Cryptocurrency, Terrorism Financing, and the Dark Web: An Exploratory Study of the Role of Anonymous Transactions in Supporting Terrorist Activities

African Journal of Stability & Development
Vol 17 No. 2, Nov. 2025
pp. 971-988

AbdulMalik Olalekan Oladipupo[1]

Abstract

The expansion of cryptocurrency has reshaped financial systems by enabling decentralised transactions and new digital applications. However, its pseudonymity and global reach have also enabled ransomware, darknet trading, money laundering, and terrorism financing, creating challenges for regulators seeking to protect financial integrity. This study examines the intersection of cryptocurrency, cybercrime, and governance. It identifies techniques exploited by criminals, evaluates forensic and regulatory countermeasures, and considers the governance dilemmas posed by these developments. A qualitative, desk-based approach was adopted, drawing on peer-reviewed literature, institutional policy reports (FATF, IMF, Europol), and industry analyses (Chainalysis, Elliptic, TRM Labs). Thematic content analysis

1. Department of Politics and International Relations, Lead City University, Ibadan, Nigeria; oladipupo.abdulmalik@lcu.edu.ng; https://orcid.org/0000-0001-5441-7062.

was used to trace patterns of illicit cryptocurrency use, enforcement actions, and regulatory innovations. The findings reveal that blockchain forensics and coordinated policy efforts have strengthened oversight. Yet criminals increasingly use privacy coins, decentralised finance protocols, mixers, and cross-chain laundering to bypass detection. Enforcement remains inconsistent, hindered by fragmented regulation and gaps in cross-border cooperation. Cryptocurrency-enabled crime and terrorism financing remain adaptive threats that test financial stability and governance frameworks. Stronger international coordination, harmonised regulation, and advanced forensic tools are essential to reduce risks. The study recommends deepening cross-border collaboration, investing in blockchain analytics, and adopting flexible governance models that balance innovation with accountability.

Keywords: Cryptocurrency Regulation, Terrorism Financing, Blockchain Forensics, Dark Web Transactions, Global Financial Governance

Introduction

The relationship between cryptocurrency, terrorism financing, and the dark web has emerged as one of the most contentious debates in contemporary security and financial governance scholarship. At the centre of this debate lies a paradox: while cryptocurrencies were designed to decentralise finance and expand access through transparent, immutable ledgers, they simultaneously provide tools for pseudonymity that non-state actors, including terrorist organisations can exploit. The puzzle, therefore, lies in how technologies premised on transparency have become embedded in clandestine economies that rely on secrecy and concealment. This study seeks to interrogate this paradox by focusing specifically on anonymous transactions facilitated through the dark web, which are increasingly implicated in fundraising, resource mobilisation, and logistical support for terrorist activities.

Scholarly and policy discourses present competing arguments regarding the scale and significance of this phenomenon. On one side of the debate, security practitioners and some academics argue that cryptocurrencies constitute a major emerging threat, offering terrorists new pathways to solicit funds, evade detection, and launder proceeds (Elliptic, 2023; Europol, 2021). They highlight the convergence of digital anonymity, encrypted communication channels, and decentralised exchanges as a "perfect storm" that challenges conventional counter-terrorism financing (CTF) measures. On the other side, sceptics argue that the narrative of crypto-enabled terrorism is overstated. They stress that empirical evidence consistently shows the vast majority of terrorist financing still relies on traditional channels such as cash, hawala, and regulated banking systems (U.S. Department of the Treasury, 2024). For these scholars and policymakers, cryptocurrencies play only a peripheral role, more symbolic than operational, with blockchain transparency offering more opportunities for law enforcement than risks (Chainalysis, 2024).

This debate is not merely academic but has profound policy implications. If cryptocurrencies represent only a marginal risk, regulatory overreach could stifle legitimate innovation and compromise privacy rights. If, however, they are rapidly becoming central to terrorist financing networks, delayed or inadequate intervention may undermine global security frameworks. Thus, the controversy centres not only on whether cryptocurrencies are used by terrorists but also on how frequently, at what scale, and with what implications for governance. Leading authorities frame this debate in distinct ways. The Financial Action Task Force (FATF, 2021) positions virtual assets as a high-priority risk area and advocates a risk-based regulatory approach, including the "travel rule" for virtual asset service providers. Meanwhile, Europol's Internet Organised Crime Threat Assessment underscores the dark web's role as a facilitator of illicit services, with cryptocurrency as its preferred medium of exchange. By contrast, empirical reports from blockchain-analytics firms such as Chainalysis and TRM Labs provide more nuanced views, noting that while the absolute volume of terrorist financing via crypto is small, the sophistication of tactics and obfuscation methods is increasing. This divergence between institutional risk framing and data-driven industry analysis illustrates the complexity of the issue and justifies deeper scholarly examination.

The present study contributes to this debate by providing a systematic exploration of anonymous transactions on the dark web and their role in supporting terrorist activities. Unlike earlier analyses that either generalise about "crypto and terrorism" or focus narrowly on individual case studies, this study triangulates across official risk assessments, industry reports, and emerging academic literature published since 2020. This temporal focus ensures that the analysis captures the most recent trends, such as the shift from Bitcoin to stablecoins and privacy coins, the use of decentralised finance protocols, and the targeting of mixers and anonymisation services by regulators.

The contribution of this paper are threefold. First, it isolates the mechanisms by which anonymous transactions, particularly through privacy-enhancing coins and mixers accessible via the dark web, are integrated into terrorism financing scripts. This includes their use in online solicitation, micro-donation campaigns, propaganda dissemination, and procurement. Second, it challenges the binary framing of "major risk versus marginal risk" by demonstrating that the significance of cryptocurrency in terrorism financing is not reducible to volume alone but must be assessed in terms of strategic utility, resilience, and symbolic resonance. Third, it provides new evidence of how regulatory and enforcement actions, such as the sanctioning of Tornado Cash or the seizure of wallets linked to Hamas fundraising campaigns, have reshaped the behaviour of actors, pushing them toward more complex obfuscation strategies. By foregrounding these dynamics, the study advances a more nuanced understanding that is both empirically grounded and policy relevant.

At the heart of this analysis lies an overarching intellectual question: *to what extent do anonymous transactions facilitated by cryptocurrencies and the dark web constitute a transformative risk in terrorism financing, and how should regulators and security actors respond without undermining financial innovation and privacy rights?* This question guides the inquiry across the literature review, theoretical framing, and empirical synthesis.

To address this, the paper adopts a qualitative, exploratory methodology that relies on document analysis of FATF and Treasury guidance, triangulated with empirical data from blockchain-analytics firms and peer-reviewed

studies on the dark web. This approach enables the capture of both policy discourse and operational realities, while recognising the limitations of attribution and data availability in an illicit domain. The importance of this study extends beyond the terrorism-crypto nexus to broader debates on global governance, digital sovereignty, and technological risk. As states grapple with the dual promise and peril of digital financial technologies, the way in which cryptocurrency is framed in security debates influences not only counter-terrorism strategies but also the legitimacy of regulatory regimes and the trajectory of financial innovation.

Literature Review

The Evolving Scale and Salience of Crypto-Enabled Terrorist Financing

Since 2020, the role of cryptocurrencies in terrorist financing has shifted from marginal curiosity to a subject of heightened concern among regulators, academics and financial-intelligence units. While empirical analyses consistently emphasise that cryptocurrencies represent only a small share of known terrorist financing compared to fraud, ransomware and large-scale hacks, their symbolic and tactical importance has expanded within extremist ecosystems (Elliptic, 2023; TRM Labs, 2025). This apparent paradox arises because, although traditional channels such as cash, hawala and regulated financial institutions remain dominant, digital assets provide unique advantages in terms of reach, speed and partial anonymity, making them attractive in specific operational contexts. Industry telemetry shows that extremist fundraising has moved beyond rudimentary appeals for Bitcoin donations, which were common in the mid-2010s, towards a more diversified use of crypto tools. Elliptic (2023) documents campaigns involving micro-donations, solicited through Telegram and Twitter, sometimes amount to a few dollars per contributor, yet collectively support propaganda dissemination or logistics. Similarly, TRM Labs (2025) identifies instances where stablecoins such as Tether were deployed to bypass banking restrictions, illustrating a shift from simple donation drives toward a modular approach that includes cross-border settlement with illicit brokers, targeted procurement of digital services, and value storage during periods of heightened regulatory scrutiny.

A notable feature of this evolution is the interplay between accessibility and exposure. Cryptocurrencies allow extremists to solicit contributions from sympathisers across jurisdictions with minimal entry barriers. Donation links, QR codes and wallet addresses can be distributed widely on messaging applications and dark-web forums, enabling transnational participation. However, the same open ledger that facilitates pseudonymous transactions also creates opportunities for tracing. Law-enforcement agencies, working with blockchain-analytics companies, have repeatedly disrupted such schemes. The U.S. Department of Justice (2025), for instance, reported successful seizures of digital wallets linked to Hamas fundraising campaigns, demonstrating that blockchain transparency, when combined with subpoenas, sanctions and platform enforcement, can generate significant investigative leverage.

Yet the literature underscores that extremist actors are learning from these disruptions. TRM Labs (2025) observes an increased use of obfuscation tools, such as coin mixers, cross-chain swaps and privacy coins, to complicate tracing efforts. This adaptive behaviour raises enforcement costs, as analysts must disentangle layers of transactions across different blockchains and protocols. The adoption of these techniques indicates that while crypto may not yet rival traditional financing channels in scale, its salience is rising because it compels states and compliance institutions to allocate resources, develop new analytical tools and update regulations continuously. Elliptic (2023) also notes that terrorist-linked actors exploit the reputational perception of cryptocurrencies as anonymous, even though most blockchains are publicly auditable. This perception enhances the appeal of crypto fundraising among sympathisers, amplifying propaganda and recruitment effects. In this sense, cryptocurrencies serve not only as financial conduits but also as symbolic markers of technological modernity, defiance against state controls, and solidarity with decentralised ideals. These intangible dimensions elevate the salience of crypto financing beyond its absolute monetary contribution.

Tension Between Pseudonymity and Traceability

A defining feature of cryptocurrencies is the paradoxical interplay between pseudonymity and traceability. On one hand, blockchain transactions are

publicly recorded and permanently accessible, allowing investigators to trace flows of value across addresses and build behavioural profiles using clustering techniques. On the other hand, offenders can exploit the pseudonymous design of wallet addresses and employ obfuscation strategies that raise the cost of detection and attribution. This tension has been at the centre of contemporary debates on cryptocurrency's role in terrorism financing. Recent evidence shows that terrorist-linked actors are increasingly deploying an "obfuscation stack" that combines privacy coins such as Monero, decentralised mixers, peel chains, nested services, and cross-chain bridges to conceal transactional trails. The growing use of stablecoin rails adds another dimension, as these assets provide liquidity and fiat parity, making them particularly attractive for micro-donations and settlement purposes (TRM Labs, 2025). These techniques fragment investigative pathways, complicating compliance checks and slowing law enforcement responses.

The Financial Action Task Force (FATF) has repeatedly highlighted this challenge in its 2024 and 2025 targeted updates. It noted that although there has been progress in disrupting illicit networks, patchy implementation of the travel rule, inconsistent sanctions screening, and cross-border supervisory gaps create opportunities for exploitation (FATF, 2024, 2025). These weaknesses are magnified in jurisdictions with limited technical capacity or fragmented regulatory frameworks. At the same time, traceability has enabled significant enforcement wins. For example, blockchain analytics has facilitated seizures of crypto wallets linked to extremist groups, demonstrating that while offenders can obscure flows, they cannot easily erase them (U.S. Department of Justice, 2025). This duality underscores that pseudonymity is not absolute, but contingent on adversaries' ability to exploit systemic gaps faster than regulators and investigators can adapt. In practice, this creates a dynamic cat-and-mouse contest, where the balance oscillates between concealment and exposure, shaping the trajectory of terrorism financing in the digital era.

The Dark Web as an Enabling Environment

The dark web has emerged as a critical enabler for cryptocurrency-based illicit finance, including terrorism-related activities. Evidence of a measurable complementarity between dark-web usage and the adoption of privacy-

focused cryptocurrencies was revealed by Scharnowski (2024), using multi-source traffic and trading data. He demonstrated that increases in Tor-mediated dark-web traffic correlate positively with secondary-market trading volumes of privacy coins such as Monero. This relationship suggests that as individuals seek anonymity in communication and browsing, they also demand greater financial obfuscation. Although Scharnowski does not argue that privacy-coin prices are wholly driven by dark-web usage, the econometric correlation points to an underlying behavioural pattern that links digital concealment and financial anonymity.

This academic finding dovetails with law-enforcement and forensic assessments as the Egmont Group (2023) describes dark-web fora and marketplaces as hubs where illicit services are exchanged, including hacking tools, forged documents, and value-transfer mechanisms that rely heavily on crypto-assets. Such platforms facilitate not only criminal enterprises but also terrorist actors who exploit the dark web to disseminate propaganda, recruit supporters, and solicit donations in digital currencies. By routing transactions through privacy coins or mixers, these actors attempt to shield identities and transaction flows from scrutiny. Together, these findings highlight the dark web's dual role as both a communication infrastructure and a financial ecosystem that complements crypto-enabled terrorist financing. Monitoring dark-web traffic patterns may therefore serve as an early-warning mechanism for shifts in terrorist financing practices, offering regulators and investigators a way to anticipate new tactics and pre-empt exploitation of anonymous payment systems (Scharnowski, 2024; Egmont Group, 2023).

Standards, Supervision and Uneven Implementation

From a governance standpoint, the Financial Action Task Force (FATF) has established itself as the cornerstone of anti-money-laundering (AML) and counter-terrorist-financing (CTF) regulation for virtual assets. Its *Recommendation 15* and the accompanying *Interpretive Note* explicitly extend customer due diligence, sanctions screening, and the so-called "travel rule" to virtual asset service providers (VASPs), requiring them to collect and transmit originator and beneficiary information across borders (FATF, 2024, 2025). These measures are intended to reduce the opacity of

cryptocurrency transactions and close regulatory gaps that enable terrorist financiers to exploit anonymity tools.

Despite this strong normative framework, implementation remains highly uneven. FATF's 2025 targeted update revealed that only a minority of jurisdictions assessed had achieved "largely compliant" ratings. This shortfall generates fertile ground for regulatory arbitrage, whereby illicit actors migrate their activities to permissive or weakly supervised jurisdictions (FATF, 2025). As Reuters (2025) noted, the global nature of virtual asset flows means that a single vulnerable hub can undermine collective controls. This has several consequences: activity is displaced toward unregulated peer-to-peer exchanges and informal brokers, compliant VASPs bear a disproportionate burden of screening high-risk inbound flows, and law enforcement faces jurisdictional frictions that complicate cross-border investigations.

Scholarly work reinforces these concerns. Rauchs and Saleh (2021) argue that fragmented oversight and inconsistent supervisory practices not only limit the effectiveness of FATF standards but also risk creating "compliance islands," where only certain jurisdictions carry the costs of robust enforcement. Thus, uneven implementation not only weakens the deterrent effect of global standards but also imposes structural inefficiencies on legitimate market actors. Addressing these gaps requires harmonised supervisory cooperation, enhanced capacity building in developing jurisdictions, and investment in cross-border investigative mechanisms.

Modality Choices: Privacy Coins, Mixers and Stablecoins

Several studies highlight how terrorist financiers are experimenting with different crypto modalities to navigate the tension between pseudonymity and traceability. Although Bitcoin remains widely recognised, its public ledger has repeatedly enabled law enforcement and blockchain-analytics firms to identify, disrupt, and seize funds linked to extremist networks (Elliptic, 2023; TRM Labs, 2025). This investigative visibility has pushed actors toward privacy coins, mixing services, and stablecoins, each offering distinct affordances that can reduce detectability while still enabling value transfer.

Privacy coins, such as Monero and Zcash, are designed to obscure transaction flows using cryptographic techniques like ring signatures and

stealth addresses. Reports and open-source analyses link some Islamic State affiliates and ISKP cells to the use of Monero in fundraising campaigns, particularly for the collection and early layering stages of financing (Wilson Center, 2024). Privacy-enhanced assets symbolically reinforce extremist narratives of resisting surveillance while providing a higher degree of transactional anonymity (Bahamazava & Nanda, 2024). However, empirical work shows their practical use is constrained by limited liquidity and reduced exchange support, following regulatory pressure and delistings (Scharnowski, 2024). This makes privacy coins effective for tactical concealment but less useful for sustained financing operations.

Mixers and tumblers form another critical element of the obfuscation stack. These services combine and redistribute coins from multiple sources, thereby breaking links between wallets and recipients. The Financial Action Task Force (2024) has emphasised the role of mixers and cross-chain swaps in laundering funds linked to illicit activity, including terrorism. Enforcement actions, such as U.S. prosecutions of Tornado Cash developers and asset seizures tied to Hamas' fundraising, demonstrate both the centrality of these tools and the authorities' ability to disrupt them (U.S. Department of Justice, 2025; Reuters, 2024). Yet decentralised and open-source designs complicate regulation, prompting debates about whether sanctions against software itself encroach upon civil liberties (Atlam et al., 2024). Despite these challenges, mixers remain popular because they are relatively simple to access and can be combined with privacy coins or cross-chain protocols to deepen obfuscation.

Stablecoins have become increasingly significant in illicit finance because of their liquidity, global reach, and price stability. Assets like Tether (USDT) and USD Coin (USDC) are dollar-pegged, making them attractive for small-ticket donations, settlement with illicit brokers, and value storage during periods of market volatility. TRM Labs (2025) notes that stablecoins are disproportionately represented in illicit transactions relative to their share of legitimate market activity. Wired (2024) similarly reports that stablecoins facilitated billions of dollars in illicit flows since 2022, including terrorism-linked transactions. Their broad circulation in peer-to-peer markets also enhances usability, particularly where banking restrictions make fiat difficult to access. Studies emphasise that extremist groups are drawn to stablecoins

not only for their transactional efficiency but also because they integrate seamlessly into informal economies and encrypted communication channels used for propaganda and fundraising (Elliptic, 2023).

Scholarship on regulatory responses illustrates how policy choices shape the visibility of these modalities. Restrictive measures, such as cutting off cryptocurrency exchanges from banking systems, were intended to reduce exposure to money laundering and terrorism financing. However, subsequent analyses found that these prohibitions often displaced activity into less visible peer-to-peer markets, where stablecoins circulate outside traditional oversight (Oladipupo, 2022; Irmiya, 2023). In a comparative study, Oladipupo (2025) demonstrates how terrorist financiers in Nigeria and Kenya continue to rely predominantly on cash, regulated financial institutions, and hawala, but also increasingly use cryptocurrencies as tactical adjuncts for solicitation and layering. His findings reinforce calls for calibrated implementation of FATF standards, greater investment in blockchain-analytics capacity, and structured typology sharing to strengthen supervisory effectiveness. These recommendations echo intergovernmental and industry guidance and emphasise proportionate, risk-based oversight rather than blunt prohibitions that inadvertently reduce transparency (FATF, 2024, 2025; TRM Labs, 2025).

Theoretical Underpinning

This study adopts Routine Activity Theory (RAT) as the theoretical underpinning to explain how terrorist financiers leverage cryptocurrency modalities to achieve their objectives with minimal exposure. Developed originally by Cohen and Felson in 1979, RAT argues that crime occurs when three elements converge: a motivated offender, a suitable target, and the absence of a capable guardian. Applied to the financing of terrorism through cryptocurrency, the theory helps to illuminate the mechanisms by which offenders exploit technological and regulatory environments to move funds discreetly. Within this framework, the motivated offenders are extremist groups or their supporters seeking to transfer value across borders for recruitment, propaganda, or procurement. The suitable targets include digital asset ecosystems that enable transactions with high liquidity and global reach, particularly exchanges, peer-to-peer platforms, and stablecoin networks.

The absence of capable guardianship manifests in regulatory gaps, weak enforcement in some jurisdictions, and inconsistent information-sharing across borders (U.S. Department of the Treasury, 2024). These conditions create opportunities for offenders to adopt privacy coins, mixing services, and stablecoins to obfuscate transactions and evade oversight. RAT also explains how interventions alter offender behaviour. For instance, when capable guardianship is reinforced through sanctions on mixers or the introduction of stricter compliance obligations, offenders are displaced towards alternative modalities or smaller peer-to-peer markets. Thus, the theory not only accounts for the current reliance on obfuscation tools but also predicts adaptive responses to regulatory actions. This makes RAT particularly suited to analysing the evolving nexus of cryptocurrency, anonymity, and terrorism financing.

Research Methodology

This study adopts a qualitative, exploratory research design aimed at understanding how cryptocurrencies and anonymous transactions intersect with terrorism financing. The approach is particularly suited to emerging security challenges in which empirical data are fragmented and evolving. The research draws primarily on document analysis, reviewing authoritative policy guidance and risk assessments produced by the Financial Action Task Force, the United States Department of the Treasury, and Europol. These documents provide a foundational understanding of regulatory expectations, typologies, and evolving vulnerabilities within the virtual asset ecosystem.

To enrich this foundation, the study integrates a triangulation strategy that combines industry and empirical insights. Reports by Chainalysis, TRM Labs, and Elliptic are examined to identify current typologies, on-chain indicators, and case studies that illustrate practical manifestations of terrorist use of cryptocurrencies. This is complemented by a synthesis of peer-reviewed scholarship focusing on the dark web, privacy coins, mixers, and crypto-enabled illicit finance. Such academic work provides deeper theoretical and analytical perspectives on mechanisms of obfuscation and the limitations of enforcement responses. The inclusion criteria restricted sources to publications from 2020 onward, with emphasis on relevance to

terrorism financing and verifiability. The unit of analysis is the financing practice itself rather than individual groups, allowing for a broader mapping of modalities and adaptive behaviours.

Results

The results of this exploratory study reveal four significant themes in the relationship between cryptocurrency modalities and terrorism financing. These findings highlight the complexity of pseudonymous transactions, the adaptive behaviour of offenders, and the tension between technological innovation and regulatory enforcement.

First, terrorism financing through cryptocurrency remains small in scale but increasingly salient. Analyses of blockchain data, industry reports, and enforcement records indicate that extremist-linked flows represent only a fraction of illicit crypto activity compared to ransomware, fraud, and market manipulation (Elliptic, 2023; TRM Labs, 2025). However, the strategic importance of such flows lies not in their size but in their potential to bypass conventional financial controls and facilitate transnational networks. Campaigns linked to groups such as Hamas and Islamic State affiliates demonstrate repeated attempts to exploit digital assets for micro-donations, propaganda support, and procurement. These findings support the U.S. Department of the Treasury's (2024) conclusion that while cash and hawala remain dominant, cryptocurrencies now function as tactical complements.

Second, offenders rely on an "obfuscation stack" to disguise flows. Evidence points to the use of privacy coins, mixers, cross-chain bridges, and peer-to-peer exchanges to disrupt traceability (FATF, 2024). Mixers and tumblers remain central because they pool and redistribute funds, thereby obscuring provenance. Enforcement actions such as sanctions against Tornado Cash illustrate both the importance of these tools and the state's capacity to disrupt them. Nonetheless, decentralised and open-source mixers demonstrate resilience, underscoring the difficulty of applying traditional enforcement mechanisms to borderless digital infrastructures. The persistence of such services affirms the adaptability of terrorist financiers when confronted with regulatory and investigative pressure.

Third, stablecoins have emerged as disproportionately represented in illicit flows. Their dollar-pegged stability, high liquidity, and broad circulation

across exchanges and peer-to-peer markets make them attractive for both micro-transactions and larger settlements (Wired, 2024). TRM Labs (2025) highlights their increasing presence in terrorism-related fundraising, noting that extremist groups exploit stablecoins for cross-border payments where fiat is inaccessible or heavily scrutinised. This suggests that stablecoins, once seen primarily as instruments of efficiency in digital finance, now present unique challenges for counter-terrorism financing regimes. Their adoption demonstrates how offenders leverage market trends and liquidity preferences to balance anonymity with usability.

Fourth, regulatory posture strongly shapes risk visibility. Restrictions such as banking prohibitions on cryptocurrency exchanges, as seen in Nigeria, sought to mitigate exposure to illicit flows but inadvertently displaced activity to peer-to-peer networks. Scholarship shows that these markets offer thinner compliance and weaker observability, creating blind spots for regulators (Oladipupo, 2022; Irmiya, 2023). Oladipupo (2025) further argues that terrorist financiers exploit these weakly governed channels to solicit and layer funds, highlighting the limits of prohibition-based policies. These findings echo FATF (2025) recommendations for proportionate, risk-based supervision that preserves transparency while reducing opportunities for arbitrage.

Taken together, these results demonstrate that cryptocurrency is not replacing traditional terrorist financing methods but is increasingly integrated into a diversified toolkit. Privacy coins and mixers facilitate tactical obfuscation, while stablecoins provide operational convenience. Regulatory interventions such as sanctions and seizures have disrupted specific campaigns, yet offenders adapt quickly by shifting modalities or jurisdictions. The discussion underscores the need for balanced policies: enforcement must be targeted and technologically informed, while regulatory frameworks should emphasise analytics, cross-border cooperation, and public-private partnerships. Overly restrictive measures risk driving activity underground, thereby weakening visibility and hampering effective counter-terrorism financing efforts.

Conclusion

This study shows that cryptocurrency has not supplanted traditional terrorism financing, yet it has become a tactical complement that can lower frictions

in online solicitation, layering and cross-border settlement. Privacy coins, mixers, and cross-chain tools help offenders raise investigative costs, while stablecoins provide liquidity and price stability that support small donations and rapid settlements. The dark web amplifies these effects by providing discovery, tooling and trusted channels for propaganda and coordination. Seen through Routine Activity Theory, the convergence of motivated offenders, suitable crypto targets and weak guardianship explains the observed patterns, and also why enforcement and supervision can shift behaviour rather than eliminate it.

Operational outcomes are achievable. Takedowns, sanctions, and targeted seizures have disrupted specific campaigns and increased deterrence. Yet prohibitions that sever formal payment rails can reduce visibility and push activity into peer-to-peer markets where oversight is thinner. The evidence therefore supports proportionate, risk-based regulation that improves guardianship without extinguishing transparency. Priority actions include interoperable travel-rule compliance, stronger cross-chain analytics, faster asset-freeze pathways with custodial and over-the-counter intermediaries, and structured public-private information sharing that links on-chain indicators to off-chain intelligence. Limitations of the evidence base remain. Attribution quality varies, open-source datasets are incomplete, and case counts can both overstate and understate true activity. Future research should track stablecoin typologies, measure displacement after enforcement, and evaluate cross-border recovery outcomes.

Recommendations

i. Governments and regulators should implement and enforce the FATF standards for virtual assets through risk-based supervision of exchanges, brokers, and hosted wallets. This must include strong travel-rule interoperability and effective sanctions screening.
ii. Law-enforcement agencies should prioritise developing mixer and cross-chain tracing capabilities, support smaller jurisdictions with blockchain analytics, and establish rapid asset-freezing mechanisms with custodial and over-the-counter intermediaries.
iii. Authorities and financial intelligence units should expand typology sharing via public-private partnerships, ensuring that on-chain

indicators are linked with off-chain intelligence on procurement networks and logistics brokers.

iv. Cybersecurity and financial regulators should target extremist use of the dark web by combining traffic-analysis tools with financial surveillance and stricter due diligence for merchants operating in high-risk sectors.

v. Policymakers should maintain proportionate privacy protections by encouraging research into privacy-preserving compliance tools and setting clear legal boundaries for the regulation of code, speech, and decentralised services.

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.

Chainalysis. (2024). *Assessing terrorism financing on-chain is crucial and complex*. Retrieved from https://www.chainalysis.com/blog/assessing-terrorism-financing-on-chain/ Chainalysis

Egmont Group. (2023). *Report on abuse of virtual assets for terrorist financing: Summary report*. Retrieved from https://egmontgroup.org/wp-content/uploads/2023/12/2023-July-HoFIU-06-IEWG-Project-Abuse-of-VA-for-TF-Summary-1.pdf

Elliptic. (2023). *Terrorist financing through cryptoassets in 2023*. Elliptic. https://www.elliptic.co/resources/terrorist-financing-and-cryptoassets-in-2023

Europol. (2021). *Internet Organised Crime Threat Assessment (IOCTA) 2021*. Retrieved from https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021 Europol

Europol. (2022). *Europol Spotlight – Cryptocurrencies: Tracing the evolution of criminal finances*. Retrieved from https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf Europol

FATF. (2024). *Targeted update on implementation of the FATF standards on virtual assets and virtual asset service providers*. https://www.fatf-gafi.org/en/

publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2024.html

FATF. (2025). *Targeted update on implementation of the FATF standards on virtual assets and virtual asset service providers*. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2025.html

Irmiya, S. R. (2023). Effects of CBN regulatory restriction on cryptocurrency adoption in Nigeria. *Afropolitan Journal of Management and Business Research, 1*(1), 1–20.

MONEYVAL. (2022). *Virtual assets: Typologies report on money laundering and terrorist financing risks in the world of virtual assets and their service providers* [Report]. Retrieved from https://www.coe.int/en/web/moneyval/-/virtual-assets-typologies-report-on-money-laundering-and-terrorist-financing-risks-in-the-world-of-virtual-assets Portal

Oladipupo, A. O. (2022). Impact of cryptocurrency ban on the development of Nigeria's financial market. *Renaissance University Journal of Management and Social Sciences, 7*(2), 113–125.

Oladipupo, A. O. (2025). Comparative analysis of cryptocurrency and terrorism financing in Nigeria and Kenya. *POLAC International Journal of Economics and Management Science, 12*(1). https://www.pemsj.com/papers/PEMSJ-Vol-12Issue-1_768.pdf

Rauchs, M., & Saleh, F. (2021). Cryptocurrency regulation and market integrity: A cross-jurisdictional analysis. *Journal of Financial Regulation and Compliance, 29*(4), 482–498. https://doi.org/10.1108/JFRC-06-2021-0056

Reuters. (2024). Court overturns U.S. sanctions against cryptocurrency mixer Tornado Cash. https://www.reuters.com/legal/court-overturns-us-sanctions-against-cryptocurrency-mixer-tornado-cash-2024-11-27/

Reuters. (2025). Global financial crime watchdog calls for action on crypto risks. https://www.reuters.com/sustainability/boards-policy-regulation/global-financial-crime-watchdog-calls-action-crypto-risks-2025-06-26/

Scharnowski, S. (2024). Dark web traffic, privacy coins, and cryptocurrency trading activity. *Finance Research Letters, 67*, 105875. https://doi.org/10.1016/j.frl.2024.105875

TRM Labs. (2025). *2025 crypto crime report*. TRM Labs. https://www.trmlabs.com/reports-and-whitepapers/2025-crypto-crime-report

U.S. Department of Justice. (2025, March 27). *Justice Department disrupts Hamas terrorist financing scheme through seizure of cryptocurrency*. U.S. Department of Justice. https://www.justice.gov/opa/pr/justice-department-disrupts-hamas-terrorist-financing-scheme-through-seizure-cryptocurrency

U.S. Department of the Treasury. (2024). *2024 National Terrorist Financing Risk Assessment*. Retrieved from https://home.treasury.gov/system/files/136/2024-National-Terrorist-Financing-Risk-Assessment.pdf

Wilson Center. (2024, October 4). *The rise of Monero: ISKP's preferred cryptocurrency for terror financing*. https://gnet-research.org/2024/10/04/the-rise-of-monero-iskps-preferred-cryptocurrency-for-terror-financing/

Wired. (2024, January 12). 'Stablecoins' enabled $40 billion in crypto crime since 2022. *Wired*. https://www.wired.com/story/stablecoin-sanctions-violations-crypto-crime.

.