Electronic Journal of Social and Strategic Studies Volume 6 Issue 2
Date of publication: 30 Sep 2025 Aug – Sep 2025
DOI: https://doi.org/10.47362/EJSSS.2025.6211

Emerging Role of Cryptocurrency as Means of Terror Financing: A Qualitative Study

Parth Vipulkumar Dave[1]

Abstract

Recent investigations have indicated that cryptocurrency is being used to finance terrorist-related activities. This phenomenon has brought attention to the danger of the using more cutting-edge technologies in the entire toolkit for financing terrorism. The use of cryptocurrencies in terror financing raises security concerns in addition to having an impact on the world economy. However, there haven't been many thorough analyses conducted in this area. This article highlights the evolution of terror financing methods vis-à-vis Technological Innovation in Financial Sector. This article also investigates the factors, scale and scope of cryptocurrency that have encouraged terrorist organization from using it. In light of the global and South-Asian context of terror financing focusing on India, this paper evaluates the security threat posed by cryptocurrency.

Keywords

Terrorism, Terror Financing, Cryptocurrencies, Blockchain, Technological Innovation, Digital Currency, South-Asia

Introduction

While the cryptocurrency, a form of digital currency, promised to revolutionise the global financial sector by providing unprecedented anonymity, decentralisation, and accessibility, its increasing use for illegal activities, including terror finance has raised serious concerns globally. Available evidence suggests that cryptocurrency has emerged as a new and relatively safe mode for financing and sustaining their transnational organised network of terrorism. Given the transnational character of contemporary terrorism, the expertise they have acquired on emerging technologies and growing consensus among affected states on coordinated efforts to curb the financial network of terrorist organisations, the use of virtual assets is becoming a preferred mode for transnational terrorist and organised criminal networks. It is increasingly being recognised as a serious challenge to the national security of states. In

[1] Parth Vipulkumar Dave is a Research Scholar at Center for Security Studies, Central University of Gujarat, India.

DOI: https://doi.org/10.47362/EJSSS.2025.6211

the context of South Asia, one of the epicentres of global terrorism, the emergence of cryptocurrency as a tool for terror financing poses significant challenges to regional security.

This article explores the evolving landscape of cryptocurrency-enabled terror financing in South Asia. The increased internet access and technological advancements have led to a surge in cryptocurrency exchanges in India, Pakistan, Bangladesh, and Sri Lanka. These countries are experiencing rapid growth in cryptocurrency exchanges and trading platforms, accompanied by a growing user base. Despite the national security implications of cryptocurrencies and terrorism, the subject has received little systematic and comprehensive examination. One reason for the lack of literature is the confinement and inaccessibility of information in open sources. This paper attempts to understand the linkage between terrorism and cryptocurrency, identify emerging trends in terror finance, and examine their impact on national security. The paper uses qualitative research methodology. It analyses data collected from open-source information, published reports, books, and academic articles using certain parameters. The article has three sections. The first examines the growth of terror financing strategies with financial technology. The second discusses the factors, scale, and scope of cryptocurrencies for terror financing. The last part looks at reported cases of cryptocurrencies in terror financing in South Asia and their implications for the national security of regional states.

Evolution of Terror Financing Methods and Technological Innovation in Financial Sector

After the Cold War, the international system witnessed an increasing role of non-state groups, particularly terrorist organisations in shaping international security architecture and inter-state relationships. While the era of globalisation marked with interdependence, the increasing role of global financial networks facilitated economic development and trade, it also helped terrorist and organised criminal groupings who took advantage of the global financial system and their operations evolved into smaller, geographically scattered organisations with independent networks. In addition to the structural changes, the means of financing also started to evolve steadily. The terrorists employed recently developed techniques and resources. Concurrently, the progress of technology in internationally linked financial markets opened up possibilities for the emergence of innovative methods for funding terrorism. More precisely, there were advancements in the methods used to acquire and transfer funds for financing acts of terrorism, while governments also made efforts to control or restrict the extent of such financing. In the 1980s, the state actions were mostly focused on reducing the prevalent state

DOI: https://doi.org/10.47362/EJSSS.2025.6211

assistance. Simultaneously, terrorist organisations developed creative methods for acquiring and transmitting finances. The US Embassy bombing in Africa placed a major focus on alternate banking systems, with the likelihood that the terrorists would exploit this avenue for money transfer. The 9/11 attacks in 2001 were entirely funded using a legitimate banking route (Freeman & Ruehsen, 2013). A significant proportion of funding was allocated to provide organizational support instead of being employed for direct terrorist operations. As stated by Balasubramaniyan and Raghavan, Al-Qaeda has nearly 10 percent of its overall funds for direct operational planning and execution annually, while the remaining 90 percent of the funds are devoted to the organization's maintenance (Balasubramaniyan & Raghavan, 2017). However, the financial necessities differ among terrorist groups depending on their objectives, organisational structure, and other factors, such as the deployment of means, modus operandi, and target audience.

The advancement of technology and growth in the banking industry have increased the potential for terrorists to transfer funds. There was a significant increase in the use of money service businesses for the purpose of transferring money to support terrorist financing. The complex issue involving Hezbollah and the Lebanese Canadian Bank in 2011 offers additional proof of this type of inventive adaptation (Keatinge & Danner, 2021). Before 2011, Hezbollah used money laundering in a sophisticated strategy that involved depositing cash into the Elissa Exchange and the Hassan Ayash Exchange MSBs, both of which had connections to the Lebanese Canadian Bank. After the detection of these transactions and the consequent closure of both financial service enterprises by law enforcement authorities, they were immediately substituted by two further MSBs associated with Hezbollah. As a result, money laundering continued until the discovery of these two additional MSBs in 2013 (Keatinge & Danner, 2021). According to a 2014 investigation on drug trafficking in Afghanistan, it has been discovered that the Taliban exploited both the regulated banking system and money services businesses to transfer the earnings obtained from drug trafficking (Allagh, 2020).

The advent of technological innovation has given rise to numerous innovative electronic and online payment systems. Terrorist financing is popularly facilitated by its speed, convenience, and low cost. Terrorists have utilised internet-based payment systems, such as PayPal and CashU, which facilitate online transactions from preloaded accounts (Norton & Chadderton, 2016). The 2016 Mohamed Elshinawy case in the United States exposed how ISIL employed the global online payment platform PayPal to transfer funds. They accomplished this by establishing companies and subsidiaries in various countries, such as the United Kingdom,

Turkey, and Bangladesh. Their aim was to channel attack funding into the United States while bypassing detection by law enforcement agencies (U.S. Department of Justice, 2018).

Nevertheless, the effectiveness of counter-terrorism finance (CTF) methods in reducing terrorist exploitation of the official financial sector (such as banking and MSBs) and emerging technological innovations in finance like PayPal and similar platforms. Following 2010, the increasing popularity of social media and the development of innovative technologies led to the emergence of new avenues and techniques for fundraising and transferring funds. There are concerns about terrorist organisations possibly increasing their utilisation of digital cryptocurrencies like Bitcoin to finance their activities. The amalgamation of crowdfunding through social media platforms and the utilisation of cryptocurrencies and virtual assets has the potential to become an important means of financing terrorism.

Crypto-Currencies and **Terror Financing: Factors, Scale and Scope**

Cryptocurrency refers to a category of digital currencies that are issued by their inventors. The first cryptocurrency, Bitcoin, was developed by the pseudonymous individual known as Satoshi Nakamoto as a reaction to the 2008 global financial crisis (Whyte, 2019). It is a means for individuals to independently manage their finances. The technology that forms part of blockchain was introduced in a 2008 white paper by the enigmatic developer of Bitcoin. The distributed ledger system known as blockchain serves as the fundamental infrastructure of the cryptocurrency market. A blockchain is a decentralised and distributed digital ledger that ensures the security of information by duplicating and distributing it over a network of computer systems (Krishnan, 2020). By 2023, the global count of cryptocurrencies exceeded 9,000. While the number of digital coins was higher in the early months of 2022, it is important to note that a major fraction of cryptocurrencies may lack significance. There are several approximations suggesting that around 20,000 cryptocurrencies exist, although the majority of these are either inactive or no longer in use. Undoubtedly, the collective value of the top 20 cryptocurrencies accounts for approximately 90 percent of the entire market (Statista, 2024).

The global financial crisis has brought attention to the vulnerabilities of the existing financial system and its overdependence on centralised financial institutions. Bitcoin was developed in part as a reaction to the current financial system, aiming to construct a more robust and reliable financial system that would not be susceptible to the same risks. The transparent ledger that encompasses records of each transaction on the Bitcoin network facilitates the monitoring and surveillance of financial transactions. This facilitates the prevention of

DOI: https://doi.org/10.47362/EJSSS.2025.6211

fraudulent behaviours, such as insider trading, market manipulation, and other unethical actions. Cryptocurrency, in contrast to conventional digital and fiat currencies, serves as a reliable and inflation-resistant means of preserving value. Cryptocurrencies offer a wide range of transactional benefits compared to other digital and traditional currencies (Whyte, 2019). Cryptocurrencies provide individuals with a high level of protection, while simultaneously presenting a formidable task for governments in terms of regulation and control. Law enforcement and banking organisations encounter numerous problems when addressing the issue of terror financing within the realm of cryptocurrencies. The issues encompassed in this context are anonymity or pseudonymity, lack of rules and jurisdictions, technological sophistication, cross-border complexity, scarcity of resources within government agencies, and the proficiency gap among law enforcement experts. The problems encountered by law enforcement and financial institutions in identifying and thwarting cryptocurrency-based terrorism funding are complex, hence increasing its appeal for use in financing acts of terror.

Terrorist actors are multifaceted, encompassing a diverse array of ideologies, motivations, capabilities, tactics, and behaviours. This classification begins with an individual actor, small groups, a network that aids in coordination, and a hierarchical organisation that lacks a centralised basis or territorial control group. Cryptocurrencies do not offer significant advantages to individuals or small groups who can already easily fund themselves through traditional means like cash, credit cards, or self-funding. However, organisations that have a hierarchical structure and control (such as Al-Qaeda) as well as organisations that dominate certain territories, are constantly seeking alternate means to transfer funds. The utilisation of cryptocurrencies for the purpose of financing terrorism is often exploited by such groups.

Terrorist organizations and their sympathizers have been discussing the use of cryptocurrencies for financing acts of terror since 2015. In June 2015, Ali Shukri Amin, a teenager, was found guilty in the United States for utilizing social media to offer assistance to ISIS. Amin confessed to utilizing Twitter to provide guidance to others on how Bitcoin may be employed to conceal the provision of funds in aid of ISIS (U.S. Department of Justice, 2015). In February 2018, Michael S. Smith II, a terrorism analyst at the US national security consultancy Kronos Advisory, observed that the Al-Qaeda online publication al-Haqiqa published an article discussing the applications of Bitcoin. The article explored the compatibility of Bitcoin with sharia law and ultimately concluded that while there are numerous potential uses of cryptocurrencies for their objectives, there are also significant

DOI: https://doi.org/10.47362/EJSSS.2025.6211

challenges (Keatinge et al., 2018). In January 2017, Indonesia's anti-money laundering and counter-terrorist financing (AML/CTF) agency publicly made the initial explicit allegations of terrorists utilizing cryptocurrencies. According to Indonesian authorities, Bahrun Naim, a member of Daesh (also known as ISIS), supposedly used PayPal to distribute Bitcoin to other members in Indonesia (Gunaratna, 2017). This method allowed them to avoid using the official financial system for transferring funds. This instance demonstrates the potential of cryptocurrencies as a substitute for the conventional Hawala method of transactions employed by terrorist organizations. Cryptocurrencies and Hawala have common features of anonymity and decentralization; however, cryptocurrencies possess a distinct advantage over Hawala. Cryptocurrency transactions are immediate, secure, and have lower fees.

The aforementioned incidents demonstrate the significant interest that numerous terrorist organisations have in cryptocurrencies. However, the utilisation of cryptocurrencies extends beyond just facilitating the transfer of payments. They can also serve as a method for generating and safeguarding funds. The July 2016 campaign was conducted by the Ibn Taymiyya Media Centre (ITMC), an online media division of the Mujahideen Shura Council in the Environs of Jerusalem (MSC), a coalition of Salafi-Jihadist organisations in the Gaza Strip. The MSC has been officially recognized as a foreign terrorist organization by the US State Department due to its deliberate targeting of Israel and its expressed support for the Islamic State. ITMC introduced the "Jahezona" online campaign, which allows people to donate funds in Bitcoin. They provided clear instructions on how to use this technology on their website. At the moment this activity was detected, there were just two transactions made to the associated Bitcoin address. These transactions amounted to around 0.929 Bitcoin, which is equivalent to around USD 540 at that time. As of March 2018, the Bitcoin address linked to it has received around 1.46 Bitcoin. Due to the substantial increase in Bitcoin's value, this amounted to roughly USD 8,000 at that time (Keatinge et al., 2018). As indicated in the aforementioned example, there has been a convergence in the utilisation of social media for the purpose of crowdfunding and cryptocurrencies in relation to financing terrorism. Terrorist organisations like ISIS, Al-Qaeda, and Hezbollah have been increasingly utilising social media platforms such as Twitter, Facebook, Instagram, and Telegram to access their support network and request and transfer donations (Keatinge et al., 2018). Hajjaj Bin Fahd al-Ajmi, a terrorist financier,was using multiple social media sites to raise funds and channel them to Nusra Front, a Syrian affiliate of Al-Qaeda (Hajjaj Bin Fahd Al Ajmi, n.d.-a). An individual from Canada has been accused by the FBI of utilising online operations that were disguised as humanitarian

DOI: https://doi.org/10.47362/EJSSS.2025.6211

efforts in order to solicit funds for ISIS. The individual in question established several GoFundMe campaigns under the guise of aiding humanitarian efforts. It is claimed that they also provided a sum of US$20,347 to a cryptocurrency connected to the terrorist organization (Canadian Press, 2022).

Regarding traceability in the context of the utilisation of cryptocurrency and social media, both have faced intense scrutiny from law enforcement agencies and the government. Bitcoin, in reality, lacks complete anonymity, and cryptocurrency networks have centralised "chokepoints" in the form of exchanges. The implementation of new rules on crypto-exchanges, along with the advancement of forensic techniques for tracking cryptocurrency transactions, has imposed restrictions on the ability of terrorist groups to utilise cryptocurrencies. In recent years, there has been significant innovation in the utilisation of new privacy-oriented alternative cryptocurrencies that offer higher levels of anonymity compared to Bitcoin. Although they utilise open-source, public blockchains like Bitcoin, the specific identifying features remain concealed. Monero, Dash, and Zcash are examples of such currencies. Extremist and terrorist groups have recognised the usefulness of privacy-focused cryptocurrencies, while their use remains limited. They are increasing their utilisation of Monero in order to circumvent Bitcoin's traceability characteristic. There is also evidence indicating that a Jihadist campaign is actively seeking donations via privacy coins. The al-Sadagah Organisation, self-identified as a charitable organisation, carried out a crowdfunding initiative in late 2017 through social media platforms and Telegram associated with al-Qaeda. The campaign initially solicited anonymous and secure Bitcoin donations from supporters to finance a project aimed at constructing amenities in a specific site within Latakia province, Syria. On November 30, 2017, a donation of 0.075 Bitcoin, valued at USD 685, was received at the al-Sadaqah address. On the following day, the funds were moved to a different address with a higher value of USD 803, which was a result of Bitcoin's significant price surge. After facing public scrutiny, the campaign is currently testing the usage of more extensively anonymised coins. The organization's Twitter account announced its acceptance of the privacy-oriented alternative cryptocurrencies Monero, Dash, and Verge. As of April 1, 2018, al-Sadaqah has used Twitter to request money, urging followers to financially assist the Muji group in Syria. The appeal emphasises that payments will be fully secret and impossible to track (Keatinge et al., 2018). The various instances demonstrate the utilisation of cryptocurrencies for the purpose of conducting experiments related to terror financing. However, there are three prominent emerging technologies that can intersect with cryptocurrencies and present a

DOI: https://doi.org/10.47362/EJSSS.2025.6211

significant risk in the near future. One significant development is the merging of cryptocurrencies with other technologies that provide anonymity, such as the Dark Web. The Dark Web comprises numerous websites that employ the Tor technology to disguise IP addresses and encrypt communication. Transactions on the Dark Web mostly utilize cryptocurrencies (Keatinge et al., 2018). Data available on the intersection of cybercrime and terrorism is extremely restricted. The story of Ardit Ferizi, a Kosovo national also known as the 'Albanian Hacker', exemplifies the intersection of cybercrime, terrorism, and cryptocurrencies, offering insight into potential future developments. In August 2015, Ferizi deployed malicious software to acquire personal data from individuals employed by the US government and military. This material was subsequently disseminated by ISIS as a compilation of targeted individuals. Subsequently, the individual insisted on receiving a payment in bitcoin from the company as a condition for eliminating the virus (Keatinge et al., 2018). The third convergence pertains to the integration of non-fungible tokens (NFTs) and cryptocurrencies. NFTs serve as a platform for disseminating propaganda and generating funds. Additionally, when combined with cryptocurrencies, they facilitate the movement of funds. In August 2022, an individual who supports ISIS produced the first non-fungible token (NFT) that promotes the ideology of ISIS. Terrorist organisations and their supporters are engaging in the exploration of novel technology, as evidenced by this (TRM Labs, n.d.).

Furthermore, innovative methods are currently being devised in the cryptocurrency industry, which could potentially be utilised by terrorists. One of the initial advancements being developed is the implementation of 'atomic swaps', which are techniques that allow two parties to immediately exchange two different cryptocurrencies on distinct blockchains, without any delay or disruption (Faster Capital, n.d.). Another approach, which does not appear highly advanced, for circumventing centralized cryptocurrency exchanges is utilizing websites like localBitcoins.com. These platforms facilitate direct transactions between users of cryptocurrencies and users of traditional fiat currencies. There have been multiple instances when people have been acting as brokers for cryptocurrencies on Local Bitcoins, demanding a fee to facilitate the conversion of physical money for digital currencies (Keatinge et al., 2018).

Cryptocurrency and Terrorism in South Asia: Assessment of Reported Cases

According to a report by Binance, the world’s largest cryptocurrency exchanges highlighted that South Asia’s crypto market is rapidly maturing along with greater adoption of cryptocurrencies (The Hindu Bureau, 2025). According to the crypto adoption report by Chain

analysis of 151 countries in 2024, India ranked first, Pakistan ranked 9th, Afghanistan ranked 31st, Bangladesh ranked 35th, while Nepal and Sri Lanka ranked 71st and 72nd respectively (Chainalysis, 2024). Crypto Currencies are illegal in Afghanistan, Bangladesh and Nepal. While in India, Cryptocurrency neither banned nor legalised as a tender. In Pakistan also, the legality of the use of cryptocurrency is governed under grey zone. Despite a formal government ban, Pakistanis currently own between $20 and $25 billion in digital currencies, placing them ninth in the world for cryptocurrency adoption, according to a survey by the Asian Development Bank. According to the Asian Development Bank report, a 165% currency devaluation since 2017 and 38% inflation peaks in 2023 are the main causes of the widespread adoption of cryptocurrencies. For Pakistanis whose access to foreign cash is restricted and their local purchasing power is declining, cryptocurrencies provide a financial lifeline. Citing concerns about capital flight and pressure on depleted foreign exchange reserves, authorities tightened their restrictions on ownership and trading in April 2023. Despite the widespread restriction, grey market crypto trading has developed as residents seek safe-haven assets to protect their savings (CoinMarketCap, 2025). Some factors motivated crypto adoption in Afghanistan with fear of US sanctions after Taliban takeover during 2021-2022 (Silic, 2022). Cryptocurrencies usage in South Asian countries is increasing despite of governments reluctancy in fully legalising it. Local law enforcement agencies are still trying to understand the phenomenon. They also lack technological sophistication to deal with it. The benefit crypto currencies offer such as anonymity, decentralised and fast transfer of money have attracted the global terror organisations, organised criminal syndicates to use it with integration various other illegal instruments such as dark net in these countries. In South Asia, two types of cases were noticed where a terror organisation used cryptocurrencies. First type of cases in which global terrorist groups are using crypto currencies such as ISIS and its local affiliates and Hamas. The Second trend includes local terror groups are using cryptocurrencies such as terror groups in Jammu and Kashmir.

According to the US Department of Treasury, ISIS has been increasingly utilising virtual asset service providers to finance their subordinates in Central and South Asia (TRM Labs, n.d.). Overall, bitcoin appears to be a very small but growing source of funding for ISKP. TRM Labs has identified the utilisation of cryptocurrency by pro-ISIS groups originating from Tajikistan and Pakistan to spread propaganda and attract individuals to support their objectives (TRM Labs, n.d.). In 2021, Hamas illicitly seized the cryptocurrency owned by an individual residing in Delhi. The New Delhi case marked the beginning of Hamas' activities in India. In

DOI: https://doi.org/10.47362/EJSSS.2025.6211

late 2021, the Special Cell of the Delhi Police launched an investigation into the theft of bitcoin valued at 40 million rupees ($480,900 approximately) from a businessman's wallet in West Delhi. In his complaint, the merchant claimed that unidentified burglars unlawfully transferred his Bitcoin, Ethereum, and Bitcoin cash from his cryptocurrency wallet (WION, 2023). In Mangalore, a premature explosion occurred in a moving autorickshaw in 2022. The case of Mangalore Blast an inquiry that was started by the State Police and then picked up by the NIA. The ISIL-affiliated network provided funding for the explosives, which were intended to be planted in a shrine. Three suspects were the focus of the first investigations because of their roles in the plot and the acquisition of the explosives. Crypto wallets were used to receive numerous small amounts of money to finance the attempted terrorist act, according to operational analysis obtained from FIU-IND. By obtaining fund flow data from eight distinct VASPs, the investigating authorities were able to determine whose accounts the funds originated from and, using IP addresses, identify the online handler responsible for the transfers. It was discovered that the accused had received money via their buddies' and other close connections' cryptocurrency wallets (The Financial Action Task Force (FATF), 2024). A blockchain forensic company based in Israel alleges that the suicide bombers who carried out the attacks in Sri Lanka during the Easter period utilised cryptocurrencies as a means of fundraising (Allagh, 2020). PFI members are also urged by the Islamic State to join ISIS in order to carry out jihad and build a caliphate in India. Another example is the Popular Front of India, which used cryptocurrency to accept donations and fund its terror support operations. The PFI's subversive activities persist in spite of multiple bans. The PFI requests Zakat in cryptocurrency, with support from organizations such as the Party of Islamic Renewal on a global scale. According to investigations, the PFI gathers Zakat for a number of alleged purposes, such as helping victims of tragedies like the Delhi Riots, assisting pilgrims performing the Hajj, and providing funds to fictitious organizations like the National Development Front and the Rehab Foundation. The PFI's illegal actions in India are made possible by foreign sponsorship in nations where it works under false pretences, like the Kuwait India Social Forum (KISF). ISIS, the Party of Islamic Renewal, and KISF are among the terror groups that have supported the PFI with cryptocurrency donations, according to a report titled The Popular Front's Online Narratives Attempting to Radicalise Indian Muslims, which was produced by the UK-based tech company Logically. These groups' propaganda encourages supporters to donate to the PFI using cryptocurrency wallets like Exodus, Samourai, Atomic Monero, and Bitcoin and to use fast transfer services like XRP, Ripple, and Cardano in order to be anonymous and get around security barriers (Awasthi, 2024).

DOI: https://doi.org/10.47362/EJSSS.2025.6211

The remaining cases involve the utilisation of cryptocurrencies to finance terrorism by organisations in Jammu and Kashmir, with the aim of instigating unrest in the region. During their raids in the districts of Poonch, Baramulla, and Kupwara, the Jammu and Kashmir Police uncovered the link between bitcoin and terrorism. Evidence suggests that the Pakistani ISI has utilised bitcoin as a method to finance its terrorist activities in the region of Jammu and Kashmir (Zulfikar Majid et al., 2022). Notably, members of the Ansar-Al-Islam (AAI) and Ansarullah Bangla Team (ABT) have openly confessed to transferring large amounts of bitcoins to terrorist groups active in Kashmir since 2014 (Clark, 2023). The incident highlighted the intention and capacity of Pakistani terrorist organisations to use emerging technology by using cryptocurrencies to fund acts of violence in Jammu and Kashmir through Bangladesh. The July 2025 Pahalgam terror attack and subsequent intelligence inputs sparked the current inquiry, which focuses on suspected transactions using TRX tokens connected to wallets in extremist-active regions like Pakistan, Jammu & Kashmir (J&K), and Syria. Authorities believe private crypto wallets and lax Know Your Customer (KYC) and Anti-Money Laundering (AML) practices may be facilitating these illicit flows. The Enforcement Directorate (ED) is investigating Binance for violations of the Foreign Exchange Management Act (FEMA) and freezing accounts connected to Indian partners as part of a coordinated effort with the State Investigation Agency (SIA) of Jammu & Kashmir. SIA recently conducted Unlawful Activities Prevention Act (UAPA) raids in Jammu, Doda, and Handwara (South Asia Terrorism Portal, n.d.).

Conclusion

Terrorist organizations may find more use for cryptocurrencies in focused crowdfunding campaigns aimed at raising money online, or in sporadic and ad hoc international Peer-to-Peer transfers among group members as a means of transferring funds rather than looking to them as a source of continuous, sustained funding. The partition of funding and rising through cryptocurrencies looks limited as of now with limited data availability. But in the merging with the other new emerging technologies in the domain such as Non-Fungible Token, atomic swipe and convergence of cyber-crime, terrorism and currency requires much attention from the security agencies. This shows potential of crypto threats posed by the use of cryptocurrencies and the possibility of them being a major source and tool in the overall terror finance basket.

References

Allagh, P. (2020). Terrorism financing through cryptocurrencies [Journal-article]. *International Journal of Legal Science and Innovation*, *2*(1), 400–415. https://ijlsi.com/wp-content/uploads/Terrorism-Financing-Through-Crypto-currencies.pdf

Awasthi, S. (2024, May 8). *Exploring the nexus: Cryptocurrency, Zakat, and terror funding*. orfonline.org. https://www.orfonline.org/expert-speak/exploring-the-nexus-cryptocurrency-zakat-and-terror-funding

Balasubramaniyan, D. V., & Raghavan, D. S. (2017). *Terror Funds in India: Money Behind Mayhem*. Lancer Publishers LLC.

Canadian Press. (2022, December 15). *Ontario man charged in FBI investigation into alleged ISIS financial support. Toronto Star.* https://www.thestar.com/news/canada/ontario-man-charged-in-fbi-investigation-into-alleged-isis-financial-support/article_a065b89a-2df3-58ba-9288-57653b5c4567.html

Chainalysis. (2024). The 2024 Geography of Crypto Report. In *Chainalysis*. Retrieved July 15, 2025, from https://www.chainalysis.com/blog/central-southern-asia-crypto-adoption-2024/

Clark, A. (2023, July 5). *Cryptocurrency terrorist financing in Kashmir*. Grey Dynamics. https://greydynamics.com/cryptocurrency-terrorist-financing-in-kashmir/

CoinMarketCap. (2025, July 17). *Pakistan Crypto News: Pakistan emerges as 8th-Largest crypto market with 25 billion in digital assets, ADB reports*. CoinMarketCap Academy. https://coinmarketcap.com/academy/article/pakistan-crypto-news-pakistan-emerges-as-8th-largest-crypto-market-with-25-billion-in-digital-assets-adb-reports

Faster Capital. (n.d.). *Atomic swaps and regulatory compliance: Navigating the legal landscape.* Retrieved February 18, 2024, from https://fastercapital.com/content/Atomic-Swaps-and-Regulatory-Compliance--Navigating-the-Legal-Landscape.html

The Financial Action Task Force (FATF). (2024). *India's measures to combat money laundering and terrorist financing*. Retrieved July 15, 2025, from https://www.fatf-gafi.org/content/dam/fatf-gafi/mer/India-MER-2024.pdf.coredownload.inline.pdf

Freeman, M., & Ruehsen, M. (2013). Terrorism Financing Methods: An Overview. *Perspectives on Terrorism*, *7*(4), 5–26.

Gunaratna, R. (2017). *Mastermind of Terror: The Life and Death of Bahrun Naim*. *9*(4).

Hajjaj Bin Fahd Al Ajmi. (n.d.). Counter Extremism Project. Retrieved February 17, 2024, from https://www.counterextremism.com/extremists/hajjaj-bin-fahd-al-ajmi

IJLSI. (2020, July 18). 44. Terrorism Financing Through Cryptocurrencies. *International Journal of Legal Science and Innovation*. https://www.ijlsi.com/terrorism-financing-through-cryptocurrencies/

Keatinge, T., Carlisle, D., & Keen, F. (n.d.). *Virtual Currencies and terrorist financing: Assessing the risks and evaluating responses*.

Keatinge, T., & Danner, K. (2021). Assessing Innovation in Terrorist Financing. *Studies in Conflict & Terrorism*, *44*(6), 455–472. https://doi.org/10.1080/1057610X.2018.1559516

Keatinge, T., & Keen, F. (2020). *New Technologies and Terrorism Finance* (A Sharper Image, pp. 51–58). Royal United Services Institute (RUSI). https://www.jstor.org/stable/resrep40327.8

Krishnan, A. (2020). Blockchain Empowers Social Resistance and Terrorism Through Decentralized Autonomous Organizations. *Journal of Strategic Security*, *13*(1), 41–58.

Majid,DHNS, Z. (n.d.). *ISI using Bitcoin trade to fund terrorism in J&K: SIA probe*. Deccan Herald. Retrieved February 17, 2024, from https://www.deccanherald.com/india/isi-using-bitcoin-trade-to-fund-terrorism-in-jk-sia-probe-1132614.html

Norton, S., & Chadderton, P. (2016). *Terrorism Financing* (Detect, Disrupt and Deny, pp. 10–17). Australian Strategic Policy Institute. https://www.jstor.org/stable/resrep04244.6

Silic, B. A. (2022, March 16). *Afghans turn to cryptocurrencies amid US sanctions*. https://www.bbc.com/news/world-asia-60715707

South Asia Terrorism Portal. (n.d.). *India intensifies crypto crackdown amid terror financing concerns.* Retrieved February 17, 2024, from https://www.satp.org/terrorism-update/india-intensifies-crypto-crackdown-amid-terror-financing-concerns

Statista. (n.d.). *Number of cryptocurrencies 2013–2024.* Retrieved April 1, 2024, from https://www.statista.com/statistics/863917/number-crypto-coins-tokens/

The Hindu Bureau. (2025, April 28). *Crypto market in India, Sri Lanka, and other South Asian countries is "rapidly maturing": Report*. The Hindu. https://www.thehindu.com/sci-tech/technology/crypto-market-in-india-sri-lanka-and-other-south-asian-countries-is-rapidly-maturing-report/article69500705.ece

TRM Labs. (n.d.). *Terrorist financing: Six crypto-related trends to watch in 2023.* Retrieved February 17, 2024, from https://www.trmlabs.com/post/terrorist-financing-six-crypto-related-trends-to-watch-in-2023

U.S. Department of Justice. (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

U.S. Department of Justice. (2015, August 28). *Virginia man sentenced to more than 11 years for providing material support to ISIL*. https://www.justice.gov/opa/pr/virginia-man-sentenced-more-11-years-providing-material-support-isil

Whyte, C. (2019). Cryptoterrorism: Assessing the utility of blockchain technologies for terrorist enterprise. *Studies in Conflict and Terrorism*, *46*(7), 1126–1149. https://doi.org/10.1080/1057610x.2018.1531565

WION. (2023, October 11). *Israel vs Hamas: Indian officials scramble to prevent crypto assets from reaching terror group*. Retrieved February 18, 2024, from https://www.wionews.com/india-news/as-israel-cracks-down-on-wallets-maintained-by-hamas-indian-officials-on-toes-to-prevent-repeat-of-2021-645323