



Five myths about cryptoterrorism: understanding trends and modus operandi of terrorism financing through cryptoassets

Cinco mitos sobre criptoterrorismo: entendendo tendências e o modus operandi do financiamento do terrorismo através de criptoativos

Cinco mitos sobre criptoterrorismo: entendiendo tendencias y modus operandi del financiamiento del terrorismo a través de criptoactivos

Jorge, M. Lasmar, PhD.
Rashmi Singh, PhD.

DOI: 10.5752/P.1809-6182.2024v21n1pX-X

ABSTRACT

This article debunks five common myths about crypto terrorism, examining how terrorists exploit digital assets. While the terrorist use of cryptocurrencies is limited and involves small amounts, it extends beyond Bitcoin and leaves detectable traces. To address this evolving threat effectively the misuse, not the assets, should be criminalized.

Keywords: Cryptocurrency; Crypto terrorism; Terrorism financing

RESUMO

Este artigo desmistifica cinco mitos comuns sobre o cripto terrorismo, examinando como os terroristas exploram os ativos digitais. Embora o uso de criptomoedas por terroristas seja limitado e envolva pequenas quantias, ele vai além do Bitcoin e deixa rastros detectáveis. Para enfrentar essa ameaça em evolução de forma eficaz, deve-se criminalizar o uso indevido, não os ativos em si.

Palavras-Chave: Criptomoeda; Cripto terrorismo; Financiamento do terrorismo

RESUMÉN

Este artículo desmiente cinco mitos comunes sobre el cripto terrorismo, examinando cómo los terroristas explotan los activos digitales. Aunque el uso de criptomonedas por parte de terroristas es limitado y abarca pequeñas cantidades, se extiende más allá de Bitcoin y deja rastros detectables. Para abordar esta amenaza en evolución de manera efectiva, se debe criminalizar el uso indebido, no los activos en sí.

Palabras clave: Criptomoneda; Cripto terrorismo; Financiamiento del terrorismo

Introduction

Cryptocurrencies are digital currencies, i.e. a medium of exchange (used to acquire goods or services) or a store of value, that use cryptography (coded information) and blockchain technology (a digital decentralized public ledger) to conduct transactions through a computer network. Unlike traditional currencies and assets, cryptocurrencies and other crypto assets operate in a decentralized manner and do not rely on central authorities such as banks or governments. As a consequence, they have been less subjected to control and regulations although this is quickly changing.

However, in an era in which digital currencies are transforming global finance, the complexities of terrorism financing that relies on crypto assets (crypto terrorism) presents unprecedented challenges. While cryptocurrencies remain a technical and somewhat distant concept for many, recent advancements in artificial intelligence-powered blockchain analysis have shed light on how terrorists exploit these digital assets. Despite this progress, widespread misunderstandings and myths still cloud public perception. By debunking these misconceptions, we can better understand the true trends and tactics of terrorism financing through cryptoassets. In this article, we explore five prevalent myths to gain a clearer understanding of how extremist groups utilize cryptocurrencies, how their strategies are evolving, and the implications for counterterrorism efforts.

Myth 1: The Majority of Terrorist Funding Comes from Cryptoassets

Reality: Limited Adoption Compared to Traditional Methods and Cryptoassets Play a Minor Role

Terrorists and extremist groups use a wide variety of methods to raise, move, and use funds that usually mix licit and illicit sources. These methods employ varying degrees of professionalism and complexity. Examples of terrorism financing from illicit sources include crimes such as online and offline fraud, kidnapping, extortion, tax evasion, contraband, theft, and the misuse of NGOs. Legal sources include donations, self-financing, and even the use of licit companies (LASMAR, 2019). The use of both legal and illegal sources as well as the simultaneous employment of different financing techniques is one of the defining characteristics of terrorism financing (FATF 2015). To avoid disruption, diversity is key. Terrorist groups make sure to employ several different mechanisms to increase their chances of passing unnoticed by the authorities and decrease the impact of any disruption to one or more of their financial activities.

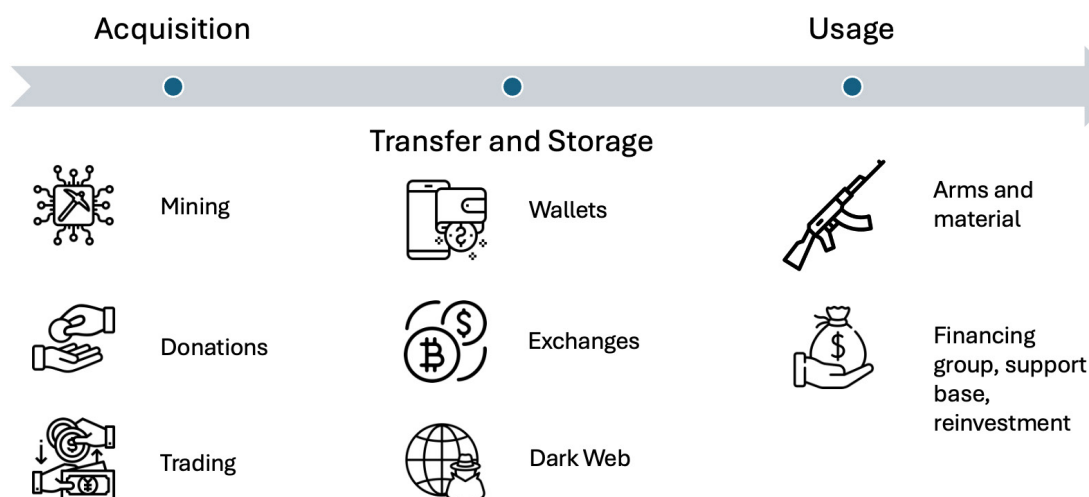
In this context, terrorist groups have been increasingly interested in using cryptoassets to raise, transfer, and use funds. For example, Da'esh (also known as the Islamic State) and Al-Qaida affiliates have been using cryptocurrency in Syrian areas under the control of Hay'at Tahrir al-Sham. We also know that Da'esh affiliates in Asia increasingly rely on cryptocurrencies (CTED, 2024). However, this is not a new phenomenon. The first evidence

of terrorist financing through cryptocurrencies was found in 2014 when American authorities found a Dark Web site called “Fund The Islamic State Anonymously”, which encouraged Da’esh sympathizers to donate Bitcoin (the first widely-used cryptocurrency) to the group. From 2015 onwards, Da’esh stepped up efforts to receive Bitcoin donations, after which other extremist groups started doing the same, as can be seen in Annex I (Timeline of High Profile TF Through Cryptoassets) below.

The timeline demonstrates that terrorist groups are looking into cryptoassets as another tool of terrorism financing. However, despite all the high-profile cases in the media, these instances remain relatively rare and of low volume, especially when compared to the financing of terrorism through traditional methods. To date, most terrorist financing continues to rely on traditional offline methods, both in terms of sources and means of transfer (Chainalysis, 2024). In fact, the use of cryptoassets

for financing terrorism remains limited, even when focusing solely on the illicit cryptoasset ecosystem. Within the cryptoasset ecosystem, only a small portion is misused for criminal activities. The company Chainalysis estimates that the share of all crypto transaction volumes associated with illicit activity in 2023 remained at 0,34% of the total on-chain transaction volume (Chainalysis, 2024, p. 6). Of these illicit uses, only a small part is used for terrorism financing. That is not to say, of course, that the threat should be ignored. Any financing of terrorism, no matter how small, has serious social, political and humanitarian consequences and should be prevented and countered. Nevertheless, it is important to understand that cryptoassets can be abused in the same way that the traditional financial system can be exploited for nefarious activities. Thus, it is important to criminalize the misuse of cryptoassets and not the cryptoassets themselves.

Terrorist methods of acquiring, transferring, storing and using cryptocurrency



Myth 2: Terrorist Groups move millions of dollars in cryptocurrencies

Reality: Terrorist-related cryptocurrencies transactions amounts remain relatively low

Information about underworld and criminal activities is never precise. Owing to the nature of illicit activities, reliable information is scarce and rarely available. Thus, it is difficult to obtain accurate estimates of the illicit flow volume. Most studies that quantify illicit flows rely on seizure data to build their estimates. However, while this information can give us some idea of the magnitude of the problem, often seizure data is unreliably recorded at the source. Moreover, a focus on seizures ignores illicit flows that have not been intercepted by the authorities.

The same applies when estimating the criminal use of cryptoassets. Recent developments in artificial intelligence (AI) and blockchain analysis techniques have advanced significantly, providing us with more precise information (more on this below) about these transactions. However, all the information we have on how terrorists operate blockchain-hosted assets depends on first identifying which crypto address belongs to a real-life terrorist entity. Hence, the analysis is made in retrospect and can change as more attributions (i.e., the linking of a virtual address with a physical person or entity) are made. Thus, for example, the existing estimates for terrorist use of cryptoassets in 2022 can change in 2032 if new terrorist-linked addresses come to light in future investigations.

With that in mind, over the past few years

we have developed a much more comprehensive picture of how terrorists use cryptoassets. After the 07 October 2023 Hamas attacks in Israel, the media was inundated with news about how cryptoassets were used to finance terrorism. One report widely circulated in the news claiming that terror groups raised over \$130 million in cryptos in the past few years (Nocera; Livni, 2023). However, the blockchain analysis company that provided the data used in this study strongly contested this (Idem). According to the company, this figure represents the total amount circulated in and out of specific addresses that received or sent funds but not all of these funds were linked to known terrorist entities (Chainanalysis, 2023a). Therefore, this figure is not only a gross exaggeration but also serves to incorrectly criminalize all these addresses. It is important to understand that not all the money that goes in or out of a crypto address is necessarily related to terrorism. This is because crypto-terrorist assets move within the crypto ecosystem, which includes both legal and illegal transactions. Both legal and illegal transactions make use of what are legitimate virtual asset service providers (VASPs) such as centralized exchanges.¹ Consequently, not all the money that a legal exchange moves are necessarily linked to terrorism, even if a terrorist group uses it at some point. Imagine that a terrorist group uses a legitimate bank to make a money transfer, as in the case of the

1 According to the FATF, VASPs are “any natural or legal person [...] [that] conducts one or more of the following activities or operations for or on behalf of another natural or legal person: i. Exchange between virtual assets and fiat currencies (i.e. government issued currencies); ii. Exchange between one or more forms of virtual assets; iii. Transfer of virtual assets; and iv. Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; v. Participation in and provision of financial services related to an issuer’s offer and/or sale of a virtual asset.” (FATF, 2021, p.22).

9/11 bombers who transferred their remaining funds (26,000 USD) back to a al Qaeda facilitator in the UAE in the days before the attacks. This does not mean that all transactions made by or through that particular bank are linked to terrorism and/or terrorism financing (NCoTA, 2004, p.3).

To date, terrorist groups have been using cryptoassets for two different kinds of transactions: funding campaigns and running their organizational. Both these objectives often involve moving funds across international borders. This distinction is relevant as funding campaigns have so far been marked by very few individual contributions/donations which are generally of relatively small amounts. On the other hand, transfers for organizational maintenance tend to be characterized by larger transactional sums. In the timeline, it is interesting to note that before 2020 there are practically only transactions linked to funding campaigns. However, this changes in the post-2020 period and the timeline now shows transactions linked to both funding campaigns and organizational maintenance. It is not clear why this shift occurred. However, it is clear that after 2020 terrorist groups started making use of crypto assets for transborder transfers to avoid sanctions and monitoring. In this case, transactions were usually made by specialized financiers that moved money for more than one terrorist organization. Further, these transactions tended to involve higher amounts. In these cases, it is technically true that terrorist groups have moved millions of dollars through cryptos. Nevertheless, the numbers are still on the lower end (around 2 million USD) and represent not only a fraction of the total amount of terrorism financing when compared with traditional methods, but also a miniscule percentage of the

illegal crypto asset ecosystem, which itself represents a very small portion of the same.

Myth 3: The Majority of Terrorist Crypto-Funding comes from Bitcoin

Reality: Terrorists Know that not all Cryptocurrencies are Equally Vulnerable

Not all cryptocurrencies are created equal in terms of privacy and security, and terrorists are well aware of these differences. Different cryptocurrencies have been developed, with different needs and characteristics in mind. Below are a few examples of different cryptocurrencies:

Bitcoin: This was the first widely spread and most recognized cryptocurrency. Owing to its widespread use, it has relatively high liquidity.

Ethereum: This is the second-largest cryptocurrency. Its blockchain also functions as a platform for decentralized applications (dApps) and has the capacity to host smart contracts. dApps are programs that run on a decentralized network as opposed to a single computer or server. Consequently, they facilitate peer-to-peer transfers of funds which allows more privacy. Smart contracts are also built on the Ethereum blockchain and can be used as a mechanism to provide security for peer-to-peer transfers in the absence of an intermediary.

Stablecoins: cryptocurrencies pegged to other assets such as government issued (i.e., fiat) currencies, gold, or oil. Tether and USD Coins are examples of stablecoins. These coins offer the stability of traditional currencies whi-

le retaining the benefits of digital assets.

Smaller and Emerging Cryptocurrencies: These are lesser-known emerging digital assets. These cryptocurrencies may offer lower visibility and reduced scrutiny by authorities, making them attractive for illicit activities. For example, Avalanche (AVAX), Polkadot (DOT), and Ripple (XRP).

Meme coins: cryptocurrencies inspired by internet memes, characters or trends. Although they are often created as satires, some meme coins, such as Dogecoin (DOGE), Shiba Inu (SHIB), and Pepe (PEPE), have achieved significant value.

Privacy Coins: privacy-oriented cryptocurrencies such as Monero (XMR), Zcash (ZEC), and Dash (DASH). These coins use advanced cryptographic techniques to obfuscate transaction details, making it extremely difficult for authorities to trace the origins, destinations, and amounts involved in transactions.

It is common to hear the term Alt Coins. The term Alt Coins simply refers to any cryptocurrency that is not Bitcoin. It encompasses stablecoins, meme coins, privacy coins, and all other cryptocurrencies. It is also important to note that when one refers to crypto assets, the expression includes not only crypto currencies but also other digital assets. These other digital assets include crypto-related funds (investment funds related to cryptocurrency or blockchain) and crypto tokens. The expression 'token' is used to refer to a digital asset that represents ownership, a specific value, or a utility – like a free-meal coupon or a casino chip. Although cryptocurrencies are technically tokens, as they function as digital representations of a value designed to facilitate transaction, the expression 'token' is usually employed to designate a digital representation of an interest that is built

on an existing blockchain (i.e. is not intrinsic to that blockchain). This contrasts with cryptocurrencies which are intrinsic to their own blockchain. Thus, digital tokens act as a digital "key" to a service or ownership and can have different functions. For instance, a *utility token* provides access rights or enables the purchase of specific products or services; a *security token* proves ownership in real-world assets, and; a *non-fungible token* or NFT registers ownership over a non-fungible asset, that is, a unique digital items such as pictures, videos, or songs) (Sharma, 2024).

Understanding the differences and nuances between different cryptocurrencies is very important. On the one hand, this variety responds to different market demands; on the other hand, criminals and terrorists also exploit these distinctions according to their particular needs. Different types of criminals have different needs (Chainanalysis, 2024; TRM, 2023). White-collar criminals, for example, exploit cryptoassets for money laundering. For them, cryptoassets such as Bitcoins, Alt coins, and NFTs that are very volatile are attractive because their price variations can be used to justify gains or losses. Criminals involved in illicit commerce use cryptoassets to sell their products, but do not seek to accumulate cryptocurrency. Individuals involved in activities such as bribery, corruption, espionage, and even the financing of terrorism use the crypto ecosystem as a means to make illicit payments. These actors tend to want to preserve their gains and thus favor stablecoins. Rogue states and sanctioned entities use cryptocurrencies to move money across jurisdictions and evade sanctions. They also favor the use of stablecoins. Cybercriminals and cyber-enabled criminals who commit fraud and scams, thefts,

hacks, ransomware attacks, etc. still prefer to use Bitcoin. While Bitcoin accounted for 97% of the crypto-illicit volume in 2016, with the evolution of other currencies Bitcoin use plummeted to less than 3% of the crypto-illicit volume in 2022 (TRM, 2023, p. 4).

When discussing the financing of terrorism, it is important to understand that terrorist groups do not rely solely on Bitcoin. Although Bitcoin is the most well-known cryptocurrency, terrorist organizations employ a range of cryptoassets for various reasons, leveraging the unique features of different digital currencies to suit their needs. When extremist groups started exploiting cryptocurrencies in 2016, attempts to finance terrorism through cryptocurrencies were almost exclusively made using Bitcoin. However, as other digital currencies evolved, preferences changed. For instance, there is currently a clear preference for assets in the TRON blockchain. According to the TRM, in 2022, there was a 240% year-on-year increase in the use of Tether (a stablecoin), compared to a 78% rise in Bitcoin use (TRM, 2023, p.14). Tether accounted for 92% of all terrorism financing cases involving cryptocurrencies by 2022 (TRM, 2023, p.4). A few other interesting cases not involving Bitcoins include an extremist group in South Africa who tried to raise funds by creating their own cryptocurrency in 2021, and an NFT minted on an NFT trading website bearing the Da'esh emblem in 2022. Minting is the process whereby a unique digital asset is created so that it can be bought, sold and traded. The NFT was minted by a supporter, who also minted two other NFTs using Da'esh's emblems. While there was no proof that NFTs were part of a Da'esh financing campaign, they demonstrated the potential misuse of NFTs by terrorist

groups. (DoT, 2024, P.14).

Myth 4: Cryptoassets Are Untraceable and Impossible to Seize

Reality: Tracing and Seizure are Possible

There is a widespread myth that cryptocurrencies are anonymous. They are not. Cryptocurrencies are pseudonymous, rather than anonymous. This is an important distinction. Most cryptocurrency transactions are not directly linked to an individual's identity. However, as most cryptocurrencies blockchains work as public ledgers, they hold open information on all transactions that have ever taken place in that chain. Thus, by analyzing information on the blockchain, it is possible to link certain transactions to specific individuals or entities (a process called, attribution). In a sense, certain cryptocurrency operations are more traceable than fiat transactions.

Blockchain analysis makes it possible to identify the sources and destinations of funds, verify digital wallets (i.e. an app or online service that allows you store funds, make transactions and track payment histories), and cluster addresses that belong to the same individual or entity. By following transactions to an address controlled by a VASP or gatekeeper (i.e., those who connect the digital and real world) that has carried out due diligence and verified the identity of the owner/controller of a wallet address, it is possible to attribute those transactions to a specific individual. This is feasible even when the terrorist uses private wallets or de-centralized applications (i.e., autonomous

software programs that run on a blockchain using decentralized computing in peer-to-peer transactions). If an off-chain investigation or threat intelligence discovers a suspect's crypto address, for example, it becomes possible to draw connections between off-chain and on-chain data points, and trace all transactions related to the suspect. This is possible when, for instance, a known terrorist group posts a crypto address soliciting donations online.

Blockchain analysis techniques have significantly evolved over the past few years. When blockchain analysis first emerged in 2010, it involved organizing raw blockchain data to help retail investors look up their cryptocurrency transactions. These raw data include information such as the timestamp of the transaction, the sending and receiving addresses, and the amount of cryptocurrency transferred. However, the identities of those who own or have control of the addresses are not publicly accessible. But, after the Mt. Gox hack in 2014², blockchain analytics tools have entered the second generation. To overcome the limitation of knowing who owns or controls addresses, blockchain analysis has begun to combine the raw blockchain data with other databases. This information crossing allows blockchain analysis instruments to link on-chain activities to real-world entities. These databases include blacklists of sanctioned entities, criminal and terrorist addresses, and other information that allows law enforcement and financial institutions to detect known terrorists and trace the sources and destinations of funds within specific cryptoassets. This significantly advances

attribution capacity by linking addresses to real-world entities. With the advancement of artificial intelligence, the capacity to process vast amounts of data and find patterns has evolved significantly, and blockchain analysis has entered a third generation (TRM 2024). Thus, ownership analytics have evolved to map the composition of an entity's addresses (i.e. identify all addresses linked to the same owner or entity) and reveal nested relationships. It has also become possible to analyze cross-chain transactions and trace the source and destination of funds, even when an asset swaps across different blockchains. However, one of the biggest advances was the capability to proactively recognize transaction patterns that may indicate illicit activities such as money laundering, fraud, or even the financing of terrorism. Terrorist finance (and other crypto-related crimes) usually operates in patterns that can become signatures, and thus, a recognizable behavior even if you do not know to whom the address belongs (TRM 2024). A few examples of signatures are (TRM 2024):

Common traits:

Funds are moved through a sequence of transactions that share common traits, such as amount, timing, or structure, and thus, seem to be linked to the same entity.

Cross-chain swap:

A common technique among criminals and terrorists is the transfer of an asset from one blockchain to a different one to break their direct trails.

Peel Chain

Cryptocurrencies from a single address are fully dispersed in smaller amounts by successive transfers to other addresses.

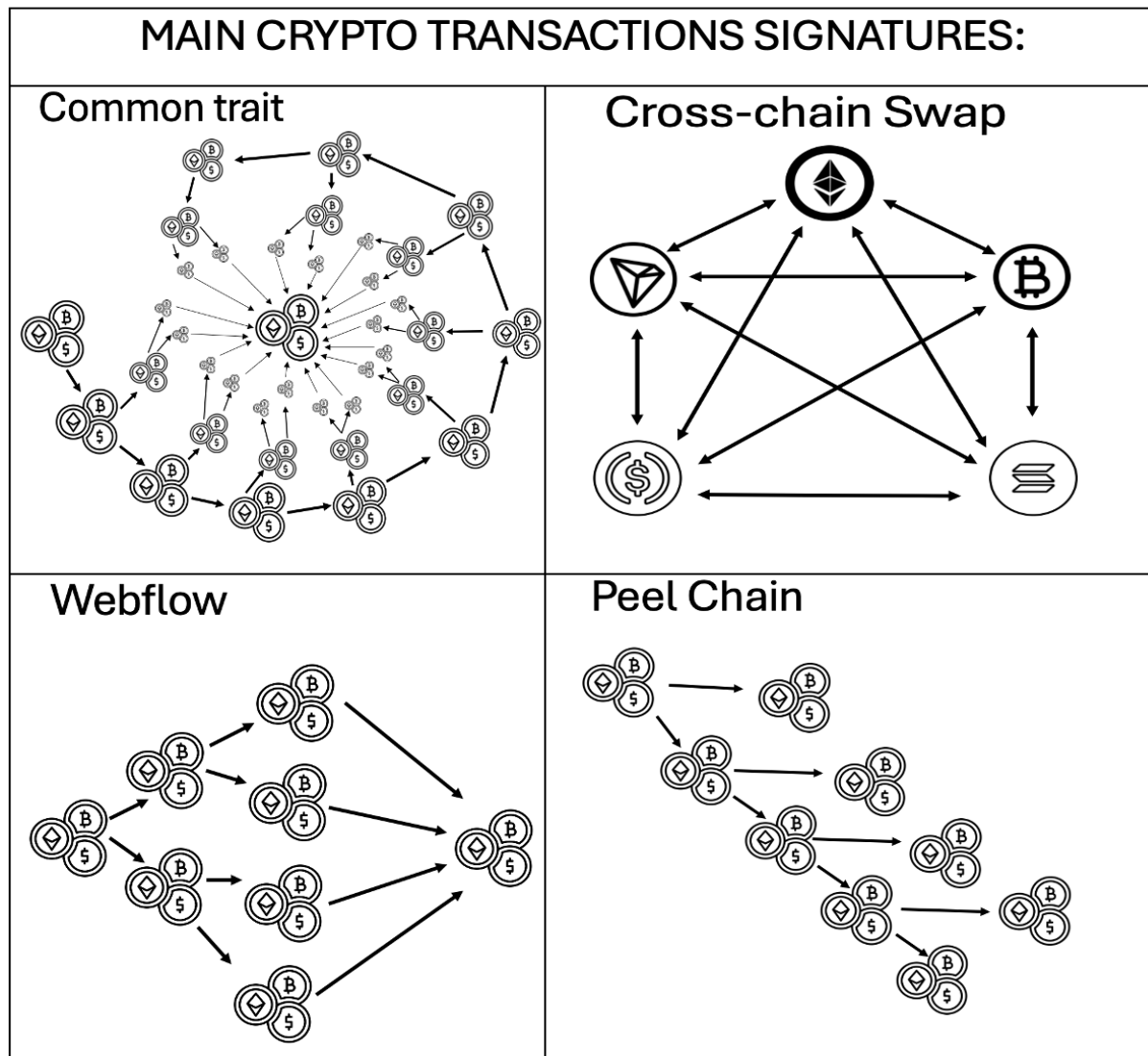
Webflow

Complex, web-like transactions that dis-

2 Mt. Gox was a Japanese exchange that handled over 70% of all Bitcoin transactions in 2014. In April that year, the exchanged was hacked and had about 850,000 Bitcoins stolen leading to its bankruptcy.

perse funds through many nonlinear addresses to then be collected again in another address. This pattern is also known in network analysis

as “one to many” and “many to one” transactions and are highly indicative of obfuscation attempts.



Source: The authors from various sources

Consequently, crypto transactions are highly traceable, representing a great opportunity for intelligence and law enforcement agencies. Terrorists and criminals are aware of this fact and employ other obfuscation techniques to hide their transactions. In addition to the techniques mentioned above, two other techniques deserve attention: privacy coins and mixers/tumblers.

Privacy coins are cryptocurrencies that are designed to enhance the privacy of users and transactions. Popular privacy coins include Monero (XMR), Z-cash (ZEC), DASH (DASH), 0x0.ai (0x0) and MimbleWimble (MWC). Although each of these currencies has different privacy features, with particular appeals to different users, Monero is a good example of how they operate. Monero uses

‘ring signatures’ that group senders’ addresses together, adopts methods to not publicly reveal the value of the transactions (known as zero knowledge proof), and generates ‘stealth addresses’ to receive funds and combine technology protocols to obscure IP addresses. Therefore, it is easy to understand why criminals are interested in private coins. Da’esh, for example, launched a Monero Campaign. The campaign titled “Jihad with Wealth” posted a call for Monero donations: “Oh believers! Shall, I guide you to an exchange that will save you from painful punishment? [...] Please donate with safe cryptocurrency Monero (XMR) for waging jihad with wealth and financing those who are waging the same with their lives.” (Daesh, s.d.).

However, as mentioned above, Tether remains the main cryptocurrency of choice for extremist groups. In fact, even among criminals, Monero and privacy coins are the cryptocurrencies of choice for only very specific criminals (TRM 2023). This is because privacy coins increasingly have a liquidity problem as many governments increase regulatory pressure and move to criminalize their use. For instance, privacy coins were banned in Japan and were delisted from several major exchanges. Delisting is relevant because exchanges are one of the key mechanisms to transform crypto assets into cash (off-ramping). Additionally, recent advances in blockchain analysis tools allow transactions to be traced, even when done with privacy cryptocurrencies.

Another common technique involves the use of mixers and tumblers. These services mix coins from several different transactions, join potentially identifiable assets with unidentifiable assets, and then pool them into a destination address. These services are not necessarily

illegal, but in many cases they are used by criminals to obfuscate the origins of the funds. Mixers and tumblers are popular among criminal and terrorist group financiers. Western governments have historically fought off mixers and tumblers involved in money laundering through regulatory measures and enforcement actions. For example, the United States has engaged in both the sanctioning and criminal prosecution of persons involved in providing this service. Notable cases include the OFAC sanctioning of Blender.io and Tornado Cash in 2022, the designation of Simbad.io, and a seizure of 46 million USD in Bitcoin from Chipmixer in 2023. However, as a report points out, sophisticated criminal actors can quickly adapt and find other obfuscation services when one is shut down (Chain 2024, p. 31).

Another misconception is that blockchains are immutable; thus, it is impossible to seize or freeze cryptocurrencies. Technology has also evolved greatly in this area. Initially, authorities had to physically hold the criminal’s private keys and transfer seized funds to government-held wallets. However, as crypto markets become more regulated, governments can demand that centralized exchanges freeze sanctioned assets under their custody. This is not a perfect solution because these regulations still cannot effectively reach crypto ATMs, dApps, over-the-counter tradings (OTCs), and exchanges that do not follow strict anti money-laundering and counter the financing of terrorism and proliferation (AML-CFTP) procedures. However, centralized exchanges are still the easiest way to convert crypto assets into cash (off-ramping). This practicality explains why centralized exchanges remain the preferred destination for funds sent from illicit addresses (Chananalysis, 2024, p.24). Additionally, with

the creation of blockchains that support smart contracts, it has become possible to have native blacklisted addresses, to freeze, or even to burn and re-issue cryptoassets running on the chain. Some smart contract administrators, such as Tether (USDT), even can freeze sanctioned funds on external DeFi (i.e. decentralized finances) applications.³ This is relevant because it means that it is technically possible to freeze assets held in an external wallet. In fact, several Ethereum addresses that were transacted via the Tornado Cash dApp (a USA sanctioned mixer service) were frozen by Circle (a USD Coin, USDC, issuer) (Coinmarketcap, 2023). In another operation in October 2023, Tether announced that it froze 32 crypto wallets containing \$873,118 USD linked to “terrorism and warfare” in Israel and Ukraine (Howcroft; Wilson, 2023).

Myth 5: Terrorists are technophobes – crypto assets do not appeal to them.

Reality: Terrorist groups are extremely tech savvy.

In some cases, the very idea of crypto currencies appeals to extremist ideologies. This is the case with violent extremism due to xenophobia, racism, and other forms of intolerance, or in the name of religion or beliefs (XRIRB). The idea of a de-centralized financial system

that functions independently of governments is very appealing to extremist ideologies such as Radical Anarchism, Anti-Government Extremist and Accelerationists, who question the need for a government to exist in first place.

Likewise, contrary to common beliefs, terrorist groups tend to be tech-savvy. Extremists have explored new technologies and their vulnerabilities to advance their goals and objectives since the invention of the dynamite, telegraph and railroads in the 1800s. These groups are usually quick to adopt new technologies and adapt their *modus operandi* in response to changes in their security environment. Here are a few cases that illustrate this trend:

Hamas and the Use of Cryptocurrencies

Hamas was one of the first designated terrorist organization to use cryptocurrencies. In 2019, Hamas’s military wing, Izz-Al Din-Al Qassam Brigades, launched campaigns to fund its military activities using cryptocurrencies. Hamas tested soliciting bitcoins via Telegram and directly on its alqassam.net website. Since then, we have seen rapid evolution and increased sophistication in Hamas’s fundraising campaigns via cryptocurrencies. We can clearly identify three phases in Hamas’s cryptocurrency fundraising sub-campaigns (Chainanalysis, 2020):

First Phase:

Initially, sites linked to Al Qassam Brigades began to publish donation requests, providing a QR code linked to a unique Bitcoin address. However, because the address was linked to an exchange in the United States, US authorities quickly froze accounts and investigated the individuals involved.

³ Decentralized finance (DeFi) is an emerging financial technology that offers services without relying on intermediaries such as brokerages, exchanges, or banks. It functions in a peer-to-peer manner by using smart contracts on a blockchain. In 2023, Tether blacklisted 704 contracts and froze over \$150 million USD, Acala froze 16 wallets containing around \$3 billion USD, and Circle froze criminal-related Ethereum funds that interacted with Tornado Cash dApp on external DeFi applications (PHILLIPS, 2023).

Second Phase:

From then on, Hamas began to publish addresses linked to private wallets, not under the custody of exchanges. However, authorities still manage to map transactions using blockchain analyses.

Third Phase:

Finally, the group became quite sophisticated by incorporating wallets and payment methods on their own sites. Thus, Hamas started to create a unique address for each donor and diversify transactions with cryptocurrencies other than Bitcoin. In April 2023, the group even recommended that its supporters not donate Bitcoin to avoid being compromised and announced the end of their Bitcoin donation campaign (Chainanalysis, 2023b). In this phase, the group also experimented with decentralized finances (DeFi), teaching its donors how to create private wallets to make donations. Detailed videos were also released, teaching how to use money exchangers (e-Hawala operators) to make transactions or how to maintain anonymity through the use of public Wi-Fi networks, recommended wallets, and exchange lists.

Since then, the US has announced the freezing of 150 crypto accounts linked to at least three major global fundraising campaigns by the Izz-Al Din-Al Qassam Brigades. These campaigns used sophisticated cyber-tools. Israeli authorities have also closed dozens of cryptocurrency addresses linked to Hamas with a volume of tens of thousands of dollars. Seizures have demonstrated increasing technical sophistication by using various channels, chains, and cryptocurrencies to avoid detection. Currently, the group prefers to use payment channels on their websites rather than to share cryptocurrency addresses.

Additionally, with the beginning of the conflict between Israel and Hamas in October 2023, GAZANOW, a group that actively supports Hamas – requested donations to a cryptocurrency address that received around \$5,000 USD. Since then, the group has started contacting its supporters through direct messages on Instagram, which has interrupted the campaign. Other campaigns like “Tofan al-Aqsa” have been requesting donations via X (formerly Twitter). Thus far, the campaigns have obtained few resources. Israel announced on October 10, 2023, the freezing of cryptocurrency accounts belonging to Hamas. The US Treasury Department’s Office of Foreign Assets Control (OFAC) imposed sanctions on ten members, agents, and financial facilitators of Hamas. The sanctions were also directed at two Gaza-based money service businesses⁴ (MSBs), Buy Cash Money and Money Transfer Company. According to OFAC, Buy Cash has been used to transfer funds by affiliates of terrorist groups, including Hamas, Al-Qaeda, and Da’esh, and to facilitate cryptocurrency fundraising for Hamas (OFAC 2023).

Al-Qaeda in France

In 2019, the French Financial Intelligence Unit (Tracfin) uncovered a new complex terrorism financing scheme used by Al-Qaeda to circumvent the traditional supervisory mechanisms. Supporters of the group would anonymously buy prepaid vouchers for amounts under €200, mainly in tobacco stores, and send voucher information to combatants in warzones. Combatants then used the vouchers to buy

⁴ Businesses, including traditional banks but not only, that provide services in transmitting, converting, or exchanging money.

cryptocurrencies on virtual exchange platforms. Subsequently, the money was transferred through different Bitcoin address clusters to a VASP in the warzone, which then converted the cryptocurrency into cash. After the investigations, 63 donors and two facilitators were arrested in France, and the related crypto-asset wallet was seized.

Other Terrorist-Designated Groups and Their Use of Cryptocurrencies

Other terrorist-designated groups have also launched fundraising campaigns through cryptocurrencies. In 2022, multiple entities linked with the financing of terrorism, including various cryptocurrency exchanges, started experimenting with decentralized exchanges (DEXs) which are peer-to-peer platforms where individuals trade cryptocurrencies directly between themselves in a non-custodial way (TRM, 2023, p.15). In June 2023, Israel's National Bureau for Counter Terror Financing (NBCTF) froze \$1.7 million worth of Hezbollah-linked cryptocurrencies. The NBCTF targeted over 40 USDT addresses on the TRON network, connected to Hezbollah and associated with entities and exchanges in Iraq, Syria, and the Gaza Strip. Typically, the funding pattern of terror operations involves financial facilitators transferring funds to Hawala services and OTC brokers, who then transfer the funds to addresses controlled by Hezbollah on various exchanges. These facilitators often provide services to multiple terrorist groups. In Syria, for example, areas under Hay'at Tahrir al-Sham (HTS) control are consolidating as hub for cryptocurrency where the exchanges provide services to groups such as Da'esh, Al-Qaida and its affiliates (CTED 2024). The

same funding pattern has also been employed by other organizations, such as the Palestinian Islamic Jihad (PIJ) and Da'esh. Da'esh uses the same pattern on on-going fundraising campaigns for ISIS families in internment camps in northeastern Syria. According to TRM Labs, these campaigns ask for donations to improve the detainees' conditions and have raised varying amounts, from a few dollars to tens of thousands (CTED 2024). Additionally, Da'esh affiliates and their supporters in South and Central Asia have been increasingly using cryptocurrency (idem). For example, the al-Azaim Foundation for Media – a group affiliated with Da'esh in Afghanistan – held Bitcoin, Ethereum and TRX (Tron) addresses that received less than 1,000 USDT. Tajik Da'esh-affiliated groups also used cryptocurrencies to recruit members and support Tajik families imprisoned in Syria (TRM 2022).

These cases illustrate how the terrorist use of cryptoassets groups has been evolving. The growth in the use of Tether (USDT) and other currencies such as Ethereum, Dogecoin, Monero, and Zcash. The use of mixers and cold wallets instead of verified accounts. The increasing use of decentralized exchanges and non-custodial peer-to-peer marketplaces as a response to the increasing regulation of VASPs. And the experiments with NFTs all demonstrate how terrorist groups enhance their operational security as a response to the changes in the crypto ecosystem.

Conclusion

The myths surrounding cryptoterrorism significantly cloud our understanding of how digital currencies intersect with terrorist financing. While cryptocurrencies present unique

challenges due to their pseudonymous nature and the sophistication of privacy coins, the reality is that their use by terrorists is still relatively limited compared to traditional financing methods. Understanding that most terrorist funding does not originate from cryptoassets is crucial. Despite high-profile cases, most terrorist financing relies on more conventional methods. Similarly, while terrorists move funds using cryptocurrencies, the amounts involved are typically smaller than reported and far less than the sums moved through traditional channels. In addition, it is important to recognize that not all cryptocurrencies are equally vulnerable to misuse. Although Bitcoin is often highlighted, other cryptocurrencies, particularly privacy coins and stablecoins, are also used for their unique features. This diversity in cryptoassets reflects terrorists' different needs and tactics.

Advancements in blockchain analysis and artificial intelligence have significantly enhanced our ability to trace and seize illicit crypto transactions. These tools allow law enforcement to link transactions to real-world identities and to disrupt terrorist financing networks. However, the race between obfuscation techniques and analytical tools to counter these continues and requires ongoing vigilance and innovation. The notion that terrorists are technophobic is both inaccurate and outdated. Extremist groups are adept at leveraging new technologies to achieve their goal. The evolution of cryptocurrency use, as demonstrated by groups such as Hamas, underscores their capability to adapt and innovate in response to counterterrorist measures.

In conclusion, while the threat of crypto-terrorism should not be ignored, it is essential to accurately contextualize its scale and scope. Effective countermeasures involve a multi-fa-

ceted approach that combines regulation, international cooperation, advanced technology, and public-private partnerships. By dispelling these myths, we can better focus our efforts on realistic and impactful strategies to combat terrorist financing in the digital age.

Annex I

Timeline of High-profile TF through Crypto assets

2014

US authorities found a Dark Web site called "Fund The Islamic State Anonymously" that encouraged Da'esh sympathizers to donate bitcoins for the group.

2015

January: Abu-Mustafa raised 5 bitcoins (USD 1,000 at the time) for Da'esh. His account was closed by the FBI.

May: Abu Ahmed Al Raqqa asks for bitcoin donations via darkweb.

June: A pro-Da'esh forum called "Fund the Islamic Struggle Without Leaving a Trace" began posting how to donate bitcoins for the group.

Ali Shukri Amin is arrested for using Twitter to teach Da'esh members and sympathizers how to use bitcoin.

July: Da'esh-linked Ibn Taymiyyah Center launched the campaign "Jahezona" ("Equip Us") accepting donations in bitcoins

August: Da'esh linked hacker demands 2 bitcoins (USD 500) in ransomware.

2016

Reports suggest that a wallet containing 3 million USD in bitcoin, may been used in the Charles Hebdo attacks that year.

July: Mujahideen Shura Council receives 0.929 bitcoins (USD 540) in 2 transactions after giving this donation option. Twitter infographic with QR code.

2017

January: Indonesia Announces that Middle Eastern Militants are using Bitcoin to fund terrorism.

November: An Al Qaeda-related organization, Al-Sadaqah (voluntary giving), asks for donations in Bitcoins on Facebook, Telegram and Twitter. At least one donation of BTC 0.075 (685USD at the time) was made.

December: A woman is arrested in New York for wiring 62,000USD in bitcoin to Da'esh via China, Pakistan and Turkey. She forged information to acquire loans and credit cards and convert the cash into Bitcoins.

Darknet Isdarat website is launched asking for donations in Bitcoins for Da'esh.

Zoobia Shahnaz, was arrested in the USA for unlawfully obtaining and transferring approximately 85,000USD to Da'esh, 62,700USD of which were transferred in bitcoin and other cryptocurrencies.

2019

Al-Qassam Brigades (linked to Hamas) started a fund-raising campaign posting infographics and instructional videos on how to donate in bitcoins. They raised around USD 3.5k until the

Source: Compiled by J. M. Lasmar from multiple sources

authorities seized 150 cryptocurrency accounts linked to the group in 2020.

Brenton Tarrant, author of the Christchurch attacks in New Zealand in March 2019, used virtual assets to transfer funds for ideologically aligned actors in Europe.

2021

The cryptocurrency exchange platform Coinbase identified Hamas as one of several terrorist groups involved in cryptocurrency fundraising.

July: The Israeli National Bureau of Counterterrorism Finance (NBCFS) seized Bitcoin, Doge, Tron, and other cryptocurrency addresses controlled by agents linked to Hamas.

The Office of Foreign Assets Control (OFAC) sanctioned Farrukh Furkatovitch Fayzimatov, a Syria-based fundraiser and recruiter for Hay'at Tahrir Al-Sham (HTS). According to OFAC, he asks for bitcoin donations on behalf of HTS on the social media. Since his designation, he keeps creating new crypto addresses in various currencies and has raised 12,000USD. These funds came from small contributions using not only mainstream exchanges but also, hosted wallets, and Russian exchanges.

A XRIRB group in South Africa created their own stable coin on a 1:1 ratio with the South African Rand. The group raised EUR 14,720.

2020

August: US Department of Justice (DOJ) announces the largest seizure to date of crypto assets associated with terrorism. Millions of dollars in over 300 cryptocurrency accounts associated with Hamas, Al-Qaeda and Da'esh were Frozen. I total, 150 accounts were linked to Hamas, 100 to Al Qaeda and the rest to Da'esh. The groups moved money through a Bitcoin network and used Telegram and other social media to ask for donations. In some cases, they posed as charities but in most cases openly stated their cause.

2022

The company TRM Labs identifies dozens of cryptocurrency fundraising campaigns for Da'esh families held in internment camps in Al-Hawl. The campaigns moved from a few dollars to tens of thousands.

May: OFAC sanctions five individuals for facilitating money transfers from Indonesia to Da'esh members in Syria. Over USD 517,000 was sent through Indonesia-based exchanges to pro-ISIS fundraising campaigns in Syria. The transfers usually amounted of around USD 10,000 and were made using USDT on Tron.

A Da'esh affiliate in Pakistan began to ask for cryptocurrency donations. According to TRM Labs, the related addresses moved around USD 40,000 over 12 months.

August: A Da'esh supporter created what is probably the first pro-Da'esh NFT.

December: According to TRM Labs, al-Azaim Foundation for Media (AFM), the official media unit of Da'esh affiliates in Afghanistan, used cryptocurrency to raise funds.

Source: Compiled by J. M. Lasmar from multiple sources

2023

A widely circulated but contested report stated that Hamas raised 130 million USD in crypto in the few previous years.

February: A UN report stated that Da'esh is increasingly using virtual currencies. However, the group is moving toward stable coins. The report present evidence that the group has been using Tether in transactions greater than \$100,000, demonstrating increased sophistication in the use of privacy-enhanced cryptocurrencies.

The same report identifies Al-Karrar office as a financial hub of Da'esh affiliates. The Al-Karrar office sent USD \$25,000 worth in cryptocurrency month to Da'esh.

June: Israel's National Bureau for Counter Terror Financing seized USD \$1.7 million in cryptocurrency linked to Hezbollah and Iran's Quds Force through a Syria-based financial facilitator named Tawfiq Muhammad Said Al-Law.

December: Turkish police arrested Shamil Hukumatov, an alleged high ranking Da'esh recruiter and fundraiser. He controlled an address that received around USD 2 million in USDT on the Tron blockchain from donations. The donations came from both centralized exchanges as well as from unhosted addresses.

US DOJ prosecuted an individual for material support to Hamas, including through Bitcoin.

U.S. law enforcement authorities revealed that Qassam Brigades used the cryptocurrency exchange Binance to facilitate cryptocurrency transactions as early as 2019.

TRM Labs also identified multiple pro-Da'esh groups using cryptocurrency in Tajikistan. One of the related addresses received around USD 2 million in USDT on Tron in 2022. Later, on June 22, 2023, Turkish authorities arrested Shamil Hukumatov who was allegedly responsible for the fundraising campaign.

2024








February: Spain arrested a Jordanian who appears to have used USDT on the Tron blockchain to send 200,000 Euros in Cryptocurrencies to Da'esh.

August: The second phase of the Brazilian Federal Police's Operation 'Trapiche – Terrorism Financing' made connections with other money-laundering investigations related to organized crime (Colossus, Hydra) and found existent connections between Brazilian crypto assets operators and Hezbollah-held wallets.

2025

February: According to the Counter Extremism Project, the leader of the neo-Nazi group The Base requested on at least three platforms donations in Bitcoin, Monero, or Tether

Source: Compiled by J. M. Lasmar from multiple sources

KEY:	
	Da'esh
	Hamas
	Hezbollah
	XRIRB actor
	Hay'at Tahrir Al-Sham
	Al Qaeda
	Mujahideen Shura Council

Elaborated by J. M. Lasmar from multiple sources

BIBLIOGRAPHY

CHAINANALYSIS. 2020. Terrorism Financing in Early Stages with Cryptocurrency But Advancing Quickly. Available at <https://www.chainalysis.com/blog/terrorism-financing-cryptocurrency-2019/> accessed 5/Aug/2024.

CHAINANALYSIS. 2023a. *Correcting the Record: Inaccurate Methodologies for Estimating Cryptocurrency's Role in Terrorism Financing*. Available at <https://www.chainalysis.com/blog/cryptocurrency-terrorism-financing-accuracy-check/> accessed in 5/Aug/2024.

CHAINANALYSIS. 2023b. *Hamas' Al-Qassam Brigades Announces End of Cryptocurrency Donation Efforts*. Available at <https://www.chainalysis.com/blog/hamas-al-qassam-brigades-cryptocurrency-donations-shutdown/> accessed 5/Aug/2023.

CHAINANALYSIS 2024. *The 2024 Crypto Crime Report: The latest trends in ransomware, scams, hacking, and more*. Chainanalysis: S.l..

CTED 2024. *CTED hosts Insight Briefing on "Latest trends in the use of cryptocurrency by terrorist groups and their supporters"*. Security Council Counter-Terrorism Committee, Counter-Terrorism Committee Executive Directorate: New York. Available at <https://www.un.org/securitycouncil/ctc/news/cted-hosts-insight-briefing-%E2%80%9Clatest-trends-use-cryptocurrency-terrorist-groups-and-their> accessed 5/Aug/2023.

DAESH. S.d. *Jihad with Wealth*. Voice of Khurasan. Islamic State Khurasan Province: s.l..

DoT 2024. *Illicit Finance Risk Assessment of Non-Fungible Tokens*. US Department of Treasury: Washington.

FATF. 2015. *Emerging Terrorist Financing Risks*. Financial Action Task Force: Paris.

FATF. 2021. *Updated Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers*. Financial Action Task Force: Paris.

HOWCROFT, E.; WILSON, T.. 2023. *Tether Freezes Crypto Linked To 'Terrorism and Warfare' in Israel and Ukraine*. Reuters, October 17, 2023. Available at [https://www.reuters.com/technology/tether-freezes-873000-crypto-linked-terrorism-warfare-israel-ukraine-2023-10-16/#:~:text=Press%20Releases,Tether%20freezes%20crypto%20linked%20to%20'terrorism.warfare'%20in%20Israel%20and%20Ukraine&text=LONDON%2C%20Oct%2016%20\(Reuters\).the%20company%20said%20on%20Monday](https://www.reuters.com/technology/tether-freezes-873000-crypto-linked-terrorism-warfare-israel-ukraine-2023-10-16/#:~:text=Press%20Releases,Tether%20freezes%20crypto%20linked%20to%20'terrorism.warfare'%20in%20Israel%20and%20Ukraine&text=LONDON%2C%20Oct%2016%20(Reuters).the%20company%20said%20on%20Monday) Accessed 5/Aug/2024.

[com/technology/tether-freezes-873000-crypto-linked-terrorism-warfare-israel-ukraine-2023-10-16/#:~:text=Press%20Releases,Tether%20freezes%20crypto%20linked%20to%20'terrorism.warfare'%20in%20Israel%20and%20Ukraine&text=LONDON%2C%20Oct%2016%20\(Reuters\).the%20company%20said%20on%20Monday](https://www.reuters.com/technology/tether-freezes-873000-crypto-linked-terrorism-warfare-israel-ukraine-2023-10-16/#:~:text=Press%20Releases,Tether%20freezes%20crypto%20linked%20to%20'terrorism.warfare'%20in%20Israel%20and%20Ukraine&text=LONDON%2C%20Oct%2016%20(Reuters).the%20company%20said%20on%20Monday) Accessed 5/Aug/2024.

LASMAR, Jorge M. 2019. *As Dinâmicas Financeiras do Terrorismo in FAGUNDES, C.F.F.; LASMAR, J.M.; CHUY, J. F. M. "Perspectivas do Terrorismo Contemporâneo"*. Arraes: Belo Horizonte.

NCoTA. 2024. *The 9/11 Commission Report*. The National Commission on Terrorist Attacks: Washington.

NOCERA, Joe; LIVNI, Ephrat. 2023. *Is Crypto Financing Terrorism?* In The New York Times, 28 October, 2023. Available at <https://www.nytimes.com/2023/10/28/business/dealbook/is-crypto-financing-terrorism.html> accessed 5/Aug/2024.

OFAC. 2023. *Counter Terrorism Designations: Specially Designated National List Update, 10/18/2023*. U.S. Department of The Treasury, Office of Foreign Assets Control: Washington. Available at <https://ofac.treasury.gov/recent-actions/20231018> accessed 5/Aug/2024.

PHILLIPS, Daniel. 2023. *How can Cryptocurrencies be Frozen on a Blockchain?* Crypto Basics. Available at <https://coinmarketcap.com/academy/article/how-can-cryptocurrencies-be-frozen-on-a-blockchain> accessed in 5/Aug/2024.

SHARMA, Toshendra K. 2024. *Security Tokens Vs. Utility Tokens: A Concise Guide*. Blockchain Council. Available at <https://www.blockchain-council.org/blockchain/security-tokens-vs-utility-tokens-a-concise-guide/> accessed in 5/Aug/2024.

TRM. 2022. *New Evidence Confirms ISIS Affiliate in Afghanistan Accepting Cryptocurrency Donations*. TRM Labs. Available at <https://www.trmlabs.com/post/new-evidence-confirms-isis-affiliate-in-afghanistan-accepting-cryptocurrency-donations> accessed in 5/Aug/2024.

TRM. 2023. *Illicit Crypto Ecosystem Report*. TRM Labs.

TRM. 2024. *Detecting the Invisible: The Power of TRM Labs' Signatures™ in Blockchain Investigations*. TRM Labs.