Rooted in Tradition. Driven by Justice.

PEER-REVIEWED • OPEN ACCESS • MULTI-DISCIPLINARY LEGAL RESEARCH JOURNAL

LAUNDERING ON THE BLOCKCHAIN: VIRTUAL DIGITAL ASSET SERVICE PROVIDERS UNDER THE PREVENTION OF MONEY LAUNDERING ACT AFTER THE 2023 NOTIFICATION

ADV. RAMAKANT YADAV

Research Articles • MOS-00003 • Published 28 October 2026

ABSTRACT

Cryptocurrencies were designed to move value across the world without banks, and that very feature has made them attractive to those who wish to move the proceeds of crime without scrutiny. India responded slowly and in fragments: a banking ban that the Supreme Court set aside, a punitive tax regime introduced in 2022, and, on 7 March 2023, a notification that brought virtual digital asset service providers within the Prevention of Money Laundering Act, 2002 as reporting entities. This paper examines that notification from the standpoint of enforcement. It explains how virtual digital assets are defined in Indian law and how they are used to launder money, traces the regulatory journey that preceded the notification, and analyses the obligations it imposes on exchanges, wallet providers and other intermediaries. It then studies enforcement in practice, including the action taken by the Financial Intelligence Unit against offshore exchanges, the attachment and custody of crypto assets, the proof of blockchain evidence in court and the constitutional safeguards affirmed in Vijay Madanlal Choudhary. The Indian framework is compared with the standards of the Financial Action Task Force and the approaches of the European Union and the United States. The paper argues that the 2023 notification was a necessary first step but cannot by itself carry the weight of regulating a sector that remains without a dedicated statute, and it proposes reforms on licensing, the travel rule, seizure protocols and institutional capacity.

KEYWORDS

Virtual Digital Assets, Prevention of Money Laundering Act, Cryptocurrency, FIU-IND, Reporting Entity, Enforcement Directorate, FATF, Asset Attachment

VOLUME 1, ISSUE 1 (INAUGURAL ISSUE), OCTOBER TO DECEMBER 2026 • THEME: LABOUR, EMPLOYMENT & SOCIAL SECURITY LAW

Mos Legis Review, Vol. 1, Issue 1 (2026), pp. 32-46

Licensed under CC BY 4.0

LAUNDERING ON THE BLOCKCHAIN: VIRTUAL DIGITAL ASSET SERVICE PROVIDERS UNDER THE PREVENTION OF MONEY LAUNDERING ACT AFTER THE 2023 NOTIFICATION

Adv. Ramakant Yadav
Spl.P.P. CBI & E.D.

Abstract

Cryptocurrencies were designed to move value across the world without banks, and that very feature has made them attractive to those who wish to move the proceeds of crime without scrutiny. India responded slowly and in fragments: a banking ban that the Supreme Court set aside, a punitive tax regime introduced in 2022, and, on 7 March 2023, a notification that brought virtual digital asset service providers within the Prevention of Money Laundering Act, 2002 as reporting entities. This paper examines that notification from the standpoint of enforcement. It explains how virtual digital assets are defined in Indian law and how they are used to launder money, traces the regulatory journey that preceded the notification, and analyses the obligations it imposes on exchanges, wallet providers and other intermediaries. It then studies enforcement in practice, including the action taken by the Financial Intelligence Unit against offshore exchanges, the attachment and custody of crypto assets, the proof of blockchain evidence in court and the constitutional safeguards affirmed in *Vijay Madanlal Choudhary*. The Indian framework is compared with the standards of the Financial Action Task Force and the approaches of the European Union and the United States. The paper argues that the 2023 notification was a necessary first step but cannot by itself carry the weight of regulating a sector that remains without a dedicated statute, and it proposes reforms on licensing, the travel rule, seizure protocols and institutional capacity.

Keywords

Virtual Digital Assets, Prevention of Money Laundering Act, Cryptocurrency, FIU-IND, Reporting Entity, Enforcement Directorate, FATF, Asset Attachment

1. Introduction

Every age of financial innovation has produced its own methods of laundering money. Shell companies, benami property, trade mis-invoicing and hawala networks each had their moment, and each eventually drew a legal response. Cryptocurrency is the latest chapter in this long story, and in some respects the most challenging. When the pseudonymous Satoshi Nakamoto described Bitcoin in 2008 as a system for electronic payments that would allow parties to transact directly without a trusted financial institution,[1] the promise was financial freedom. For law enforcement, the same design meant that value could move across borders in minutes, outside the banking channels on which anti-money laundering law had been built.

The scale of illicit use has been the subject of considerable debate. An influential study estimated that a substantial share of early Bitcoin users and transactions were associated with illegal activity, largely linked to darknet markets.[2] Blockchain analytics firms, on the other hand, report that illicit activity accounts for a small fraction of total on-chain volume, though the absolute amounts run into billions of dollars each year.[3] Both views can be true at once. Most crypto activity is lawful speculation or investment, but the technology offers real advantages to anyone seeking to hide the origin of money, and investigators in India have increasingly encountered crypto assets in cases of online fraud, illegal lending apps, gaming scams and cross-border fund transfers.

India's legal response has been hesitant and piecemeal. There is still no statute that regulates crypto assets as a class. Instead, the State has acted through a banking circular, a tax regime and, most significantly for criminal enforcement, a notification under the Prevention of Money Laundering Act, 2002 (PMLA). Issued on 7 March 2023, that notification designated a range of crypto-related businesses as persons carrying on designated business or profession, making them reporting entities subject to the full discipline of the anti-money laundering regime.

This paper examines whether that notification has been effective and what remains to be done. Written from the perspective of enforcement and prosecution, it asks practical questions: what the notification requires of exchanges, how investigators trace and seize crypto assets, how blockchain evidence is proved in court and where the gaps lie. Part 2 explains virtual digital assets, the ways they are used to launder money and why intermediaries matter. Part 3 traces India's regulatory journey, including the advent of the digital rupee. Part 4 analyses the 2023 notification. Part 5 examines enforcement in practice.

[1] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (2008), available at: https://bitcoin.org/bitcoin.pdf (last visited on Oct. 7, 2026).
[2] Sean Foley, Jonathan R. Karlsen and Tālis J. Putniņš, "Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies?" 32 *Review of Financial Studies* 1798 (2019).
[3] Chainalysis, *The 2024 Crypto Crime Report* (Chainalysis, New York, 2024).

Part 6 places India within global standards. Part 7 identifies the gaps in the current framework, Part 8 proposes reforms and Part 9 concludes.

2. Virtual Digital Assets and the Mechanics of Crypto Laundering

2.1 The Legal Meaning of a Virtual Digital Asset

Indian law first defined crypto assets not in a regulatory statute but in the tax code. The Finance Act, 2022 inserted a definition of "virtual digital asset" into the Income-tax Act, 1961, covering any information, code, number or token generated through cryptographic means or otherwise that provides a digital representation of value, along with non-fungible tokens and other assets that the government may notify. The same Act introduced a flat thirty per cent tax on income from the transfer of such assets and a one per cent deduction of tax at source on transfers.[4] The definition is deliberately wide. It captures Bitcoin and Ether, stablecoins, utility tokens and NFTs alike, and it does not depend on the technology used. The 2023 PMLA notification adopted this tax definition, so that the reach of the anti-money laundering regime is tied to the same broad concept.

2.2 How Crypto Assets Are Used to Launder Money

Money laundering is traditionally described in three stages: placement, where illicit cash enters the financial system; layering, where it is moved through transactions designed to obscure its origin; and integration, where it re-emerges as apparently legitimate wealth. Crypto assets can be used at every stage, and they are particularly effective for layering. Blockchains are public ledgers, but the addresses recorded on them are pseudonymous strings of characters rather than names. A single person may control thousands of addresses, and assets can be moved between them in seconds at little cost.

The Financial Action Task Force (FATF) has catalogued the red flags that typically accompany misuse of crypto assets. They include the rapid conversion of funds through several assets with no apparent business purpose, known as chain-hopping; the use of mixing and tumbling services that pool transactions from many users to break the link between sender and recipient; the use of privacy coins designed to hide transaction details; and the routing of funds through exchanges in jurisdictions with weak supervision.[5] Peer-to-peer trading, in which users buy and sell crypto directly with one another, often settling the fiat leg through bank transfers or digital payments, creates a further point of vulnerability because the exchange platform may never see where the rupees came from.

[4] The Finance Act, 2022 (Act 6 of 2022), inserting s. 2(47A), s. 115BBH and s. 194S in the Income-tax Act, 1961.

[5] Financial Action Task Force, *Virtual Assets: Red Flag Indicators of Money Laundering and Terrorist Financing* (FATF, Paris, 2020).

In Indian investigations, a recurring pattern combines these techniques with mule bank accounts. Proceeds of online fraud are collected in accounts opened in the names of persons who rent out their identity, quickly converted into stablecoins on an exchange or through peer-to-peer trades, and then transferred to wallets controlled from abroad. By the time a complaint reaches the police, the funds may have passed through dozens of addresses. It is precisely at the points of conversion between rupees and crypto, and at exchanges that hold customer assets, that the law has the best chance of intervening. That is why the regulation of service providers, rather than of the technology itself, has become the centrepiece of the global response.

2.3 Why Intermediaries Matter

For all the talk of decentralisation, most ordinary users still reach crypto assets through intermediaries. They buy their first tokens with rupees on an exchange, store them in a custodial wallet provided by that exchange and sell them through the same platform when they wish to return to fiat currency. These intermediaries are the gateways between the regulated banking system and the open blockchain, and they hold the identity records that can link a pseudonymous address to a real person. Criminals face the same constraint. However skilfully funds are layered on-chain, the proceeds of crime usually have to be converted into rupees or another fiat currency to be spent on property, vehicles or lifestyle, and that conversion typically passes through an exchange or a peer-to-peer counterparty. Regulating intermediaries therefore allows the law to concentrate its attention at the points where it has the greatest leverage, rather than attempting the impossible task of policing every transaction on a global network.

3. India's Regulatory Journey: From Prohibition to Taxation

3.1 The Banking Ban and Its Reversal

India's first significant regulatory step was an attempt to cut crypto off from the banking system. On 6 April 2018, the Reserve Bank of India directed the entities it regulates not to deal in virtual currencies or provide services to any person dealing in them.[6] The circular effectively starved domestic exchanges of access to bank accounts. In 2020, however, the Supreme Court set it aside, holding that although the Reserve Bank had the power to regulate the area, the measure was disproportionate because there was no evidence that regulated entities had suffered any harm from their dealings with crypto exchanges.[7]

Around the same time, an inter-ministerial committee constituted by the Department of Economic Affairs had recommended a ban on private cryptocurrencies along with criminal

[6] Reserve Bank of India, *Prohibition on Dealing in Virtual Currencies (VCs)*, Circular DBR.No.BP.BC.104/08.13.102/2017-18 (Apr. 6, 2018).
[7] *Internet and Mobile Association of India v. Reserve Bank of India* (2020) 10 SCC 274.

penalties.[8] In 2021, a bill titled the Cryptocurrency and Regulation of Official Digital Currency Bill was listed for introduction in Parliament, proposing to prohibit private cryptocurrencies with certain exceptions.[9] It was never introduced. The policy of prohibition thus gave way, without any formal announcement, to a policy of tolerating crypto while making it costly and visible.

3.2 Taxation and Visibility

The 2022 tax regime marked that turn. Its high flat rate and the bar on setting off losses were widely seen as discouraging trading, but its more important effect for enforcement was visibility. The one per cent deduction at source created a trail of transactions linked to the permanent account numbers of Indian users. Shortly before, the Indian Computer Emergency Response Team had issued directions requiring virtual asset service providers, among others, to maintain know-your-customer information and records of financial transactions.[10] These measures brought some of the market into view, but none of them imposed the full set of anti-money laundering duties that apply to banks and other financial institutions. That gap was filled, at least on paper, in March 2023.

3.3 The State's Own Digital Currency

The government's caution towards private cryptocurrencies has been accompanied by enthusiasm for a sovereign alternative. The Reserve Bank published a concept note on central bank digital currency in 2022 and began pilots of the digital rupee later that year, presenting it as a way to capture the benefits of digital money while retaining the safeguards of a central bank liability.[11] The contrast matters for enforcement. A central bank digital currency operates within a regulated, identifiable system, whereas private crypto assets do not. The existence of the digital rupee therefore strengthens rather than weakens the case for regulating private assets: the State has shown that digital money can be designed with accountability built in, and it is reasonable to expect intermediaries dealing in private assets to supply comparable accountability through law.

[8] Department of Economic Affairs, Ministry of Finance, *Report of the Committee to Propose Specific Actions to be Taken in Relation to Virtual Currencies* (Government of India, New Delhi, 2019).
[9] The Cryptocurrency and Regulation of Official Digital Currency Bill, 2021, listed for introduction in the Lok Sabha, Lok Sabha Bulletin Part II (Nov. 2021).
[10] Indian Computer Emergency Response Team, Directions under Sub-section (6) of Section 70B of the Information Technology Act, 2000 relating to Information Security Practices, Procedure, Prevention, Response and Reporting of Cyber Incidents (Apr. 28, 2022).
[11] Reserve Bank of India, *Concept Note on Central Bank Digital Currency* (RBI, Mumbai, Oct. 2022).

4. The 2023 Notification: Service Providers as Reporting Entities

4.1 The Scope of the Notification

The PMLA imposes its preventive obligations on "reporting entities", a category that includes banking companies, financial institutions, intermediaries and persons carrying on designated business or profession. The last category may be expanded by the Central Government through notification.[12] Using this power, the Ministry of Finance notified that the following activities, when carried out for or on behalf of another person in the course of business, would bring the person within the regime: exchange between virtual digital assets and fiat currencies; exchange between one or more forms of virtual digital assets; transfer of virtual digital assets; safekeeping or administration of virtual digital assets or instruments enabling control over them; and participation in and provision of financial services related to an issuer's offer and sale of a virtual digital asset.[13]

These five categories closely track the FATF definition of a virtual asset service provider. They cover centralised exchanges, custodial wallet providers, brokers, platforms facilitating token offerings and, arguably, many crypto lending and staking services. They do not, however, cover persons who merely write software or individuals who hold their own assets in self-hosted wallets, since the activities must be carried out for another person and in the course of business. This boundary is sensible, but it leaves decentralised protocols, where no identifiable intermediary may exist, in a grey zone.

4.2 The Obligations of a Reporting Entity

Once designated, a service provider must comply with the obligations in Chapter IV of the PMLA and the Prevention of Money-laundering (Maintenance of Records) Rules, 2005. In essence, it must verify the identity of its clients and beneficial owners, maintain records of transactions for the prescribed period and report cash and suspicious transactions to the Financial Intelligence Unit-India (FIU-IND).[14] FIU-IND followed the notification with sector-specific guidelines requiring service providers to register with it, to appoint a Principal Officer and a Designated Director, and to implement client due diligence and transaction monitoring suited to the risks of the sector.[15] Failure to comply exposes the entity to the supervisory powers of the Director of FIU-IND, which include issuing warnings, directions and monetary penalties for each failure.

[12] The Prevention of Money-laundering Act, 2002 (Act 15 of 2003), ss. 2(1)(sa), 2(1)(u), 2(1)(v), 2(1)(wa), 3, 5, 8, 12, 13, 17 and 45.
[13] Ministry of Finance (Department of Revenue), Notification S.O. 1072(E) (Mar. 7, 2023).
[14] The Prevention of Money-laundering (Maintenance of Records) Rules, 2005, r. 9.
[15] Financial Intelligence Unit-India, *Anti Money Laundering and Countering the Financing of Terrorism Guidelines for Reporting Entities Providing Services Related to Virtual Digital Assets* (Mar. 10, 2023).

The practical value of these obligations lies in the suspicious transaction report. An exchange that notices a customer depositing funds from several unrelated bank accounts, converting them immediately into stablecoins and withdrawing them to an external wallet is now under a legal duty to report that pattern. For investigators, these reports often supply the first lead in a case and the material needed to justify further action.

4.3 Reaching Offshore Exchanges

The most visible test of the notification came in its application to exchanges based outside India. Many Indian users traded on large offshore platforms that had not registered with FIU-IND. In December 2023, FIU-IND issued show cause notices to nine offshore service providers, including Binance, KuCoin and Kraken, for operating in India without complying with the PMLA, and requested that the Ministry of Electronics and Information Technology block their websites.[16] Blocking orders of this kind rest on the power of the Central Government to direct that public access to information be blocked in the interest of, among other things, public order.[17]

The approach proved effective. Binance registered with FIU-IND in 2024, and the Director of FIU-IND later imposed a penalty of Rs. 18.82 crore on it for the period during which it had served Indian users without complying with its statutory obligations.[18] A further penalty of Rs. 9.27 crore was imposed on Bybit for expanding its Indian operations without registration.[19] These orders established an important principle: an offshore platform that serves Indian customers is a reporting entity in India, regardless of where it is incorporated. They also showed that, in the absence of a licensing statute, the combination of PMLA registration and website blocking can operate as a de facto licensing regime.

5. Enforcement in Practice: Investigation, Attachment and Prosecution

5.1 Tracing the Money

For an investigating agency, the blockchain is both an obstacle and an opportunity. Pseudonymity makes it hard to identify who controls an address, but the permanence of the ledger means that every movement of funds can, in principle, be followed. Investigators use analytics tools to cluster addresses, identify known exchange wallets and trace funds to the point where they meet a regulated entity. At that point, the know-your-customer records held by the exchange become the bridge between an address and a person.

[16] Press Information Bureau, Ministry of Finance, "FIU IND Issues Compliance Show Cause Notices to Nine Offshore Virtual Digital Assets Service Providers (VDA SPs)" (Dec. 28, 2023).
[17] The Information Technology Act, 2000 (Act 21 of 2000), s. 69A.
[18] Order in Original No. 10/DIR/FIU-IND/2024 in the matter of Binance under Section 13 of the PMLA (Director, FIU-IND, June 19, 2024).
[19] "FIU Slaps INR 9.3 Cr Penalty On Crypto Platform Bybit", *Inc42*, available at: https://inc42.com/buzz/fiu-slaps-inr-9-3-cr-penalty-on-crypto-platform-bybit (last visited on Oct. 7, 2026).

The difficulty arises when that bridge is missing. The Enforcement Directorate's action against the operators of the WazirX exchange in 2022, in connection with its investigation into fraudulent instant loan applications, illustrates the problem. The Directorate alleged that funds diverted by the loan companies had been converted into crypto assets on the exchange and transferred to foreign wallets, and that lax know-your-customer norms and the failure to record certain transfers on the blockchain made it impossible to account for the missing assets. It froze bank balances of Rs. 64.67 crore under the PMLA.[20] Whatever the final outcome of such proceedings, the episode demonstrated why record-keeping obligations on intermediaries are not a formality but the foundation of any investigation.

5.2 Attachment and Custody of Crypto Assets

The PMLA defines property in the widest terms, to include property of every description, whether corporeal or incorporeal, tangible or intangible, and any instrument evidencing title to or interest in it. Crypto assets fall comfortably within this definition, and the definition of proceeds of crime extends to the value of property held outside the country. The Act's provisions on provisional attachment, search and seizure, and adjudication therefore apply to crypto assets as they apply to any other property.

Applying them, however, raises problems that the drafters never anticipated. A crypto asset is controlled by whoever holds its private key. Seizing a device or a password is meaningless if a co-accused abroad holds a copy of the key and can move the assets before they are secured. Agencies must therefore transfer the assets to a wallet under their own control, which in turn requires secure key management, internal controls against misappropriation and clear rules on who may authorise a transfer. Valuation is another difficulty. The price of many tokens can fall sharply within days, so that attached assets worth crores at the time of seizure may be worth far less when the case concludes. Where the victims are identifiable, as in many fraud cases, the PMLA now provides a route for restoration of attached property to them,[21] but realising the value of volatile assets in the meantime requires a legal mechanism for interim sale that does not yet exist in a crypto-specific form.

5.3 Proving Blockchain Evidence

A case built on the blockchain must ultimately be proved in court. Transaction histories, exchange records, wallet screenshots and analytics reports are all electronic records. Under the earlier law, the Supreme Court held that a certificate under section 65B(4) of the Indian Evidence Act, 1872 was a mandatory condition for the admissibility of secondary electronic evidence.[22] The Bharatiya Sakshya Adhiniyam, 2023 retains this requirement and prescribes a

[20] Directorate of Enforcement, Press Release, "Freezing of Assets of WazirX Crypto Exchange" (Aug. 5, 2022).
[21] The Prevention of Money-laundering (Restoration of Property) Rules, 2016.
[22] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020) 7 SCC 1.

more detailed form of certificate.[23] Prosecutors must therefore ensure that exchange records are obtained with proper certification and that the methodology of any analytics tool is explained by a competent witness. Courts are entitled to ask how an address was attributed to an accused, and a conclusion drawn from software that no witness can explain is vulnerable in cross-examination.

5.4 The Constitutional Framework of PMLA Enforcement

Crypto-related prosecutions operate within the constitutional framework that governs the PMLA as a whole. In *Nikesh Tarachand Shah*, the Supreme Court struck down the twin conditions for bail as they then stood.[24] After Parliament amended the provision, a three-judge bench in *Vijay Madanlal Choudhary* upheld the amended twin conditions along with the provisions on search, seizure, arrest and attachment, while emphasising that these powers must be exercised in accordance with the safeguards built into the Act.[25] For the crypto sector, the decision confirms that the full force of the Act is available, but it also reminds agencies that the legality of each step will be scrutinised.

Privacy is a further consideration. In the Aadhaar judgment, the Supreme Court struck down the requirement under the PMLA rules that bank accounts be mandatorily linked with Aadhaar, holding it disproportionate.[26] Know-your-customer obligations on crypto service providers must likewise be proportionate. The State is entitled to require identification and monitoring, but blanket surveillance of all users without regard to risk would invite constitutional challenge and would, in any case, bury investigators under data of little value.

5.5 The Scheduled Offence Requirement

A further point deserves emphasis because it shapes every crypto prosecution. Money laundering under the PMLA is not a free-standing offence. It requires proceeds of crime, which in turn must be derived from a scheduled offence. *Vijay Madanlal Choudhary* made clear that where there is no scheduled offence, or where the accused is finally discharged or acquitted of it, there can be no prosecution for money laundering on that basis. In crypto-related cases, the predicate is most often cheating, now punishable under the Bharatiya Nyaya Sanhita, 2023,[27] together with the cyber offences of impersonation and fraud under information technology law. The practical consequence is that investigators in the predicate case, usually State police, and the Enforcement Directorate must work closely together. A weak investigation of the underlying fraud will bring down the money laundering case built upon it, however strong the blockchain evidence may be.

[23] The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023), s. 63.
[24] *Nikesh Tarachand Shah v. Union of India* (2018) 11 SCC 1.
[25] *Vijay Madanlal Choudhary v. Union of India*, 2022 SCC OnLine SC 929.
[26] *K.S. Puttaswamy v. Union of India* (2019) 1 SCC 1.
[27] The Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023), s. 318.

6. Global Standards and Comparative Approaches

6.1 The FATF Standards

The global benchmark is set by the FATF. Through amendments adopted in 2018 and 2019, it extended its Recommendation 15 to require countries to regulate virtual asset service providers for anti-money laundering purposes, to license or register them and to subject them to effective supervision. The same standard applies the obligations of Recommendation 16, commonly known as the travel rule, which requires originator and beneficiary information to accompany transfers.[28] The FATF later issued detailed guidance explaining how these obligations apply to stablecoins, peer-to-peer transactions and decentralised finance.[29] Its periodic reviews have found that implementation of these standards, particularly the travel rule, remains uneven across the world.[30]

India's own performance was assessed in the mutual evaluation adopted in 2024. India was placed in the regular follow-up category, the best outcome available, reflecting a high level of technical compliance. The assessors nonetheless noted that supervision and preventive measures for virtual asset service providers were still at an early stage.[31] That finding is a fair summary of where India stands: the legal hook exists, but the supervisory machinery is still being built.

6.2 The European Union

The European Union has chosen comprehensive legislation. The Markets in Crypto-Assets Regulation creates a licensing regime for crypto-asset service providers across the Union, with requirements on governance, custody of client assets, conflicts of interest and market abuse.[32] A companion regulation extends the travel rule to transfers of crypto assets, requiring service providers to collect and transmit information about the originator and beneficiary and to apply enhanced checks to transfers involving self-hosted wallets.[33] The European approach thus integrates anti-money laundering duties within a broader prudential and conduct framework, which is exactly what India lacks.

---

[28] Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations* (FATF, Paris, 2012, as updated), Recommendations 15 and 16.

[29] Financial Action Task Force, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (FATF, Paris, 2021).

[30] Financial Action Task Force, *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers* (FATF, Paris, 2024).

[31] Financial Action Task Force, Asia/Pacific Group on Money Laundering and Eurasian Group, *Anti-money Laundering and Counter-terrorist Financing Measures: India, Fourth Round Mutual Evaluation Report* (FATF, Paris, 2024).

[32] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-Assets.

[33] Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on Information Accompanying Transfers of Funds and Certain Crypto-Assets.

6.3 The United States

The United States has relied heavily on enforcement under existing laws. In November 2023, Binance and its founder pleaded guilty to federal charges including failure to maintain an effective anti-money laundering programme, as part of a resolution exceeding four billion dollars.[34] The Treasury Department also targeted the infrastructure of laundering itself when it sanctioned the Tornado Cash mixing service in 2022, alleging that it had been used to launder billions of dollars, including funds stolen by a state-linked hacking group.[35] Those sanctions were lifted in 2025 after litigation questioned whether immutable software could be treated as sanctionable property, an episode that shows how difficult it is to apply traditional legal categories to decentralised code. Scholars have long warned that blockchain systems can create a sphere of "rule by code" that sits uneasily with conventional legal control.[36]

6.4 International Coordination

India has also helped shape the international agenda. Under its G20 presidency, the Financial Stability Board's high-level recommendations on crypto-asset activities[37] and a joint synthesis paper by the International Monetary Fund and the Financial Stability Board[38] were brought together into a coordinated policy approach, which the leaders endorsed in the New Delhi Declaration.[39] On the tax side, the OECD's Crypto-Asset Reporting Framework provides for the automatic exchange of information on crypto transactions between tax authorities.[40] These frameworks matter for enforcement because crypto laundering is almost always cross-border, and no single country can trace or recover assets alone.

7. Gaps in the Indian Framework

7.1 A Regulatory Vacuum Beyond Anti-Money Laundering

The most fundamental gap is the absence of a dedicated regulatory statute. The PMLA is a law about crime, not about markets. It tells service providers to know their customers and report suspicion, but it does not set capital requirements, rules on segregation and custody of client assets, standards for listing tokens or protections against market manipulation. When an

[34] U.S. Department of Justice, Press Release, "Binance and CEO Plead Guilty to Federal Charges in $4B Resolution" (Nov. 21, 2023).
[35] U.S. Department of the Treasury, Press Release, "U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash" (Aug. 8, 2022).
[36] Primavera De Filippi and Aaron Wright, *Blockchain and the Law: The Rule of Code* (Harvard University Press, Cambridge, MA, 2018).
[37] Financial Stability Board, *High-level Recommendations for the Regulation, Supervision and Oversight of Crypto-asset Activities and Markets: Final Report* (FSB, Basel, 2023).
[38] International Monetary Fund and Financial Stability Board, *IMF-FSB Synthesis Paper: Policies for Crypto-Assets* (IMF and FSB, 2023).
[39] G20 New Delhi Leaders' Declaration (Sept. 9–10, 2023).
[40] OECD, *International Standards for Automatic Exchange of Information in Tax Matters: Crypto-Asset Reporting Framework and 2023 Update to the Common Reporting Standard* (OECD Publishing, Paris, 2023).

exchange fails or is hacked, customers have no regulator to turn to. The Supreme Court has expressed its frustration with this situation. In May 2025, while hearing a bail plea in a Bitcoin-related case, a bench observed orally that trading in Bitcoin in India resembled a refined form of hawala and noted that there were still no regulations in place.[41]

Parliament has taken note. In 2026, the Standing Committee on Finance, in its report on the proposed Securities Markets Code, observed that virtual digital assets were unregulated except for limited purposes and recommended a comprehensive regulatory framework, with an interim arrangement through self-regulatory organisations under the oversight of a designated regulator.[42] Until such a framework exists, the PMLA will continue to be asked to do work for which it was never designed.

7.2 Self-Hosted Wallets, Decentralised Finance and the Travel Rule

The 2023 notification regulates intermediaries, but a growing share of activity takes place without them. Users can hold assets in self-hosted wallets and trade through decentralised protocols governed by smart contracts. Initial coin offerings showed how quickly such markets can attract fraud,[43] and decentralised finance raises the same concerns at greater scale. India's framework says little about how service providers should treat transfers to and from self-hosted wallets, and there is no detailed statutory travel rule comparable to the European regime. Without it, funds can leave a compliant Indian exchange for an unknown wallet abroad, and the trail ends.

7.3 Institutional Capacity

Enforcement also depends on people and systems. Investigating crypto cases requires analytics tools, trained officers, secure custody infrastructure and prosecutors who understand the technology well enough to explain it to a court. Capacity has grown, but it remains concentrated in a few central agencies, while most fraud complaints are first received by State police stations. There is no published, uniform standard operating procedure across agencies for the seizure, storage and disposal of crypto assets, which creates risks of loss, theft and challenges to the integrity of evidence.

[41] "Trading in Bitcoin in India is Refined Way of Doing Hawala Business: SC", *The Week* (PTI), May 5, 2025, available at: https://www.theweek.in/wire-updates/national/2025/05/05/lgd55-sc-crypto-currency.html (last visited on Oct. 7, 2026).
[42] "Parliamentary Finance Committee Calls for Regulatory Framework for Virtual Digital Assets", *MediaNama*, July 2026, available at: https://www.medianama.com/2026/07/223-parliamentary-panel-crypto-vda-regulation/ (last visited on Oct. 7, 2026).
[43] Dirk A. Zetzsche, Ross P. Buckley, Douglas W. Arner and Linus Föhr, "The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators" 60 *Harvard International Law Journal* 267 (2019).

7.4 Fragmented Oversight

Responsibility for the sector is also scattered. FIU-IND supervises anti-money laundering compliance, the tax authorities monitor deductions at source, the Ministry of Electronics and Information Technology controls website blocking and cybersecurity reporting, the Reserve Bank watches over the banking channels through which rupees enter and leave exchanges, and the securities regulator considers whether particular tokens resemble securities. Each acts within its own mandate, and none has overall responsibility for the health of the market. Kevin Werbach has argued that blockchain systems do not eliminate the need for trust but relocate it, and that law remains essential to make that trust reliable.[44] In India, that trust currently rests on a patchwork of agencies whose information does not automatically flow between them. A single designated regulator, with formal arrangements for sharing information with FIU-IND and enforcement agencies, would close many of the gaps through which illicit funds now pass.

8. The Way Forward: Recommendations

First, India should enact a comprehensive statute for virtual digital assets that establishes a licensing regime administered by a designated regulator. The statute should set prudential, governance and custody requirements and incorporate the existing PMLA obligations, so that registration with FIU-IND becomes one part of a single authorisation rather than the only gateway. The interim self-regulatory model recommended by the Standing Committee could serve as a bridge, provided it operates under genuine statutory oversight.

Second, the travel rule should be given clear legal force. Service providers should be required to collect and transmit originator and beneficiary information for transfers above a threshold and to apply risk-based checks to transfers involving self-hosted wallets, following the FATF standard and the European model.

Third, a uniform protocol for the seizure and custody of crypto assets should be notified for all enforcement agencies. It should provide for transfer to government-controlled wallets with multi-signature authorisation, chain-of-custody documentation that satisfies the evidentiary certificate requirement, independent audit and a judicially supervised mechanism for the interim sale of volatile assets, with proceeds held in an interest-bearing account pending adjudication.

Fourth, capacity must be built where crimes are reported. State police cyber cells need access to analytics tools and training, and a central coordinating unit should support them with expertise and shared intelligence. Specialised training for prosecutors and judges would help courts evaluate blockchain evidence with confidence.

[44] Kevin Werbach, *The Blockchain and the New Architecture of Trust* (MIT Press, Cambridge, MA, 2018).

Fifth, the law should adopt risk-based treatment of self-hosted wallets and decentralised platforms. It should not attempt to prohibit self-custody, which has legitimate uses and would be impossible to enforce. Instead, regulated service providers should be required to identify transfers to and from unhosted wallets, apply enhanced checks above defined thresholds and refuse transfers linked to sanctioned or high-risk addresses. Where decentralised platforms have identifiable developers or controllers exercising real influence over their operation, those persons should be treated as service providers for regulatory purposes.

Sixth, victims should be placed at the centre of asset recovery. In most crypto fraud cases the real losers are identifiable individuals, and the restoration mechanism under the PMLA should be made faster and simpler for them, including through interim release of realised value where ownership is clear. Regulated exchanges could also be required to participate in a rapid freezing protocol, so that funds reported as stolen can be held within hours rather than weeks.

Finally, India should deepen international cooperation through faster mutual legal assistance, participation in information-sharing frameworks and agreements with jurisdictions that host major exchanges. Crypto assets move across borders in seconds, and the law must find ways to follow them almost as quickly.

9. Conclusion

The 2023 notification under the PMLA was a turning point. It ended the uncertainty about whether crypto intermediaries owed any duties to the State and gave enforcement agencies a legal basis to demand records, require reporting and penalise non-compliance. Its application to offshore exchanges, culminating in penalties against major global platforms, showed that Indian law can reach those who serve Indian users from abroad.

Yet a notification cannot substitute for a policy. The PMLA addresses the movement of criminal money; it does not protect investors, ensure the solvency of exchanges or govern decentralised markets. The Supreme Court's remarks in 2025 and the recommendations of the Standing Committee in 2026 both point to the same conclusion: India needs a coherent legal framework for virtual digital assets, within which anti-money laundering obligations sit as one essential part. For those who investigate and prosecute economic offences, such a framework would mean clearer duties for intermediaries, better records, safer custody of seized assets and stronger cases in court. For the public, it would mean that the promise of financial innovation is not overshadowed by its misuse. The blockchain keeps a permanent record of every transaction. The task of the law is to ensure that this record serves justice rather than concealment.