

5**The Anatomy of Digital Crypto-Terror Networks: Cryptocurrency, Money Laundering and Architecture of Contemporary Terror Financing****Mrinal Mishra***

Researcher, Indian Institute of Technology, Patna & Faculty, National Forensic Sciences University.

*Corresponding Author: mrinal_25s21res66@iitp.ac.in**Abstract**

Cryptocurrencies are no longer just a part of the literature concerning the financing of terrorism but are now part of the daily routine of prosecutors and financial intelligence units. Its role in the financial landscape at large, however, is not widely understood and is frequently exaggerated. This chapter will cover the ways in which terrorist groups and their sponsors have used digital assets to solicit funds, transport funds, store funds, and spend funds. It starts with technology itself. Today, more cryptocurrencies exist in USD-denominated stable coins than in Bitcoin, as a cryptocurrency is a bearer instrument recorded on a shared public ledger and transferred without the use of a bank. Technical properties form the basis and starting point for this paper, as they determine not only why the channel is attractive to the illegal users, but also why it exposes them. The chapter then situates digital assets within the comfort zone of the traditional three-stage model of money laundering, demonstrating what placement, layering and integration look like on a blockchain, as well as collating enforcement records and analytics to draw a connection between virtual assets and terrorist financing. Case reconstruction follows. It refers to the Al-Qassam Brigades of Hamas, Palestinian Islamic Jihad networks, and Al-Qaeda and Islamic State networks via Turkey, Central Asia and Southeast Asia, as well as the Iran-aligned architecture that supports Hezbollah, Hamas and the Houthis. These cases are then grouped into a 4-layer model of solicitation, custodial concentration, obfuscation and cash-out, which is applicable to otherwise diverse organizations. The record only has one paradox. The publicly accessible blockchain that affords financiers access and freedom from banks also leaves a clear paper trail that has helped make it easy to attribute, seizure and prosecution many times. Finally, the chapter finds that donor financing for fundraising and the use of state-proxy treasury are separate issues that require separate solutions, and that policy to combat the financing of terrorism should be based on the actual volume of financing documented in transactions, not the numbers generated in the immediate aftermath of an attack.

Keywords: Terror Financing, Cryptocurrency, Money Laundering, Blockchain, Sanctions Evasion.

Introduction

In August 2020, the United States Department of Justice (DOJ) stated it had shut down over 150 cryptocurrency accounts associated with the armed branch of the Hamas terror movement. It had been seeking "Bitcoin donations" from its supporters publicly and on social media. It has educational videos to tell donors that these funds were untraceable. They were wrong, and the seizure proved it. This case is a good place to start, as it, in miniature form, contains the argument of this chapter. For the last 20 years, in fact, the investigation of terrorist financing has focused on three channels: money moved by couriers, value transferred via hawala and other informal money remittance methods, and money transferred through charities or banks. A fourth channel, as part of indictments and seizure orders, emerged around 2015. Armed groups had started to ask for, and to receive, cryptocurrency. Why shouldn't it be? No bank account, no correspondent bank is required for a transfer of Bitcoin or of a dollar-pegged stable coin like Tether. It takes only minutes to settle. Can be sent via a regular cell phone and disregards borders, at least sanctions lists. These are indeed real benefits for an organization that can't access the banking system.

Hamas' al-Qassam Brigades have been the first to test them from 2019. Less significant campaigns were conducted by Islamic State facilitators in Turkey, Central Asia and Southeast Asia. Iran's Islamic Revolutionary Guard Corps has been much more active since 2023, providing digital assets for Hezbollah, Hamas, and the Houthis (Chainalysis, 2026). There's the rub, and it's everywhere that goes. The same feature that is useful to a financier is the same feature that exposes him in a public blockchain. Each transfer is recorded on a permanent, time-stamped and open record that all can access. When you give someone a cash gift, you leave a memory. Blockchain payment is recorded, is unalterable and can be revisited years later with tools which didn't exist at the time of payment. That is the reason that the Department of Justice, Israel's National Bureau for Counter Terror Financing, and the United States Treasury's sanctions authorities have been able to trace the networks in such a fine-grained manner that is usually reserved for cash investigations.

The chapter is organized around two questions. For one, what does a crypto terror network look like when the record is reconstructed based on court filings and seizure orders, and not from the numbers that circulate in the days immediately following a seizure? Second, what are the common characteristics that emerge from organizations with no ideology or geographical location which would warrant them being studied together? These are answered in the chapter's additional sections. Technology is explained in section two. Third section situates the standard model of money laundering and outlines the evidence of the links between digital assets and terrorist financing. The jihadist cases are explored in the fourth section while the Iran and the proxy question is then addressed in the fifth section. Case histories material

is used to construct a four-layer model, while the policy implications are teased out in the last section along with a summary of the argument is provided in conclusion.

The scholarship remains sparse, in comparison with the policy attention the subject enjoys. In the pre-binding-ISFS regime period, Kfir (2020) laid out the initial conceptual argument that a rapidly evolving technology of payments could not coexist with the lack of a binding international regime for digital assets. Later, Akcinaroglu and Shi (2025) provided the first empirical statistical test in large samples, which indicated that the growing trend of cryptocurrencies slightly increases the opportunities available for armed groups, but volatility and increased regulation have the opposite effect. This chapter bases its narrative on the primary enforcement documents of the period, and from these to develop a model which it can apply to those cases not specifically addressed by it.

Understanding Cryptocurrency

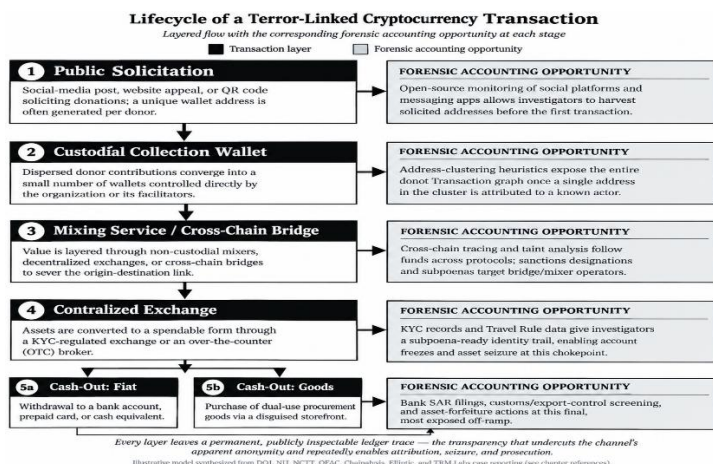
Part of what has led to much confusion in public debate regarding crypto-terror funding is an imprecise understanding of technology. This section, therefore, begins by defining what is a cryptocurrency, in common parlance, before the chapter moves on to its improper uses. Begin with an issue that the technology was designed to address. Digital files are able to be copied. In the case of money, if it were a file, there would be no barrier to consuming twice, hence the traditional payment systems are based on a trustworthy institution that maintains an authoritative record of who has what, typically a bank. The design was released by the pseudonym Satoshi Nakamoto did. The traditional way to maintain such a private ledger would be for each bank to keep their own copy, but thousands of independent computers hold copies of a shared copy and agreement among the computers is how the record is settled (Nakamoto, 2008). It is that common ledger that is the blockchain.

This has three implications, and each is relevant to illicit finance. First, that the holdings are not managed by an identity but rather by a key. An address on a blockchain is a string of characters. It is not a name. Anyone with the corresponding private key can transfer the money, just like anyone with a key can unlock a padlock. Cryptocurrency is thus more like cash in bearer form than a bank deposit. Nothing in the address itself indicates the identity of its owner. The second is that there is no middle institution. When one privately held wallet pays for another wallet, no regulated company is involved and none of the reporting responsibilities that banks have are activated. The third is that value can be transferred via automation scripts. These involve mixing services, which combine funds from numerous users and withhold distinct units to sever the link between the sender and receiver, and bridges that transfer value across disconnected blockchains, as well as decentralized exchanges, where one asset is traded for another without any company holding the customer funds.

There is one difference which runs through the remainder of the chapter and it is good to correct it early on: Where the assets of a user are stored by a centralized exchange, the exchange is a virtual asset service provider and, in most countries, first of all have to identify the users, keep records, and comply with legal orders. It can bring balance to a standstill. There are no such firm and no such option where assets exist in a privately held wallet. Much of the counter-financing effort described below involves driving illicit flowing into the first situation, where enforcement means. The market has also evolved in a manner that influences the threat. The Bitcoin asset most popular in the older literature is volatile and completely transparent. Dollar-pegged stablecoins like Tether are easier to buy and sell, maintain a stable price, and have largely replaced Bitcoin in many areas of the illegal economy, accounting for approximately 84 per cent of all illicit transaction value on public blockchains (Chainalysis, 2026). Most of that activity is on the low-fee Tron network. The privacy coins, as examined here, are still marginal because of thin liquidity and limited exchange support, which are unintentional aspects of their operation, in addition to the intended privacy aspects of hiding amounts and counterparties.

The end product is a channel that is anything but anonymous. In and of themselves, addresses are not associated with names but can be made linkable by a customer record at an exchange, a published donation appeal, an informant, or a simple error. When one of the addresses in a group is linked to a known actor, analysts can start working their way out and unravel the entire chain of transactions, such as payments going back years. Terrorist financiers are not provided with a frictionless channel to cryptocurrency. It provides them with a clear one, for trading exposure now. Several organizations eventually concluded that this was a bad deal, as demonstrated in a later section.

Figure 1: Lifecycle of a terror-linked cryptocurrency transaction, showcasing cyber forensics accounting opportunity available to investigators at each level



Money Laundering and Crypto Terror Network

There are two different offences—money laundering and terrorist financing, as many tend to get them mixed. Money is criminal in origin; laundering is done to hide the origins of the money trail. Terrorist financing obscures the use of money, and often it is legitimate in the first place: a donation is not off-limits until its recipient is identified. The two have in common the middle part of the operation, the part in which the value has to be transferred and camouflaged before it can be utilized. The standard model breaks it down into three stages, each of which has a specific manifestation on a blockchain. The process of placing value in the financial system is called placement. In the cash economy, it translates to putting notes with a bank or giving to a hawala agent. On a blockchain, it refers to the purchase of the asset: When a supporter purchases Bitcoin or Tether in an exchange, for instance, he or she sends the currency to an address listed in an appeal. Typically, a regulated firm is involved at this stage and hence donor ID is most likely to be recovered here.

Layering involves the transfer of value from one transaction to the next in order to hide the source of funds. Within a blockchain, this is achieved through the use of mixers, bridges and decentralized exchanges, as well as by splitting large amounts into numerous small transactions. Launderer patterns are evident in laundering services, where there are significantly more destination wallets than source wallets for large transfers and a significant increase in smaller and medium transactions between money in and money out. This is the standard structuring or smurfing activity, but on a new platform (Chainalysis, 2026).

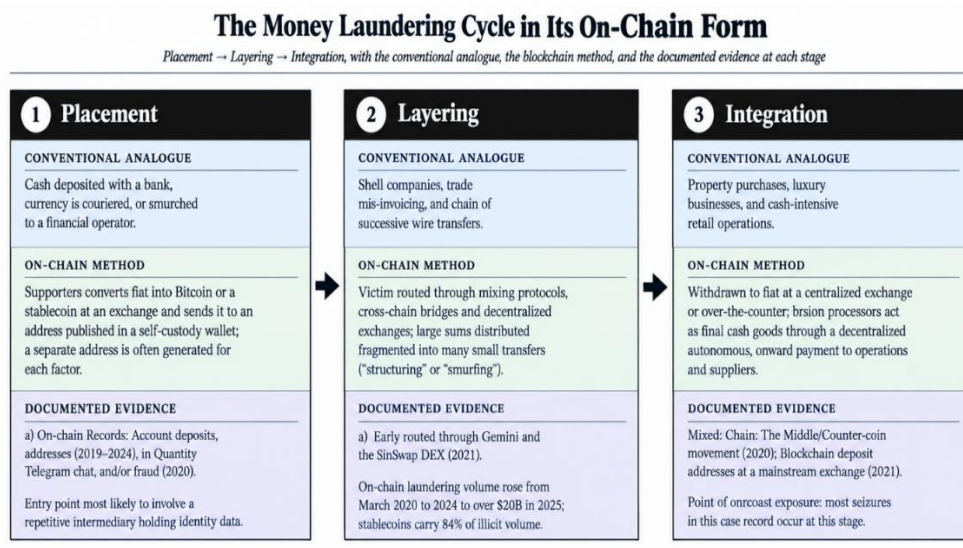
Integration is the reconversion of the value to apparently normal uses, such as cash withdrawals from an exchange, purchases by a front company, payments to operatives and suppliers. On-chain laundering has significantly increased in size. The value sent through identified laundering services increased from approximately \$10 billion in 2020 to over \$82 billion in 2025, and at least \$154 billion was sent to illicit addresses across 2025. Two qualifications matter. The total amount of that is dominated by fraud, theft and sanctions evasion, and terrorist financing is a small part. Illegitimate transactions also only make up less than one per cent of the number of transactions in cryptocurrencies that are measured (Chainalysis, 2026). It's not all criminal technology. The issue is what the criminal minority does with it and how visible is the minority?

Thus, the proof of the association of digital assets with terrorist financing is not through volume, but through the regularity of documented use. Virtual assets are one of several methods in use, and the most recent assessment by the Financial Action Task Force placed virtual assets in the same class as cash couriers, hawala, money transfer services, online payment services and social-media crowdfunding. According to the same assessment, 69 per cent of the jurisdictions assessed exhibited significant or structural deficiencies in terms of investigating and

prosecuting the financing of terrorism (FATF, 2025a). That discovery indicates that institutional capacity is the problem, and not any real challenge in the traceability of the technology, and the United Nations Office of Counter-Terrorism has come to a similar conclusion.

Laundering enforcement efforts have yielded some interesting results. In May 2022, the United States Treasury designated the mixer Blender.io, and in August 2022, the mixer Tornado Cash was designated, which had processed over \$7 billion since 2019 (U.S. Department of Treasury, 2022). In March 2025, Tornado Cash was delisted from the sanctions list following litigation that automated contracts owned and controlled by no one do not fit well within a designation regime that is designed for people, companies and property (U.S. Department of Treasury, 2025). There is a true ceiling in this method—software that no one otherwise uses is difficult to approve, regardless of how well known its utility is. The focal point of control has shifted to the asset level. Unlike bitcoin, stablecoins can be issued by identifiable companies that have the ability to freeze balances at named addresses. Within weeks of the 2023 seizure order issued by NBCTF, Tether has frozen several addresses associated with the Hezbollah and Quds Force Network (Chainalysis, 2023a). In the past, as illegal activity migrated to more stable coins, it migrated to the one class of digital asset that has an off switch.

Figure 2: The three-stage money laundering cycle in its on-chain form, with the conventional analogue, the blockchain method and the documented evidence at each stage.



Detection concentrates where the chain touches a regulated intermediary — the exchange, the over-the-counter broker, and the stablecoin issuer.

The middle stage, conducted through automated protocols with no conventional operator, offers investigators the most direct purchase.

Sources: synthesized from UN, FINCEN, OFAC, Chainalysis, TRM and extra reporting on crypto laundering.

Case Records

Al-Qassam Brigade (2019-2023)

Background. The military branch of Hamas solicited Bitcoin donations on its website and Telegram channels starting about 2019, providing a different receiving address for each donor and giving incorrect advice that would lead donors to believe the donations were untraceable. **Enforcement.** The Department of Justice seized over 150 accounts and announced it had seized the largest amount of cryptocurrency in a terrorism case in August 2020. The same action was applied to two additional schemes: a Telegram-based money laundering operation, used by two Turkish nationals, Mehmet Akti and Husamettin Karatas, who were working for an affiliate of Al-Qaeda, and a fake protective-equipment website, FaceMaskCenter.com, operated by Islamic State facilitator Murat Cakar during the Covid-19 pandemic. In July 2021, Israel's NBCTF has seized additional wallets. **Outcome.** The organization said in April 2023 that it was halting cryptocurrency fundraising because there is an "unacceptable risk" of the funds being tracked by governments. **Why it matters.** The first group to use the channel left it voluntarily over five months prior to the attacks on 7 October 2023, due to ledger transparency making the campaign an asset rather than a liability (U.S. Department of Justice [DOJ], 2020; NBCTF 2021; Chainalysis, 2023b).

October 2023 Figures and their Corrections

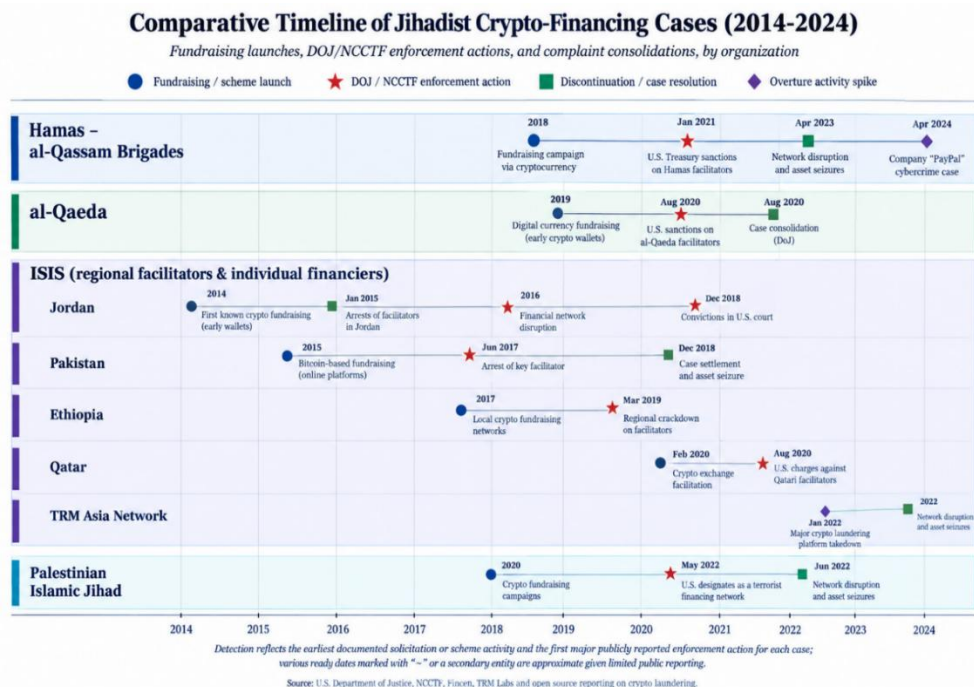
Since 7th October 2023, many media outlets have reported that Hamas-affiliated actors have raised approximately \$130 million in cryptocurrency since August 2021. The firm that the reporting was based on issued a public correction. It was not the amount of funds raised by or belonging to any one organization, but gross transaction volume passing through wallets that ended up being linked to Palestinian Extremist. In fact, funds received by Hamas-affiliated channels since 7th October exceeded \$21,000, until the addresses were frozen by exchange and stablecoin issuers (Elliptic, 2023a). The episode is not just about terrorist financing; it's about teaching a lesson about reading the data on the blockchain. Gross inflow to a group of wallets is the total amount of money that went through the wallets, including money that was moved multiple times between addresses in the same group. Taking that number as an estimate of the money available for operations gives estimates off by many orders of magnitude and those estimates get into policy debate quicker than the corrections that follow.

Al-Qaeda and Islamic State

In the action recounted above, Al-Qaeda's 2020 operation was a mix of a fake charitable organization and solicitation via the Telegram network, with Bitcoin transferred for weaponry and funding operations in Syria being falsely identified as humanitarian aid. Islamic State's use of cryptocurrency has been more diffused and

more individual. In 2014 and 2015, the then teenaged Ali Shukri Amin published instructions on how to fund the Islamic State using bitcoin in a pro-IS blog and pleaded guilty to providing material support (DOJ, 2015). In 2018, Zoobia Shahnaz of Long Island was found guilty after taking several loans for approximately \$85,000 and then using the funds to send money to those linked to the Islamic State in Pakistan, China and Turkey (CNBC, 2018). From an operative overseas, Mohamed Elshinawy (Md.) received crypto currency and cryptocurrency transfer payments via a disguised payment platform for a planned attack, receiving a twenty-year sentence (DOJ, 2018). A later pattern, more organized, developed throughout Central and South Asia. In 2022 and 2023, Pro-ISIS fundraising transacted approximately \$2 million worth of Tron-based Tether; money was transferred via an exchange in Indonesia to the tune of more than \$517,000 in a span of one year, while Pakistani affiliates were able to collect approximately \$40,000 in 12 months; the Al-Azaim Foundation in Afghanistan received transfers of about \$10,000. One campaign appeared to be a response to the Turkey-Syria earthquake of February 2023. The case study highlights how exchange record-keeping traces a senior fundraiser, Shamil Hukumatov to his arrest in Turkey in June 2023.

Figure 3: Comparative timeline of documented jihadist cryptocurrency financing cases, 2014-2024, coded by organization and marking fundraising launches, seizure actions and campaign closures.



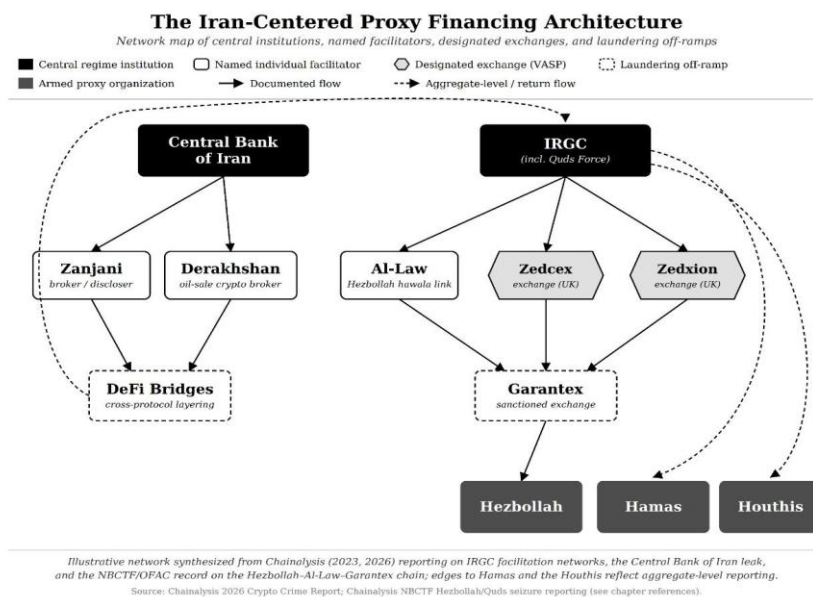
State-Proxy Financing: Iran and Its Militias

The above cases are small potatoes compared to the state-supported architecture that has been developed since 2023. By the end of 2025, addresses associated with IRGC facilitation networks received more than half of all value received by Iranian cryptocurrency services, receiving more than \$3 billion in value throughout the year, compared to approximately \$2 billion in the previous year. That's a conservative figure as it doesn't even account for the United Kingdom-registered exchanges Zedcex and Zedxion, which were sanctioned in January 2026 and were determined to have handled tens of billions of dollars in transactions linked to IRGC-affiliated networks. By 2025, Iran's cryptocurrency sector had been estimated to be valued at \$7.78 billion, with one of the aims of the architecture being to support regional militias such as Hezbollah, Hamas and the Houthis (Chainalysis, 2026).

Below are two enforcement actions that illustrate how the system operates on an individual payment basis, not a total basis. On 27 June 2023, the NBCTF has disrupted an operation to transfer approximately \$1.7 million in Tether from a group of forty (40) addresses, which included both Hezbollah and the Quds Force. The funds had been transferred from financial facilitators to a wallet account of the Syria-based hawala operator Tawfiq Muhammad Said Al-Law, who then transferred the funds to an address belonging to Hezbollah at a mainstream exchange. In March 2024, Al-Law identified himself, and the address was placed on the sanctions list (Chainalysis, 2023a). In a separate development, documents published at the end of 2025 by the designated Iranian businessman Babak Morteza Zanjani revealed cryptocurrency addresses of the Central Bank of Iran, which were linked to a pipeline that involved translating deposits into stablecoins, passing them through automated bridges, and returning them to IRGC-related entities. We've also identified another individual, Alireza Derakhshan, who was involved in over \$100 million in cryptocurrency assets associated with Iranian oil sales from 2023 to 2025 (Chainalysis, 2026).

This layer is not just bigger than the crowdfunding cases, it's fundamentally different. The Iran-aligned system focuses on a handful of exchanges and brokers near the central bank, whereas the Al-Qassam Brigades collected thousands of small public donations. It's more like a sort of sanctioned state parallel settlement system that provides its own buying and serves the budgets of its proxies. As Section seven will show, the two patterns are not treated the same in terms of remedies.

Figure 4: The Iran-Centered proxy financing architecture, mapping central institutions, named facilitators, designated exchanges and laundering off-ramps.

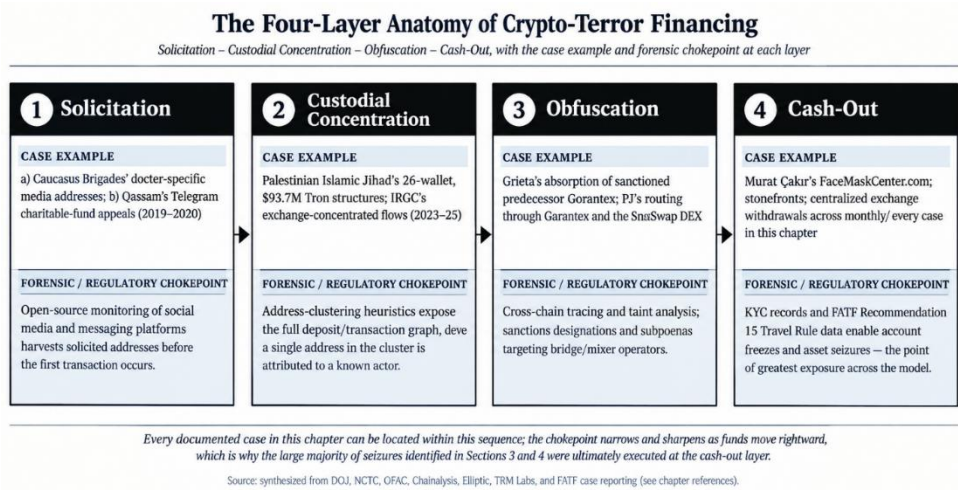


A Four-Layer Model

The solicitation layer is the one that faces the public, the one that asks for value, such as donor-specific addresses, a charity front, instant messaging apps, or an appeal on social media platforms. This layer is the most exposed in the chain as it is supposed to be seen by the intended audience. All cases in this chapter were detected here. The custodial concentration layer is a layer that collects and consolidates dispersed contributions in a handful of wallets under the control of a custodial entity. This is where the power of clustering analysis really lies: An address that shows up on thousands of small payments is a fingerprint of behavior. The IRGC concentrated on the exchanges and the PIJ's 26 wallets are evidence of the layer at scale. The obfuscation layer includes mixers, bridges, decentralized exchanges and rebranded successor exchanges, layering in value and obscuring the apparent connection between origin and destination. From the routing of PIJ funds via Garantex and SunSwap, two facilitators who moved funds with no layering at all were traced within a few months. The cash-out layer is where the holdings are converted into cash, goods or services, typically via an exchange, a broker or a fake front store like Cakar's. This is the most highly exposed step in the entire model and the step where the majority of seizures occurred in this chapter, an exchange must identify its customers.

Two aspects of the model should be emphasized. The layers are not necessarily sequential; a state-backed campaign can have an institutional step where solicitation and concentration occur in the same place, and a small campaign may not even have an obfuscation stage. All that is being asserted is that someone must carry out each function, and that there is a distinct imprint or signature on each execution. The second feature is that investigative leverage is unevenly spread. It is weakest in the middle, where automated systems, with no accountable owner, operate and are strong at the two ends, where a network has to talk to its supporters and value has to be brought into the regulated economy. Measures that do not consider this distribution investment where the technology offers least purchase.

Figure 5: The four-layer anatomy of crypto-terror financing, annotated with the case example and the forensic or regulatory chokepoint at each layer



Policy Implications

The first one is about measurement. Overall, relative to known methods of financing, the role of cryptocurrency has been smaller than originally thought following attacks. One example of this is the confusion over the volume of transfers on PIJ wallets as funding for Hamas in October 2023 (Elliptic, 2023a). Figures of 'wallet-inflow' should be viewed as a ceiling in potential funding, rather than an indication of how much an organization might spend. This is NOT to be complacent. It's an argument for accuracy, as resources deployed based on numbers are resources diverted from the most profitable channels to channel terrorist resources. The second relates to differentiation. Donor-funded fundraising and state-proxy treasury operation are two distinct issues and the instruments and solutions that work for one are not suitable for the other. Where value meets a regulated firm is where customer identification at exchanges, cooperation by social-media and messaging

platforms, and the travel rule (FATF, 2025b) extended to VASPs, help address the issue of fundraising. State-proxy operations require designations targeting exchanges, brokers and infrastructure providers. In its analysis of the al-Qassam campaign, the Congressional Research Service (2023) came to a similar conclusion, noting that it is "traceability, not prohibition, that has determined the fate of a financing channel when it comes into contact with modern blockchain analysis.

Third has to do with the location of control. The delisting of Tornado Cash was a testament to the bluntness of designation as a tool against automated software and the freezing of addresses on the blockchain linked to Hezbollah by a stablecoin issuer proved that a centrally issued asset has a switch that can be turned off, and a decentralized one does not. The freezing powers of issuers should be specifically addressed in international guidance and not be left to the will of companies; this is because the focus of illegal activity has been on stable coins. The fact that FATF has found that most of the jurisdictions assessed were weak in investigating terrorist financing points to the fact that the issue is institutional rather than technical after all. Many states don't have the capacity to act on the evidence already available on public ledgers (FATF, 2025a).

Conclusion

It is not a picture of an ungoverned financing frontier. It is more accurate and more effective. While blockchain-based transfers do provide some tangible, albeit limited, benefits to terrorist funders in reach and bank independence, these benefits have been outweighed on many occasions by the fact that blockchain technology also creates an indelible record. The most telling indication of the organizations giving up on cryptocurrency fundraising was the decision made by the Al-Qassam Brigades to discontinue the practice in 2023. Much more ominously is the state-proxy level where the IRGC has developed settlement facilities for Hezbollah, Hamas and the Houthis at a level now running into billions of dollars annually and continuing to grow. A counter-financing strategy for the remainder of this decade must balance both realities: the necessity to maintain a constant level of vigilance at the exchange level to combat the comparatively modest amount of organization fundraising, alongside a sanctions-based disruption of the infrastructure which allows the central bank of a given state, in practice, to be a financing mechanism for its proxies. The problem of both is primarily an institutional issue, not a technical issue. Whatever Ledger records are what is recorded, and what is recorded is already more than what we can investigate.

References

1. Akcinaroglu, S., & Shi, M. (2025). Exploring the impact of cryptocurrency on terrorism. *Terrorism and Political Violence*, 37(1), 111-135.
<https://doi.org/10.1080/09546553.2023.2275057>

2. Chainalysis. (2023a, June 29). Terrorism financing: Israel seizes \$1.7M in crypto from Hezbollah and Iran's Quds Force.
<https://www.chainalysis.com/blog/israel-nbctf-hezbollah-iran-quds-crypto-seizure/>
3. Chainalysis. (2023b, April 27). Hamas' Al-Qassam Brigades announces end of cryptocurrency donation efforts. <https://www.chainalysis.com/blog/hamas-al-qassam-brigades-cryptocurrency-donations-shutdown/>
4. Chainalysis. (2026). The 2026 crypto crime report. Chainalysis Inc.
5. CNBC. (2018, November 26). New York woman pleads guilty to using bitcoin to launder money for terror group ISIS.
<https://www.cnbc.com/2018/11/26/new-york-woman-pleads-guilty-to-using-bitcoin-to-launder-money-for-isis.html>
6. Congressional Research Service. (2023). Terrorist financing: Hamas and cryptocurrency fundraising (IF12537). Library of Congress.
<https://www.congress.gov/crs-product/IF12537>
7. Elliptic. (2023a). Setting the record straight on crypto crowdfunding by Hamas. <https://www.elliptic.co/insights/setting-the-record-straight-on-crypto-crowdfunding-by-hamas/>
8. Elliptic. (2023b, July 4). Israel seizes crypto wallets worth \$94 million linked to Palestinian Islamic Jihad. <https://www.elliptic.co/blog/analysis/israel-orders-seizure-of-crypto-wallets-worth-94-million-linked-to-palestinian-islamic-jihad>
9. Financial Action Task Force. (2025a). Comprehensive update on terrorist financing risks. FATF-GAFI. <https://www.fatf-gafi.org/en/publications/Methodsandtrends/comprehensive-update-terrorist-financing-risks-2025.html>
10. Financial Action Task Force. (2025b). Targeted update on implementation of the FATF standards on virtual assets and VASPs. FATF-GAFI. <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2025.html>
11. Israel National Bureau for Counter Terror Financing. (2021, July 12). Minister of Defense Benny Gantz signs an administrative order to seize electronic wallets used by Hamas to trade different types of cryptocurrency. <https://nbctf.mod.gov.il/en/Pages/CryptoSeizureEN072021.aspx>
12. Kfir, I. (2020). Cryptocurrencies, national security, crime and terrorism. *Comparative Strategy*, 39(2), 113-127.
<https://doi.org/10.1080/01495933.2020.1718983>

13. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. <https://bitcoin.org/bitcoin.pdf>
14. TRM Labs. (2023, July 21). TRM finds mounting evidence of crypto use by ISIS and its supporters in Asia. <https://www.trmlabs.com/post/trm-finds-mounting-evidence-of-crypto-use-by-isis-and-its-supporters-in-asia>
15. United Nations Office of Counter-Terrorism. (2024). Countering the misuse of virtual assets and virtual asset service providers for terrorism financing purposes. United Nations. https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/unct_cft_va_report_2024_en.pdf
16. U.S. Department of Justice, Office of Public Affairs. (2015, June 11). Virginia teen pleads guilty to providing material support to ISIL. <https://www.justice.gov/archives/opa/pr/virginia-teen-pleads-guilty-providing-material-support-isil>
17. U.S. Department of Justice, Office of Public Affairs. (2018, March 30). Maryland man sentenced to 20 years in prison for providing material support to ISIS and terrorism financing. <https://www.justice.gov/opa/pr/maryland-man-sentenced-20-years-prison-providing-material-support-isis-and-terrorism>
18. U.S. Department of Justice, Office of Public Affairs. (2020, August 13). Global disruption of three terror finance cyber-enabled campaigns. <https://www.justice.gov/archives/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns>
19. U.S. Department of the Treasury. (2022, August 8). U.S. Treasury sanctions notorious virtual currency mixer Tornado Cash. <https://home.treasury.gov/news/press-releases/jy0916>
20. U.S. Department of the Treasury. (2025, March 21). Tornado Cash delisting. <https://home.treasury.gov/news/press-releases/sb0057>.

