence: 20–30 key informant interviews with regulators and law-enforcement (e.g., EFCC, FIU), VASP compliance officers and cyber-forensic practitioners, alongside 2–3 focus group discussions organised by stakeholder type. Where accessible, redacted confessional statements, charge sheets and court judgments on crypto-enabled offences are analysed. Semi-structured guides align with study objectives; transcripts undergo thematic analysis and process tracing, with a triangulation matrix linking primary testimony to secondary indicators. Ethical approval, informed consent, anonymisation and encrypted data handling are observed. This augmentation adds mechanism-level insight and addresses concerns about reliance on secondary data. Findings were triangulated across multiple sources to strengthen validity and mitigate bias, thereby producing a balanced synthesis of contemporary debates on cryptocurrency-enabled cybercrime.

Results

The analysis revealed four recurring patterns that define the evolving nexus between cryptocurrency and cybercrime on the dark web.

Criminal Tactics

Recent empirical data show that ransomware payments surged in 2023, exceeding US$1 billion**,** marking a return to high levels after a dip in 2022. Criminal actors have increasingly used what is known as *big game hunting*, targeting large organisations or critical infrastructure with high ransom demands. For example, the Cl0p group's exploitation of the MOVEit vulnerability accounted for large sums, including more than 44 percent of all ransomware value in certain months. Alongside such high-stakes attacks, there has also been a proliferation of smaller scale attacks and "spray and pray" campaigns which affect less protected targets. The variation in attack type implies a dual strategy: high value, high risk attacks intermingled with volume-based attacks

to diversify risk. Moreover, criminals are evolving their tactics: not just encrypting data but also exfiltrating and threatening to leak or sell it, thereby reducing reliance on decryption pressures alone.

Market Adaptation

The dark web criminal ecosystem shows signs of rapid adaptation in response to enforcement pressure. As law enforcement actions increase, ransomware payments dropped by about 35 percent in 2024 relative to 2023, indicating that more targets are refusing to pay and that enforcement and deterrence measures are having some effect. Nevertheless, this is countered by shifts among criminal actors: emerging new ransomware strains (sometimes as rebranded or leaked versions of older ones), faster negotiation time frames (often beginning just hours after initial data exfiltration), and increased use of illicit wallets or exchanges that are harder to trace. The adaptation thus manifests both in changes to who is targeted, as well as in how and when demands are made. Criminals are also using reputation systems and secure communication methods more effectively to retain customers in illicit markets, improving trust and lowering transactional friction.

Forensic Innovations

In response to the evolving tactics of cybercriminals, forensic tools have become more sophisticated. Blockchain analytics firms such as Chainalysis have improved capabilities to trace ransomware payments even through complex obfuscation techniques, clustering addresses, and identifying patterns in high-stakes groups like Cl0p, Black Basta, and ALPHV/BlackCat. Another innovation is the development of privacy-balancing tools. For example, *SeDe: Selective De-Anonymization* is a framework that attempts to enable privacy-preserving blockchain applications while allowing for the detection of illicit transactions through regulated de-anonymization (i.e. only under certain conditions, through collective entities) using cryptographic tools such as zero-knowledge proofs. These tools show promise in allowing the coexistence of user privacy and regulatory oversight. Yet forensic efforts face persistent challenges: criminals' use of privacy coins, mixers, chain hops, and decentralized exchanges, which by design resist standard oversight.

Regulatory Responses

Regulatory response appears to be ramping up, both in scope and in interjurisdictional coordination. For instance, law enforcement takedowns (like of ransomware gangs such as Hive) combined with statutes and guidance have strengthened the willingness of victims to refuse ransom payments, contributing to the decline in payments in 2024. Additionally, policy instruments such as the FATF travel rule, AML/KYC requirements for exchanges, and greater information sharing between states are increasingly emphasised in academic and policy literature. There is also more regulatory focus on identifying and shutting down high-risk exchanges or mixers and on wallets associated with criminal behaviour. The drop in crypto inflows to known illicit entities by about 65 percent in the first half of 2023, compared to 2022, is a sign that some of these regulatory and enforcement measures are making an impact. Nonetheless, weak or inconsistent regulatory

enforcement in many jurisdictions remains a critical gap. Criminals exploit regulatory arbitrage, shifting operations to places with lax oversight.

Discussion

The findings of this study reveal four central patterns that characterise the nexus between cryptocurrency, cybercrime, and governance: evolving criminal tactics, market adaptation, forensic innovations, and regulatory responses. Each demonstrates the dynamic interplay between illicit actors and countermeasures. The professionalisation of cybercriminal enterprises is evident in the diversification of ransomware and illicit services. High-value ransomware campaigns such as the Cl0p group's MOVEit exploitation illustrate the trend of "big game hunting," while double extortion techniques, data theft combined with encryption, have become standard practice (Chainalysis, 2024). Europol (2023) further documents the increasing division of labour within dark web markets, where coders, service providers, and launderers collaborate across borders to maximise efficiency and reduce risks. These findings indicate that cryptocurrencies not only enable but also scale the sophistication of criminal ecosystems.

Illicit markets have shown strong resilience to enforcement shocks. Although the total value of stolen cryptocurrency fell by over 50% in 2023, the number of incidents rose, underscoring shifts in attacker strategies rather than reductions in intent (Chainalysis, 2024). At the same time, laundering activity has migrated to cross-chain bridges and decentralised exchanges, with Elliptic (2025) estimating that billions of dollars are now routed through such infrastructures. Elliptic (2022) adds that mixers and DEXs increasingly serve as preferred laundering channels, enabling offenders to evade scrutiny and exploit gaps in regulatory coverage. These adaptive behaviours highlight a displacement effect: pressure in one area pushes illicit activity into new domains. Blockchain analytics have advanced considerably, with firms such as Chainalysis developing address clustering and attribution techniques that have successfully traced major ransomware groups like ALPHV and Black Basta (Chainalysis, 2024). Academic research supports this trend, noting rapid growth in forensic tools capable of tracking multi-hop and multi-chain transactions (Atlam et al., 2024). Nevertheless, privacy-enhancing technologies continue to limit forensic reach. Zero-knowledge proofs, privacy coins, and advanced mixing protocols can obscure flows, complicating investigations. Chaudhary and Ivey-Law's (2023) proposal of selective de-anonymisation illustrates a potential compromise between user privacy and regulatory oversight, though it raises unresolved governance and ethical concerns.

The international regulatory environment has strengthened, particularly following the Financial Action Task Force's (2021) updated guidance for virtual assets and service providers, which extended anti-money laundering and counter-terrorist financing measures such as the travel rule. National authorities have complemented these frameworks with targeted enforcement actions, including the United States Department of Justice's takedown of Hydra, the world's largest darknet market, in 2022 (United States Department of Justice, 2022). These measures contributed to a reported 65% decline in illicit inflows to known criminal entities in the first half of 2023 (Chainalysis, 2023). However, regulatory fragmentation persists across jurisdictions, creating opportunities for criminals to exploit weak oversight. As Elliptic (2025) notes,

decentralised infrastructures pose particular challenges for enforcement due to their borderless, non-custodial nature. Taken together, these findings support the view that cryptocurrency-enabled cybercrime is not static but adaptive, with offenders exploiting technical and regulatory gaps even as enforcement and forensic capacities advance. Effective governance will require not only the refinement of tracing and compliance tools but also the closure of jurisdictional loopholes and enhanced cooperation between public and private actors.

Conclusion

This study demonstrates that cryptocurrency embodies a paradox of innovation and risk. While it holds the potential to transform global finance by promoting inclusion, efficiency, and decentralization, it simultaneously creates unprecedented avenues for cybercrime, money laundering, and other illicit activities. The analysis revealed how darknet markets, mixers, and cross-chain technologies have become increasingly central to criminal exploitation of digital assets. These evolving tactics highlight the persistent adaptability of illicit actors in response to regulatory and technological interventions. The study also underscores that current regulatory frameworks, although advancing, remain insufficient to fully address the borderless and anonymous nature of cryptocurrency-related crime. Regulatory gaps, limited enforcement capacity, and inconsistent international coordination weaken efforts to disrupt illicit financial flows. At the same time, excessively stringent regulations risk stifling the innovation and financial opportunities that cryptocurrencies provide, particularly for marginalized populations and emerging economies. A recurring theme across the findings is the need for balance. Effective governance must not rely solely on punitive approaches but should integrate technological innovation, multi-stakeholder collaboration, and harmonized global standards. This balance is necessary to simultaneously encourage legitimate uses of digital currencies and mitigate the risks posed by their exploitation.

In conclusion, cryptocurrency should no longer be regarded simply as a financial technology but as a critical element of global governance. Ensuring its benefits while limiting its dangers requires coordinated action, shared responsibility, and forward-looking policies. Without such measures, the expansion of the dark web of cryptocurrency will continue to undermine financial integrity, security, and trust in the global digital economy.

Recommendations

1. Countries should accelerate full and effective implementation of FATF guidance for virtual assets and VASPs to reduce regulatory arbitrage and enhance traceability. Technical assistance should be scaled to lower-capacity jurisdictions.
2. Formalised cooperation between law enforcement, forensic firms and exchanges should be expanded, with clear protocols for data sharing that preserve due process and privacy safeguards.
3. Policy and enforcement focus should target the limited set of withdrawal routes and exchanges that receive large volumes of illicit funds. Licensing, compliance monitoring and sanctions risk management at these chokepoints can reduce laundering success.

4. Continued investment in chain analysis tools and in training for cross-border investigations will improve asset recovery and attribution. Support should be prioritised for jurisdictions that lack resources.
5. Regulatory design must seek proportionate, risk-based approaches that protect consumers and financial integrity without unnecessarily hindering beneficial crypto use cases. Sandbox approaches and regulatory cooperation can help reconcile these objectives.

References

Atlam, H. F., Wills, G., Alenezi, A., Alharthi, A., & Alassafi, M. (2024). Blockchain forensics: Systematic review of methods, tools and future directions. *Electronics, 13*(17), 3568.

Bahamazava, K., & Nanda, R. (2024). Cybercrimes in the cryptocurrency domain: Identifying types, understanding motives and techniques, and exploring future directions for technology and regulation. *Journal of Governance and Policy Studies, 14*(2), 1–18.

Bains, P., Ismail, A., Melo, F., & Sugimoto, N. (2022). *Regulating the crypto ecosystem: The case of unbacked crypto assets* (FinTech Notes No. 2022/007). International Monetary Fund. https://doi.org/10.5089/9798400221361.063

Chainalysis. (2023, July). *Crypto crime mid-year update 2023*. Chainalysis. https://www.chainalysis.com/reports/crypto-crime-2023-midyear/

Chainalysis. (2024, February 7). *Ransomware payments exceed $1 billion in 2023, hitting record high after 2022 decline*. Chainalysis. https://www.chainalysis.com/blog/ransomware-2024/

Chainalysis. (2024, January 24). *Funds stolen from crypto platforms fall more than 50% in 2023, but hacking remains a significant threat*. Chainalysis. https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2024/

Chang, E., Darcy, P., Choo, K.-K. R., & Le-Khac, N.-A. (2022). Forensic artefact discovery and attribution from Android cryptocurrency wallet applications. *arXiv*. https://arxiv.org/abs/2205.14611

Chaudhary, A., & Ivey-Law, H. (2023). SeDe: Balancing blockchain privacy and regulatory compliance by selective de-anonymization. *arXiv*. https://doi.org/10.48550/arXiv.2311.08167

Chinalysis. (2023). *The 2023 crypto crime report*. Chainalysis. https://go.chainalysis.com/2023-crypto-crime-report.html

Elliptic. (2022, May 10). *DEXs, mixers and the changing shape of crypto money laundering*. Elliptic. https://www.elliptic.co/blog/dex-mixers-money-laundering-2022

Elliptic. (2025, February 12). *Cross-chain money laundering reaches multi-billion scale: Implications for compliance and enforcement*. Elliptic. https://www.elliptic.co/resources/cross-chain-money-laundering-2025

European Monitoring Centre for Drugs and Drug Addiction, & Europol. (2023). *Cryptocurrencies and drugs: Analysis of cryptocurrency use on darknet markets in the EU and neighbouring countries*. EMCDDA. https://www.emcdda.europa.eu/publications/joint-publications/cryptocurrencies-and-drugs-analysis_en

Europol. (2022). *Europol spotlight—Cryptocurrencies: Tracing the evolution of criminal finances*. Europol. https://www.europol.europa.eu/publications-events/publications/europol-spotlight-cryptocurrencies-tracing-evolution-of-criminal-finances

Europol. (2023). *Internet organised crime threat assessment (IOCTA) 2023*. Europol. https://www.europol.europa.eu/publications-events/publications/internet-organised-crime-threat-assessment-iocta-2023

Financial Action Task Force. (2021). *FATF guidance for a risk-based approach to virtual assets and virtual asset service providers*. FATF/OECD. https://www.fatf-gafi.org/en/publications/Virtual-Assets/fatf-guidance-rba-virtual-assets-vasps.html

Gonzálvez-Gallego, N., & Pérez-Cárceles, M. C. (2021). Cryptocurrencies and illicit practices: The role of governance. *Economic Analysis and Policy, 72*, 203–212.

Holt, T. J., & Bossler, A. M. (2021). *The Routledge handbook of cybercrime and cyberdeviance*. Routledge. https://doi.org/10.4324/9781315179799

Irwin, A. S. M., & Turner, A. (2023). Cryptocurrencies, crime, and regulation: Understanding the dark side of digital finance. *Journal of Financial Crime, 30*(1), 60–75.

Irwin, A. S. M., & Turner, I. (2023). Cryptocurrency regulation and financial crime: Evaluating global approaches. *Journal of Financial Crime, 30*(2), 437–452.

Korpas, L. M., Frey, S., & Tan, J. (2023). Political, economic, and governance attitudes of blockchain users. *arXiv*. https://doi.org/10.48550/arXiv.2301.02734

Leiser, M. R. (2022). 'Dark patterns': The case for regulatory pluralism between the European Union's consumer and data protection regimes. In E. Kosta, R. Leenes, & I. Kamara (Eds.), *Research handbook on EU data protection law* (pp. 240–269).

Ma, W., Zhu, C., Liu, Y., Xie, X., & Li, Y. (2023). A comprehensive study of governance issues in decentralised finance applications. *arXiv*. https://doi.org/10.48550/arXiv.2311.01433

Möser, M., Böhme, R., & Breuker, D. (2021). An inquiry into money laundering tools in the Bitcoin ecosystem. *Future Internet, 13*(9), 230.

Motsi-Omoijiade, I. D. (2022). *Cryptocurrency regulation: A reflexive law approach*. Routledge. https://doi.org/10.4324/9781003184181

Okorie, D. I., & Lin, B. (2021). Cryptocurrencies in developing countries: Opportunities and regulatory challenges. *Research in International Business and Finance, 58*, 101451.

Ozili, P. K. (2025). Cryptocurrency regulation in Africa: Advantages, motivation, regulatory models, challenges, consequences, and principles vs. rules-based regulation. *International Journal of Blockchains and Cryptocurrencies, 10*(2), 294–313.

Rau, R., Wardrop, R., & Zingales, L. (Eds.). (2021). *The Palgrave handbook of technological finance*. Palgrave Macmillan. https://doi.org/10.1007/978-3-030-65117-6

Scott, S. V., Zachariadis, M., & Barrett, M. (2023). Governing blockchain and cryptocurrencies: The need for multi-stakeholder global governance. *Journal of Information Technology, 38*(1), 3–18.

TRM Labs. (2022). *The illicit crypto ecosystem report*. TRM Labs. https://www.trmlabs.com/resources/reports/the-illicit-crypto-ecosystem-report-2022

United Nations Office on Drugs and Crime. (2023). *Use of the dark web and social media for drug supply*. In *World Drug Report 2023: Booklet 2 – Contemporary issues on drugs* (pp. 123–134). United Nations.

United States Department of Justice. (2022, April 5). *Justice Department investigation leads to shutdown of Hydra, the largest darknet marketplace*. U.S. Department of Justice. https://www.justice.gov/opa/pr/justice-department-investigation-leads-shutdown-largest-online-darknet-marketplace

World Economic Forum. (2023). *Pathways to the regulation of crypto-assets: A global approach*. World Economic Forum. https://www3.weforum.org/docs/WEF_Pathways_to_the_Regulation_of_Crypto_Assets_2023.pdf

Xia, P., Yu, Z., Wang, K., Ma, K., Chen, S., Luo, X., Zhou, Y., & Wu, L. (2024). The devil behind the mirror: Tracking the campaigns of cryptocurrency abuses on the dark web. *arXiv*. https://arxiv.org/abs/2401.04662

Yar, M., & Steinmetz, K. F. (2019). *Cybercrime and society* (3rd ed.). SAGE Publications. https://uk.sagepub.com/en-gb/eur/cybercrime-and-society/book261040