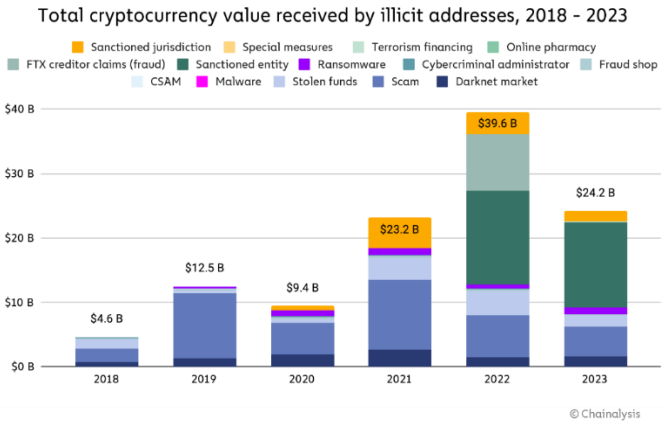
BIPSS Commentary
www.bipss.org.bd April -2025
BIPSS Towards a Secure World

Cryptocurrencies and Terror Financing: A New Frontier in Asymmetric Threats

Farhana Rashid[1]

Cryptocurrencies are redefining the financial landscape worldwide by decentralizing control and providing fast, borderless, and pseudonymous transactions. While these digital assets offer numerous benefits, such as financial inclusion, cross-border efficiency, and reduced transaction costs, they have also created new avenues for criminal exploitation. Because of digitalization, the methods and ways of committing some crimes have changed. One of the gravest concerns in this domain is the use of cryptocurrencies for terror financing. It is an evolving form of asymmetric warfare that exploits the vulnerabilities of stronger adversaries through unconventional means. Terrorist financing is the raising of money involving the solicitation, collection or provision of funds, with the intention that it may be used to support terrorist acts, terrorists or terrorist organizations.[2]



[1] Farhana Rashid is a Research Intern at the Bangladesh Institute of Peace and Security Studies (BIPSS). She completed her BSS & MSS in International Relations from the University of Chittagong.

[2] "Global AML/CFT Context." n.d. EU AML/CFT Global Facility. https://www.global-amlcft.eu/global-anti-money-laundering-and-countering-terrorism-financing-context/.

As terrorist groups adapt to counterterrorism measures targeting traditional financial systems, cryptocurrencies have emerged as a new frontier for asymmetric threats. This commentary explores how cryptocurrencies are being leveraged for terror financing, the challenges they pose to global security, and the measures being taken to counteract their misuse.

The Appeal of Cryptocurrencies for Terrorist Financing

Cryptocurrencies offer a set of features that are both revolutionary for legitimate users and attractive to those seeking to evade oversight. The core appeal lies in their decentralization, pseudonymity, and borderless nature.[3] Unlike traditional financial systems, which are subject to regulatory scrutiny and centralized control, cryptocurrencies operate on distributed ledgers, allowing transactions to occur directly between parties without intermediaries. This decentralization reduces the effectiveness of conventional anti-money laundering (AML) and counter-terrorist financing (CFT) measures, as there is no single authority to monitor or block suspicious activity.[4]

Pseudonymity further complicates detection. While all transactions are recorded on public blockchains, wallet addresses do not inherently reveal the identity of their owners. Law enforcement must rely on sophisticated blockchain analysis and, often, external data to link addresses to real-world actors.[5] This opacity is compounded by privacy-focused cryptocurrencies such as Monero and Zcash, which obscure transaction details and make tracing nearly impossible without advanced tools.[6]

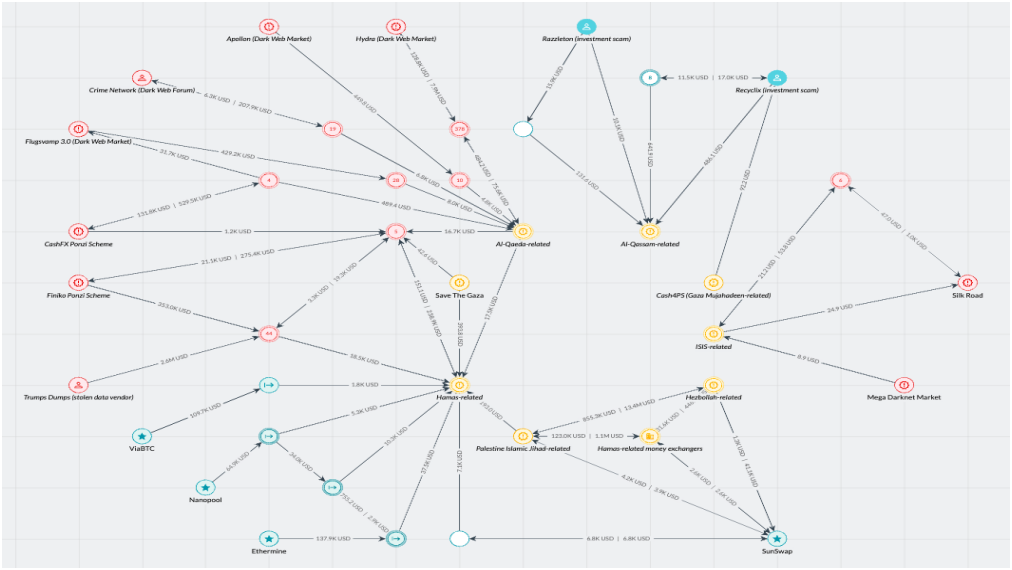
---

[3] "Tackling the Role of Crypto in Terrorist Financing." n.d. IFC Review. https://www.ifcreview.com/articles/2024/january/tackling-the-role-of-crypto-in-terrorist-financing/.

[4] Dyntu, Valeriia, and Oleg Dykyj. 2021. "CRYPTOCURRENCY as an INSTRUMENT of TERRORIST FINANCING." Baltic Journal of Economic Studies 7 (5): 67–72. https://doi.org/10.30525/2256-0742/2021-7-5-67-72.

[5] "Virtual Currencies and Terrorist Financing: Assessing the Risks and Evaluating Responses – European Sources Online." 2018. Europeansources.info. 2018. https://www.europeansources.info/record/?p=512089.

[6] "TERRORIST FINANCING in the DIGITAL AGE: AN ANALYSIS of CRYPTO CURRENCIES and ONLINE CROWD FUNDING." 2024. Journal of Terrorism Studies 6 (2). https://doi.org/10.7454/jts.v6i2.1080.



Graph showing extremist groups receiving funds from a range of sources. (Source:Elliptic)

Emerging Trends in Cryptocurrency Use by Terrorist Groups

While the overall scale of cryptocurrency use in terror financing remains limited compared to traditional methods, there is clear evidence of growing interest and sophistication among terrorist groups. Early uses were experimental and small-scale, but recent years have seen a diversification in both the types of cryptocurrencies used and the methods of fundraising and value transfer.

One prominent trend is the use of social media and encrypted messaging platforms to solicit donations. Groups such as Hamas's al-Qassam Brigades have run high-profile campaigns on platforms like Telegram and Twitter, providing supporters with wallet addresses to send funds in Bitcoin and other cryptocurrencies.[7] These campaigns are often accompanied by instructions on how to avoid detection, such as using unverified accounts or privacy coins. Blockchain analysis has revealed that once received, these funds are frequently converted into fiat currency or used to purchase goods and services, making them harder to trace and seize.

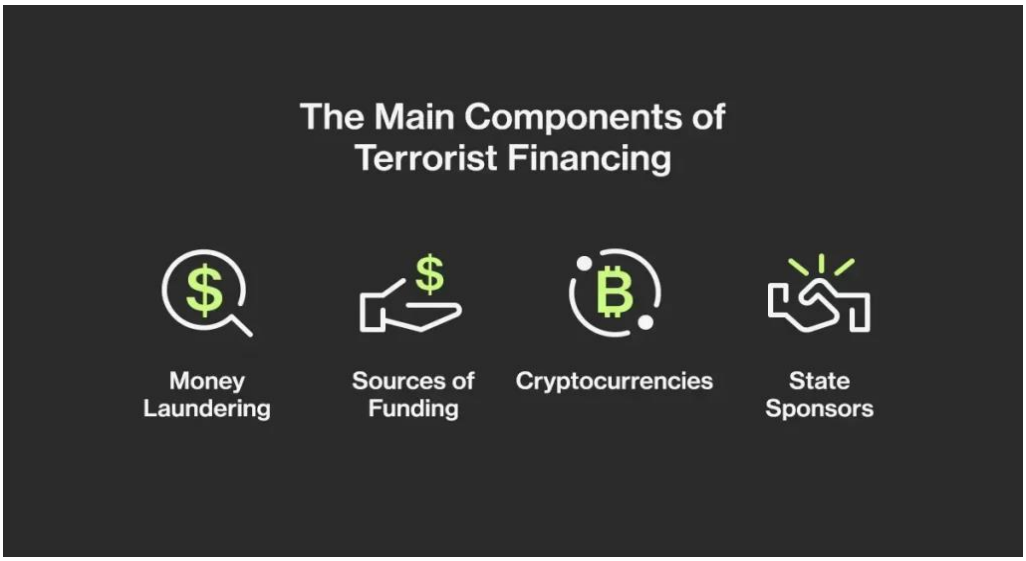
[7] Elliptic. n.d. "How Terrorist Groups Are Exploiting Crypto to Raise Funds and Evade Detection." Www.elliptic.co. https://www.elliptic.co/blog/how-terrorist-organizations-are-exploiting-crypto-to-raise-funds-and-evade-detection.

Source: TRM Labs

Another trend is the adoption of stablecoins, such as Tether (USDT), which are pegged to fiat currencies and offer price stability. Stablecoins reduce the risk of value loss due to the volatility of assets like Bitcoin, making them more attractive for both donors and recipients.[8] Terrorist organizations have also begun to use decentralized finance (DeFi) platforms and decentralized exchanges, which allow for peer-to-peer trading without the oversight of centralized entities. These platforms further complicate efforts to monitor and disrupt illicit flows, as they often lack robust KYC (Know Your Customer) processes.[9]

[8] "Tackling the Role of Crypto in Terrorist Financing." n.d. IFC Review. https://www.ifcreview.com/articles/2024/january/tackling-the-role-of-crypto-in-terrorist-financing/.

[9] "Terrorist Financing: Hamas and Cryptocurrency Fundraising." 2025. Congress.gov. 2025. https://www.congress.gov/crs-product/IF12537.



Source: TRM Labs

There is also evidence of terrorist groups leveraging online crowdfunding and the dark web for fundraising. Some groups have published detailed guides on how to donate using cryptocurrencies, highlighting the perceived security and anonymity of these transactions. While large-scale use remains rare, the increasing technical sophistication of these groups suggests a willingness to experiment with a range of digital assets, including privacy coins and even non-fungible tokens (NFTs) for propaganda and fundraising purposes.[10]

Realities and Limitations: The Actual Scale of the Threat

Despite the high-profile nature of some cases, it is important to contextualize the actual scale of cryptocurrency-enabled terror financing. Most terrorist funding still occurs through traditional means-cash, hawala networks, charities, and front companies-because these methods are well-established, familiar, and less dependent on technical infrastructure.[11] The use of cryptocurrencies

[10] Elliptic. n.d. "How Terrorist Groups Are Exploiting Crypto to Raise Funds and Evade Detection." Www.elliptic.co. https://www.elliptic.co/blog/how-terrorist-organizations-are-exploiting-crypto-to-raise-funds-and-evade-detection.

[11] "Terror on the Blockchain: The Emergent Crypto-Crime-Terror Nexus | START.umd.edu." 2024. Umd.edu. 2024. https://www.start.umd.edu/publication/terror-blockchain-emergent-crypto-crime-terror-nexus.

by terrorist groups is, to date, largely opportunistic and limited in volume, often supplementing rather than replacing conventional channels.

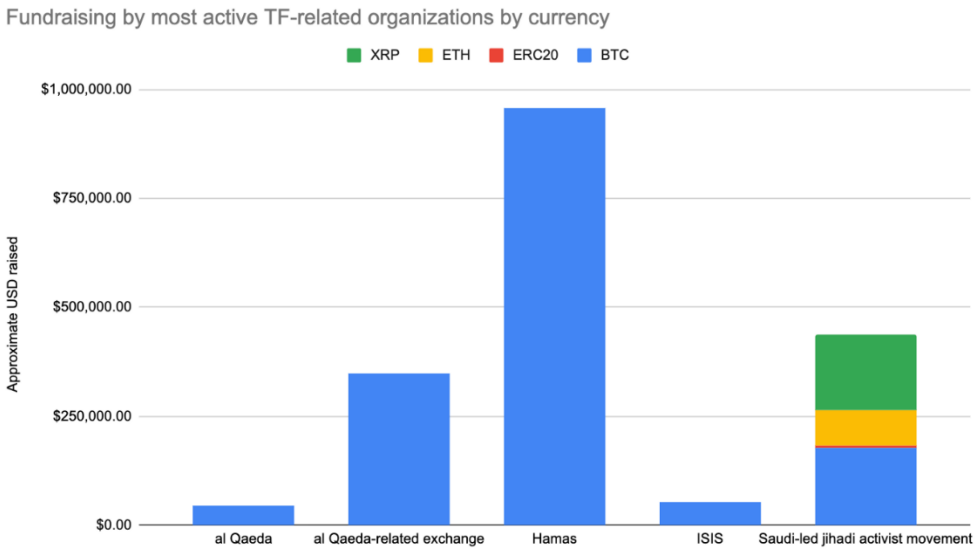
Several factors constrain the widespread adoption of cryptocurrencies by terrorist organizations. First, converting large sums of cryptocurrency into usable resources without attracting attention remains challenging, especially as exchanges and wallet providers come under increased regulatory scrutiny. Second, technical barriers-such as the need for digital literacy and secure internet access-limit the ability of some groups to fully exploit these tools, particularly in conflict zones with poor infrastructure. Third, the public and traceable nature of most blockchain transactions, while not a complete deterrent, does introduce risks for groups that lack the expertise to properly anonymize their activities.

Nonetheless, the threat is evolving. As cryptocurrencies become more liquid, widely accepted, and technically accessible, the potential for larger-scale abuse increases. The risk is particularly acute for "lone wolf" actors or small cells, who require only modest sums to carry out attacks and can easily slip through the cracks of existing counter-financing systems.

Case Studies: Hamas, ISIS, and Al-Qaeda

The cases of Hamas, ISIS, and al-Qaeda provide concrete examples of how terrorist organizations are integrating cryptocurrencies into their financial operations. Hamas, for instance, began openly soliciting cryptocurrency donations in 2019, using its website and social media to bypass international sanctions and access global support networks.[12] The al-Qassam Brigades published detailed instructions for supporters on how to donate Bitcoin anonymously, and blockchain analysis has shown that these campaigns have raised significant sums, though still modest compared to the group's overall budget.

[12] Elliptic. n.d. "How Terrorist Groups Are Exploiting Crypto to Raise Funds and Evade Detection." Www.elliptic.co. https://www.elliptic.co/blog/how-terrorist-organizations-are-exploiting-crypto-to-raise-funds-and-evade-detection.



Source: Coinbase

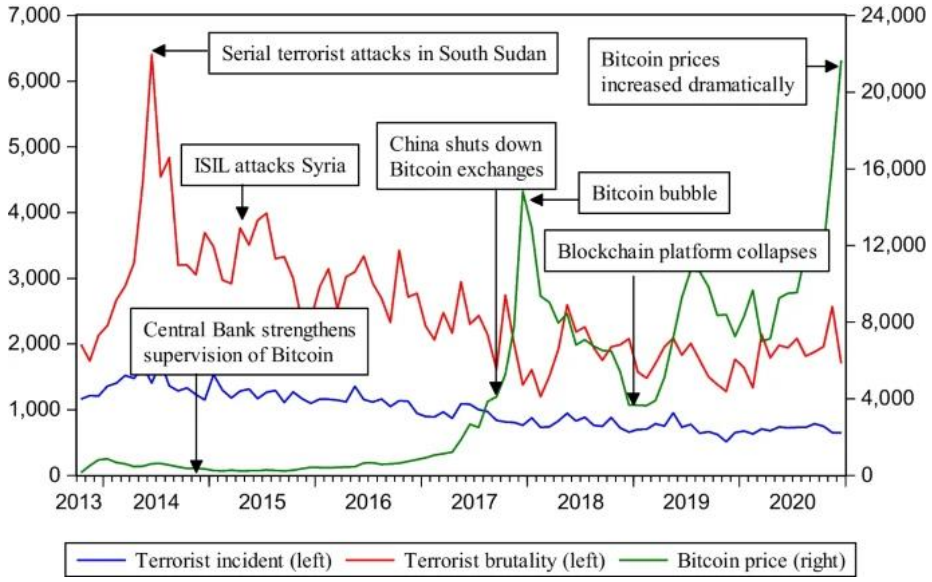
ISIS and its affiliates have also experimented with cryptocurrencies, particularly for fundraising and value transfer in regions where traditional banking is inaccessible or heavily monitored. There are documented cases of ISIS supporters in Indonesia and the United States using Bitcoin to fund operations, as well as reports of the group's use of privacy coins to further obscure transactions. Al-Qaeda-linked networks have similarly used cryptocurrencies for fundraising, often combining them with other illicit activities such as cybercrime and extortion.

These cases illustrate both the potential and the limitations of cryptocurrencies for terror financing. While they offer new avenues for fundraising and value transfer, they are not yet a primary channel for most groups. However, the willingness of these organizations to innovate and adapt suggests that the threat could grow as the technology matures and regulatory gaps persist.

Regulatory and Law Enforcement Responses

The growing awareness of the risks posed by cryptocurrencies has prompted a range of responses from governments, international organizations, and the private sector. Regulatory bodies such as the Financial Action Task Force (FATF) have issued guidelines requiring virtual asset service providers (VASPs)-including exchanges and wallet providers-to implement robust AML/CFT

measures, including KYC protocols and the reporting of suspicious transactions.[13] The European Union's Fifth Anti-Money Laundering Directive (5AMLD) brought crypto exchanges and custodial wallet providers within the scope of AML regulation, marking a significant step toward greater transparency and oversight.[14]



The trends of terrorist incidents, terrorist brutality, and Bitcoin price[15]

Law enforcement agencies have increasingly turned to blockchain analytics tools to trace illicit flows, map financial networks, and identify patterns indicative of terror financing. These tools have enabled high-profile seizures of cryptocurrency assets linked to terrorist organizations, such as the U.S. Department of Justice's confiscation of millions of dollars in crypto from accounts

[13] Center for a New American Security. 2019. "Terrorist Use of Virtual Currencies." Cnas.org. 2019. https://www.cnas.org/publications/reports/terrorist-use-of-virtual-currencies.

[14] "Terrorist Financing: Hamas and Cryptocurrency Fundraising." 2025. Congress.gov. 2025. https://www.congress.gov/crs-product/IF12537.

[15]Song, Yu, Bo Chen, and Xin-Yi Wang. 2023. "Cryptocurrency Technology Revolution: Are Bitcoin Prices and Terrorist Attacks Related?" Financial Innovation 9 (1). https://doi.org/10.1186/s40854-022-00445-3.

associated with al-Qaeda and ISIS.[16] Public-private partnerships have also become essential, as collaboration between governments, blockchain companies, and financial institutions enhances the collective ability to detect and disrupt illicit activity.

Despite these efforts, significant challenges remain. The rapid pace of innovation in the crypto sector often outstrips the ability of regulators and law enforcement to keep up. Privacy coins, mixers, and decentralized platforms continue to present formidable obstacles to tracing and enforcement. Moreover, the global and borderless nature of cryptocurrencies means that effective regulation requires international cooperation and harmonization of standards-something that remains a work in progress.

Broader Implications and the Road Ahead

The convergence of cryptocurrencies and terror financing is emblematic of the broader challenges posed by emerging technologies in the security domain. On one hand, digital assets offer significant benefits for legitimate users, including financial inclusion, efficiency, and innovation. On the other, they create new vulnerabilities that can be exploited by malicious actors, from terrorists and criminals to rogue states.[17]

The future trajectory of this threat will depend on several factors. The continued evolution of privacy-enhancing technologies, the adoption of cryptocurrencies in regions with weak regulatory oversight, and the integration of digital assets into the broader financial system all have the potential to increase the risks associated with terror financing. At the same time, advances in blockchain analytics, greater regulatory clarity, and enhanced international cooperation offer hope for mitigating these risks.

[16] "Virtual Currencies and Terrorist Financing: Assessing the Risks and Evaluating Responses – European Sources Online." 2018. Europeansources.info. 2018. https://www.europeansources.info/record/?p=512089.

[17] Dyntu, Valeriia, and Oleg Dykyj. 2021. "CRYPTOCURRENCY as an INSTRUMENT of TERRORIST FINANCING." Baltic Journal of Economic Studies 7 (5): 67–72. https://doi.org/10.30525/2256-0742/2021-7-5-67-72.

Policymakers face the difficult task of balancing the promotion of innovation with the imperative to protect national and international security. This requires not only robust regulation and enforcement, but also ongoing dialogue between the public and private sectors, investment in technical capabilities, and a willingness to adapt to the rapidly changing landscape of digital finance.

Conclusion

Cryptocurrencies have opened a new frontier in the fight against terrorist financing, offering both opportunities for legitimate economic development and significant challenges for global security. While the scale of crypto-enabled terror financing remains limited, the trend is unmistakable: terrorist groups are experimenting with and, in some cases, successfully exploiting digital assets to raise, move, and obscure funds. The international community must remain vigilant, investing in both technological and regulatory solutions to stay ahead of this evolving threat. As the digital financial ecosystem continues to grow and mature, so too will the tactics of those who seek to abuse it for violent ends. Only through sustained, coordinated, and innovative responses can the risks be effectively managed and the promise of cryptocurrencies realized for the benefit of all.