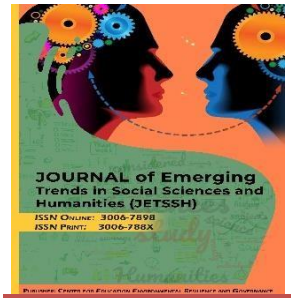

Journal of Emerging Trends in Social Sciences and Humanities

A Double-Blind, Peer-Reviewed, HEC recognized Y-category Research Journal

E-ISSN: 3006-7898 **P-ISSN:** 3006-788X

Volume 2, Issue 4, 2025, 32-41

Cryptocurrency and terrorism: ISIS's use of privacy coins and global regulatory gaps

Summaiyya Qureshi

M Phil International Relations, University of the Punjab, Lahore, Punjab, Pakistan.

Corresponding Author: Summaiyya Qureshi, **Email:** summayyaqureshi4@gmail.com

Article Information

Received:

2025-09-20

Revised:

2025-10-21

Accepted:

2025-11-01

Keywords

Cryptocurrency; Terrorism Financing; ISI; Blockchain; Counter-Terrorism Policy; Privacy Coins.

ABSTRACT

The paper explores the problem of terrorist financing, taking into consideration the new tendency of using privacy-focused cryptocurrencies and decentralized systems. In particular, the case of ISIS increased use of Monero and Tron, which provide greater anonymity. As the traditional money transfer systems, especially hawala and cash courier systems, are increasingly regulated and subject to being tracked, terror groups have turned to digital assets which allow them to remain anonymous, transfer funds across national borders without restrictions, and avoid regulation entirely. Reports shows that ISIS had used these mechanisms to receive over USD 2 million in 2023-2024 in untraceable crypto transfers. The study uses a qualitative case-study analysis method based on Rational Choice Theory (RCT) and Actor-Network Theory (ANT). The results highlight three immediate problems that face global attempts at counter-terrorism: the limited ability of blockchain analytics to track privacy coins, the utilization of country locations with low regulatory control, and the technology gap between terrorist developers and regulators. The paper ends with a set of policy recommendations that will enhance international cooperation, increase the regulation of cryptocurrencies, improve the blockchain forensics, and create a balance between the opportunity of financial innovation and the needs of global security.

Publisher: **Institute for Educating Environmental Resilience and Governance**

Introduction

In the context of modern terrorist financing, the modality has been completely changed. Whereas hawala networks and cash couriers were previously the major means, terrorist organizations currently use decentralized and anonymous financial technologies, and cryptocurrencies are most prominent among them. This transition has increased the range in which operations of entities like ISIS can take place and at the same time negatively affected the effectiveness of current international counter-terrorism measures (Ruehsen & Michael Freeman, 2013).

Privacy-focused coins, including Monero, are a particularly sharp threat among the cryptocurrencies brought into the fold of these organisations. Unlike Bitcoin, which maintains a semi-public record of transactions, Monero is based on making the identities of the users, the values of transactions and the wallet addresses anonymous, thereby making it highly resistant to the existing blockchain surveillance measures. At the same time, decentralised exchanges with the examples of Tron and unregulated peer-to-peer wallets enable terrorist organisations to bypass centralized exchanges, state control and restrictive measures in the case of economic sanctions. The derived ecosystem allows cross-border, near-invisible financial payments that are becoming harder to track or interfere (Wang & Xixi Zhu, 2021) (Dyntu & Oleg Dykyj, 2021).

ISIS has adapted fast to this environment. Previously funded by traditional methods like oil smuggling, taxation and extortion, the group has gone to greater lengths to raise funds using cryptocurrency, especially in areas with limited or non-existent regulatory control. According to reports by TRM Labs and United Nations, ISIS and its affiliates have raised over 2 million dollars using Monero and Tron since 2023, most of which has come through anonymous wallets and decentralized exchanges, greatly increasing the challenge of detection and disruption (FATF, 2008).

Despite the regulatory implications, the existing gap in the attention given to the issue of privacy coins in the light of terrorism financing remains significant. Most of the literature available is still overwhelmingly biased towards cryptocurrencies that are more traceable without proper recognition of anonymity characteristics and forensic restrictions inherent to Monero. Similarly, at the same time as there is an emerging policy discourse regarding money laundering and the overall regulation of cryptocurrencies, there is also a lack of systematic consideration of the structural and jurisdictional gap that allows terrorist financing in the decentralized digital economy.

This research aims to fill that gap by addressing the following questions:

How do privacy-focused cryptocurrencies like Monero improve operational efficiency and evasion compared to traditional terrorist financing methods such as hawala?

What global regulatory gaps have enabled the rise of cryptocurrency-based terrorism financing, particularly in the context of privacy coins?

The current overview of the recent cryptocurrency campaigns of ISIS explains how the phenomenon of privacy-based digital currencies creates challenging situations within the traditional counter-terrorist financing models. It analytically looks at the shortcomings of the current world regulations and brings forth practical, progressive steps that can harmonize technological advancement and financial stability.

Terrorism Financing: Explained

Financing of terrorism is an ongoing security threat, the steady availability of funding sources would allow terrorist organizations to expand their operational capacity, obtain followers and carry out violent acts. Traditionally, groups like Al-Qaeda, Hamas and ISIS have depended on the conjoined combination of state support, illegal commerce, intimidation, donations and the organized informal systems, especially the hawala network to fund their activities **(**Ruehsen & Michael Freeman, 2013). These modalities were preferred due to their relative inability to be traced and few regulatory oversights.

Hawala system, an informal value-transfer network, based on trust between individuals, remains the favorite of the terrorist financiers due to its ease of operation and the low likelihood of detection (Ahmed et al., 2021). The Rational Choice Theory offers an abstract description of

such a bias: the financing routes chosen by terrorist actors are the ones that grant maximum effect but limit the impact of law-enforcement control**.** However, technological development has started to transform the picture where cyber-based instruments, most prominently cryptocurrencies and crowdfunding platforms have started to play an increasingly important role in facilitating financial terrorism. These virtual tools pose a more complex issue of monitorability of international anti-terror financing (CTF) systems.

According to Freeman and Ruehsen (2013), there are six major terrorism-finance channels i.e. cash couriers, hawala-like informal systems, money service businesses (MSBs), the conventional banking system, high-value commodities including diamonds and gold, false trade invoicing. Each of the six channels was quite efficient and anonymous. However, the digital age has brought with it new tools, which despite being more complicated technologically are just as difficult to trace as before, or perhaps even more so. Cryptocurrencies and privacy-oriented digital resources including Monero have developed into some of the key enablers of digital terrorism financing among them.

Digital Turn in Terrorist Financing

At the height of ISIS, which was subsequently reduced in the period between 2014 and 2017, the organization had shown the integration of its ancient sources of revenue, namely oil smuggling and internal taxation, with a network of decentralized, technology-supported fund-raising techniques. With increasing external pressure and shrinking territory, ISIS and its affiliates started to shift to cryptocurrency and decentralized networks, in which they could find a high level of operational anonymity and global reach which were impossible to achieve with the use of traditional finance.

Bitcoin became the first cryptocurrency to gain a wide use by terrorist actors. Even though the records of Bitcoin transactions are permanently stored in an immutable blockchain, the pseudonymous nature of Bitcoin transactions makes it difficult to trace them without specific blockchain-analysis tools (Labs, 2023). Monero, on the contrary, is a much more significant threat. Monero was constructed using privacy-preserving protocols to conceal the amount of every transaction, the identities of people carrying out transactions, and the flow of funds in a wallet, making surveillance by law-enforcement agencies practically impossible.

ISIS and related networks are said to have extracted over 2 million of the gains realized on Monero and Tron in the 2023-2024 period indicating a sharp rise in the practice of using privacy-focused cryptocurrencies in financing terror activities **(**UNSC**, 2024)**. Their ability to evade state level financial controls, in jurisdictions with weak regulatory frameworks, such as South Asia and sections of Africa, adds to the law enforcement issues that already face authorities.

Crowdfunding and Decentralized Platforms

It is clear that the terrorist groups are becoming more active in using the crowdfunding websites and the encrypted social media platforms like Telegram and YouTube. These establishments are not only sources of propaganda but also a means of gathering micro-donations supposedly towards the humanitarian activities (Farid & Ashraf, 2025). With this micro-donation strategy, terrorist groups can raise large amounts of money with the help of a global base of adherents without triggering alert mechanisms within traditional financial surveillance mechanisms.

As an example, ISIS and Hamas have used GoFundMe, Ko-Fi, and even Patreon to seek donations in the excuse of helping widows and casualties of war. The usage of Ethereum smart contracts and low-cost transaction platform of Tron also makes these campaign faster and anonymous (Soliev, 2023).

The dark web, which can be accessed using an encrypted browser like Tor, both makes it possible to buy an illegal weapon and makes it possible to donate anonymously on crypto-donations. In this environment, terrorist agents are able to plan attacks, move money and hoard wealth without going through centralized control.

Enforcement Gaps and Regulatory Issues

In spite of the fact that blockchain analytics and AI-based transaction monitoring have shown some degree of success, international regulatory discrepancies inhibit their effectiveness. As per the FATF **(**FATF, Virtual Assets: Targeted Update on Implementation of the FATF Standards on Virtual

Assets and Virtual Asset Service Providers, 2023**),** jurisdictional gaps in states with low amounts of crypto regulation, such as much of Central Asia, have allowed terrorist groups to use non-custodial wallets and decentralized finance (DeFi) protocols that are not subject to the provisions of existing anti-money laundering (AML) laws.

Advancements in the EU by AMLD5 and at the United Nations have increased the focus on virtual asset service providers (VASPs); however, VC-to-VC transactions, decentralized exchanges, and hybrid wallets lack proper regulatory frameworks, and this lack of regulation is described as an enforcement blind spot (KEATINGE, David CARLISLE, & Florence KEEN, 2018). The increasing interest of jihadist groups in the platforms like Tron and Tether (USDT) testifies that stablecoins, due to their low volatility and transaction speed, will probably become a more significant part of the terror funding mechanisms in the future.

Tropina (2024) and Irwin & Milad (2016) argue that the current paradigm of counter-terror finance should be changed, and enforcement strategies should be replaced with future-oriented governance strategies that would allow to combat new forms of terrorism invented by terrorists (Irwin & George Milad) **(**Tropina**,** 2020**).**

Research on terrorism financing through cryptocurrencies has widened, but of the two major blind spots, research remains heavily skewed toward Bitcoin and regulated exchanges, as opposed to privacy coins and pure decentralized systems. Dyntu & Dykyj and Wang & Zhu (2021) among other authors emphasize the necessity of new methods of de-anonymizing blockchain transactions, especially within privacy-focused ecosystems like Monero. (Dyntu & Oleg Dykyj, 2021)

In addition, the application of big data, AI, and open-source intelligence (OSINT) appears to be promising, but the benefits of that technology are not evenly distributed due to geopolitical differences in digital infrastructure and the determination of the governments (Sarwar & Farid, 2024). These differences increase the gap between regulatory and innovation created by terrorists.

Thakkar promote further research into decentralized financial systems (DeFi), DAOs, and non-fungible tokens (NFTs) as potential future facilitators of terrorism financing. Simultaneously, the regional analyses of Southeast Asia, Middle East, and Central Asia point to the poor financial controls and financial illiteracy in the theaters of the conflict making them particularly vulnerable to the crypto exploitation (Thakkar, et al., 2024).

Overall, terrorist players are using ever more sophisticated means to fund their activities, be they crowdfunding platforms and encrypted social media, the dark web, and the crypto economy. Although regulatory asymmetries and technological unevenness pose tough challenges, anticipatory governance models and stringent empirical studies, especially those of privacy-based blockchains, are crucial in the event that these risks are to be addressed adequately.

Theoretical Framework: Rational Choice and Actor-Network Perspectives

The strict understanding of the financial technologies embraced by terrorist groups, especially those privacy-sensitive cryptocurrencies, requires a theoretical framework that is able to encompass stratetic decision-making and the complex layers of human and non-human actors that mediate those choices. The study will use two theoretically complementary sets namely Rational Choice Theory (RCT) and Actor-Network Theory (ANT). Together, they provide a detailed interpretive framework to follow the shift in operation of traditional systems, like hawala, to the more sophisticated digital tools, like Monero, Tron, and decentralized exchanges.

Rational Choice Theory:

The Rational Choice Theory (RCT) is the main analytical instrument. Based on the assumption that people or groups of people act to maximize their self-interest after calculating costs, benefits and risks, RCT sheds light on why certain financial approaches are adopted by such groups of people as ISIS. Under the RCT, the decision-making process is not inspired by ideology, but it is compelled by pragmatic ideals of efficiency, safety, and strategic benefit (Ruehsen & Michael Freeman, 2013).

With the regulatory pressure increasing since the 11 September 2001 incident and the longstanding ability to use mechanisms like hawala becoming

increasingly monitored, the costs and returns of alternative financial channels had changed significantly. In the case of ISIS, the privacy coins such as Monero were a more logical option: they reduced the chances of being detected, increased anonymity levels, and offered liquidity without borders. Based on this, the group was in a position to maximize financial mobility and at the same time reduce traceability- an option that is particularly convenient in areas where the traditional structure of surveillance remains weak or otherwise non-existent.

Using parallel arguments to Actor-Network Theory (ANT) we can see that the privacy coin strategic choice is not as framed in isolated rational choices; it is framed in a larger network of actors, human and non-human. It is these actors and the impediments as well as opportunities that they present that mediate the possibility of a choice in the first place (Rosa, 1998). As ISIS considers which systems of payment are relatively more advantageous, it has to bargain not just the cost-benefit analysis described by RCT, but also the material capabilities and limitations delimited by ANT.

Table 1: *RCT-Based Comparison – Traditional vs. Crypto Financing*

Financing Method	Cost Efficiency	Detection Risk	Cross-Border Speed	Traceability	Technical Barrier
Hawala	High	Medium	High	Low	Low
Cash Couriers	Medium	Low	Medium	Very Low	Low
Monero (XMR)	High	Very Low	Very High	None	Medium
Bitcoin (BTC)	Medium	Medium	High	Medium	Medium
Tron (USDT)	High	Low	Very High	Low	Low

(Source: Compiled from TRM Labs, FATF Reports, Freeman & Ruehsen, 2013)

This table shows that from an RCT lens, **Monero provides the highest operational advantage** for a terrorist network seeking anonymity, speed, and global reach.

Actor-Network Theory (ANT)

Empirically the Rational Choice Theory (RCT) offers the why of human behavior, but the Actor-Network Theory (ANF) offers the lens through which we can understand how. Bruno Latour and co-authors developed ANT, in which people and non-humans (tools, platforms, protocols) are equal members of a network, which jointly generates results. Such an analytic tool is particularly useful in questioning the domain of decentralized digital ecosystems, where technology plays an active participatory role in influencing the behavior.

As an example, one can take the case of ISIS cryptocurrency fundraising. Such campaigns do not only occur as a result of the personal decisions taken by their operators and supporters; they are co-produced by a collection including:

- **Actors:** ISIS operatives, sympathizers, crypto donors, exchange operators
- **Technologies:** Monero, Tron, mixers, wallets, Telegram bots
- **Protocols:** Blockchain, decentralized apps (dApps), anti-KYC exchanges
- **Environments:** Regulatory loopholes, weak financial jurisdictions, online platforms

ANT allows us to map these actors as interacting and dynamic nodes of an adaptable resilient system that is hard to destabilize. The case of ISIS cryptocurrency financing activities, as an example, is based on automated Telegram bots, Monero wallets, and Tron-based donation links placed in the YouTube videos or shared through Twitter. When taken individually, each of the components is limited in risk; but together, they arrange a self-financing infrastructure.

Table 2: *Key Actor-Network Components in ISIS Crypto Campaigns*

Actor Type	Examples	Role in the Network
Human Actors	Fundraisers, Tech-savvy ISIS affiliates	Operate wallets, manage messaging platforms
Non-Human Actors	Monero, Tron, Telegram Bots, dApps	Enable anonymous transactions and automation
Regulatory Gaps	Weak AML jurisdictions, unregulated VASPs	Provide loopholes for cross-border laundering
Media Platforms	YouTube, Telegram, Twitter	Disseminate donation links, QR codes, crypto info

(Source: TRM Labs, UN CTED Report, 2024)

ANT helps illuminate **why breaking one node (e.g., shutting down a Telegram group)** does little to dismantle the network, as the actors can rapidly reroute using new tools or platforms.

Due to the combination of theoretical constructs of Actor-Network Theory (ANT) and Rational Choice Theory (RCT), authors provide a more developed analytic perspective on the investigation of crypto-based terrorism financing.

RCT indicates the rational calculations of the use of Monero and decentralized payment systems: the decisions are made to maximize operational utility and minimize exposure. ANT, in turn, throws light on the pragmatic networks by virtue of which these instruments enter into a state of operation-individual actors, software applications, and regulatory gaps that become co-constitutive of an enabling infrastructure. Put together, these views explain the rationality behind the financial approach of ISIS, as well as the network characteristics that make it robust to the conditions of regulatory asymmetry and the emergence of privacy-centric coins.

Case Selection and Methodology

The research paper currently uses qualitative case study to evaluate the use of privacy-based cryptocurrency and de-centralized financial aid systems by ISIS in its 2023-2024 fundraising initiatives. Due to the very nature of illicit financing clandestinity, such a strategy can provide an interpretive frame over the questioning of motives, mechanisms and changes in context. The case study design thus best fits the dual objectives of the investigation looking at understanding the organisational decision-making process and also the changing configurative power of networked actors within a given geopolitical and operational environment.

The main body of evidence is secondary data. Such sources are open-source intelligence (OSINT), investigative reporting by TRM Labs and the United Nations, policy recommendations issued by the Financial Action Task Force (FATF), and peer-reviewed university-level scholarship. The use of triangulation in these areas enhances the validity and the completeness of the results despite the sensitivity and confidentiality of the topic. These materials are thematically analysed and interpretatively read according to RCT and ANT perspectives: RCT explains the risks, costs, and benefits calculus of ISIS in procuring privacy coins over traditional payment methods, like a hawala; ANT creates a configurative map of actors, both human and non-human, such as the software wallet, both transactions, decentralised exchanges, or regulatory blind spots, which co-produce the environment in which the ISIS crypto-financial operations can continue (Sarwar & Farid, 2025). The convergence of these theories provides a complex appreciation of both the tactical change and the technological-structural enablers underpinning the same.

ISIS's Use of Privacy Coins and Decentralized Platforms

In 2023-2024, ISIS started to considerably broaden its financial infrastructures by using more privacy-focused cryptocurrencies and decentralized money tools. This was the strategic direction aimed at avoiding financial monitoring,

minimising exposure and providing sustenance of cross-border monetary movements. Terrorist operations under pressure had to be conducted using cryptocurrencies like Monero and Tron (USDT) due to their ability to conduct anonymous, speedy, and regulatorily untraceable transactions, attributes that made them indispensable to the operations of terrorists under pressure (Labs, Virginia Man Convicted for Crypto Financing Scheme to ISIS, 2024).

Unlike the traditional methods of terrorist-financing, such as hawala, money-service businesses (MSBs) and cash couriers, these new technologies also allowed ISIS to operate outside the formal financial framework. In particular, Monero proved to be the cryptocurrency of choice due to its strong privacy framework: all transactions are encrypted, wallet addresses stay anonymous, and transaction amounts get obscured, and blockchain tracking proves to be ineffective in most cases (Irwin & George Milad). These operational advantages are particularly eminent in high-surveillance settings.

Tron-based stablecoins (and in particular Tron-tethered USDT), which are fast, low-cost, and liquid, were also used by ISIS along with Monero. According to (Soliev, 2023) and FATF (2025), extremist groups have been commonly exploiting such platforms as Tron due to convenient mobile wallets and interaction with the decentralized non-custodial services. The features enable reception, storage and transfer of funds in a manner that regulators find hard to detect.

In order to encourage donations, the ISIS-related groups used encrypted services, like Telegram, and social networks, like YouTube, and Twitter. These websites operated as distribution centers of donation links, QR codes, and wallet addresses. Telegram bots would be set up to create single-use wallet addresses, which would further make it difficult to trace the ill-gotten funds (UNSC, 2024)**.** Such methods of fundraising were not by chance as they targeted the sympathizers alongside the use of online arenas, where anonymity is an illusion of humanitarianism (Tropina, 2020).

Another central aspect of the ISIS laundering campaign was crypto mixers technologies, which break the traceable on-chain record by mixing the black money with clean cryptocurrencies and, thus, cover the source of the money. The security access to these mixers was ensured using decentralized applications (dApps), unregulated wallet services, and dark-web nodes. When combined with non-KYC decentralized exchanges, the resulting set ups allowed ISIS to decouple identities of wallets with organizational membership and, therefore, obscure the flow of money out of the sight of law-enforcement.

Another way that increased the operational resiliency of the crypto-financing efforts of ISIS was through the usage of regional regulatory loopholes. A great number of the related wallets and laundering services were located in the jurisdiction of weak AML/CFT frameworks or those with insufficient adherence to the Financial Action Task Force Travel Rule. The territories of South Asia, some regions of East Africa, and several states of the post-Soviet area provided viable grounds because of low state capacity, a lack of regulation, and the instability of the political situation**.**

A transition to a decentralized affiliate model of the ISIS financial structure is clearly described in the National Terrorist Financing Risk Assessment (NTFRA) 2024 report. One example is the ISIS-Khorasan (ISIS-K) which operates semi-autonomously and uses mobile money, extortion, and movements of cryptocurrency frequently utilizing peer-to-peer platforms and anonymous donation systems. These are smaller and more mobile groups that are harder to track and interfere with (Treasury, 2024)**.**

All these findings indicate that ISIS has been not only a response to disruption of finances but a deliberate transformation toward a tech-savvy, decentralized network of financing all exploiting anonymity, automation, and asymmetric regulation. These systems enable the organization to raise, obscure and mobilize funds cross-border and with little visibility, high liquidity and low exposure to risks. This development does not only reflect a shift in tactics, but a structural change to the way terrorism is funded and points to glaring gaps in the existing regimes of counter-terror-finance.

Global Enforcement Gaps and Crypto Blind Spots

Although international regulatory institutions like Financial Action Task Force (FATF) and

European Union with their 5 th Anti-Money Laundering Directive (5AMLD) have attempted to adapt to present frameworks, they have been incapable of effectively responding to the use of privacy-focused cryptocurrencies in the financing of terrorism activities. Whereas 5AMLD subjected the crypto exchanges and wallet providers to regulation, crypto-to-crypto (virtual currency to virtual currency) transactions, non-custodial wallets, and decentralized exchanges are areas with weak governance (HOUBEN & Alexander SNYERS, 2024).

Some regions--especially the Central and South Asia, some African regions or state of Eastern Europe post-Soviet hemisphere are still unable to effectively enact anti-money laundering (AML) or counter-terrorism financing (CTF) frameworks. Such regulatory gaps are being fully utilized by terrorist organizations such as ISIS to channel and wash funds. The UN CTED Report (2024) and TRM Labs (2025) showed that wallets that were used by ISIS members and affiliates were frequently located in the jurisdictions that lack any supervision or weakly adhere to FATF suggestions (FATF, Strengthening efforts to combat terrorist financing, 2025).

Even new tools of blockchain forensics, increasingly advanced, have trouble following transactions involving privacy coins such as monero or mixing services, neither one of which is accidentally difficult to trace. According to Tropina and Dyntu & Dykyj (2021), such privacy technologies make it impossible to use classic surveillance services, such as Chainalysis or TRM Labs, above a certain level, which deprives law enforcement personnel of important visibility.

Networked Financing and Strategic Logic

This decision of ISIS to abandon traditional forms of money like hawala through cryptocurrency is grounded on the Rational Choice Theory (RCT). Since their activity was strengthening the focus of attention on this group through more traditional routes, it was logical to use the system of finances which are based on safer use, bigger anonymity and extended transnational spread. Another, namely Monero, can be used to achieve complete payment obfuscation, which is a rationally stronger tool than hawala, which uses human elements instead and is much more easily infiltrated (Treasury, 2024).

ANT also sheds new light on how ISIS manages to create a resilient ecosystem of human (operatives, donors, crypto traders) and non-human actors (Telegram bots, wallets, dApps, smart contracts). This network is relatively self-governing and can very fast adapt through using diversified platforms or re-routing flows. According to Soliev (2023), the 2023 24 ISIS funding campaign featured Tron wallets, telegram-based donation platforms, and QR codes shared through social media, and which communicate within a dynamic, decentralized network.

In a reported 2024 case, 53,000 dollars were sent using Monero and laundered via a non-KYC exchange in Eastern Europe and finally cashed out using ATMs in Syria. This demonstrates how the strategic moves presented in RCT are realized through actor-networks, where each tool or platform serves as the functioning node of the financial environment (Dyntu & Oleg Dykyj, 2021).

Policy Recommendations

The most appropriate measures in dealing with the current dynamics of terrorism financing involve a multi-pronged approach that has to deal with not only strategic attitudes of the terrorist groups but also vulnerabilities within the structures that support them. The following measures will therefore be advised:

1. Privacy Coin Regulatory Framework

Privacy-oriented cryptocurrencies like Monero and Zcash should also be fully banned (or at least severely restricted) by countries as they both offer 100 percent zero-traceability features

2. Increased KYC/AML Requirement of All VASPs

The Travel Rule (Recommendation 16) by FATF ought to be revised to cover the non-custodial wallets and decentralised exchanges (DEXs), and specialized technical support should be available in the most vulnerable regions**.**

3. Mixer Services and Decentralised Protocols Geo-blocking

ISPs must be permitted to censor use of well-established mixer services and non-compliant decentralised finance (DeFi) platforms in fragile states, such as the proposal of TRM Labs in 2025.

4. Advanced Blockchain Forensics Investment

It is essential to increase coordination with companies like Chainalysis and Cipher Trace and create big-data analytics systems to identify suspicious activity.

5. International Systems of Sharing Intelligence

A system of real-time warnings of suspicious cryptocurrency wallets, crowd-funding campaigns and related individuals, comparable to the system suggested by the UN Security Council in 2024, should be set in place at FATF, Interpol, and the UN CTED.

6. High Risk Region Reg Sandboxes

Jurisdictions with high risks might follow the model of regulated innovation developed by the United Arab Emirates, where the professionals in charge monitor digital asset innovations without losing compliance with regulations. This model can be globalized.

Limitations of the Study

The present research draws its foundation on publicly available secondary sources, most prominently the report produced by TRM Labs, FATF, and other UN organizations. The authenticity of these sources is already proven; however, due to the fact that the funding of terrorism takes place in a rather illicit manner, the statistic obtained as a result is necessarily inhomogeneous and could be biased. The case has failed to gain access to classified intelligence or operational communication, though there has been the use of triangulation of sources to achieve an all-inclusive and reliable analysis.

Conclusion

This study examined the ways in which ISIS can adjust to the global financial surveillance by shifting away from the traditional system of financing such as hawala to decentralized and privacy-oriented financial systems. Using the Rational Choice Theory, we can realize this change as the rational initiative to balance the security and efficiency of operation as much as possible. Actor-Network Theory was useful to depict the thick ecosystem of technologies, actors and platforms which collectively creates a robust financing structure.

The results show that the existing international mechanisms like FATF and 5AMLD are inappropriate in dealing with the pace and the complexities of crypto-based terrorism financing. The risk is to change still further with the advent of the AI-assisted laundering, NFT-based raising funds, and unregulated DeFi realms.

To deal with this the international community needs to move quickly in modernizing the regulations, developing capacities on technical enforcement and in international collaboration. The time slot to curb the use of cryptocurrencies by terror organizations is slowly closing. With a lack of intervention, a complete system of financing may be so deeply embedded and sophisticated that it could fall beyond the reach of international law.

Conflict of Interest

The authors showed no conflict of interest.

Funding

The authors did not mention any funding for this research.

References

Ahmed, S., Farid, A., & Ashraf, S. (2021). Climate Change: Implications and Policy Recommendations. *Pakistan Languages and Humanities Review, 5*(2), 170-180.

Dyntu, V., & Oleg Dykyj. (2021). *Cryptocurrency as an Instrument of Terrorist Financing.* Baltic Journal of Economic studies.

FATF. (2008). *FATF Terrorist Financing Typologies Report.* Financial Action Task Force.

FATF. (2023). *Virtual Assets: Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers.* Financial Action Task Force.

FATF. (2025). *Strengthening efforts to combat terrorist financing.* Financial Action Task Force.

Farid, A., & Ashraf, S. (2025). Water Security in South Asia: How Indo-Israeli Technological Cooperation Shapes the Future of the Indus Waters Treaty. *Pakistan Social Sciences Review, 9*(2), 456-476.

HOUBEN, D. R., & Alexander SNYERS. (2024). *Cryptocurrencies and blockchain.* Policy Department for Economic, Scientific and Quality of Life Policies.

Irwin, A. S., & George Milad. (n.d.). The use of crypto-currencies in funding violent jihad. *Journal of Money Laundering Control, Emerald Group Publishing Limited, 19*(4), pages 407-425.

KEATINGE, T., David CARLISLE, & Florence KEEN. (2018). Virtual currencies and terrorist financing: assessing the risks and evaluating responses. *Think Tank European Parliament*.

Labs, T. (2023, February 15). *Terrorist Financing: Six Crypto-Related Trends to Watch in 2023*. Retrieved from TRM Labs: https://www.trmlabs.com/resources/blog/terrorist-financing-six-crypto-related-trends-to-watch-in-2023

Labs, T. (2024). *Virginia Man Convicted for Crypto Financing Scheme to ISIS.* TRM Labs.

Ruehsen, M., & Michael Freeman. (2013). Terrorism Financing Methods: An Overview. *Perspective on Terrorism, 7*(04).

Sarwar, G., & Farid, A. (2024). Unveiling Gender Disparities in Pakistan: Challenges, Progress, and Policy Implications for Achieving SDG 5. *Journal of Development and Social Sciences, 5*(2), 506-517.

Sarwar, G., & Farid, A. (2025). The Indus Under Pressure: Hydro-Politics, Climate Change, and Strategic Anxiety in South Asia. *Journal of Political Stability Archive, 3*(3), 45-59.

Soliev, N. (2023). *The Digital Terror Financing of Central Asian Jihadis.* Combating Terrorism Center.

Thakkar, H., Datta, S., Priyam Bhadra, Siddharth Baburao Dabhade, Haresh Barot, & Shankar O. Junare. (2024). Mapping the Knowledge Landscape of Money Laundering for Terrorism Financing: A Bibliometric Analysis. *J. Risk Financial Manag*.

Treasury, d. o. (2024). *2024 National Terrorist Financing Risk Assessment.* US: dept of Treasury.

Tropina, T. (2020). Big Data: Tackling Illicit Financial Flows. *Foreign and International criminal law*.

UNSC. (2024). *CTED Trends Tracker | Evolving Trends in the Financing of Foreign Terrorist Fighters' Activity: 2014 – 2024.* UNSC.

Wang, S., & Xixi Zhu. (2021). Evaluation of Potential Cryptocurrency Development Ability in Terrorist Financing. *Policing: A Journal of Policy and Practice*.