AN ANALYSIS OF RAMPANT GROWTH IN USAGE OF VIRTUAL ASSETS IN TERROR FUNDING

Shubhayu Chakraborty, School of Law, Christ University

ABSTRACT

The emergence of cryptocurrencies has opened new avenues for terrorist outfits and crime syndicates to conduct illicit financial activities, ranging from terror financing and drug trafficking to human trafficking and corruption. Cryptocurrencies, particularly Bitcoin, offer decentralization, pseudo-anonymity, and global accessibility, making them highly attractive to groups seeking to evade traditional financial oversight. Terrorist organizations have been among the earliest adopters of these technologies, leveraging them as a digital means of payment that bypasses the need for central authority confirmation and provides a degree of anonymity that shields actors from responsibility.

In regions such as the Middle East, extremist groups like ISIS have exploited cryptocurrencies to fund operations through dark web campaigns, encrypted social media solicitations, and untraceable cross-border transfers. Conflict zones with weakened state institutions create a fertile environment for such practices. Furthermore, terrorist organisations in Southeast Asia have switched to untraceable virtual route and claims of international donation and state sponsored funding through crypto wallets have emerged.

The global level, governments and institutions have responded with uneven regulatory frameworks which prevent certain harm.The Financial Action Task Force (FATF) has issued guidelines including the "Travel Rule" to impose obligations on virtual assets, while the United States and European Union have incorporated a few broad regulations on cryptocurrencies anti-money laundering and counter-terrorism financing regimes. Yet in Asia, the landscape remains fragmented with lack of attempts to tackle new methods of terror funding.

In my paper I shall argue that outright prohibition of cryptocurrencies is neither practical nor desirable, given their role in financial innovation and inclusion. Instead, harmonized regulation, enhanced blockchain analytics, and improved international intelligence-sharing are necessary to counter their misuse. Ultimately, coordinated global action is essential to disrupt the weaponization of virtual assets for terrorism financing and to safeguard both economic development and international security.

Keywords: Bitcoin, FATF (Financial Action Task Force), Terror Financing, Crypto Currency

Research Objectives

1. To examine the role of cryptocurrencies, particularly **Bitcoin**, in facilitating terrorism financing and related illicit activities.

2. To analyze the regional dynamics of virtual asset misuse in the **Middle East and Southeast Asia,** focusing on case studies of extremist organizations and diverted humanitarian aid.

3. To evaluate existing global and regional regulatory frameworks, including FATF guidelines, U.S. and EU initiatives, and Asia's varied approaches.

4. To identify enforcement challenges, including **anonymity, decentralized exchanges**, and **regulatory arbitrage**.

5. To propose recommendations for regulation, improved international cooperation, and the use of blockchain analytics as tools to mitigate the risks of crypto-enabled terrorism financing.

Research Methodology

Doctrinal Legal Research: Analysing international conventions, national legislation, and FATF recommendations related to counter-terrorism financing.

Comparative Analysis: Studying regulatory responses across jurisdictions – Looking into Global Laws and comparing domestic laws in U.S, EU, India, Middle East and Pakistan.

Research Problem

The increasing exploitation of cryptocurrencies by terrorist organizations and criminal syndicates, combined with the inadequacy of existing counter-terrorism financing and anti-money laundering frameworks, highlights an urgent gap in global financial governance, as the decentralized and pseudo-anonymous nature of virtual assets enables untraceable cross-border transfers, dark web transactions, and misuse of charitable funds, particularly in conflict-prone

regions of the Middle East and Southeast Asia, thereby necessitating a cohesive international legal and regulatory framework to curb terrorism financing while balancing innovation and consumer protection.

1. INTRODUCTION

A) Background on virtual assets and cryptocurrency adoption.

The history of cryptocurrency is connected with the quest of decentralised and trust less digital currency. Computer scientists and cryptographers had tried to generate digital currencies that are not governed by governments or central banks over decades[1]. Some of the first attempts, like the DigiCash of David Chaum in the 1990s, were technically insightful but did not reach widespread adoption because of centralization and inability to scale[2]. The actual breakthrough was in 2008, when someone, or possibly a collective of people, under the name Satoshi Nakamoto, published the now-famous whitepaper, Bitcoin: A Peer-to-peer Electronic Cash System[3]. The innovation of Bitcoin was to integrate the blockchain technology with proof-of-work consensus, which essentially resolved the problem of double-spending without any third party.[4]

Bitcoin was released at the beginning of 2009, and the first transaction was documented when Nakamoto sent coins to computer scientist Hal Finney. The first commercial transaction soon followed in May 2010 when a programmer notoriously paid 10,000 bitcoins to purchase two pizzas, which is a good example of the potential of Bitcoin as a medium of exchange. The idea has over the years moved out of small technical circles, to include investors, developers, and entrepreneurs. The development of alternative cryptocurrencies, or altcoins, including Litecoin and subsequently Ethereum, increased the ecosystem. The new projects brought about new innovations such as quicker transactions, smart contracts and more advanced blockchain applications. By mid-2010s[5], cryptocurrency was already out of the sphere of experimental imagining and was becoming a disruptive technology that was taken seriously by regulators, businesses, and the global markets.[6]

[1] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System (2008).
[2] Dav*Id* Chaum, Blind Signatures for Untraceable Payments, in Advances in Cryptology 199 (1983).
[3] Nakamoto, *Supra*note 1.
[4] Laszlo Hanyecz, Bitcoin Pizza Transaction (2010)
[5] Andreas M. Antonopoulos, Mastering Bitcoin (2017)
[6] ECB, Virtual Currency Schemes (2012).

B) Understanding Blockchain Technology

Blockchain technology is premised on the capability of the algorithm to access. agreement in a decentralised system without the use of an authority. to give evidence and complete the deal. Blockchain technology not, therefore, as such. only resolves certain technical issues of the system but also brushes upon very. societal problems of trust, authority and consensus which are important.[7] If the mathematical algorithm does not permit any one to possess special control over the. network and transactions that occur within it, then it attains the status. of a neutral mechanism to any possible application, enabling. connections between people[8]. To be more specific, a blockchain is an immutable. on cryptographically hashed blocks, an irreversible linear chain of which. transactions are recorded. This chronological account of time-stamped events is linear. authenticated and registered in a decentralised and DLT-based way, and network. nodes witness to transactions and come to an agreement about which transactions are. treated as regular using a consensus Proof of Work algorithm.[9] The code substitutes in this instance. the law, intermediary person, institution or authority, and cryptographic evidence guarantees the authenticity of the record and arranges consensus. In in this manner, the transactions occur directly between the participants and do not go through. the regulation of financial institutions, and above all the creation itself. The determination and execution of of money is carried out by an immutable protocol, and not by government or state intervention.[10]

C) Virtual Assets and Adoption of Cryptocurrencies in the World.

In addition to the history of cryptocurrency, virtual assets are a far larger category of intangible and digitised value. They include cryptocurrency, tokens, digital securities, stablecoins, and even non-fungible tokens (NFTs). The common denominator of these assets is that they are entirely digital and are verified and transferred using distributed ledger technologies (DLT) or other such architecture.

The virtual asset has an economic significance in that it can destabilise the conventional financial systems. Digital transactions in cryptocurrencies can be instant and cross-border unlike traditional bank transfers, which in many cases, involve third parties and take a long

[7] European Central Bank, Virtual Currency Schemes (2012).
[8] *Supra*note 5
[9] Primavera De Filippi & Aaron Wright, Blockchain and the Law (2018).
[10] *Id*

time to settle. This is especially effective to the unbanked population who can access directly to the decentralised financial services by just having a mobile phone and an internet connexion.

In the past ten years, the use of cryptocurrencies has gained momentum in the world, driven by various reasons. Digital currencies have attracted investors in the developed economies as an alternative asset class, similar to gold, to diversify their portfolios and as a way to hedge against inflation. In developing nations, cryptocurrencies have a tendency to be useful in remittances, international transactions, and safeguarding savings against local currency fluctuations. Hyperinflation has led to the use of Bitcoin and stablecoins to replace national currencies by communities in countries such as Venezuela and Zimbabwe.[11]

The adoption has been met with caution, enthusiasm or scepticism by governments and regulators. Others have adopted Bitcoin as legal tender, including El Salvador in 2021, whereas others have imposed severe regulations or complete prohibitions[12]. Meanwhile, central banks around the globe are considering Central Bank Digital Currencies (CBDCs) as a government-regulated analogue to cryptocurrencies because they see the value and disruptive promise of decentralised assets.

II. The Nexus Between Terrorism and Virtual Assets

The relationship between terrorist organizations and virtual assets has deepened significantly in recent years. Traditional terror financing methods such as hawala systems, cash smuggling, charities, and informal money service businesses remain relevant, but digital currencies have introduced new opportunities for extremist groups to raise, conceal, and transfer funds in ways that challenge regulators and enforcement authorities

A. Adoption of Cryptocurrencies by Terrorist Network.

Due to a combination of these characteristics, terrorist organisations raise funds and send them across national borders using virtual assets: it is decentralised, pseudonymous (or anonymous in some cryptocurrencies), fast, requires fewer centralised intermediaries, and can be mixed or layered to conceal the source. These characteristics make finance in conflict zones or weakly regulated and supervised jurisdictions less risky and frictional to financiers

[11] IMF, Crypto in Fragile Economies (2021).
[12] Bitcoin Law, El Salvador (2021).

Moreover, as researchers suggest, the general trend toward a cryptocurrency economy provides systematic incentives to move virtual resources into the established criminal systems. What started as speculative investment or fair use may turn into cross-border layering, conversion to fiat, or use in complicated webs of shell wallets[13]. Such mixing of legal and illegal streams complicates the detection process, the grey areas between legal and illegal usage are now used by criminals who want to have plausible deniability. For example, in Syria, Islamic State and al-Qaeda networks have used digital currencies to solicit funds, transfer money between their followers, and obscure final beneficiaries. The 'Combating Terrorism Centre'[14] reported that such groups raise, transfer, and conceal finances through virtual currency, frequently in conjunction with more traditional systems such as hawala or through money service companies

Evidence suggest that in Al-Qassam Brigades and Al-Qaeda joint operation where Bitcoin addresses were announced via Telegram and other social media to gather donations and then transmitted via clusters of cryptocurrency addresses or mixed via exchanges and services to make them hard to trace.

B. Case Studies of Usage

1. **Syria (Al-Qaeda affiliates)-**

   A closer examination of Syria reveals that certain terrorist groups are exploring the idea of decentralised finance (DeFi) and virtual currency transfer, particularly between associates in Syria. These organisations obtain funds through crypto donations, transfer such funds using different crypto services and try to conceal the sources by clustering addresses or exchanging them in border regions.[15]

2. **Al-Qassim Brigades -**

   The case in point can be seen as an example of how social media (e.g. Telegram, Twitter, Facebook) are utilised by groups where they request donations through published crypto addresses. Money raised through various addresses is collected and distributed using networks. Combined through exchanges or service providers. In many cases,

[13] Europol, Crypto and Terrorism (2022).
[14] Combating Terrorism Center, Terrorist Use of Crypto (2021)
[15] UN Security Council Report, S/2023/151.

several addresses will be associated with charities, businesses, or otherwise seemingly legitimate organisations to hide intent or ownership.[16]

3. Other campaigns taken over by U.S. agencies-

The U.S. Department of Justice has broken a number of terror finance campaigns that utilised cryptocurrencies. In 2020, they confiscated crypto associated with the military wing of Hamas, Al-Qassam Brigades, and ISIS. Cyber-enabled solicitations and online fundraising were also used in these campaigns.[17]

C. Problems of Anonymity, Decentralisation and Technology.

Cryptocurrencies have certain enforcement problems:

- Pseudonymity / anonymity- Cryptocurrencies such as Bitcoin do not need the same identity cheques as the traditional financial system. Privacy-focused coins such as Monero and Z cash and others mixers make it even more challenging to trace money. [18]Terrorist actors use these features to conceal the identity of donors and funds transfer.

- Decentralised exchanges and DeFi protocols: These minimise the use of centralised intermediaries who are regulated. DeFi will be able to permit peer-to-peer exchanges, smart contracts and opaque protocols that are less known to regulators.[19]

- Cross-border and jurisdictional borders: Money can be transferred across national borders easily. This is the case with countries that have weak regulation, no enforcement or limited capacity[20]. Trades in less restrictive jurisdictions cannot impose rigid know-your-customer (KYC) or anti-money laundering (AML) regulations.

- Social media/dark web fundraising campaigns: Organisations are utilising encrypted messaging applications, social media, or alternative online fundraising campaigns to raise crypto. These approaches enable decentralised donor bases in different countries, and it is difficult to oversee them.

[16] DOJ Press Release (Aug. 13, 2020).
[17] *Id*.
[18] Keatinge, Unchartered Waters (RUSI 2021).
[19] Europol, *Supra*note 13
[20] FATF, Terrorist Financing Risk Assessment (2015).

Other qualities that Bitcoin certainly has are that it is slowly losing its standing due to illicit use as it has created the myth of total anonymity as its added attribute. It requires a thorough examination and a close look at the specifics of how the anonymity of Bitcoin functions and how it can be breached. To begin with, it is necessary to note that Bitcoin possesses a number of anonymous characteristics:

1. At the protocol level, the Bitcoin address is not associated with the personal information of the user.

2. The identity of the user is also not associated with transactions. In case miners consent to add the transaction to the block, any person can send bitcoins between one address and any other address without necessarily revealing personal data.[21]

The information about Bitcoin transactions is relayed by random nodes on the P2P network.[22] Bitcoin nodes are linked together through IP addresses. In this way, the nodes do not know whether the transaction was generated by the node transmitting the information or it merely redirected the information.

D. Communication with Traditional Terror Financing Techniques.

It is noteworthy that there is no even distribution of virtual assets to substitute the traditional channels of financing. Hybrid models are used by many terrorist networks. An example is that in Syria numerous activities use hawala networks, cash couriers, and informal value transfer, and then transfer or layer the money into crypto to keep wealth, transfer it across borders, or avoid detection.[23] Crypto serves as an ancillary yet increasingly important role - particularly where liquidity, anonymity or cross-border access is needed.

III. International Regulatory Environment.

With the increasing pace of the use of virtual assets around the world, regulatory and supervisory regimes have been unable to keep up. Successful responses should strike the right balance between the two competing demands of facilitating financial innovation and deterring misuse to money laundering and financing terrorism (ML/TF). The Financial Action Task

[21] *Supra* note 9
[22] Walch, Deconstructing Decentralization, 5 Stan. J. Blockchain L. & Pol'y 1 (2021).
[23] Chainalysis, Crypto Crime Report (2023).

Force (FATF) has become the standard-setter of the globe, with national jurisdictions, most notably the United States, the European Union, and other Asian states, adopting various degrees of rigour, coherence, and effectiveness.

A. FATF and International Standards.

The FATF has been at the forefront in trying to incorporate virtual assets and their service providers within the anti-money laundering & counter-terrorism financing (AML/CFT) regulations. More recently, it has officially expanded its scope to include virtual assets and Virtual Asset Service Providers (VASPs).[24] The new standards mandate jurisdictions to supervise, regulate, or monitor VASPs and also to implement preventative controls, including customer due diligence, record-keeping, reporting suspicious transactions, and acquiring originator and beneficiary details when a virtual asset is transferred. (It is reflected in the changed Recommendation 15 and its explanatory notes.)

Since virtual asset transactions can move across borders easily, the FATF insists that nations should implement standardised practises to prevent regulatory arbitrage, whereby illegal actors direct money through lax jurisdictions. The concept of the Travel Rule, which is the information of the originator and the beneficiary of the transfer, has become the key element of the FATF strategy to introduce transparency to the flow of virtual assets.[25] More recent updates have identified areas of implementation weakness, especially licencing of offshore VASPs, identification of DeFi participants, and cross-border oversight.

However, the standards of the FATF are not self-implementing; their success depends on national adoption, enforcement and cooperation.[26]Virtual asset markets are global, which implies that failures in one jurisdiction can jeopardise protection in others.

B. The United States Approach to Regulating Virtual Assets

In the United States, a virtual asset is governed by a stacked system of laws and regulatory bodies, each focusing on various facets of cryptocurrency usage.

[24] FATF Recommendation 15.
[25] FATF, Travel Rule Gu*Id*ance (2023).
[26] FATF Mutual Evaluation Reports (2024).

1. **FinCEN Regulation and Bank Secrecy Act (BSA).**

The U.S. is largely dependent on the Bank Secrecy Act (BSA) that requires financial institutions to report suspicious transactions and maintain records. FinCEN, a division of the U.S. Treasury, has imposed BSA requirements on some crypto businesses, and has considered many virtual asset service providers to be money services businesses (MSBs).[27] These organisations are required to perform customer identification, file suspicious activity reports (SARs), and keep a record of big transactions.

2. **Sanctions and Office of Foreign Assets Control (OFAC).**

Focusing on avoiding sanctions and illegal financing, OFAC has already labelled cryptocurrency addresses associated with terrorist groups.[28] The U.S. authorities have taken advantage of their jurisdiction over U.S. exchanges, intermediaries or dollar-clearing mechanisms, to freeze assets, impose sanctions, or force cooperation. The crypto sanctions regimes are becoming more and more concerned with layering, mixing services, and illegal actors.

3. **DOJ Actions and Criminal Prosecution.**

Cases of terrorists or extremist groups funding their activities through crypto fundraising campaigns have been prosecuted by the Department of Justice (DOJ). In numerous cases, U.S. officials have intercepted crypto wallets, monitored transactions, or used cooperation agreements with other regulators to shut down networks.[29] These instances demonstrate the effectiveness of integrating legal instruments with blockchain analytics, particularly in conjunction with established methods of investigation.

4. **Securities and Commodity Regulation.**

Investment-like virtual assets can be subject to either securities laws (SEC) or commodities laws (CFTC). Although this is more applicable to token offerings and trading platforms, it demonstrates the intersection of various regulatory regimes in the U.S. The U.S. model can be viewed as one of the more rigid global regimes- even

[27] 31 U.S.C. § 5311.
[28] OFAC, Crypto Sanctions Gu*Id*ance (2022).
[29] DOJ Crypto Enforcement Framework (2020)

though there are still issues, including how to enforce compliance in decentralised structures, crypto derivatives, and cross-border flows outside the jurisdiction of the U.S.

C. European Union's Approach

The European Union has attempted to harmonise crypto regulation in the member states with a regulatory framework that blends both centralised and national enforcement.

1. Crypto-Assets (MiCA) markets.

In 2023, the EU implemented MiCA (Regulation (EU) 2023/1114)[30], which aims to regulate crypto markets, stablecoins issuers, and crypto service providers across the union on an equal basis. The goal of MiCA is to offer legal predictability, protection to investors, and market integrity and reduce the risks of abuse.[31] It establishes principles of issuance, custody, operations, and obligations of crypto service providers such as transparency, capital requirements, and operational resilience.[32] It started implementation in December 2024.

2. Anti-Money Laundering and Counter-Terror Financing (AMLD / AMLA)

In addition to MiCA, the AML Directives of the EU (AMLD5, AMLD6) are revised to cover virtual assets.[33] New AML Authority (AMLA) is being created to oversee large institutions, including crypto firms, throughout the EU. It is aimed at minimising differences between national regimes and avoiding regulatory arbitrage within the union.[34] Recent official reports point out that crypto has become a priority threat in terms of laundering and terror financing in Europe.

3. Travel Rule and Transfer Regulation.

The Travel Rule will be enshrined in the regime of the EU Transfer of Funds Regulation (TFR),[35] which will come into effect during further stages and demand that transfers of

[30] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-Assets, 2023 O.J. (L 150) 40.
[31] *Id*
[32] *Id*
[33] Directive (EU) 2018/843 of the European Parliament and of the Council (AMLD5), 2018 O.J. (L 156) 43; Directive (EU) 2018/1673 (AMLD6), 2018 O.J. (L 284) 22.
[34] Regulation (EU) 2024/1620 establishing the Anti-Money Laundering Authority (AMLA), 2024 O.J. (L 169) 1.
[35] FATF, Gu*Id*ance on the Travel Rule for Virtual Assets ¶¶ 12–18 (2023).

crypto also include originator and beneficiary information. This brings the financial payment systems of EU in line with the virtual transfer of assets.

Although the method used by the EU is ambitious, the enforcement is still at its initial stages and will rely on the ability of the national authorities and their collaboration with data-sharing systems.

E. Comparative Reflections: Strengths, Weaknesses and Gaps.

Comparing the regulatory regimes in the world, one makes a number of observations:

- Advantages of repressive regimes: Fully licenced, supervised, enforced, and cooperative systems (e.g. U.S., EU) are in better positions to trace illegal flows, freeze assets, and shut down channels of misuse.

- Impairments in implementation: A big number of jurisdictions have difficulties in enforcement, technical knowledge of blockchain, inter-agency coordination, and resource limitations. This is particularly acute in developing states or conflict prone areas.

- Regulatory arbitrage and jurisdiction shopping: Illicit actors take advantage of differences in regimes by transferring funds through weaker or less developed jurisdictions, by taking advantage of anonymity, offshore transactions, or decentralised protocols. This threat is enhanced by the fact that crypto is borderless.

- Decentralised finance (DeFi) and anonymity technologies: There are numerous regimes that have difficulties controlling or overseeing DeFi protocols, mixers, privacy coins, and peer-to-peer tools that do not involve central intermediaries. The technologies are not always covered by the conventional definitions or areas of oversight of the law.

- The cross-border cooperation is necessary and inadequate: Cross-border vigilance is facilitated by mutual legal assistance treaties, information-sharing frameworks, and FATF standards, but delays, legal barriers, and sovereignty issues still make it difficult to act in a timely manner.

IV. Geographical Focus: Middle East and South Asia.

To determine the intersection of virtual assets with terror financing and money laundering in

the real world, it is imperative to look at how regulatory, institutional, and socio-political environments of the Middle East and South Asia define the possibilities of abuse and the attempts to regulate them. This part will examine region-specific dynamics, vulnerabilities, case examples, regulatory reactions, and implementation issues.

A. Middle East: Regulation, Innovation, and Vulnerability

The Middle East which was perceived as a free market when it comes to digital assets is experiencing massive regulatory maturity. In the United Arab Emirates, virtual asset services are now regulated at both federal and emirate level. One of the most important legal tools is the Cabinet Decision No. (111) of 2021[36] that enables the Securities & Commodities Authority (SCA) to licence and supervise Virtual Asset Service Providers (VASPs) throughout the UAE.[37] In the meantime, the Central Bank takes care of the factors concerning fiat-backed stablecoins and stored value systems.[38] On the emirate level, Dubai has a regulatory framework run by VARA (Virtual Assets Regulatory Authority) in respect of activities not covered by the Dubai International Financial Centre (DIFC).[39]

The cryptocurrency companies in the UAE should adhere to strict KYC (know-your-customer), AML (anti-money-laundering), transaction monitoring, cybersecurity, and licencing requirements. Payments can only be made using licenced tokens (e.g. those which are approved by the regulator). Unlicensed crypto-activity is practically banned.[40]

In addition to the UAE, the members of the Gulf Cooperation Council (GCC) are trying divergent strategies: some of them allowed controlled use of digital assets; others maintained their strict positions or even prohibited some crypto operations. Islamic finance issues are also an issue in the region-some jurisdictions determine whether cryptocurrencies meet Sharia principles, which affects the regulation or restriction of tokens.[41]

The Middle East is witnessing more institutional interest, stablecoin activity, and DeFi growth on the adoption side. UAE specifically has been experiencing equal participation in both small and large crypto transactions which are indicative of a mature adoption curve. The regulatory

[36] UAE Cabinet Decision No. 111 of 2021.
[37] *Id*
[38] Central Bank of the UAE, Stored Value Facilities Regulation (2020).
[39] Dubai Law No. 4 of 2022 (VARA).
[40] BIS, Crypto-Assets and Financial Stability in MENA 12–14 (2023).
[41] IMF, Virtual Assets in the GCC 9–11 (2022).

clarity also contributes to the adoption, and it is progressively regarded as a competitive edge to attract blockchain companies.[42]

B. Major Vulnerabilities in Regulation

Although the Middle East has matured legal systems, it has structural deficiencies that are exploitable by extremist players[43]. Cryptocurrency-assisted fundraising, cross-border transfers, and money laundering thrive best in conflict zones (e.g. Syria, Iraq)[44] and weak states. Sympathisers in different parts of the globe can be targeted by terrorist groups which will seek crypto donations via encrypted pathways, social media campaigns or crowdfunding sites.[45] The money can then be layered or transferred through international platforms and then converted.

The other weakness is the fact that the region is a regional financial centre with the cross-border capital flows. [46]Money that passes through Gulf financial hubs can be less scrutinised and crypto-to-fiat gateways in the area could offer entry and exit points to dirty money. In addition, local exchanges can be coerced to adhere to local or foreign AML regimes in a disjointed manner, which allows regulatory arbitrage.[47]

An example is licencing of regional crypto exchanges. As an example, CoinMENA has licences in Bahrain and Dubai, and it operates within the borders of the GCC. Without a close monitoring, such cross-jurisdiction operations can be used to transfer funds across the borders, which can be used to hide the origin of funds.[48]

C. Gaps and Challenges in Implementation.

Paper regulation does not necessarily mean total enforcement. There are gaps and challenges which include:

- Capacity issues: Some emirates or smaller Gulf states might not have enough technical capacity or human resources to oversee intricate blockchain transactions by regulatory

[42] *Supra*Note 40
[43] UNODC, Handbook on Terrorist Financing 45–47 (2021).
[44] UN Security Council, S/2023/151.
[45] Europol, Crypto and Terrorist Financing 18–20 (2022).
[46] FATF, Risk-Based Approach to VASPs 67–72 (2019).
[47] *Id*
[48] Bahrain Economic Development Board, Crypto Licensing Overview (2023).

bodies.[49]

- Fragmented authority: There is a risk of overlapping federal and local regulators, so jurisdictions will challenge authority over specific crypto functions, leading to ambiguity.[50]

- Offshore / unlicensed players: The unlawful or offshore VASPs that work in the jurisdictions with weak or no regulation may go unregulated, weakening the regional regime.[51]

- Enforcement issues across borders: To effectively track money that crosses international borders, the cooperation of states is required; a lack of political goodwill, absence of mutual legal cooperation or sluggish joint investigations can impede such cooperation.[52]

- Privacy enhancing tools: Mixers, privacy coins, tumblers, and other anonymity measures can be used to avoid detection even in regulated areas.[53]

E, Focus on South Asia

The geopolitical fault lines in South Asia influence the utilisation and misuse of virtual assets in financing terror. [54]India and Pakistan have historic mutual suspicions and cross-border support of militant organisations, particularly in Kashmir, has always been at the heart of the regional security dynamics. In this tense space, virtual resources introduce additional forms of raising, moving, and hiding money, and the already existing networks, charity vehicles, and informal money-transfer systems remain open in parallel with online ones.[55]

F. Pakistan: organisations, enumerated bodies, and foreign inspection.

The situation in Pakistan is intricate: non-state militant groups are active and powerful, and this country has been the target of the international community in terms of being weak in counter-

[49] BIS, *Supra*note 40
[50] *Id*
[51] FATF Mutual Evaluation Reports (2024).
[52] uropean Criminal L. Rev., Cross-Border AML Failures 211–13 (2022).
[53] Europol IOCTA (2023).
[54] Asian Dev. Bank, Crypto Risks in South Asia (2022).
[55] *Id*

terrorist financing regulations. Some of the violent organisations located in or affiliated to Pakistan, which are listed by the UN sanctions committee, have been involved in attacks in India and other parts of the world. These labels are the manifestations of the international issues regarding particular organisations and individuals that work beyond the boundaries.

Due to the same reasons, the Financial Action Task Force (FATF) put Pakistan under increased surveillance in 2018. The greylisting targeted the shortcomings in anti-money-laundering and counter-terrorist financing (AML/CTF) systems and demanded more effective legislation, criminal actions, asset freezes, and international collaboration[56]. Pakistan took a sequence of legal and enforcement actions and was taken off the FATF increased-monitoring list in 2022, which FATF described as a positive step but said that further efforts were still required.[57] This FATF procedure demonstrates the international pressure on Pakistan and the institutional changes of the state.[58] Whereas international organisations identify specific groups and the media to impose more controls, claims that a state sponsors terrorism are controversial and politically charged. Governmental documents, claims and counter-claims, and bilateral diplomatic processes influence the conclusions governments and international organisations make and the actions they take. It is important to note that sovereign responsibility is evaluated by the presence of state policy, material assistance, and the adequacy of domestic counter-measures-an evidentiary standard on which international responses and sanction decisions are based[59].

G. Funding modalities to Kashmir and India.

India has also reiterated several times that the activities of militant groups in Jammu & Kashmir and other parts of the world are supported across the border, either financially, logistically, or even providing sanctuaries. Some of the funding channels that have been mentioned in the past include charitable fronts, hawala and informal remittance networks, charitable NGOs acting as conduits, diaspora donations and funds transferred via legitimate businesses or trade.[60] The growing access to virtual property introduces a new dimension: cryptocurrencies are solicited online, divided into numerous addresses, and mixed through intermediaries, making it difficult

[56] FATF, Pakistan Mutual Evaluation Report (2019)
[57] FATF, Improving Global AML/CFT Compliance: Pakistan (2018)
[58] *Id*
[59] FATF Public Statement (Oct. 2022).
[60] Ministry of Home Affairs (India), Terror Financing Dossier (2021).

to trace and attribute.[61] Recent law enforcement efforts in India demonstrate that the government is investigating crypto-based fundraising and confiscating digital currencies associated with alleged terrorism financing networks. [62]These studies highlight the integration of digital currency channels into the existing financing toolskits. Media and official statements have also reported changing strategies: published wallet addresses on encrypted platforms, micro-donations pooled in extensive sympathiser networks, and then swapped into fiat via local exchanges or OTC desks[63]. These strategies are frequently used alongside older means (cash couriers, hawala) to form hybrid, robust financing chains that take advantage of regulatory loopholes as well as technological obscurity.

H. State responsibility, rejections, and international reactions.

Claims of state complicity or states condoning militant fundraising - have elicited diplomatic, legal, and multilateral responses. India has also produced evidence on several occasions and has urged international fora take action against individuals, charities or organisations it believes to be channels of cross-border financing.[64] Pakistan frequently denies the blanket charges of state sponsorship, citing its own counter-terrorism efforts and legal reforms (including prosecutions and asset freezes), and emphasises the need to pursue multilateral legal procedures to establish responsibility[65]. The FATF procedure and UN sanction listings demonstrate how global systems are trying to isolate non-state actors, enabling environments, and state policy.

V. Enforcement Challenges

The imposition of laws to prevent the abuse of cryptocurrencies to fund a terrorist organisation is a complex set of challenges due to the technological characteristics of blockchain systems, the international character of virtual resources, and the dynamism of the methods used by criminal groups. The fundamental issue with these challenges is that blockchain has pseudonymity, in which it is not completely anonymous but a user can use an alpha-numeric address instead of their real-life identity, making it harder to trace. [66]This pseudonymity is made worse by the instruments that are meant to increase privacy, including mixers, tumblers, and

[61] *Id*
[62] NIA India, Crypto Seizure Reports (2023)
[63] *Id*
[64] UN Security Council Res. 1373.
[65] Pakistan Ministry of Foreign Affairs Statements (2022
[66] Nakamoto, *Supra*note 1.

privacy coins, which is now a common part of terrorist financing. These problems are further exacerbated by regulatory arbitrage and cross-border enforcement gaps that allow terror networks to take advantage of jurisdictional differences. This chapter explores these enforcement challenges, using real-life examples and academic studies to explain why global anti-money laundering (AML) and counter-terrorist financing (CFT) systems remain vulnerable.

The first enforcement issue is the pseudonymity of blockchain transactions and the challenges of tracking illegal money. The blockchain ledgers are transparent and immutable, which in theory facilitates investigations by analyzing the pattern of transactions. Pseudonymity, however, implies that to associate a wallet address with a person, one will need extra off-chain information, including know-your-customer (KYC) records provided by virtual asset service providers (VASPs). Terrorist organizations take advantage of this with decentralized exchanges (DEXs) or peer-to-peer (P2P) systems with weak KYC regulations.[67] An example is privacy tools, such as cryptocurrency mixers (also called tumblers), which combine money of many users, reshuffle it in randomized amounts, and hide the source of transactions, making it virtually unfeasible to track the money trail without sophisticated analytics. [68]A report by Europol points to the ease with which criminals and terrorists use these services to launder money, with mixers laundering billions of illegal funds every year. Privacy coins, including Monero or Zcash, go a step beyond that and include obfuscation protocols (ring signatures and zero-knowledge proofs) built into the privacy coin, obscuring the details of transactions completely.[69] These coins have been implicated in terrorist activities; one example is the Islamic State (ISIS) accepting Monero donations to evade detection as reported in a 2023 UN report on the misuse of virtual assets. Here, enforcement agencies, such as the U.S. Department of Justice (DOJ), have a steep uphill battle to climb, because conventional subpoena authority fails against decentralized protocols. An example of this can be the 2022 Tornado Cash sanction by the U.S. Office of Foreign Assets Control (OFAC): the mixer was already used by North Korean hackers and even wallets associated with terrorists, but its open-source code resulted in forks, compromising the ban. [70]These tools do not only protect financing of terrorists, but also question the FATF Travel Rule, which mandates VASPs to provide information on the

[67] FATF, Travel Rule Gu*Id*ance (2023).
[68] Europol, *Supra*note 13.
[69] *Id*.
[70] OFAC, Tornado Cash Designation (2022).

originator and beneficiary of the transfer over 1,000 dollars - a rule frequently evaded through mixers.

Another significant obstacle is the presence of cross-border enforcement gaps, which are compounded by the fact that cryptocurrencies are not subject to borders. To evade this scrutiny, terror networks practise regulatory arbitrage, moving their operations to jurisdictions with weaker AML/CFT regimes. In a study published in 2024 in the Magna Scientia Advanced Research and Reviews journal[71], the authors explain how these loopholes are used by cryptocurrency exchanges, relocating to offshore havens such as the Seychelles or unregulated African countries, where enforcement is lax. This arbitrage enables terrorist funding; in one example, the military wing of Hamas, the Al-Qassam Brigades, has utilized Bitcoin wallets hosted on non-compliant exchanges to fund their operations, and in 2020, the organization was prosecuted by the DOJ on charges of violating the sanctions by designating the crypto addresses of the Al-Qassam Brigades. Prior to the dissolution of its National Cryptocurrency Enforcement Team (NCET), the DOJ, in memos, pointed to the difficulty of extraterritorial jurisdiction in such cases, with foreign VASPs frequently disregarding U.S. subpoenas.[72] These vulnerabilities have been repeated in the 2025 report on terrorist financing risks by the Financial Action Task Force (FATF) which finds that only 58% of jurisdictions have adopted effective VASP supervision, resulting in "jurisdiction shopping" by criminal actors. In a real life case study, the 2021 Hezbollah-linked funding system used Lebanese and Iranian P2P sites to transfer funds using privacy coins by hopping across borders and using regulatory gaps[73]. The European Criminal Law Review has suggested that fractured international collaboration, including delays in mutual legal assistance treaties (MLATs), enables terror groups to launder funds before the freezing of assets.[74] Besides, it is aggravated by corruption in loosely regulated areas; a BIS article on DeFi regulation notes how officials in Southeast Asia prone to bribes facilitate unlicensed exchanges, which indirectly facilitates terrorist remittances. The 2022 Action Plan on Illicit Financing Risks of Digital Assets by the U.S. Treasury recognizes these gaps, proposing greater international data-sharing, but there is still an imbalanced implementation.

These are not impossible challenges but must be handled in a new way. Nevertheless,

[71] Magna Scientia Advanced Res. & Revs. (2024
[72] DOJ, United States v. Al-Qassam Brigades (2020).
[73] *Id*
[74] FATF, Global Implementation Review (2025).

reevaluating terrorist financing, limited resources and political goodwill tend to stall efforts and most nations focus on economic development through crypto innovation rather than strict enforcement. The shift in responsibility to individual fraud and away from systemic regulation with the dissolution of the DOJ in 2025 could also exacerbate the U.S. fight against terror-related crypto abuse. These enforcement challenges in general demonstrate the necessity of harmonized international standards to deal with the adaptive skills of terrorist networks.

V. Conclusion

In summary, the intersection of cryptocurrencies and terrorist financing reveals a dynamic threat landscape where virtual assets offer unprecedented opportunities for illicit funding due to their speed, anonymity, and global reach. From the historical evolution of Bitcoin as a tool for decentralized finance to its exploitation by groups like ISIS and Hamas, the nexus has grown amid uneven regulatory responses. Traditional methods have given way to crypto-based campaigns, with regions like the Middle East and Southeast Asia serving as hotspots due to vulnerabilities in remittance networks and fragmented oversight. Enforcement challenges, including pseudonymity, privacy tools, and cross-border arbitrage, perpetuate these risks, as evidenced by DOJ cases and FATF assessments. While progress has been made through frameworks like the Travel Rule, gaps in implementation continue to enable regulatory evasion and jurisdictional shopping.