CRYPTOCURRENCY BASED TERROR FINANCING ON THE DARK WEB: LEGAL AND REGULATORY CHALLENGES

Kaviya R, LLM (CBCS), School of Excellence in Law,
The Tamil Nadu Dr. Ambedkar Law University, Chennai

ABSTRACT

The rise of cryptocurrency and the dark web has changed the methods of terrorist financing and creating new challenges to the regulatory and legislative framework that prevails. Cryptocurrency allows quick, seamless, and anonymous transactions, whereas dark web ensures safe and anonymous channels for communications as well as other criminal activities. This technology has enabled a decentralized funding system that remains beyond the reach of traditional monitoring measures.

This paper examines the emerging connection between cryptocurrency and the issue of terrorist financing, which includes a detailed analysis of the techniques employed by terrorist organizations, including online solicitation of funds, transaction laundering, using privacy coins, and trading at dark web markets. Further, the paper aims to study the legal aspects from both global and Indian perspectives.

Moreover, the study highlights several issues related to the topic of law and regulation, which include anonymity, jurisdiction issues, technology issues, and the absence of universal standards on the global level. The paper also discusses the impact on national security with regard to the emergence of decentralized terrorist organizations and lone-wolf terrorism. Finally, it suggests reforms involving stronger legal frameworks, improved international cooperation, and the use of advanced technological tools to address these challenges effectively.

Keywords: Cryptocurrency, Dark Web, Terror Financing, Blockchain Technology, Anonymity, Virtual Assets, National Security.

1. INTRODUCTION:

Terrorist financing has experienced a significant change in the digital era. Traditionally, terrorist group relied on cash transactions, donations and informal systems like hawala networks. While these methods were very difficult to regulate and they still operated within identifiable financial structures. However, the emergence of cryptocurrencies and the dark web have significantly changed this financial structure that goes beyond the traditional limitations.

Cryptocurrencies allow for direct transactions between individuals without any involvement of intermediaries. This allows funds to be transferred quickly across the borders with less regulatory control. Meanwhile, the dark web provides an encrypted space that supports anonymous communications and access to illegal markets. The combination of these technologies has created a separate financial system that mainly functions beyond the control of regulatory bodies.

Recent global developments shows that terrorist groups are using these technologies more and more. They are not only depending centralized finding networks, but they are also moving towards decentralized and micro-financing methods and this involving smaller transactions distributed across various sources. Terrorist groups are adopting to these technologies. This evolution has significantly increased the difficulty of detecting and preventing terrorist financing.

2. CONCEPTUAL AND TECHNOLOGICAL BACKGROUND:

2.1 Cryptocurrency:

The technology of crypto currency is based on cryptography, from where its name as well. Cryptography helps exchanging financial transactions digitally, verify the transfers and secures the creation of every new unit of currency created. Unlike digital currency, which is paperless money, is different from real money since it is operated in decentralised form.

A cryptographic attack allows an attacker to significantly reduce or eliminate the security provided by encryption. This approach is especially powerful in the case of crypto currency and could allow theft, counterfeiting, or almost any other type of attack against the system.[1]

[1] Prapti Allagh, "Terrorism Financial Through Crypto-Currencies" 2 *International Journal of Legal Science and*

It means the transfer taking place between users is in peer-to-peer network of computers. There is no authority to regulate and control over this form of money. While transacting crypto currency, one does not need to take approval from any authority, like in case of banks. Value of units of crypto currency is decided by the market participants without the help of banking institutions, or any transactional guidelines that are adhered by real currencies. Crypto currencies also take care of its user's privacy by hiding the identity of the individuals dealing in this technology, meaning everyone's privacy remains intact. Basically, anyone in the world can create a Bit coin address and start dealing in the exchange of digital currencies without even giving a name or an address.

Cryptocurrencies work with the help of **block chain technology**, which is a complex system that ensures its properly functioning. Cryptocurrencies usually represent itself in form of units which are lodged into a database to determine how much currency is held against each individual name or address. The working is similar to that of banking. Each transaction is recorded in the database and there is no actual physical exchange taking place. The movement of cryptocurrency that is recorded on a platform of blockchain is a peer-to-peer, global distributed ledger that records transactions between members on the blockchain platform without the interference of any third party. The next step is encryption of transactional data which then is distributed across the network. Data has to go through "mining" process which confirms that a transaction is valid and only then is that data recorded permanently. Specialist who does mining are called "miners" who get incentives in a form of block rewards, through which new coins or generated. This process is repeated continuously, which provides for a robust and incentivized monetary system called cryptocurrency.

Holder of cryptocurrency with the help of a privacy key authenticate their identity because of which they exchange and trade units. Search privacy key, which is formatted as whole number between 1 to 78 digits, make them have access to currency. In the absence of any key, the holder cannot spend their cryptocurrency. Losing a private key is like throwing away a wad of cash into a trash. A new key represents a new set of units. However, one main advantage of having a private key is to keep cryptocurrency safe and private.[2]

Bitcoins: Cryptocurrency has become a preferred option of payment for legal and illegal means.

Innovation 403 (2020).

[2] Prapti Allagh, "Terrorism Financial Through Crypto-Currencies" 2 *International Journal of Legal Science and Innovation* 404 (2020).

In fact, cryptocurrencies have now crossed borders and are also becoming a preferred mode of payment for offline products and services. Cryptocurrencies offer anonymity and agility of transactions. The cryptocurrency that changed the way virtual currencies functioned was "Bitcoin". It did this with its technology referred to as the "blockchain". "Bitcoin", which started in or about 2009, is the first of its kind. Bitcoin worked in a decentralised system, which is also paradoxically referred to as "trust less". The currency was launched by an anonymous person, with the pseudonym "Satoshi Nakamoto". The creator was therefore anonymous. The currency had no affiliation with a specific domain.[3]

2.2 Dark Web:

The dark web is the part of the internet where users can access unindexed web content anonymously through special web browsers like The Onion Router (TOR). Through the dark web is popularly associated with illegal activities, it is also used by the intelligence community, whistle blowers, members of the media, and ordinary citizen whose communication may be monitored or restricted by the government.

The origins of the dark web can be traced to researchers and scientists in the U.S. Naval Research Laboratory who, in 2002, recognized how easily digital activity and communication could be monitored, intercepted and exploited. It grew out of a need for a more secure communications channel in the intelligence community, despite the fact that it is often associated with nefarious activities today.[4]

The dark web resides very much within the Internet domain, but the doorway to this underworld is hidden using masking technologies. The dark wed is hidden using anonymising software including the Onion Router (Tor) technology. Very powerful encryption is used to hide these sites. The primary objective of the technology used to create the dark web was to avoid surveillance and to offer a platform for free exchange of ideas and content, without fear of repercussions, particularly through Government actions. Every attempt of the Government to regulate the Internet or to gain access to digital content has resulted in the libertarians digging deeper and seeking hidden platforms. The crypto-war, as the Government and liberty seeking individuals fight is referred to, has been the primary impetus to spawn the dark child of the

[3] N S Nappinai, *Technology Laws Decoded* 59 (Lexis Nexis Publication, 1st edn., 2022).
[4] Kurt Baker, *The Dark Web Explained,* available at https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/dark-web/ (last visited on 10 May 2026)

Internet – the Dark Web.[5]

2.3 Link between Cryptocurrency and Terrorist Financing:

Cryptocurrency and terrorism have been connected primarily due to the characteristics peculiar to digital currency. Contrary to the traditional banking system, cryptocurrency operates independently of any single authority, making financial transactions independent of any intermediary, such as a bank. This, tracking financial transactions becomes significantly difficult, especially compared to the conventional financial network.

The use of cryptocurrency as an element of terror funding can also be explained by the fact that there is little user identification. The financial operations carried out via digital currency are recorded on the blockchain technology, but they can be associated only with wallet addresses, but not the named of real users. Therefore, it is much easier for an individual or organization to remain anonymous while engaging in financial transactions. With the help of encrypted communication channels, such anonymity is further strengthened, making the tracing process more complicated.

Transferring funds is made easy using digital currency. In particular, the cryptocurrency transaction does not require the implementation of traditional banking procedures. Therefore, funds transferred from one country to another will not face restrictions or other hindrances, which makes the transactions faster and more convenient for terrorists.

Along with traditional means of funding, recently some terrorist organizations have been known to use cryptocurrency for small-scale fundraising. Rather than collecting large sums from a limited number of sources, the idea is to collect smaller sums from lots of people. Such transfers are usually unnoticed since they do not immediately attract suspension; however, with time, their aggregate sum may become impressive.

Besides, there are technological ways to disguise the flow of finances. The use of mixing techniques makes it hard to trace funds through several transactions at once. Furthermore, some cryptocurrencies were created especially for enhanced privacy and security. It should be emphasized, however, that cryptocurrency in itself cannot be considered illegal. This financial technology is widely spread around the world and has many legal uses. What turns

[5] N S Nappinai, *Technology Laws Decoded* 48 (Lexis Nexis Publication, 1st edn., 2022).

cryptocurrency into an element of the process of terrorist financing is its misuse for illegal purposes.

3. METHODS OF CRYPTOCURRENCY BASED TERROR FINANCING ON THE DARK WEB:

The use of cryptocurrency in terrorist financing has become structured and multi-layered process, particularly with the support of the dark web. Terrorist groups have stopped replying on only one source of money or way of transferring it, instead, they adopt a combination of digital strategies to raising, transferring, concealing and using funds. While the dark web offers a safe haven and anonymity, the use of cryptocurrencies offers speed and efficiency in terms of transactions.

3.1 Online fundraising and Digital Donations:

One of the most popular techniques adopted by terrorist organizations for fundraising purpose is online fundraising. Terrorist organizations use social media sites, encrypted chat applications like Telegram, as well as dark web forums to access a worldwide audience. They share cryptocurrency addresses and ask people to donate. What makes this fundraising technique more powerful than other ones is that you don't need physical access to anyone in order to receive donations. Any person across the globe can easily make an anonymous donation through online means.

For instance, organizations like Hamas conduct various cryptocurrency fundraising campaigns with the use of Bitcoin as well as other stable coins. The results of their campaigns have shown the potential of digital technology in helping with fundraising processes. Also, it should be noted that these kinds of donations are characterized by micro-transactions, which means that they consist of small sums received from multiple donors.

3.2 Transaction obfuscation techniques:

Having received finances, terrorist organizations resort to certain methods of masking the money movement. The process resembles money laundering and serves the purpose of erasing any possible track of transactions. The most popular methods here include mixers and tumblers. Both of them operate by merging any transactions made through different cryptocurrency accounts and distributing them randomly. Thus, the link between the initial sender and receiver

is destroyed, and the tracing process becomes almost impossible.

Besides, there are cases when groups resort to layering transactions to mask the origin of money. In this method, transactions between different crypto accounts are made several times until the initial account gets erased. Such methods greatly undermine the benefits of transaction visibility provided by the blockchain technology system.

3.3 Utilization of Privacy Coins:

Increased use of crypto currencies with a focus on privacy represents another stage of terror financing. In contrast with other cryptocurrencies like Bitcoin, privacy coins are designed to ensure anonymity.

These coins offer protection against:

- Sender's identity
- Receiver's identity
- Amount of money transferred

Thus, it becomes almost impossible for authorities to track transactions using traditional methods of analysis of blockchain technology.

As per sources, terror outfits associated with ISIS have increasingly shifted from other forms of cryptocurrency to privacy coins such as Monero owing to its benefits in terms of anonymity. It is response to changes made by terrorists to avoid being tracked by law enforcement bodies. This is one of the biggest challenges as far as blockchain technology is concerned.

3.4 Fiat Conversation of Cryptocurrency:

While cryptocurrency is helpful for fund transfer processes, terrorist organisations have to convert the funds to fiat currency to use them in physical operations. Hence, the fiat conversion of currencies is a very important step within the financial process.

The fiat conversion can be done via multiple pathways, including:

- Cryptocurrency exchange platforms that help to convert digital currencies to fiat currency
- Peer to peer platforms that offer direct money transfers between persons without proper regulation
- Informal system like the hawala system

These methods are helpful in transforming digital money to the real world. It is important to note that this part of the process can be quite challenging from a regulation standpoint because it often takes place in countries with poor financial regulation.

3.5 Dark web markets as operational platforms:

The dark web act as a focal point for the use of funds collected via cryptocurrencies. This includes the availability of anonymous online markets that offer all sorts of illegal goods and services.

These include:

- Weapon and ammunitions
- Counterfeit documents
- Explosives and other technical devices
- Tools for hacking, spying, and communications

Almost all operations in such places are carried out via cryptocurrency transactions. Apart from being secure, they are also convenient. Moreover, one can use these platforms for communication and negotiation as well, all within the safety of protected online environment. It is interesting to note that these marketplaces are also equipped with rating facilities and even escrow services, much like conventional online shopping portals.

4. INTERNATIONAL LEGAL FRAMEWORK:

On an international level, the regulation of cryptocurrency related terror financing is mainly

regulated through the Financial Action Task Force (FATF) along with United Nations initiatives. As the transactions using cryptocurrencies take place at international level, hence international efforts are imperative in regulating it's use.

As per FATF, a risk-based approach should be adopted for regulating virtual assets. Under this, countries have to perform risk assessment for cryptocurrencies (Recommendation 1) and make sure about the coordination among regulatory bodies (Recommendation 2). Furthermore, Virtual Assets Service Providers (VASSP) such as cryptocurrency exchanges need to be registered or licensed according to Recommendation 14.

In addition, FATF insists on monitoring and transparency. This is reflected in the recommendations made by it that require countries to identify risks of new technology (Recommendation 15), monitor crypto exchange operators properly (Recommendation 26), impose sanctions (Recommendation 35), and share financial transactions data (Travel Rule: Recommendation 16). In addition to this, Recommendation 40 encourages countries to engage in information sharing.

Apart from FATF, United Nations requires it's member countries to criminalize terror financing and freeze assets of designated persons among others. However, the adoption of these recommendations by countries may vary significantly.[6]

5. NATIONAL LEGAL FRAMEWORKS:

5.1 Unlawful Activities (Prevention) Act, 1967 (UAPA)[7]:

The Unlawful Activities (Prevention) Act is the main statue that governs matters concerning terrorism and terrorist funding in India. It makes it illegal to be involved in any act that has to do with raising, gathering, or funding terrorism. Under the act, people can be classified as terrorists and have all their properties frozen. Despite being enacted prior to the development of cryptocurrencies, the provisions of the act are wide enough to include virtual currencies as well.

[6] European Parliament, "Virtual Currencies and Terrorist Financing: Assessing the Risk and Evaluating Responses" (Policy Department for Citizens' Rights and Constitutional Affairs, May 2018).
[7] The Unlawful Activities (Prevention) Act, 1967 (Act 37 of 1967).

5.2 Prevention of Money Laundering Act, 2002 (PMLA)[8]:

The Prevention of Money Laundering Act aims at stopping the laundering of funds gained from criminal endeavours. It helps in tracking, freezing, and seizing the assets that have been used in carrying out such criminal activities. In recent times, it has been amended to cover virtual digital assets as well, which makes the transactions carried out using cryptocurrency fall under its ambit.

5.3 Information Technology Act, 2000[9]:

The Information Technology Act contains all the laws that help in handling cases of cyber crime. Even though the Act does not provide any rules regarding the use of cryptocurrencies, it becomes applicable to all forms of illegal activities done on the Internet like hacking and stealing one's identity. As terrorist funding through cryptocurrencies is mostly carried out through the Internet, this Act becomes very useful.

5.4 Financial Intelligence Unit (FIU-IND):

Financial Intelligence Unit (FIU-IND) is an important government agency whose mandate entails observing financial transactions. Suspicious transaction information is collected by this unit from reporting institutions such as banks and crypto-exchanges. Financial Intelligence Unit (FIU-IND) is also crucial in the identification of patterns that indicates illegal financial activities and prevent terror financing.

6. LEGAL AND REGULATORY CHALLENGES:

Enforcement of regulation to control the use of cryptocurrency as terror financing poses several challenges. The technological advancements in digital currency, together with its anonymous nature and its use on the dark web, makes enforcement difficult for the concerned authorities. Such challenges are not only applicable in one country but on a global level as well.

6.1 Anonymity:

Anonymity is one of the main challenges related to the regulation of cryptocurrency. Unlike

[8] The Prevention of Money Laundering Act, 2002 (Act 15 of 2002).
[9] The Information Technology Act, 2000 (Act 21 of 2000).

the conventional system, which requires people to have an account that verifies their identities, cryptocurrency transactions relate to the addresses of wallets. As a result, the government finds it difficult to know the real identities behind the financial transactions. Therefore, it becomes easier for terrorist groups to get and send money without having to expose themselves to authorities, especially if they use encrypted platforms and the dark web.

6.2 Jurisdiction Issues:

Jurisdiction issues become another challenge faced by law enforcement in controlling the use of cryptocurrency in terror funding. Cryptocurrency transactions do not need financial institutions. Therefore, they can easily occur outside the jurisdiction of a particular country and thus complicate prosecution. Each nation has its laws concerning the matter.

6.3 Complexity of Technology:

The highly sophisticated nature of the technology that underlies cryptocurrencies makes the work of the law enforcement authorities more challenging. Understanding and investigating blockchains, encryptions and other technologies that enhance privacy requires high-level technical skills. However, many agencies do not possess sufficient competence and resources to track transactions and develop substantial cases against offenders.

6.4 Gaps in Regulations:

Uniform regulations of cryptocurrency at the international level are currently missing. While some nations have put in place tough regulations concerning their use, others have no regulation at all. In this way, the gap created provides room for terrorists to conduct themselves illegally. This regulatory inconsistency facilitates the movement of their activities from one jurisdiction to another.

6.5 Difficulty of Tracking the Dark Web:

The dark web constitutes yet another obstacle to the regulation of terrorist financing. Using encrypted network and their location cannot easily be traced. Thus, there are considerable limitations faced by the agencies in tracking such activities and gathering sufficient evidence.

7. IMPACTS ON NATIONAL SECURITY:

The use of cryptocurrency in funding terror attacks presents numerous threats to national security because the currency is not traceable; hence it facilitates the actions carried out by the groups.

7.1 Enables Decentralization of Terror Actions:

Through cryptocurrency, fund raising can be done using various channels rather than a single channel used in other cases. Therefore, even when one of the channels is blocked, it helps terrorists to raise money.

7.2 Allows for Lone-Wolf Attacks:

Small amounts of money can easily be sent to lone-wolf individuals via cryptocurrency. Such individuals carry out terror attacks as per instructions received without coming into contact with the terrorists.

7.3 Renders Financial Monitoring Systems Useless:

Financial institutions such as banks provide a platform where it becomes easier for the government to follow any transaction taking place in the system. But cryptocurrency is independent of such a platform.

8. SUGGESTIONS AND REFORMS:

In view of increasing instances of terror financing via cryptocurrencies on the dark web, the following recommendations and reforms may be helpful:

- **Strengthening Legal Framework:** The need to have clear and robust laws in place that regulate cryptocurrencies should be recognized. In addition, the existing laws must be upgraded to include regulation of digital assets.

- **Strict Regulation of Crypto Exchanges:** Crypto exchanges are required to comply with strict KYC norms and guidelines. Proper record keeping and reporting can reduce the risk of misuse.

- **Use of advanced Technology:** Laws and authorities should adopt sophisticated technology to monitor transactions and detect any suspicious activities. Blockchain analysis is critical in this respect.

- **International Coordination:** It may be noted that terror financing activities using cryptocurrencies involve several nations. As such, international cooperation is important in this regard.

- **Strengthening Cyber Monitoring:** Cyber monitoring dark web activities should be enhanced to spot suspicious transactions and communications by terrorist organizations.

- **Building Capability:** Enforcement agencies will require adequate training and capability development in handling such digital financial crimes. Technical capability building is particularly significant.

9. CONCLUSION:

The use of cryptocurrencies for terror financing through the dark web is among the significant issues in the contemporary digital era. The integration of such elements as anonymity, decentralization, and cross-border money transfers facilitates terrorist's operations in collecting funds and making transactions that cannot be controlled using traditional means. In addition, the dark web serves as an advantageous platform for conducting activities due to its security features.

Meanwhile, legal regulations have already been updated to combat new forms of cybercrime. Nevertheless, there remain some obstacles that prevent governments from implementing laws in various states, and technological problems.

Hence, combating this threat requires a holistic approach, including legislative reforms, cooperation between nations, and utilizing innovative technologies. It should be noted that the development of regulations needs to be done carefully to avoid limiting innovation and the proper functioning of the financial system. In summary, cryptocurrency-based terror financing constitutes an essential problem that can be addressed by regulating the usage of digital currencies.

10. REFERENCES:

1. Prapti Allagh, "Terrorism Financial Through Crypto-Currencies" 2 *International Journal of Legal Science and Innovation* (2020).

2. N S Nappinai, *Technology Laws Decoded* (Lexis Nexis Publication, 1st edn., 2022).

3. Kurt Baker, *The Dark Web Explained,* available at https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/dark-web/

4. European Parliament, "Virtual Currencies and Terrorist Financing: Assessing the Risk and Evaluating Responses" (Policy Department for Citizens' Rights and Constitutional Affairs, May 2018).

5. The Unlawful Activities (Prevention) Act, 1967 (Act 37 of 1967).

6. The Prevention of Money Laundering Act, 2002 (Act 15 of 2002).

7. The Information Technology Act, 2000 (Act 21 of 2000).