CRYPTOCURRENCY-BASED TERROR FINANCING ON THE DARK WEB: PROSECUTORIAL CHALLENGES UNDER PMLA, UAPA, AND IT ACT IN INDIA

Kumar Kartikeya, Ph.D Scholar (Law), NIMS University

Om Pratap Singh, Advocate, Allahabad High Court, Lucknow Bench
Founder, Law Foundation (NGO), Lucknow, Uttar Pradesh

ABSTRACT

The convergence of cryptocurrency and the dark web has created a formidable new theatre for terrorist financing one that is pseudonymous, borderless, and structurally resistant to conventional investigative mechanisms. In India, the legal response to this threat has been largely reactive: the Prevention of Money Laundering Act, 2002 (PMLA), the Unlawful Activities (Prevention) Act, 1967 (UAPA), and the Information Technology Act, 2000 (IT Act) constitute the primary legislative arsenal, yet none was architected with Virtual Digital Assets (VDAs) in mind. The Financial Action Task Force's (FATF) Comprehensive Update on Terrorist Financing Risks (July 2025) flags that 69% of assessed jurisdictions exhibit major deficiencies in effectively investigating and prosecuting terror financing cases a finding that carries direct implications for India's enforcement apparatus. India's own PRAHAAR counter-terror doctrine (2026) acknowledges the use of crypto wallets and dark web channels for terror financing, yet stops short of prescribing a coherent operational framework for blockchain forensics and inter-agency coordination. This paper undertakes a doctrinal and analytical examination of the existing statutory framework, identifies structural lacunae in definitional scope, jurisdictional reach, and real-time enforcement, and proposes legislative and institutional reforms calibrated to India's position as both the world's leading nation in crypto adoption and a primary target of state-sponsored cross-border terrorism.

Keywords: Cryptocurrency, Terror Financing, Dark Web, PMLA, UAPA, IT Act, Virtual Digital Assets, FATF, Blockchain Forensics, PRAHAAR, Financial Intelligence Unit, India

I. INTRODUCTION

The architecture of global terrorism financing has undergone a silent but seismic transformation over the past decade. Where once hawala networks and cash couriers were the dominant instruments of choice for terror financiers, the proliferation of cryptocurrency and the infrastructure of the dark web have introduced a new paradigm one defined by speed, anonymity, and legal indeterminacy. Terrorist organisations ranging from ISIS-Khorasan to various Pakistan-based proscribed entities have been documented using blockchain-based wallets, Monero privacy coins, and Tor-routed dark web markets to raise, move, store, and deploy funds across international borders with minimal detectability.[1]

India occupies a uniquely precarious position in this evolving landscape. On one hand, the country ranks first globally in cryptocurrency adoption,[2] with its user base crossing 100 million in 2025. On the other, it is the primary target of state-sponsored cross-border terrorism, a fact expressly acknowledged in India's National Risk Assessment for Money Laundering and Terrorist Financing (2022), which identifies Pakistan's state sponsorship of terrorism as a high-risk source.[3] The intersection of these two realities creates a structural vulnerability of singular legal and strategic consequence.

The FATF's July 2025 Comprehensive Update on Terrorist Financing Risks drawing on over 840 submissions from more than 80 jurisdictions confirmed that illicit actors are increasingly integrating digital technologies with conventional financing methods, adding new layers of complexity to counter-terror financing (CTF) efforts.[4] A notable case study contributed by India to the FATF report highlights the proliferation concerns arising from Pakistan's state-owned National Development Complex sanctioned in multiple jurisdictions demonstrating that the threat is neither abstract nor distant.

This paper proceeds as follows: Part II traces the mechanisms by which cryptocurrency and dark web infrastructure enable terror financing. Part III maps the existing Indian legal framework PMLA, UAPA, IT Act, and FEMA against the specific threat matrix. Part IV diagnoses the legislative lacunae. Part V examines prosecutorial and investigative challenges in concrete terms. Part VI benchmarks India's framework against global standards, including FATF Recommendation 15 and the COINS Act, 2025. Part VII offers a reform agenda.

II. THE MECHANISM: HOW CRYPTO AND THE DARK WEB ENABLE TERROR FINANCING

2.1 The Pseudonymity Problem

Blockchain technology is inherently pseudonymous rather than anonymous. Every transaction is permanently recorded on a public distributed ledger, yet the identities of the parties remain masked behind cryptographic wallet addresses. Tracing the real-world person controlling a wallet requires detailed forensic work using specialised blockchain analytics tools capability that law enforcement agencies in India are only beginning to develop.[5] Privacy coins such as Monero and Zcash go further still, employing zero-knowledge proof cryptography to render even on-chain transaction data opaque.

2.2 Dark Web as a Financial Infrastructure

The dark web accessible only through anonymising networks such as Tor (The Onion Router) functions as a marketplace for arms, forged documents, and narcotics, as well as a platform for recruitment, propaganda, and financial coordination. Terror suspects have been documented using the dark web to buy arms, coordinate communications, and move cryptocurrency while evading traditional surveillance architectures.[6] The Gorakhnath temple attack (2022) produced a notable precedent in Indian CTF jurisprudence: the attacker was found to have used PayPal and VPNs to fund activities linked to ISIS-Khorasan, demonstrating that even conventional digital payment tools can be weaponised through layering techniques.

2.3 The Three-Stage Crypto Laundering Cycle

Terror financing through cryptocurrency broadly mirrors the classic three-stage money laundering typology placement, layering, and integration but with distinct digital variants:

Table 1: Crypto-Terror Financing Typology in the Indian Context

Stage	**Traditional Method**	**Crypto/Dark Web Equivalent**	**Indian Case Relevance**
Placement	Cash deposits, hawala entry	Crypto exchange deposits; P2P transfers; foreign	FIU-IND investigation of Binance/WazirX for TRX transactions

Stage	Traditional Method	Crypto/Dark Web Equivalent	Indian Case Relevance
		wallet funding	linked to Pakistani and Syrian wallets (2025)
Layering	Shell companies, offshore accounts	Crypto mixers (tumblers), chain-hopping (BTC → Monero → ETH), dark web exchange	ED investigations into crypto laundering through fraudulent loan apps (2024–25)
Integration	Real estate, trade-based laundering	NFT purchases, DeFi protocol investment, conversion to fiat via unregistered exchanges	PMLA attachment proceedings involving cryptocurrency holdings linked to UAPA accused

2.4 The Rise of Stablecoins as Terror-Financing Instruments

The FATF's June 2025 Targeted Update on Virtual Assets reported a sharp increase in the use of stablecoins by terrorist financiers and illicit actors a trend accelerating because stablecoins combine the transactional anonymity of cryptocurrency with price stability, making them operationally superior to volatile assets for funding operations requiring predictable value.[7] Most on-chain illicit activity now involves stablecoins rather than Bitcoin. India has no dedicated regulatory framework governing stablecoins as a category distinct from other Virtual Digital Assets under the Income Tax Act definition adopted in 2022.

III. THE EXISTING INDIAN LEGAL FRAMEWORK

3.1 Prevention of Money Laundering Act, 2002 (PMLA)

The PMLA was the first significant legislative step to bring cryptocurrency within the anti-money laundering architecture. In March 2023, the Ministry of Finance notified Virtual Digital Assets (VDAs) as "property" under the PMLA through a gazette notification,[8] requiring all Virtual Asset Service Providers (VASPs) exchanges, wallet providers, and intermediaries to register with the Financial Intelligence Unit–India (FIU-IND), maintain KYC records, and report Suspicious Transaction Reports (STRs). The Enforcement Directorate (ED) was thereby empowered to investigate, attach, seize, and prosecute VDA-linked money laundering offences under Sections 3, 4, 5, and 17 of the PMLA.

However, the PMLA's application to terror financing specifically is derivative and indirect: the statute requires the existence of a "scheduled offence" as a predicate. Absent a specific FIR under the IPC/BNS or UAPA, the ED cannot initiate an Enforcement Case Information Report (ECIR) under PMLA creating a critical sequencing dependency that undermines proactive crypto surveillance.

3.2 Unlawful Activities (Prevention) Act, 1967 (UAPA)

The UAPA provides the primary legal framework for counter-terrorism in India. Section 15 defines "terrorist act" broadly enough to encompass cyber-facilitated attacks targeting India's sovereignty, integrity, or security. The State Investigation Agency (SIA) in Jammu & Kashmir has conducted UAPA raids targeting crypto wallets suspected of funding terrorist activities a significant enforcement precedent.[9] Section 40 of the UAPA criminalises raising funds for a terrorist organisation, and Section 17 criminalises the use of funds for terrorist purposes.

The deficit, however, is definitional: UAPA contains no reference to "virtual assets," "cryptocurrency," "digital wallets," or "blockchain." The application of UAPA to crypto-based terror financing proceeds by analogical interpretation a jurisprudential approach that is inherently contestable in trial courts and creates reversible error on appeal.

3.3 Information Technology Act, 2000 (IT Act)

Section 66F of the IT Act addresses cyber terrorism acts that penetrate computer systems with intent to threaten the unity or security of India or strike terror in the people. The provision is broad enough in principle but has rarely been applied in terror financing prosecutions. The IT Act does not address cryptocurrency, dark web operations, or the use of encryption to conceal financial transactions supporting terrorism.

3.4 Foreign Exchange Management Act, 1999 (FEMA)

The ED froze accounts linked to Binance for violations of FEMA arising from cross-border crypto transactions, reflecting the statute's role in policing foreign-origin terror financing channels. However, FEMA is a civil enforcement statute and cannot sustain criminal sanctions adequate to the gravity of terror financing conduct.

Table 2: Statutory Coverage of Crypto-Based Terror Financing in India

Statute	Relevant Provisions	Coverage	Key Gap
PMLA, 2002	Ss. 2, 3, 4, 5, 17; 2023 VDA Notification	VDA as property; STR reporting; ED attachment	Requires predicate offence; no proactive crypto monitoring authority
UAPA, 1967	Ss. 15, 17, 40	Terrorist act; use/raising of funds for terror	No definition of VDA or blockchain-specific provisions
IT Act, 2000	S. 66F (cyber terrorism)	Cyber-attacks with terror intent	Does not address dark web or crypto-based terror financing
FEMA, 1999	Foreign exchange violations	Cross-border crypto transactions	Civil statute; inadequate for criminal terror financing response
BNS/BNSS, 2023	Organised crime; sedition-equivalent provisions	Partial overlap with UAPA in domestic terrorism	No crypto-specific provisions; predicate crime sequencing issue remains

IV. LEGISLATIVE LACUNAE: A DIAGNOSTIC ASSESSMENT

4.1 Definitional Vacuum

The most structurally significant gap is definitional. India's anti-terror statutes UAPA in particular predate both the cryptocurrency ecosystem and the dark web as operational concepts. The absence of express statutory definitions for "virtual digital asset," "blockchain transaction," "crypto wallet," "privacy coin," "crypto mixer," and "Virtual Asset Service Provider" in the UAPA means that prosecutors must rely on expansive interpretive constructions of existing language. Such constructions are regularly challenged by defence counsel and have produced inconsistent trial court outcomes.

4.2 The Predicate Offence Sequencing Problem

Under the current PMLA architecture, the ED can investigate VDA-linked money laundering only where a "scheduled offence" has already been registered. In crypto terror financing

scenarios where the evidence is embedded in encrypted blockchain data and dark web logs law enforcement agencies often become aware of the financial crime before, or simultaneously with, the predicate offence. This sequencing dependency structurally disadvantages proactive financial intelligence-driven disruption and privileges reactive post-attack investigation.

4.3 Absence of a Crypto-Specific Freezing and Seizure Mechanism

While Section 5 of the PMLA empowers the ED to attach property without prior judicial permission in urgent cases, this provision was designed for immovable property and bank accounts. Cryptocurrency wallets which may be self-custodied, hardware-based, or accessible only through private cryptographic keys present unique seizure challenges not addressed by existing attachment procedures. The Supreme Court has noted the need for cryptocurrency regulation, and the COINS Act, 2025, a proposed legislative measure, contemplates a dedicated Crypto Authority but neither a custodial seizure protocol nor a key-disclosure legal mechanism is currently operative.

4.4 Jurisdictional Indeterminacy

Cyber terrorism can have global dimensions, with attacks being launched from outside India's borders.[10] A terror financing transaction routed from a Pakistan-based handler through a Tor-accessible dark web market, converted via a Monero privacy coin chain, and ultimately received in a wallet held by an operative in Jammu may touch the jurisdictions of five or more sovereign states, none of which has complete transactional visibility. India's bilateral Mutual Legal Assistance Treaty (MLAT) infrastructure while substantial was not designed for the speed at which cryptocurrency transactions are confirmed and irreversibly settled.

4.5 The DeFi and DEX Blind Spot

The PMLA's 2023 VDA notification imposes compliance obligations on centralised exchanges and intermediaries entities that have identifiable operators and can be directed to share KYC data. Decentralised Finance (DeFi) protocols and Decentralised Exchanges (DEXs) operate without such identifiable operators, processing peer-to-peer token swaps through smart contracts. The FATF's own June 2025 targeted update acknowledges that jurisdictions continue to face significant difficulties in identifying the natural persons behind DeFi activities.[11] Indian law currently offers no mechanism to regulate or surveil DeFi-based terror financing channels.

V. PROSECUTORIAL AND INVESTIGATIVE CHALLENGES

"Law enforcement agencies may lack the expertise or resources to investigate sophisticated cyber-attacks that involve advanced tools like encryption, anonymising networks, and the dark web a challenge that directly conflicts with the need for surveillance in counterterrorism efforts."

Academic literature on UAPA and cyber terrorism, 2025

5.1 Evidentiary Admissibility of Blockchain Data

The admissibility of blockchain transaction data as evidence in Indian criminal proceedings raises novel questions under the Bharatiya Sakshya Adhiniyam, 2023 (BSA). Section 63 of the BSA governs electronic records and requires a certificate from the person responsible for the device. Blockchain data, generated by a decentralised network of nodes, does not neatly fit this certification requirement. Prosecutorial reliance on blockchain analytics reports generated by private vendors (Chainalysis, Elliptic, etc.) introduces further questions of expert witness qualification and methodology disclosure.

5.2 The Capacity Deficit in Investigative Agencies

India's primary investigative agencies NIA, ED, and CBI have begun developing blockchain forensics capacity, but institutional expertise remains concentrated in a small number of specialists. The ED's 2021 scrutiny of WazirX and its more recent investigations represent the frontier of current capability. Coordinated inter-agency operations involving the Financial Intelligence Unit (FIU-IND), NIA, and state police cyber cells have been hampered by information-sharing silos and the absence of a unified crypto intelligence platform.

5.3 India's PRAHAAR Doctrine: Promise and Gap

India's PRAHAAR counter-terror doctrine (2026) anchored in the UAPA, PMLA, and the new criminal codes represents the most ambitious articulation of India's counter-terror policy architecture to date. It acknowledges the use of crypto wallets, encryption, and the dark web for terror financing and achieves a notably high NIA conviction rate of approximately 92%.[12] However, PRAHAAR does not clearly outline how cryptocurrency tracking, blockchain analysis, or coordination with global Virtual Asset Service Providers will be

operationalised in practice. The doctrine also gives insufficient attention to encrypted messaging applications and online gaming platforms as emerging terror financing vectors an omission noted in expert commentary.

5.4 The Low Conviction Rate Under PMLA

Parliamentary records reveal that the ED secured only 15 convictions in 5,892 PMLA cases taken up since 2015[13] a conviction rate of approximately 0.25%. While this figure encompasses all PMLA cases and not only those involving cryptocurrency or terror financing, it nonetheless reflects systemic prosecutorial challenges: long pre-trial detention periods, complex multi-jurisdictional evidence gathering, and inadequate capacity in Special PMLA Courts. The Supreme Court's direction for fast-track courts in PMLA cases and its call for cryptocurrency regulation without a ban provide judicial guidance awaiting legislative action.

VI. INTERNATIONAL STANDARDS AND COMPARATIVE FRAMEWORK

6.1 FATF Recommendation 15 and the Travel Rule

FATF Recommendation 15 (R.15) and its Interpretive Note updated in 2019 and again in October 2025 require all jurisdictions to apply comprehensive AML/CFT measures to Virtual Assets and VASPs. The Travel Rule (FATF Recommendation 16) requires VASPs to obtain, hold, and transmit originator and beneficiary information for all VA transfers. As of April 2025, only 73% of surveyed jurisdictions had passed legislation implementing the Travel Rule,[14] and only one jurisdiction achieved full compliance with R.15. India has made progress registering over 30 exchanges with FIU-IND including the re-admitted Binance but has not yet fully operationalised the Travel Rule, leaving identifiable traceability gaps in cross-border VA transfers.

6.2 The United States and European Models

The United States employs the Bank Secrecy Act (BSA) and the Anti-Money Laundering Act of 2020 (AMLA) to govern crypto CTF, with FinCEN designating VASPs as "money services businesses" subject to full AML obligations. The EU's Transfer of Funds Regulation (2023) extended the Travel Rule to all crypto transfers regardless of size eliminating the de minimis exemption. Both jurisdictions maintain dedicated crypto forensics units within law enforcement: the IRS-Criminal Investigation's Cyber Crimes Unit and Europol's European Cybercrime Centre (EC3). India lacks an equivalent dedicated permanent institutional

structure.

6.3 The COINS Act, 2025: A Forthcoming Indian Framework

The proposed COINS Act, 2025 is India's most consequential forthcoming legislative intervention in the VDA space. It aims to establish a dedicated Crypto Authority, ease the 30% flat tax regime, and bring greater regulatory certainty. However, available details do not indicate that the COINS Act specifically addresses terror financing via VDAs, creates blockchain forensics infrastructure, or amends UAPA to incorporate crypto-specific provisions. If enacted without these elements, it will primarily serve investor protection rather than security objectives.

VII. REFORM AGENDA: A PROPOSED LEGISLATIVE AND INSTITUTIONAL FRAMEWORK

7.1 Amending UAPA to Incorporate VDA-Specific Provisions

The UAPA should be amended to include: (a) express definitions of "virtual digital asset," "crypto wallet," "privacy coin," "blockchain transaction," and "Virtual Asset Service Provider" consistent with the PMLA 2023 notification and the proposed COINS Act; (b) an express provision deeming the use of cryptocurrency or dark web infrastructure to raise or transfer funds for a designated terrorist organisation or terrorist act as a scheduled offence; and (c) a provision empowering the NIA to conduct proactive blockchain intelligence gathering without the current predicate-offence sequencing requirement.

7.2 A Dedicated Crypto-Asset Freezing and Seizure Protocol

The PMLA should be amended to include a crypto-specific seizure provision authorising: (a) judicial orders for private key disclosure (analogous to the UK's Proceeds of Crime Act power to compel disclosure of encryption keys); (b) the creation of a government-designated cold-storage custodial wallet administered by FIU-IND or the proposed Crypto Authority for seized assets; and (c) a cross-border wallet-freezing protocol under existing MLAT frameworks, with timelines calibrated to the near-instantaneous finality of blockchain transactions.

7.3 Establishing a National Blockchain Intelligence Unit (NBIU)

India requires a permanent, institutionally independent National Blockchain Intelligence Unit

with a mandate covering: blockchain forensic investigation across all agencies; licensing and supervision of private blockchain analytics vendors; real-time on-chain monitoring for wallets on UNSC sanctions lists and NIA watch lists; and liaison with international bodies including INTERPOL's Financial Crime unit and FATF's VASP supervisory network. The NBIU should be staffed by a multi-disciplinary team of legal experts, cybersecurity professionals, and financial intelligence analysts.

7.4 Full Operationalisation of the FATF Travel Rule

India should legislatively operationalise the FATF Travel Rule for all VA transfers by amending the PMLA to require VASPs to transmit originator and beneficiary identification information for every transaction removing any de minimis threshold and to report to FIU-IND in real time for transactions involving wallets on designated entity lists.

7.5 DeFi and Privacy Coin Regulatory Architecture

The proposed COINS Act and PMLA notification framework should be extended to address DeFi protocols and DEXs accessible to Indian users, through a risk-based regulatory approach requiring the most accessible DeFi interfaces (front-end operators) to conduct KYC and maintain records. Privacy coins should be classified as "high-risk VDAs" requiring enhanced due diligence for any exchange or transfer, with a mandatory STR for any transaction exceeding a threshold value.

7.6 Judicial Capacity Building

Special Courts designated under the PMLA and UAPA should be provided with judicial training modules on blockchain forensics, the evidentiary standards applicable to blockchain analytics reports, and the admissibility framework under the Bharatiya Sakshya Adhiniyam, 2023. India's Law Commission should be directed to undertake a dedicated study on the evidentiary treatment of blockchain data in criminal proceedings.

VIII. CONCLUSION

The marriage of cryptocurrency and the dark web has not merely complicated the task of combating terror financing in India it has exposed the foundational architecture of India's anti-terror legal framework as one designed for an analogue threat in a digital world. The PMLA's

2023 VDA notification, UAPA's broad "terrorist act" definition, and PRAHAAR's doctrinal acknowledgment of crypto-based terror financing represent meaningful first steps. They are, however, insufficient steps in the face of a threat that operates at the speed of blockchain confirmation measured in seconds against legal processes measured in years.

The FATF's finding that 69% of jurisdictions worldwide exhibit major deficiencies in investigating and prosecuting terror financing cases is not a reason for complacency but a call to structural reform. India's 92% NIA conviction rate and its recognition by FATF as demonstrating substantial effectiveness in proliferation financing controls achievements that reflect institutional commitment must now be matched by legislative precision.

The reforms proposed in this paper UAPA amendment incorporating VDA-specific provisions, a crypto-asset seizure protocol, a National Blockchain Intelligence Unit, full Travel Rule operationalisation, and a DeFi regulatory architecture are not merely technical adjustments. They are constitutional necessities, rooted in the State's obligation under Articles 21 and 51A to protect the life and security of its citizens from threats that have evolved far beyond the imagination of the legislators who first drafted these statutes. The dark web cannot remain a sovereign-free zone for those who wish to finance the destruction of the Indian State.

REFERENCES

1. FATF, *Comprehensive Update on Terrorist Financing Risks* (July 2025), available at https://www.fatf-gafi.org/en/publications/Methodsandtrends/comprehensive-update-terrorist-financing-risks-2025.html

2. Giottus, *Crypto Regulation in India 2025: KYC, Taxes & Compliance* (September 2025), India's crypto user base exceeding 100 million.

3. Government of India, *National Risk Assessment for Money Laundering and Terrorist Financing* (2022), Ministry of Finance.

4. FATF, *Comprehensive Update on Terrorist Financing Risks*, op. cit. (July 2025).

5. Cryptotimes, *How India's 'PRAHAAR' Aims to Block Terrorists' Use of Crypto & Dark Web* (February 24, 2026), available at https://www.cryptotimes.io/2026/02/24/how-indias-prahaar-aims-to-block-terrorists-use-of-crypto-dark-web/

6. Chauhan (2025), *Exploring the Role of Encryption and the Dark Web in Cyber Terrorism: Legal Challenges and Countermeasures in India*, Cogent Social Sciences (March 17, 2025), DOI: 10.1080/23311886.2025.2479654

7. FATF, *Targeted Update on Implementation of the FATF Standards on Virtual Assets and VASPs* (June 2025), Paris.

8. Ministry of Finance, Gazette Notification S.O. 1072(E) (March 7, 2023), bringing VDAs within the ambit of PMLA, 2002.

9. South Asia Terrorism Portal (SATP), *Reports on SIA Raids under UAPA targeting crypto wallets* (2025).

10. Chauhan (2025), op. cit.

11. FATF, *Targeted Update on Virtual Assets and VASPs* (June 2025), op. cit.

12. ORF Online, *PRAHAAR: India's New Counter-Terror Policy in a Hybrid Threat Era* (February 26, 2026), available at https://www.orfonline.org/expert-speak/prahaar-india-s-new-counter-terror-policy-in-a-hybrid-threat-era

13. Drishti IAS, *Money Laundering Issue in India*, citing Finance Minister's Report to the Rajya Sabha (2023).

14. FATF, *Targeted Update on Virtual Assets and VASPs* (June 2025): 73% of surveyed jurisdictions passed Travel Rule legislation as of April 2025.