https://doi.org/10.51483/IJCCR.5.2.2025.42-65

ISSN: 2790-1386

SvedbergOpen
DISSEMINATION OF KNOWLEDGE

International Journal of Cryptocurrency Research

Publisher's Home Page: https://www.svedbergopen.com/

Research Paper

Open Access

Terrorism Financing and Cryptocurrency: Implications for Financial Accountability, Security, and Sustainable Economic Practices

Oladeji, Taiwo Nurudeen[1] and Oladipupo, AbdulMalik Olalekan[2*]

[1]The Light Mega Inter Biz, Lead City University, Ibadan, Nigeria. E-mail: taiwo@thelighteducate.com

[2]Department of Politics and International Relations, Lead City University, Ibadan, Nigeria. E-mail: oladipupo.abdulmalik@lcu.edu.ng

Article Info

Volume 5, Issue 2, December 2025

Received : 02 August 2025

Accepted : 09 December 2025

Published : 22 December 2025

doi: 10.51483/IJCCR.5.2.2025.42-65

Abstract

This study examines the intersection of cryptocurrency, terrorism financing, and sustainable economic practice, highlighting impacts on financial accountability and global security. While cryptocurrencies offer financial inclusion and innovation, their pseudonymous and decentralized nature also facilitates illicit activities like terrorism financing. Using Financial Liberalization and Illicit Financial Flows theories, the research employs qualitative thematic analysis with 12 experts from regulatory, technical, law enforcement, and academic backgrounds. Findings reveal cryptocurrencies' dual potential for abuse and benefits such as low transaction fees. The study calls for effective global regulatory frameworks, enhanced public-private collaboration, and advanced tools like AI and blockchain analysis to manage risks. It advocates a balanced regulatory approach that promotes transparency and harnesses cryptocurrencies' benefits while ensuring security, recommending harmonized regulations, cooperative task forces, regulatory sandboxes, and mandatory compliance audits.

Keywords: *Blockchain, Cryptocurrency, Terrorism financing, Financial accountability, Global security, Blockchain technology, Financial liberalization theory, Illicit financial flows, Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF)*

1. Introduction

In recent years, the rise of cryptocurrency has left its mark on the global financial space. The rise of digital assets, such as Bitcoin, Ethereum and others, as a decentralized alternative to traditional banking systems has seen much interest from those with an interest in how these could help bring financial inclusion, aid in transaction costs and generally improve an economy's efficiency. However, amplifying these benefits are doubts that cryptocurrencies can be used to fund terrorism. Cryptocurrencies provide anonymity, allowing

* *Corresponding author: OLADIPUPO, AbdulMalik Olalekan, Department of Politics and International Relations, Lead City University, Ibadan, Nigeria. E-mail: oladipupo.abdulmalik@lcu.edu.ng*

for transactions without direct oversight, and are a problem for authorities trying to trace illicit financial flows (Pocher, 2023). Such features make crypto attractive to terrorist organizations which would prefer to evade traditional financial monitoring systems. The reasons behind the challenges in financial accountability and security lie in the fact that this type of cryptocurrency does not exist within the frameworks of regulated financials (Goodell *et al.*, 2021). Blockchain technology, the underpinning blockchain systems that use crypto coins transacts, is transparent to the network but anonymous to those transacting (Yadav, 2022). However, the fact that blockchain transparency is not paralleled to user pseudonymity has become a significant obstacle for law enforcement agencies and financial institutions working to prevent the funding of terrorist activities.

1.1. Statement of the Problem

The global use of cryptocurrency has brought a new paradigm of financial systems, decentralization and anonymity. The successful use of these features has positioned cryptocurrency as an appealing weapon for terrorism financing and has become a threat to accountability and security by financial means. Cryptocurrency transactions currently enjoy anonymity that enables malicious financial flows to be difficult to trace, monitor and prevent terrorist financing. However, advances in 'financial tech' do not necessarily stem from more appropriate or fully developed regulatory regimes across jurisdictions. Despite many global nations being unable to effectively monitor cryptocurrency transactions, terrorist organizations continue to misuse them. Furthermore, the complexity of the technical aspects of blockchain networks makes it difficult to monitor and check the commitments of the systems because transactions can be made between parties without an intermediary, which might impose requirements.

The knowledge space about cryptocurrency has focused so far mostly on the technical aspects of the same, such as blockchain architecture, encryption methods, and financial inclusion capabilities. They have also studied links between cryptocurrency and money laundering, along with regulatory measures to reduce these risks. Despite this, we know of no literature on the intersection of cryptocurrency and terrorism financing, particularly with respect to its contribution to financial accountability and security. Although there has been considerable research on the technological and economic aspects of cryptocurrency, few works have systematically studied how cryptocurrency is exploited in particular for terrorism financing. In addition, there is a paucity of scientific research on how these activities have not only challenged the answerability of the amount itself to global security but also undermined the idea of guaranteeing a 'true' electronic account. Additionally, very little work has been directed towards the creation of regulatory frameworks and technological ways to address innovation in cryptocurrency whilst maintaining security and fiduciary transparency.

1.2. Aims of the Study

This study aims to fill these gaps by:

- Examining the specific ways in which cryptocurrency is used to finance terrorism.
- Assessing its impact on financial accountability and global security.
- Proposing regulatory and technological measures that can promote transparency, deter misuse, and foster sustainable economic practices.

1.3. Research Objectives

- To explore how cryptocurrency is used in terrorism financing.
- To assess its impact on financial accountability and security.
- To propose sustainable economic measures to mitigate associated risks.

1.4. Hypotheses

H1: The use of cryptocurrency significantly contributes to challenges in tracking and preventing terrorism financing.

H2: Increased reliance on cryptocurrency negatively impacts financial accountability and transparency in global financial systems.

H3: Regulatory and technological interventions can mitigate the risks associated with cryptocurrency in terrorism financing while fostering sustainable economic practices.

2. Literature Review

2.1. Theoretical Framework

The theoretical foundation for exploring the intersection of cryptocurrency and terrorism financing is rooted in two primary frameworks: Financial Liberalization Theory and the theory of Illicit Financial Flows (IFF). These theories provide insights into the decentralized and opaque nature of cryptocurrency systems and their implications for financial accountability and security.

2.2. Financial Liberalization Theory

Financial liberalization theory claims that eliminating government control over financial markets and institutions generates innovation, efficiency, and, ultimately, economic growth. Deregulation frees up the market movement of capital and increases the ability of investors and entities that use capital to use global financial markets and minimize costs while focusing on resource allocation. Since cryptocurrencies comprise financial liberalization, they have a de-centralized structure that removes intermediaries like banks and government supervision. The main application of blockchain technology is cryptocurrencies, but it brings in two major advantages such as financial inclusion to unbanked populations and transparency and relieves the transaction costs. As such, however, these same features render them vulnerable in particular to financial accountability and oversight. Unlike the traditional banking system, which depends on the presence of a central authority, this form of banking has no central authority. Financial independence and innovation with this spawn regulatory control mechanisms, turning away already and permitting illicit use, including terrorist financing (IMF, 2023). Cryptocurrencies, being natured pseudonymously, are difficult enough to trace a transaction. The blockchain ledger includes all of these transactions, but the identities of the parties are kept concealed as terrorists turn this veil of secrecy to their advantage in order to fund their operations (US Department of the Treasury, 2023). The existence of cryptocurrencies enables highly inexpensive and instant cross-border payments, which circumnavigate the archaic financial system. Because they are capable of doing this, they are the perfect tool to get around international financial regulations as well as sanctions. They argue, however, that the rash growth of cryptocurrencies poses a threat to the integrity of global financial systems. Moreover, the absence of uniform regulatory frameworks across jurisdictions only makes it harder since bad actors can take advantage of legal and technical loopholes. The expenses, therefore, come by way of security and accountability, overshadowing the benefits of financial liberalization.

2.3. Illicit Financial Flows (IFF) and Technology

Illicit Financial Flows theory investigates the flow of money generated, transferred or used illegally across geographical boundaries. Often associated with money laundering, tax evasion and terrorism financing, these flows. With the rise of cryptocurrencies, IFF is unrecognizable, presenting new stumbling blocks to regulators and law enforcement. The use of cryptocurrencies has magnified the magnitude and complexity of illicit financial flows for the very reason that cryptocurrencies are unique. Although pseudonymity is offered by cryptocurrencies like Bitcoin, privacy-focused coins such as Monero and Zcash give you more anonymity. Since it is difficult to track funds, trace their origin, and know how they are being used, they can be used to take money to terrorist organizations without being detected (Investopedia, 2023). Encrypted transactions are ideal for ensuring the integrity of transaction records, but conversely, how do you enforce compliance with Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) regulations when your transactions are decentralized? These technological gaps are exploited by terrorist groups who obscure trails. Cryptocurrencies have helped the dark web become a place for illegal exchanges. Terrorists use these platforms to solicit donations, sell illicit goods and transfer funds securely (US Department of the Treasury, 2023).

Since cryptocurrencies are often governed by regulations inconsistent globally, some countries impose strict regulations on cryptocurrencies while other countries do not regulate at all (FATF, 2023). Law enforcement has yet to effectively catch and intercept illicit transactions due to the technical complexity of blockchain networks and privacy-enhancing technologies. Terrorist organizations will keep finding new cryptocurrencies and using decentralized exchanges (DEXs) to get around detection.

2.4. *Integrating the Two Theories*

The integration of financial liberalization theory and IFF theory provides a comprehensive understanding of how cryptocurrencies facilitate terrorism financing. Financial liberalization highlights the benefits of decentralization and innovation, while IFF theory underscores the risks associated with unregulated financial systems. Together, these frameworks illuminate the dual-edged nature of cryptocurrencies. On the one hand, cryptocurrencies drive financial inclusion and innovation, aligning with the principles of financial liberalization. On the other hand, their potential misuse of illicit financial flows raises concerns about accountability, security, and regulatory efficacy.

2.5. *Existing Research*

2.5.1. Mechanisms of Terrorism Financing

Cryptocurrencies have become a favored tool for financing terrorism due to their decentralized nature, which allows for pseudonymous transactions. According to the Financial Action Task Force (FATF), the decentralized nature of cryptocurrencies presents unique challenges for law enforcement, as they allow for the anonymous transfer of funds across borders, making it difficult to detect illicit transactions (FATF, 2021). Terrorist organizations like Hamas and ISIS have reportedly utilized cryptocurrencies, including Bitcoin, to fund their operations (Chainalysis, 2023). For instance, the US Department of Justice (2023) highlighted that ISIS affiliates have used cryptocurrencies to transfer funds covertly and bypass traditional financial scrutiny. These findings reflect the growing use of digital currencies in financing terrorist activities and underline the vulnerabilities in the financial system that cryptocurrencies create.

2.5.2. Cryptocurrency Vulnerabilities

While cryptocurrencies offer transparency in transaction records via blockchain, the pseudonymity of users creates significant risks. Cryptocurrencies such as Bitcoin, though traceable on the blockchain, obscure the identities of the individuals conducting the transactions. This makes it harder to monitor and control illicit financial flows effectively (FATF, 2021). The use of privacy coins like Monero and Zcash exacerbates these vulnerabilities by offering enhanced anonymity (Elliptic, 2023). Furthermore, the use of mixing services, which blend multiple transactions to obfuscate the origins and destinations of funds, has been flagged as a primary method used by criminals to launder money and finance terrorism (Elliptic, 2023). These services have been linked to over 40% of illicit cryptocurrency transactions associated with terrorist organizations (Chainalysis, 2023). Oladipupo (2024) investigates the role of cryptocurrency in political campaign financing, analyzing both the potential benefits and risks associated with its use in electoral processes. He discusses how digital currencies could enhance transparency and inclusivity in political fundraising while also addressing concerns related to anonymity, regulatory evasion, and the potential for illicit activities.

2.5.3. Impacts on Financial Accountability

Cryptocurrencies present considerable challenges to financial accountability due to the difficulty in tracing and monitoring transactions. The FATF has reported that many countries still lack effective regulations to track virtual asset transactions, which complicates efforts to ensure financial transparency (FATF, 2021). The rise of cryptocurrency exchanges that do not implement proper Anti-Money Laundering (AML) measures contributes to these accountability challenges. For example, the cryptocurrency exchange BitMEX was fined $100 million for failing to implement adequate AML practices (WSJ, 2021). The IMF (2023) notes that the lack of regulation and compliance by cryptocurrency platforms further weakens the ability to ensure financial accountability and create a transparent financial system. This gap in oversight has allowed bad actors to exploit these digital currencies for illicit activities, including terrorism financing.

2.5.4. Security Risks

Cryptocurrencies pose substantial security risks, particularly in enabling terrorist organizations to carry out rapid, cross-border transactions without the oversight of traditional financial institutions. The FATF (2021) has emphasized that terrorists increasingly use virtual assets to circumvent financial sanctions and evade law enforcement. Countries like North Korea have been reported to use cryptocurrencies to fund their missile programs and evade sanctions (Reuters, 2024). Moreover, the anonymity provided by cryptocurrency transactions presents challenges for international cooperation in combating terrorism financing. As pointed out by the IMF (2023), without robust tracking mechanisms, the security landscape remains vulnerable to exploitation by malicious actors.

2.5.5. Implications for Sustainable Economic Practices

The growing role of cryptocurrencies in global finance necessitates a balanced regulatory approach. Overregulation can stifle innovation, while under regulation creates vulnerabilities that can be exploited for illegal activities, including terrorism financing. The IMF (2023) advocates for comprehensive regulatory frameworks that can foster financial innovation while mitigating risks such as terrorism financing. Oladipupo (2024) discussed the intersection of cryptocurrency and global politics, examining how digital currencies influence international relations and economic systems; he highlights the challenges and opportunities presented by cryptocurrencies in the context of global political dynamics. Moreover, the FATF (2021) suggests that public-private partnerships are crucial in developing effective regulatory strategies to combat misuse while preserving the positive aspects of cryptocurrency, such as financial inclusion and lower transaction costs. Collaboration between regulatory bodies and the private sector can improve the detection of suspicious transactions and enhance the integrity of the financial system.

3. Methodology

This qualitative study explores expert opinions on the nexus between terrorism financing, cryptocurrency, and sustainable economic practices using a thematic analysis approach. The objective is to solicit information from practitioners in regulatory bodies, developers of cryptocurrencies, security agencies, and financial institutions. The targeted population comprises individuals working in cryptocurrency regulation, financial intelligence, law enforcement, financial inclusion, private finance, cybersecurity, exchanges, and academia. It covers CBN representatives in monetary policy, NFIU representatives in compliance and analysis, EFCC representatives on operational and cybercrime functions, Exchange Compliance Officers, managers of Financial Inclusion NGO programs, financial institutions' heads of Risk Management, Chief Technology Officers of cybersecurity firms, and finance, blockchain, and international relations academics. Such a combination shall, therefore, be well-conversed with cryptocurrency and terrorism financing. Responses from 12 individuals drawn from different institutions were obtained using purposive sampling within the study, selected by the depth of their experience in researching issues involving terror financing and cryptocurrency. Data from the perspective of cryptocurrency regulation and financial stability aspects were derived from the views expressed by the CBN's Director of Financial Policy and the Head of Financial Stability. A representative of the Nigerian Financial Intelligence Unit, NFIU, an analysis and compliance department representative, had things to say about cryptocurrency regulation and mitigating terror financing risks; two representatives from the Economic and Financial Crimes Commission, one a staff member working in operations and the other a cybercrime investigator, presented challenges on cryptocurrency crimes and how they fight against illegal transactions. There was also an exchange compliance officer who discussed AML/CTF compliance controls. A program manager from a leading NGO that works on financial inclusion discussed the application of cryptocurrencies to improve financial access and its risks. The head of risk management at a private financial institution shared institutional perspectives on how to handle risks in cryptocurrency transactions, while the CTO of a cybersecurity company assessed technical challenges and solutions for the safety of cryptocurrencies. Last but not least, three scholars, a finance professor, a blockchain research fellow, and an international relations lecturer, presented various scholarly perspectives on what cryptocurrency means in terms of financial responsibility and global security. Open-ended questionnaires were distributed to financial regulators, cryptocurrency experts, and security professionals to capture their

insights on the challenges and opportunities associated with cryptocurrency in terrorism financing. Practical insights into how to manage these risks while promoting innovation were gained from in-depth interviews with policymakers, law enforcement officers, and technology developers. Response coding and categorization were done for recurring themes that were used in addressing the research hypotheses through NVIVO statistical software.

4. Results and Discussion

Thematic Analysis of Individual Themes and literature Reflection

As indicated in Figure 1 above, the central themes concerning cryptocurrency usage in terrorism financing are improving detection and reducing anonymity. Improving detection entails the application of blockchain analytics, developing real-time monitoring tools, better data sharing between cryptocurrency exchanges and regulatory agencies, and applying artificial intelligence to detect patterns that indicate terrorism

Figure 1: Cryptocurrency Use in Terrorism Financing

Source: Thematic Map of the Researcher's Fieldwork (2025)

financing. Countering anonymity entails adherence to KYC and AML standards, user identification on decentralized platforms, and tighter regulation of privacy coins associated with criminal activity. The respondents mentioned various means by which cryptocurrencies finance terrorism. Respondent 1 enumerated terrorist organizations' use of Bitcoin wallets as a primary source of funding, referring to crypto investigations by terrorists (Chainalysis, 2023). Respondents also referred to social media as a platform for soliciting crypto donations (Respondent 2) and the dark web as a platform for purchasing weapons (Respondent 4). Most proposed methods of improving the detection of crypto transactions for terrorism financing. The majority recommended improving blockchain analytics (Respondent 1) and enforcing stricter regulations like KYC and AML compliance on all exchanges (Respondent 2). Real-time suspicious transaction monitoring software was also proposed (Respondent 3), highlighting the need for proactive action against illicit cryptocurrency flows. Respondents 4 and 5 both emphasized the imperatives of international cooperation on intelligence-sharing on cryptocurrency cross-border transactions. The Financial Action Task Force (2023) endorses global cooperation against terrorism financing facilitated by cryptocurrencies. Elliptic (2023) stipulated that criminal and terrorist organizations are now using cryptocurrencies more and more to conduct illegal activities, routinely using decentralized exchanges as well as peer-to-peer platforms in order to remain undetected (Financial Action Task Force, 2023).

Also, privacy cryptocurrencies like Monero and Zcash were cited by a number of respondents (e.g., Respondents 3 and 4) as key tools for terrorism financing due to their strong privacy capabilities that facilitate anonymous transactions. These anonymity capabilities make it hard for authorities to trace and disrupt such transactions. In accordance with the Financial Action Task Force (2021), these privacy capabilities are crucial in masking the identities of terrorism financing perpetrators. Preferential use of cryptocurrency was also prevalent. Respondents cited Bitcoin liquidity as the preferred choice for terror financing (Respondents 1 and 8), with privacy coins Monero (Respondent 2) and Dash (Respondent 5) being favored because of anonymity and evasion of detection. Literature indicates that terrorists use cryptocurrencies due to their privacy and low traceability, which helps conceal the origin of funds (Pocher, 2023; Yadav, 2022). Tether, a stablecoin, is cited for its stability in value, making it suitable for financing in volatile environments (Respondent 11). Stablecoins are increasingly being accepted due to their stability in relation to other cryptocurrencies, and it is a safe financing option (Reuters, 2024).

Anonymity is essential in the use of cryptocurrency in terrorism funding. The majority of the respondents mentioned that anonymous transactions invite illegal activities. According to Respondent 1, anonymity reduces traceability, allowing criminal actors to avoid detection by financial institutions or law enforcement agencies. The Financial Action Task Force (2023) discovered that the lack of identity verification makes cryptocurrency attractive to terrorists. Furthermore, some of the interviewees (e.g., Respondents 6 and 10) mentioned the emergence of decentralized platforms that allow for transactions without the need for intermediaries. Such websites, with improved anonymity, facilitate terrorists to circumvent financial monitoring and tracing and preventing financing for terrorism is difficult (Goodell *et al.*, 2021). Terrorism financing in cryptocurrency has lately evolved. Trends reported by respondents consist of greater utilization of privacy coins (Respondent 1) and decentralized exchanges (Respondent 2). The dark web remains a significant crypto trading-based terrorist financing channel, providing anonymous exchange of funds for illicit purposes (Respondent 4). Chainalysis (2023) foresees this trend to grow further as organizations and individuals capitalize on the lack of regulation of decentralized platforms. More recent types of digital assets like NFTs (Respondent 5) are also being used for funding, signaling a shift in the use of the cryptocurrency space by terrorist groups.

Cryptocurrency financing of terrorism is a key area of concern for the authorities. The respondents in terrorism financing emphasize anonymity, privacy coins, and decentralized platforms. Improving blockchain analytics, stricter regulations, and global cooperation can reduce the risks of cryptocurrency-based terrorism financing. The literature covered articulates the necessity of applying specialized regulatory methods towards handling the mentioned emerging threats.

4.1. Impact Of Cryptocurrency is Used to Finance Terrorism on Financial Accountability and Security

Figure 2 above focuses on assessing the impact of cryptocurrency on financial accountability and security. The

major themes are Enhancing accountability through regulation involves imposing mandatory financial reporting requirements for cryptocurrency exchanges, blockchain-based audit trail architecture to enhance transparency in transactions, and third-party auditing to examine compliance in cryptocurrency firms. Strengthening financial security is achieved by having sophisticated cybersecurity for crypto exchanges, mapping the weaknesses in the financial system, and facilitating global cooperation on cryptocurrency risk. The interviewees are extremely concerned that cryptocurrencies could undermine financial responsibility. The majority of respondents mentioned difficulties in accountability owing to decentralized, pseudo-anonymous cryptocurrency transactions. Respondent 1 mentioned that the lack of central control makes tracking difficult. Respondent 7 mentioned that ambiguous reporting requirements undermine financial accountability, and Respondent 8 mentioned that pseudo-anonymity makes institutional responsibility more difficult. Shoetan and Familoni (2024) uncover in their research that the decentralized system of blockchain typically bypasses conventional financial reporting, thus creating loopholes in accountability. Similarly, Hossain (2023) explains that the anonymity of cryptocurrencies hampers forensic accounting, where institutions cannot trace financial transactions. Respondent 6 and Respondent 12 stated that it is harder to adhere to Anti-Money Laundering

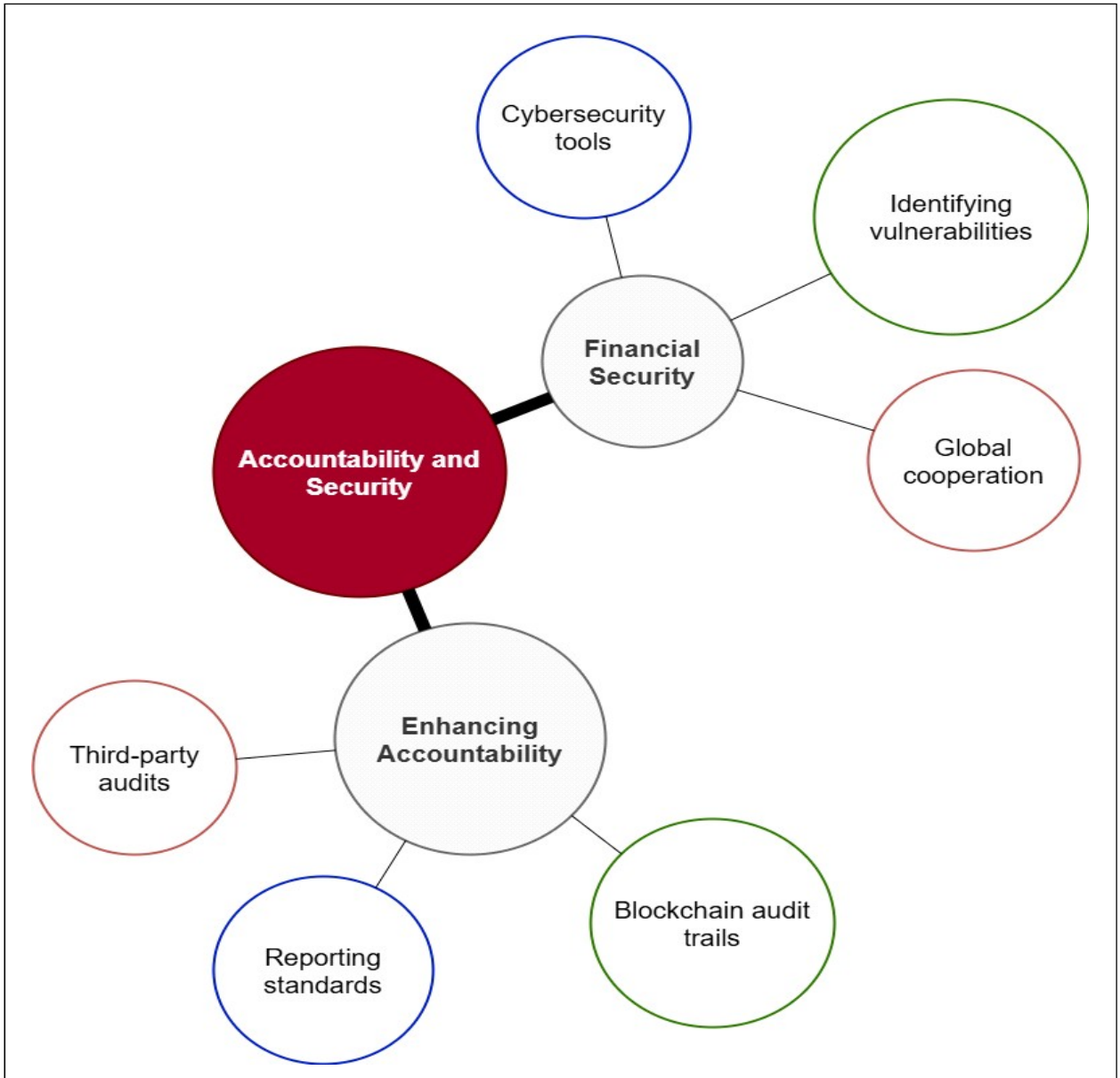

Figure 2: Cryptocurrency and Financial Accountability and Security

Source: Thematic Map of the Researcher's Fieldwork (2025)

(AML) laws due to cryptocurrencies. This bears witness to Limba *et al.* (2019), who state that inadequate regulatory frameworks allow cryptocurrencies to bypass traditional accountability.

Participants agreed in large part that cryptocurrencies are a threat to global financial stability due to their decentralized and unregulated nature. Respondent 2 cited possible risks of criminal activities like money laundering and terrorism financing, while Respondent 6 specified that cryptocurrencies circumvent traditional controls, thereby widening vulnerabilities. Haider and Akhtar (2024) confirm that the lack of regulation of cryptocurrencies facilitates illegal behavior such as money laundering and terrorism funding. Ibrahim (2019) further asserts that inadequate international regulation equally encourages such risk, enabling criminals to easily use cryptocurrencies. Respondent 9 considers the absence of central control a source of systemic risk and agrees with Massad's (2019) argument for improved regulation of cryptos to ensure more financial security. Similarly, Respondent 11 clarifies that decentralized systems encourage tax evasion, which affects the economies of nations, a problem raised by Kapsis (2023) on the role of cryptos in financial crimes. Examples were provided by the respondents illustrating the vulnerabilities of cryptocurrencies. Respondent 4 explained how dark web transactions evade monitoring, and Respondent 5 indicated that crypto-mixing services complicate the tracking of funds. These perceptions confirm Fletcher *et al.* (2021), who believe that unregulated cryptocurrencies enable crime. Respondent 3 cited crypto peer-to-peer transactions avoiding reporting, and Respondent 8 noted blockchain technologies disrupting current protocols. Baddam *et al.* (2023) further describe how the sudden rise of cryptocurrencies and digitalization outpaces financial security architectures, rendering monitoring by institutions difficult.

The respondents' reaction suggests that cryptocurrencies pose a threat to financial accountability. They told us that decentralization and anonymity of cryptocurrencies lower transparency and hinder the accountability of financial institutions. Respondent 2 stated that "cryptocurrency anonymity precludes financial reporting transparency," while Respondent 7 stated that "lack of crypto reporting standards negates accountability." Moreover, Respondent 10 stated that "crypto transactions and wallets often bypass auditing structures." These findings are in line with the literature findings. Shoetan and Familoni (2024) point out that the openness of blockchain in certain sectors is undermined by its decentralized application of cryptocurrency, which hinders control. It facilitates tax evasion, money laundering, and fraud through anonymity, as Baddam *et al.* (2023) assert. The absence of standardized global regulatory standards exacerbates the issue (Hossain, 2023). Increased responsibility requires robust regulatory protocols. Limba *et al.* (2019) support a sustainable model of cryptocurrency with international standards for regulation and compliance. Haider and Akhtar (2024) highlight that KYC and AML measures can minimize accountability risks by exercising transparency in transactions.

Interviewees highlighted significant vulnerabilities cryptocurrencies pose to global financial stability. Respondent 3 mentioned that the "absence of standardized rules erodes international financial stability," while Respondent 6 mentioned that "cryptocurrencies circumvent traditional protections, putting systems more at risk." Respondent 9 also mentioned that "crypto's decentralization heightens systemic financial threats." These align with studies that enumerate the dual threats of cryptocurrency decentralization. Fletcher *et al.* (2021) contend that the pseudo-anonymity of cryptocurrency facilitates criminal activities such as money laundering and terrorism financing. Ibrahim (2019) cites the roles played by cryptocurrencies as tools of cross-border financial crimes due to weak control. Researchers advocate for multi-tier regulatory regimes in favor of enhancing financial security. Massad (2019) advocates for enhanced global cooperation in crypto regulation, whereas Kapsis (2023) recommends blockchain forensic technology to track illicit transactions. Weichbroth *et al.* (2023) recommend global monitoring standards for DeFi platforms for enhanced financial security. The literature emphasizes accountability and security issues in cryptocurrencies. Tighter regulations and enhanced security by technology and international cooperation are needed to address such issues. Cryptocurrencies encourage innovation, but the absence of regulation calls for a balanced response in order to maximize benefits and minimize risks. Feedback from the respondents and literature show that cryptocurrencies pose issues in the areas of financial responsibility and safety. The decentralized, pseudo-anonymous character of cryptocurrencies impedes transparency, promotes criminality, and impedes institutional accountability. The regulatory institutions must be made stronger, as Ibrahim (2019) and Haider and Akhtar (2024) argue. Efforts

should establish global standards for reporting and monitoring cryptocurrency transactions to reduce risks to financial systems.

4.2. Sustainable Economic Measures to Mitigate Associated Risks of Financial Terrorism

Figure 3 illustrates sustainable economic measures to mitigate the risks of cryptocurrencies. The underlying themes include evolving regulatory frameworks for licensing, imposing international standards on compliance and taxation, and formulating enforcement mechanisms against non-compliance. Facilitating public-private partnerships in managing risk encompasses cooperation between governments and private crypto companies, stakeholder training in managing risk, and shared tech solutions to monitor illicit transactions. Respondents provided some practical recommendations for addressing the economic and regulatory risks associated with

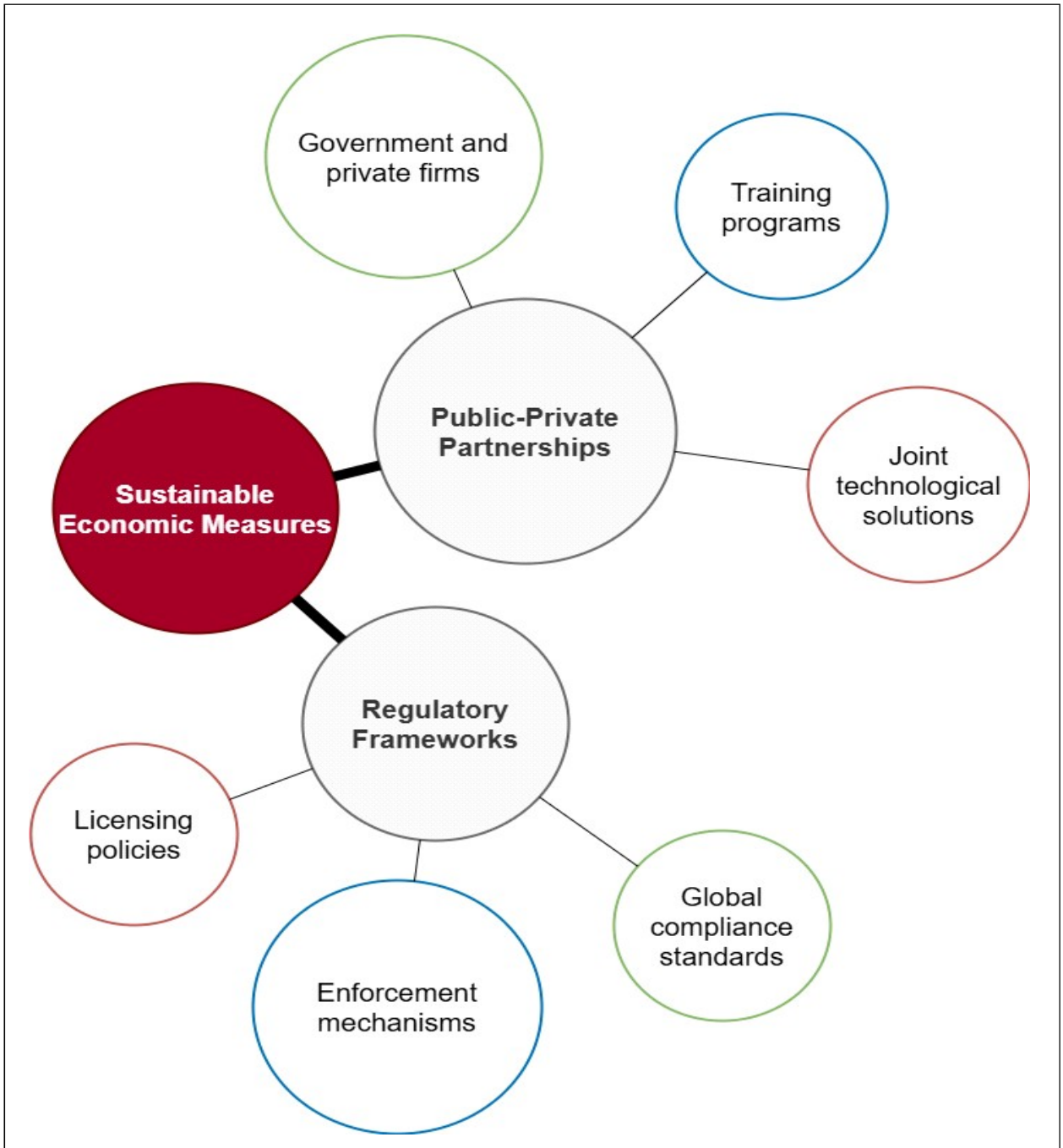

Figure 3: Sustainable Economic Measures to Mitigate Associated Risks

Source: Thematic Map of the Researcher's Fieldwork (2025)

cryptocurrency. Some of the major themes were enhancing regulatory frameworks, leveraging technology for oversight, fostering public-private collaboration, balancing security with innovation, and encouraging sustainable practices. Recommendations were to bring in global standards of compliance, enhance KYC and AML procedures, make regular audits of cryptocurrency companies mandatory, have stricter penalties for non-compliance, and have blockchain-based audit trails for transparency. All of these raised the necessity for global cooperation, such as an international cryptocurrency regulatory framework and information-sharing agreements. They further proposed employing blockchain analysis, machine-learning-based anomaly detection, and live tracking to monitor illicit cryptocurrency flows. Public-private partnerships were proposed as necessary for the development of monitoring tools, intelligence sharing, and the development of innovative risk mitigation technology. Regulation of the environmental impact of cryptocurrency mining, encouragement of sustainable blockchain technologies, and global taxation were viewed as necessary priorities. These responses echo academic and policy views of cryptocurrency risk mitigation. Akartuna *et al.* (2022) emphasize global policies against money laundering and terrorist financing in the context of emerging technologies. Their appeal for global collaboration and compliance aligns with Haider and Akhtar (2024), proposing cross-border regulations to prevent financial crimes in virtual currencies. Korauš *et al.* (2024) highlight that Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) are crucial to the sustainability of the financial system.

Schwarz *et al.* (2021) identify the ways in which blockchain's immutability and transparency allow tracking of illicit financial flows. Anggriawan and Susila (2024) identify how technology aids in aligning cryptocurrency with FATF standards. Respondents support sophisticated monitoring tools and public-private collaboration, in line with Vogel (2022), stating that they can be employed to enhance money laundering and terrorism financing prevention. Innovation and security trade-off is the dominant theme in cryptocurrency scholarship. Fletcher *et al.* (2020) suggest flexible regulations to foster innovation and reduce risks. Members support sandbox environments, incremental regulation, and innovation with security in mind. Green practices like green blockchain and energy-efficient mining are indicative of Frunzeti and Dumitru's (2024) emphasis on minimizing the environmental hazards of virtual currencies.

The replies are in agreement on the need for robust regulations to thwart cryptocurrency's economic and security threats. Most underscored international standards for compliance for uniformity across borders. Many suggested enhancing KYC and AML mechanisms, frequent auditing of crypto enterprises, and punishment for non-compliance. Among the recommendations was the utilization of blockchain for audit trails to allow for better financial transparency and block illegal transactions. Members highlighted the importance of international cooperation in coming up with a harmonized system of regulation. Recommendations also covered cross-border agreements for improved exchange of information and an international system for virtual currency issues. Akartuna *et al.* (2022) note the relevance of global policies in money laundering prevention within cryptocurrency. Haider and Akhtar (2024) similarly demand adaptable, cross-border regulation for ensuring global financial stability.

One of the recurring themes was the need for public-private collaborations to address cryptocurrency risks. They called for governments to collaborate with private companies in deploying sophisticated monitoring tools and risk management techniques. Ideas involved anomaly detection using AI, real-time transaction monitoring, and blockchain analysis for monitoring criminal activity. The participants emphasized intelligence sharing between private and public sectors to facilitate new methods of risk mitigation. This supports Vogel's (2022) hypothesis that intersectoral collaboration enhances the detection and prevention of financial crime. Anggriawan and Susila (2024) emphasized shared technological advancements towards placing cryptocurrency within global standards like those of the Financial Action Task Force (FATF). They further emphasized technology's role in reducing risks. The participants suggested the use of advanced technologies such as machine learning and blockchain analytics to enhance transparency and compliance in the cryptocurrency arena. These tools and strong public-private collaboration are central to regulating the fast-changing digital finance landscape. Two approaches were identified by respondents as most important to reduce cryptocurrency risks: building regulatory frameworks and strengthening public-private partnerships. These approaches balance innovation with risk management. International regulation, technology, and coordination between governments and the private sector can effectively combat the economic and security issues of cryptocurrency. These actions are required for a strong digital financial system.

Combining respondent views with literature identifies important steps towards sustainable economic activity in cryptocurrency. The most critical steps are to strengthen regulatory systems, leverage cutting-edge technology, promote public-private collaboration, and balance innovation and security. Prioritizing compliance, transparency, and sustainability maximizes economic value and minimizes risks. These steps are essential to a secure and robust financial system in the digital era.

5. Conclusion, Recommendations and Implications

5.1. Conclusion

This research points out the dual nature of cryptocurrencies as instruments of financial innovation and instruments of criminal activities, such as terrorism financing. Pseudonymity and decentralization are major impediments to financial responsibility and international security. Targeted interventions like regulatory measures, cutting-edge technologies, and public-private collaborations can counter such threats without eroding the innovative character of cryptocurrencies. The stakeholders can balance security and technology to minimize threats to cryptocurrency and establish a safe financial system.

5.2. Recommendations

Robust consolidated international regulatory frameworks are needed to handle cryptocurrency risks. Licensing of operators and periodic audit requirements should be mandated to comply. Blockchain audit trails can increase transaction transparency. Mechanisms and penalties for enforcement for failure to comply are needed to discourage wrongdoing and encourage responsibility.

Employing sophisticated technologies such as blockchain analytics and AI is most important to trace cryptocurrency transactions effectively. Blockchain analytics follow histories of transactions, and AI detects anomalies and foretells risks in real time. Global blockchain networks to share information between regulators will accelerate the detection and prevention of illegal activities. Machine learning algorithms sift through patterns of transactions to determine connections to suspicious activities.

Encouraging Public-Private Partnerships: Governments and private cryptocurrency companies need to collaborate in risk management. Collaborations can create surveillance software and exchange data. Training programs need to provide stakeholders with expertise in cryptocurrency risk management. Collective investment in technology, such as sophisticated tracking systems, can be used against illegal cryptocurrency-based transactions.

Balancing Security and Innovation: Promoting cryptocurrency innovation is best served by strong security measures. Regulators need to establish regulatory sandboxes for experimentation under oversight. Dynamic regulations in parallel with the technology can promote responsible innovation and reduce risks. Adherence to international security standards is essential for the integrity of the cryptocurrency ecosystem.

Promoting Sustainability: Sustainability should be the top priority of the cryptocurrency sector. Regulators need to put a cap on mining and encourage green blockchain technologies. Recycling of old technologies should be encouraged through policies in order to restrict environmental degradation. This will ensure that cryptocurrencies contribute to economic growth while ensuring environmental integrity.

Policy Implications: International standards for crypto risk must be given the highest priority by decision-makers and facilitate financial innovation. Increased compliance and international cooperation are the drivers to develop a common regulatory framework to fight illicit activity.

Tech Implications: Invest in blockchain analytics, AI, and machine learning to provide transparency and detect illegal activities. These can increase monitoring efficiency, allowing for a secure cryptocurrency ecosystem. Public-private partnerships can effectively mitigate cryptocurrency risks by leveraging the strengths of governments and private firms. Collaboration can lead to innovative solutions that enhance compliance, enhance monitoring, and promote responsibility in the cryptocurrency sector.

Sustainability Consequences: The long-term sustainability of cryptocurrencies requires the environmental impact of their use to be addressed. Encouragement of low-energy consumption mining techniques and green

blockchain technologies must be done in order to avert environmental risks. Sustainability policies will not only help the environment but also make cryptocurrencies more acceptable and reputable on a worldwide level.

References

Akartuna, E.A., Johnson, S.D. and Thornton, A. (2022). Preventing the Money Laundering and Terrorist Financing Risks of Emerging Technologies: An International Policy Delphi study. *Technological Forecasting and Social Change*, 179, 121632.

Anggriawan, R. and Susila, E. (2024). Cryptocurrency and its Nexus with Money Laundering and Terrorism Financing within the Framework of FATF Recommendations. *Novum Jus.*, 18(2), 250-277.

Baddam, P.R., Yerram, S.R., Varghese, A., Ande, J.R.P.K., Goda, D.R. and Mallipeddi, S.R. (2023). From Cashless Transactions to Cryptocurrencies: Assessing the Impact of Digitalization on Financial Security. *Asian Accounting and Auditing Advancement*, 14(1), 31-42.

Chainalysis. (2023). The 2023 Crypto Crime Report. Retrieved from https://go.chainalysis.com/2023-Crypto-Crime-Report.html

Elliptic. (2023). Trends in Cryptocurrency and Illicit Activities. Retrieved from https://www.elliptic.co/resources/trends-in-cryptocurrency-and-illicit-activities

Financial Action Task Force. (2021). Emerging Terrorist Financing Risks. Retrieved from https://www.fatf-gafi.org/en/publications/Methodsandtrends/Emerging-terrorist-financing-risks.html

Financial Action Task Force. (2023). Homepage. Retrieved from https://www.fatf-gafi.org/

Fletcher, E., Larkin, C.J. and Corbet, S. (2020). Cryptocurrency Regulation: Countering Money Laundering and Terrorist Financing. Available at SSRN 3704279.

Fletcher, E., Larkin, C. and Corbet, S. (2021). Countering Money Laundering and Terrorist Financing: A Case for Bitcoin Regulation. *Research in International Business and Finance*, 56, 101387.

Frunzeti, T. and Dumitru, A.C. (2024). Enhancing Financial Security in the Digital Age: Mitigating Risks of Virtual Currencies through Regulation and Institutional Mechanisms. *Land Forces Academy Review*, 29(2), 133-140.

Goodell, G., Al-Nakib, H.D. and Tasca, P. (2021). A Digital Currency Architecture for Privacy and Owner-Custodianship. *Future Internet*, 13(5), 130. https://doi.org/10.3390/fi13050130

Haider, K. and Akhtar, N. (2024). Money Laundering and Terrorism Financing through Virtual Currencies: Critical Analysis of International and Pakistan's Response. *Pakistan Journal of Criminal Justice*, 4(1), 195-210.

Hossain, M.Z. (2023). Emerging Trends in Forensic Accounting: Data Analytics, Cyber Forensic Accounting, Cryptocurrencies, and Blockchain Technology for Fraud Investigation and Prevention. *Cyber Forensic Accounting, Cryptocurrencies, and Blockchain Technology for Fraud Investigation and Prevention*, May 16.

Ibrahim, S.A. (2019). Regulating Cryptocurrencies to Combat Terrorism-Financing and Money Laundering. *Stratagem*, 2(1).

International Monetary Fund. (2023). Cryptocurrency and Financial Stability: Challenges and Opportunities. Retrieved from https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2023/01/01/Cryptocurrency-and-Financial-Stability-Challenges-and-Opportunities-528182

Investopedia. (2023). Cryptocurrencies Used in Crime. Retrieved from https://www.investopedia.com/

Kapsis, I. (2023). Crypto-Assets and Criminality: A Critical Review Focusing on Money Laundering and Terrorism Financing. *Organised Crime, Financial Crime, and Criminal Justice*, 122-141.

Korauš, A., Janèíková, E., Gombár, M., Kurilovská, L. and Èernák, F. (2024). Ensuring Financial System Sustainability: Combating Hybrid Threats through Anti-Money Laundering and Counter-Terrorist Financing Measures. *Journal of Risk and Financial Management*, 17(2), 55.

Limba, T., Stankevièius, A. and Andrulevièius, A. (2019). Towards Sustainable Cryptocurrency: Risk Mitigations from a Perspective of National Security. *Journal of Security and Sustainability Issues,* 9(2), Generolo Jono Žemaièio Lietuvos Karo akademija, Vilnius.

Massad, T.G. (2019). It's Time to Strengthen the Regulation of Crypto-Assets. *Economic Studies at Brookings*, 69.

Oladipupo, A.O. (2023). Cryptocurrency, International Aid, and Development: Opportunities and Challenges. *Journal of International Development Studies,* 7(3), 105-120.

Oladipupo, A.O. (2024). Cryptocurrency and Political Campaign Finance: Opportunities and Risks. *African Journal of Business Management & Research,* 4(4). Retrieved from https://abjournals.org/ajbmr/wp-content/uploads/sites/23/journal/published_paper/volume-4/issue-4/BJMCMR_7KRVPRV0.pdf

Pocher, N. (2023). Distributed Ledger Technologies between Anonymity and Transparency: AML/CFT Regulation of Cryptocurrency Ecosystems in the EU. Doctoral Dissertation, University of Bologna. Retrieved from https://amsdottorato.unibo.it/10659/1/Pocher_Nadia_Tesi.pdf

Reuters. (2024). North Korean Hackers Sent Stolen Crypto to Wallet Used by Asian Payment Firm. Retrieved from https://www.reuters.com/technology/north-korean-hackers-sent-stolen-crypto-wallet-used-by-asian-payment-firm-2024-07-15/*y financing network*. Retrieved from https://www.justice.gov/opa/pr/disruption-isis-cryptocurrency-financing-network

Schwarz, N., Chen, M.K., Poh, M.K., Jackson, M.G., Kao, K., Fernando, M.F. and Markevych, M. (2021). Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism (1): Some Legal and Practical Considerations. International Monetary Fund.

Shoetan, P.O. and Familoni, B.T. (2024). Blockchain's Impact on Financial Security and Efficiency Beyond Cryptocurrency Uses. *International Journal of Management & Entrepreneurship Research*, 6(4), 1211-1235.

US Department of the Treasury. (2023). Cryptocurrency and Terrorism Financing.

Vogel, B. (2022). Potentials and Limits of Public-Private Partnerships against Money Laundering and Terrorism Financing. In *Eucrim-the European Criminal Law Associations' Forum,* 01, 52-60.

Wall Street Journal (WSJ). (2021). Crypto Exchange BitMEX Fined $100 million for Anti-Money Laundering Failures. Retrieved from https://www.wsj.com/articles/crypto-exchange-bitmex-fined-100-million-for-anti-money-laundering-failures-11628235801

Weichbroth, P., Wereszko, K., Anacka, H. and Kowal, J. (2023). Security of Cryptocurrencies: A View on the State-of-the-Art Research and Current Developments. *Sensors,* 23(6), 3155.

Yadav, Y. (2022). Toward a Public-Private Oversight Model for Cryptocurrency Markets. Vanderbilt Law Research Paper, 22-26. Available at SSRN: https://ssrn.com/abstract=4241062 or http://dx.doi.org/10.2139/ssrn.4241062

Open Ended Questionnaire

Objective 1: To explore how cryptocurrency is used in terrorism financing.

1. Can you describe specific instances or methods in which cryptocurrencies have been used to finance terrorist activities?
2. What types of cryptocurrencies are most commonly associated with terrorism financing, and why do you think they are preferred?
3. How do you perceive the role of anonymity in cryptocurrency transactions concerning terrorism financing?
4. What trends have you observed in the use of cryptocurrencies for terrorism financing over the past few years?
5. What specific measures do you recommend for improving the detection of cryptocurrency transactions linked to terrorism financing?

Objective 2: To assess its impact on financial accountability and security.

1. How do you believe the use of cryptocurrencies affects the ability of financial institutions to maintain accountability and transparency?
2. In your opinion, how does the decentralized nature of cryptocurrencies impact global financial security?
3. Can you provide examples of how cryptocurrency has undermined traditional financial monitoring systems?
4. What specific vulnerabilities in financial systems have you identified as being exploited by cryptocurrency transactions?

Objective 3: To propose sustainable economic measures to mitigate associated risks.

1. What actionable steps do you suggest for enhancing regulatory frameworks to improve financial accountability in cryptocurrency transactions?
2. How can technology, such as blockchain analytics, be leveraged to improve the tracking of cryptocurrency used in terrorism financing?
3. What role do you see for public-private partnerships in developing effective strategies to combat the misuse of cryptocurrencies?
4. In your view, what balance should be struck between fostering innovation in cryptocurrency and ensuring security against its misuse?
5. What specific policies would you recommend to promote sustainable economic practices while addressing the risks associated with cryptocurrency?
6. How can international collaboration be strengthened to create a unified approach to regulating cryptocurrencies and mitigating their risks?

Objective 1: To explore how cryptocurrency is used in terrorism financing.

Respondent Number	Question	Response
Respondent 1	**Can you describe specific instances or methods in which cryptocurrencies have been used to finance terrorist activities?**	Bitcoin wallets linked to terror groups were found during investigations.
Respondent 2		Social media platforms are used to solicit donations in cryptocurrency for illicit purposes.
Respondent 3		Privacy coins like Monero facilitate anonymous funding of terrorism.
Respondent 4		Cryptocurrency payments have been used to purchase weapons and other resources on the dark web.
Respondent 5		NFTs are being exploited as a new method for transferring funds to terrorist organizations.

Open Ended Questionnaire (Cont.)

Respondent 6		Blockchain addresses linked to ransomware attacks have been traced back to terror cells.
Respondent 7		Crypto is often used in crowd-funding campaigns for extremist propaganda.
Respondent 8		Reports show the usage of crypto platforms for laundering terror-related funds.
Respondent 9		Cryptocurrencies are used in peer-to-peer transactions to avoid detection by authorities.
Respondent 10		Intelligence reports reveal terrorists are using decentralized exchanges to transfer funds anonymously.
Respondent 11		Evidence from investigations shows terrorist organizations rely on stablecoins for consistent value transfer.
Respondent 12		Stolen crypto wallets from individuals have been repurposed to fund terrorist activities.
Respondent 1	**What types of cryptocurrencies are most commonly associated with terrorism financing, and why do you think they are preferred?**	Bitcoin is widely used due to its global recognition and ease of exchange.
Respondent 2		Monero is preferred for its strong privacy and anonymity features.
Respondent 3		Ethereum is used for its utility in smart contracts that can disguise illegal activities.
Respondent 4		Privacy-focused coins like Zcash are common because of their encryption mechanisms.
Respondent 5		Dash is favored for its instant and private transactions.
Respondent 6		Litecoin has been noted for its speed and lower transaction fees.
Respondent 7		Tether and other stablecoins are used for their consistent value transfer.
Respondent 8		Terrorists rely on coins with high liquidity, like Bitcoin and Ethereum.
Respondent 9		Ripple (XRP) is sometimes associated due to its quick cross-border payment features.
Respondent 10		Cryptocurrencies with fewer regulatory restrictions are more commonly used.
Respondent 11		Coins designed for privacy, like Verge, are targeted for their untraceability.
Respondent 12		Utility tokens with low visibility on regulatory radars are often exploited.
Respondent 1	**How do you perceive the role of anonymity in cryptocurrency transactions concerning terrorism financing?**	Anonymity reduces traceability, making crypto appealing for illegal activities.
Respondent 2		It allows terrorists to avoid surveillance by financial institutions.

Open Ended Questionnaire (Cont.)

Respondent 3		The lack of identity verification creates a haven for illicit transactions.
Respondent 4		Privacy coins' anonymity hinders government and law enforcement investigations.
Respondent 5		The anonymous nature of wallets prevents tracking the source of funds.
Respondent 6		Decentralized platforms amplify anonymity, complicating accountability.
Respondent 7		Anonymity encourages bad actors to exploit the cryptocurrency system.
Respondent 8		The inability to tie transactions to individuals creates major regulatory challenges.
Respondent 9		It fosters an ecosystem where illegal trades can thrive unchecked.
Respondent 10		Full anonymity threatens financial integrity by shielding illegal actors.
Respondent 11		Enhanced anonymity tools, like mixers and tumblers, enable laundering.
Respondent 12		Without anonymity, crypto would lose its appeal for illicit activities.
Respondent 1	**What trends have you observed in the use of cryptocurrencies for terrorism financing over the past few years?**	Increased reliance on privacy-focused coins like Monero and Zcash.
Respondent 2		More transactions are shifting to decentralized and peer-to-peer exchanges.
Respondent 3		Terrorists now use crypto wallets linked to social media campaigns.
Respondent 4		The dark web has become a primary channel for cryptocurrency funding.
Respondent 5		NFTs and other digital assets are being explored for funding purposes.
Respondent 6		Transactions often involve small amounts to evade detection.
Respondent 7		Increased use of mixing services to obfuscate transaction origins.
Respondent 8		Stablecoins are increasingly used for predictable value transfers.
Respondent 9		Cyberattacks, like ransomware, are funding terror operations with crypto.
Respondent 10		Terrorist groups are diversifying into multiple cryptocurrencies to reduce risk.
Respondent 11		Blockchain analytics reveal growth in suspicious transactions on decentralized platforms.
Respondent 12		Crowdfunding campaigns using cryptocurrency have become more sophisticated.

Open Ended Questionnaire (Cont.)

Respondent 1	**What specific measures do you recommend for improving the detection of cryptocurrency transactions linked to terrorism financing?**	Strengthen blockchain analytics tools for transaction tracking.
Respondent 2		Mandate KYC and AML compliance for all cryptocurrency exchanges.
Respondent 3		Develop real-time monitoring tools for suspicious transactions.
Respondent 4		Enhance international collaboration for sharing intelligence on crypto misuse.
Respondent 5		Introduce regulations to monitor privacy coins closely.
Respondent 6		Use artificial intelligence to detect unusual patterns in crypto transactions.
Respondent 7		Improve data sharing between exchanges and law enforcement agencies.
Respondent 8		Create global standards for reporting suspicious cryptocurrency transactions.
Respondent 9		Train regulatory bodies in blockchain technology to improve oversight.
Respondent 10		Develop a global registry for tracking suspicious blockchain addresses.
Respondent 11		Enforce stricter penalties for exchanges that fail to comply with regulations.
Respondent 12		Implement robust audit systems for crypto transactions across borders.

Objective 2: To assess its impact on financial accountability and security.

Respondent Number	Question	Response
Respondent 1	**How do you believe the use of cryptocurrencies affects the ability of financial institutions to maintain accountability and transparency?**	Cryptocurrencies lack central oversight, making it difficult for institutions to track transactions.
Respondent 2		The anonymity of cryptocurrency transactions hinders transparency in financial reporting.
Respondent 3		Financial institutions struggle to identify the origin and destination of funds in crypto transactions.
Respondent 4		Decentralized platforms create gaps in traditional financial accountability systems.
Respondent 5		Cryptocurrencies bypass institutional controls, reducing traceability of funds.
Respondent 6		The rise of crypto has made compliance with anti-money laundering regulations more challenging.
Respondent 7		Lack of reporting standards for crypto undermines financial accountability.
Respondent 8		The pseudo-anonymous nature of cryptocurrency complicates accountability.

Open Ended Questionnaire (Cont.)

Respondent 9		Transparency is reduced because of insufficient regulatory oversight in crypto.
Respondent 10		Blockchain systems lack built-in mechanisms for ensuring institutional accountability.
Respondent 11		Crypto wallets and transactions often evade existing auditing frameworks.
Respondent 12		Financial institutions face a knowledge gap in monitoring cryptocurrency effectively.
Respondent 1	**In your opinion, how does the decentralized nature of cryptocurrencies impact global financial security?**	Decentralization removes the power of central authorities, increasing risks of misuse.
Respondent 2		It creates opportunities for criminal activities like money laundering and terrorism financing.
Respondent 3		Global financial security is undermined due to the lack of standardized regulations.
Respondent 4		Decentralization reduces governments' ability to enforce financial security measures.
Respondent 5		The decentralized system allows anonymous actors to destabilize economies.
Respondent 6		Cryptocurrencies bypass traditional safeguards, making systems more vulnerable.
Respondent 7		Decentralization reduces control over cross-border financial transactions.
Respondent 8		It creates a gap in global financial security by enabling unregulated transactions.
Respondent 9		The absence of central control in crypto increases systemic financial risks.
Respondent 10		Cryptocurrencies challenge the traditional financial system’s integrity and security.
Respondent 11		Decentralization facilitates tax evasion, undermining national economies.
Respondent 12		Global financial security suffers from a lack of unified crypto governance.
Respondent 1	**Can you provide examples of how cryptocurrency has undermined traditional financial monitoring systems?**	Cryptocurrency wallets are used to hide assets from financial regulators.
Respondent 2		Bitcoin and Monero are used to bypass anti-money laundering measures.
Respondent 3		Peer-to-peer transactions in crypto avoid reporting requirements.
Respondent 4		Dark web transactions in cryptocurrency evade traditional monitoring systems.
Respondent 5		Crypto mixing services make tracing funds impossible for financial authorities.

Open Ended Questionnaire (Cont.)

Respondent 6		Fraudulent Initial Coin Offerings (ICOs) have bypassed financial monitoring frameworks.
Respondent 7		Decentralized exchanges do not comply with traditional banking reporting standards.
Respondent 8		Blockchain technologies challenge existing transaction reporting protocols.
Respondent 9		Crypto assets stored in offshore accounts evade scrutiny from regulators.
Respondent 10		The anonymity of wallets undermines the effectiveness of Know Your Customer (KYC) rules.
Respondent 11		Cryptocurrency transactions on decentralized platforms are invisible to financial institutions.
Respondent 12		Cryptocurrencies enable tax evasion by bypassing government tracking systems.
Respondent 1	**What specific vulnerabilities in financial systems have you identified as being exploited by cryptocurrency transactions?**	Cryptocurrencies exploit weak regulatory oversight globally.
Respondent 2		Lack of compliance with Anti-Money Laundering (AML) policies creates vulnerabilities.
Respondent 3		Decentralized platforms exploit the inability to trace cross-border transactions.
Respondent 4		Cryptocurrencies enable rapid, unregulated fund transfers across borders.
Respondent 5		Weak enforcement mechanisms in global financial systems are easily exploited.
Respondent 6		Privacy coins obscure transaction histories, making them susceptible to exploitation.
Respondent 7		Financial systems lack proper tools to monitor decentralized wallet activities.
Respondent 8		Insufficient legal frameworks allow misuse of cryptocurrencies.
Respondent 9		Cryptocurrencies circumvent central banks' authority and oversight.
Respondent 10		Unregulated Initial Coin Offerings (ICOs) exploit investor trust.
Respondent 11		Decentralized finance (DeFi) platforms are prone to security breaches and fraud.
Respondent 12		Cryptocurrencies exploit delays in regulatory updates in the financial sector.

Objective 3: To propose sustainable economic measures to mitigate associated risks.

Open Ended Questionnaire (Cont.)

Respondent Number	Question	Response
Respondent 1	**What actionable steps do you suggest for enhancing regulatory frameworks to improve financial accountability in cryptocurrency transactions?**	Introduce global compliance standards for cryptocurrency exchanges.
Respondent 2		Strengthen Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations.
Respondent 3		Mandate regular audits of cryptocurrency firms by independent bodies.
Respondent 4		Enforce stricter penalties for non-compliant cryptocurrency operators.
Respondent 5		Develop blockchain-based audit trails to ensure transparency.
Respondent 6		Introduce tax regulations for all cryptocurrency transactions.
Respondent 7		Require licensing for cryptocurrency platforms to operate legally.
Respondent 8		Establish a unified legal framework for crypto regulations worldwide.
Respondent 9		Implement real-time transaction monitoring tools for cryptocurrency exchanges.
Respondent 10		Regulate privacy coins that are commonly used for illicit transactions.
Respondent 11		Develop mechanisms for the traceability of cross-border cryptocurrency transactions.
Respondent 12		Enhance collaboration between governments and cryptocurrency firms to ensure compliance.
Respondent 1	**How can technology, such as blockchain analytics, be leveraged to improve the tracking of cryptocurrency used in terrorism financing?**	Use blockchain analytics tools to detect suspicious transaction patterns.
Respondent 2		Implement AI-driven systems to identify anomalies in cryptocurrency transactions.
Respondent 3		Integrate real-time tracking technologies into financial monitoring systems.
Respondent 4		Utilize blockchain technology to trace the flow of funds linked to terrorism financing.
Respondent 5		Collaborate with blockchain firms to create platforms for monitoring high-risk transactions.
Respondent 6		Develop global blockchain networks for data sharing among regulatory agencies.
Respondent 7		Use advanced analytics to identify transactions associated with known terrorist entities.

Open Ended Questionnaire (Cont.)

Respondent 8		Employ machine learning to predict potential risks in cryptocurrency ecosystems.
Respondent 9		Enhance transparency through open blockchain platforms for real-time auditing.
Respondent 10		Combine blockchain analytics with traditional financial tracking systems to improve efficiency.
Respondent 11		Create dedicated algorithms for mapping transactions with terrorism-related flags.
Respondent 12		Leverage blockchain's immutability to build permanent records for investigative purposes.
Respondent 1	**What role do you see for public-private partnerships in developing effective strategies to combat the misuse of cryptocurrencies?**	Governments and cryptocurrency firms should jointly develop monitoring tools.
Respondent 2		Private firms can provide technology while governments enforce regulations.
Respondent 3		Public-private partnerships can organize stakeholder training on cryptocurrency risks.
Respondent 4		Collaborations can fund research on improving the detection of illicit activities in cryptocurrencies.
Respondent 5		Partnerships can foster innovation in tracking and mitigating misuse of cryptocurrencies.
Respondent 6		Governments and firms can jointly invest in advanced technology solutions for monitoring.
Respondent 7		Public-private dialogues can align policy and technological innovations.
Respondent 8		Joint efforts can standardize cryptocurrency regulations globally.
Respondent 9		Governments should incentivize private firms to participate in combating crypto misuse.
Respondent 10		Public-private collaboration can improve information sharing on suspicious transactions.
Respondent 11		Partnerships should focus on increasing the transparency of financial systems.
Respondent 12		Joint training programs for law enforcement and crypto firms can improve detection strategies.
Respondent 1	**In your view, what balance should be struck between fostering innovation in cryptocurrency and ensuring security against its misuse?**	Encourage innovation while mandating strict compliance with financial security laws.
Respondent 2		Strike a balance by regulating high-risk areas without stifling technological progress.
Respondent 3		Governments should allow innovation but strictly monitor high-risk transactions.

Open Ended Questionnaire (Cont.)

Respondent 4		Innovation and security can coexist through adaptive regulatory frameworks.
Respondent 5		Innovation should prioritize security to mitigate risks of misuse.
Respondent 6		Allow controlled innovation in low-risk crypto applications while regulating sensitive areas.
Respondent 7		Encourage industry self-regulation alongside governmental oversight.
Respondent 8		Implement a phased approach that balances innovation and risk mitigation.
Respondent 9		Introduce sandbox environments for innovation under strict regulatory observation.
Respondent 10		Ensure all innovations comply with global security standards.
Respondent 11		Adopt hybrid systems that integrate innovative technologies with robust security measures.
Respondent 12		Foster public trust in cryptocurrencies by balancing innovation and secure usage practices.
Respondent 1	**What specific policies would you recommend to promote sustainable economic practices while addressing the risks associated with cryptocurrency?**	Develop global taxation frameworks for cryptocurrency transactions.
Respondent 2		Require environmental sustainability in cryptocurrency mining operations.
Respondent 3		Mandate the disclosure of energy consumption for crypto firms.
Respondent 4		Introduce caps on energy usage for cryptocurrency mining activities.
Respondent 5		Incentivize eco-friendly blockchain technologies.
Respondent 6		Ensure compliance with international financial and environmental standards.
Respondent 7		Promote responsible innovation in cryptocurrency technologies.
Respondent 8		Regulate cryptocurrencies to ensure that economic benefits outweigh risks.
Respondent 9		Establish frameworks for fair distribution of cryptocurrency-related wealth.
Respondent 10		Implement stricter rules on the environmental impact of cryptocurrency operations.
Respondent 11		Introduce policies for recycling outdated cryptocurrency technologies.
Respondent 12		Enforce penalties for non-compliance with sustainable practices in the crypto industry.

Open Ended Questionnaire (Cont.)

Respondent 1	**How can international collaboration be strengthened to create a unified approach to regulating cryptocurrencies and mitigating their risks?**	Establish a global body for cryptocurrency regulation and compliance.
Respondent 2		Strengthen international treaties focused on financial technology regulation.
Respondent 3		Create cross-border data-sharing agreements for cryptocurrency monitoring.
Respondent 4		Promote regular summits on global cryptocurrency governance.
Respondent 5		Form alliances between nations to enforce crypto compliance standards.
Respondent 6		Enhance the role of global organizations like the IMF in cryptocurrency regulation.
Respondent 7		Standardize regulatory frameworks across countries to minimize regulatory arbitrage.
Respondent 8		Encourage collaboration between financial and technological regulatory bodies worldwide.
Respondent 9		Foster cooperation between nations for intelligence sharing on illicit crypto use.
Respondent 10		Develop international standards for cryptocurrency transactions.
Respondent 11		Promote knowledge sharing on best practices for cryptocurrency regulations.
Respondent 12		Strengthen international sanctions for countries that fail to comply with crypto risk mitigation efforts.

Cite this article as: OLADEJI, Taiwo Nurudeen and OLADIPUPO, AbdulMalik Olalekan (2025). Terrorism Financing and Cryptocurrency: Implications for Financial Accountability, Security, and Sustainable Economic Practices. *International Journal of Cryptocurrency Research,* 5(2), 42-65. doi: 10.51483/IJCCR.5.2.2025.42-65.