"CRYPTOCURRENCY AND MONEY LAUNDERING: EXAMINING LEGAL AND ENFORCEMENT MEASURES IN INDIA"

Evania Irene K, T. VAISHALI
1st Year LLM Student, Assistant professor of Law Cyber Space Law & Justice
The Tamil Nadu Dr. Ambedkar Law University, Chennai Chennai, India

Abstract
The rapid expansion of crypto currency in India has opened new avenues for digital investment and financial innovation, but it has simultaneously raised significant concerns regarding its exploitation for money laundering activities. The decentralised architecture for digital assets, high transaction speed and cross border mobility make them attractive tools for concealing the origin of illicit proceeds. In recent years, multiple investigations by enforcement authorities have highlighted the increasing trend of routing criminal earnings through crypto wallets, mixers, privacy coins and offshore exchanges, which complicates financial surveillance and detection. In response, India has progressively integrated cryptocurrency within it's anti - money laundering framework by extending the scope of the Prevention Of Money Laundering Act (PMLA) to Virtual Digital Asset service providers and enhancing reporting obligations under the Financial Intelligence Unit. Despite these legal developments, technical barriers, absence of uniform global standards, and jurisdictional fragmentation continue to pose challenges for effective enforcement. This research paper analyses the link between cryptocurrency and money laundering in the Indian context, examines statutory and institutional mechanism, and explores the evolving role of enforcement agencies. The study also proposes policy oriented recommendations to ensure that India's regulatory approach strengthens financial security while allowing responsible digital asset innovation to continue.
Key Words : Cryptocurrency, Money laundering, Decentralised, Economy, Transaction Security, Bitcoin

1. **Introduction**

Cryptocurrency has emerged as one of the most discussed breakthrough in today's financial landscape. In contrast to the conventional currency managed by banks and governments, cryptocurrency operates on a decentralised digital framework employing blockchain technology. This provides users with quick and seamless transaction, financial confidentiality and enhanced control over their assets. However, the same features that make cryptocurrency attractive have also raised serious concerns about it's misuse for illegal activities especially money laundering.

Money laundering is the process of transforming money obtained from unlawful activities into legitimate and untraceable assets. The global and anonymous characteristics of cryptocurrency facilitate criminals in concealing their identities, transferring money internationally, and evading conventional banking systems. As a result regulators and enforcement agencies across the world including India are trying to build legal measures to ensure that cryptocurrency does not become a safe route for financial crime.

Cryptocurrencies are digital currencies that differ from traditional currencies in that they are not issued by a government's financial authority. This implies a high level of risk related with financial insecurity, fraud, and an increase in financial crimes. As a result, the International Monetary Fund (IMF) has warned about the dangers that unchecked cryptocurrency expansion poses to the world. With a total market valuation of more than $2 trillion, governments should be more active, effective, and collaborative in their policies.[1]

India has seen a rapid increase in crypto trading, investments and blockchain based businesses. At the same time,

cases of illegal transactions, cyber fraud and laundering through crypto platforms have also been reported. This has pushed the government to frame laws, introduce compliance requirements, for exchange and give more powers enforcement authorities. However, due to constantly changing nature of digital currencies, challenges still remain in building a well balanced and effective legal framework. This paper studies how cryptocurrency is being used for money laundering in India, what laws and enforcement mechanisms exist to control it and what improvements are

[1] Achraf Guidara, Cryptocurrency And Money Laundering: *A Literature Review*, Volume 4, Issue 2, CORPORATE LAW & GOVERNANCE REVIEW, *36, 36, (2022)*

needed. The aim is to understand how India can promote innovation in the crypto sector while ensuring financial security and misuse.

2. Conceptual Framework

2.1 Understanding Cryptocurrency

Cryptocurrency is a sort of digital currency that exists only online and is secured via cryptography. Cryptocurrency operates on a decentralised network of computers called a blockchain, as opposed to being governed by a central body like the Reserve Bank of India. Every transaction is recorded on this blockchain, making it transparent yet difficult to modify.

Key Features of Cryptocurrency

These fundamental characteristics set cryptocurrencies apart, but they also present potential for abuse:

Decentralisation: Cryptocurrency is not governed by a single entity. This weakens government and banking regulation, making unlawful payments harder to track.

Pseudo-anonymity: Crypto users are identifiable by wallet addresses rather than names. Transactions are available to the public, but unless the wallet is connected to KYC information, the user's true identity is concealed.

Borderless Transactions: Cryptocurrency makes it simpler to transfer illicit money across borders since it can be exchanged immediately across nations without bank or regulatory approval.

2.2 Understanding Money Laundering in The Digital Era

Money laundering refers to the process of converting the money earned from illegal activities into funds that appear legitimate. Traditionally, this was done through shell companies, overseas banking systems and cash transactions. However, with the growth of digital financial systems, the methods of laundering has evolved.

In the digital era, financial crime has moved beyond physical cash using,

- Online banking networks
- Virtual assets and cryptocurrency
- Fintech platforms and prepaid cards
- Gaming tokens and online gambling systems.

Digital tools helps criminals bypass regular banking checks, reduce physical evidence, and operates across jurisdictions within seconds. As a result, tracking illegal financial flows has become more difficult for enforcement agencies, especially when transactions involve multiple digital platforms and foreign entities.

2.3 Why Cryptocurrency is used for Laundering ?

Money launderers favour cryptocurrencies because it gives an easier and faster approach to mask the source of unlawful money compared to traditional banking techniques. The features that make crypto convenient for real users

— such as privacy, speed and worldwide access — also make it useful for illicit activities.[2]

Main reasons include:

a) Identity Protection

In cryptocurrency transactions, users are identifiable by wallet numbers instead of names or bank account details. Because of this, enforcement agencies find it challenging to connect a transaction to a specific individual unless stringent KYC regulations are implemented.

b) Cross Border Transfer Without Banking

Crypto may be transferred from one country to another instantly without engaging banks or government authorisation. Criminals utilise this to transport unlawful funds across jurisdictions and avoid financial monitoring.

c) Lack of Uniform Global Regulation

Different countries follow different regulations involving cryptocurrencies, and many jurisdictions are still uncontrolled. These legal distinctions are exploited by criminals to transfer money to nations with lax control.

d) Use of Crypto-Mixers and Privacy Tools

Online services that conceal transaction history by blending or encrypting transactions include crypto-mixers, tumblers, and privacy coins like Monero and Dash. This disrupts the traceability chain and makes tracking practically hard.

e) Conversion from Peer to Peer (P2P) Without Exchange

Instead of using registered crypto exchanges, criminals often conduct direct P2P trading through private organizations and social media. Since these transactions do not go through KYC-verified platforms, the money trail remains obscured.

[2] Ranjith Karat, *Impact of Money Laundering Activities on Indian Economy*, Vol 2, EEL, 111, 114-115, (2022)

f) Simple Conversion to Legal Assets

After circulating across several wallets and platforms, crypto funds can be converted into:

- Cash through small withdrawals
- Gift cards and prepaid vouchers
- NFTs and gaming tokens
- Offshore exchange accounts

By the time it reaches the latter steps, these techniques make illicit money seem legitimate.

3. Notable Case Studies and Enforcement Actions

3.1 Enforcement Directorate's investigation into Chinese Controlled Instant Loan Apps (Crypto Laundering Case 2021-2022)

According to recent ED reports, many of the illegal loan apps in India especially the so called "instant loan apps" were controlled by syndicated with Chinese connections. These apps offered quick loans often small amounts, frequently requiring minimal verification or documentation, making them attractive to people with limited formal banking access. Once loans were disbursed, the apps operators would use aggressive or fraudulent methods for repayment or harassment if borrowers defaulted. What made these apps particularly dangerous was their integration with cryptocurrency, funds collected from borrowers or victims were converted into crypto and routed to offshore exchanges or wallets, thereby obscuring the money trail. Thus, what began as a consumer leading scam turned into a complex laundering and cross border fraud network through the use of digital assets.

In a major operation, ED invoked the Prevention of Money Laundering Act, 2002 (PMLA) against the accused loan app promoters and connected entities. Under this action, ED attached properties worth 3.72 crore belonging to one of the accused who is a Chinese national including bank balances, fixed deposits and immovable property to prevent dissipation of assets.[3] Earlier, in 2022, ED carried out raids in several business and residential properties across multiple cities (Delhi, Ghaziabad, Mumbai, Lucknow, Gaya) in connection with a money laundering probe linked to a token named "HPZ" and related entities.[4] Enforcement agencies have publicly flagged that Chinese nationals dominate a large share of such loan apps and crypto scam, reflecting a transnational element in these crimes.[5] The investigation have led to freezing of bank accounts, temporary attachment of identified properties and assets under PMLA, and ongoing criminal proceedings.

3.2 Morris Coin Cryptocurrency Investment Scam Case (Kerala)

The morris coin plan was presented as a legitimate cryptocurrency investment, launched by a promoter named Nishad K and his associated firms Long Rich Global, Long Rich Technologies and Morris Trading Solutions. Investors were promised high returns reportedly upto 3-5% per day. Investors bought "Morris Coin" via an initial offer, reportedly paying amount (For eg, 10 Morris coins = 15,000) through bank transfers to shell entities, even though the coin lacked any genuine blockchain backing or legitimate utility.[6] The scheme was effectively a Ponzi / fake ICO and money from new investors was used to pay returns to earlier ones until payouts stopped and the scheme collapsed. As per FIRs and investigation by the police and central agency, more than 900 investors were cheated with total losses estimated at 1,200 crore.

After collecting deposits, the operators diverted funds into multiple bank accounts of associated firms and then moved them through shell companies to obscure the trail. Part of the proceeds was used to purchase immovable

properties across states in Kerala, Tamil Nadu, Karnataka and other assets, instead of delivering any legitimate crypto returns. Some amounts was reportedly converted into cryptocurrencies or held as crypto equivalents by associates, making tracking and reclamation harder. Thus, the scheme combined typical Ponzi style fraud with laundering via crypto and shell company layering, and then asset conversion in real estate and other sectors to mask the illicit origin.

[3] https://enforcementdirectorate.gov.in/sites/default/files/latestnews/Press%20Release-PAO-Chinese%20loan%20app%20case-12.11.2024.pdf

[4] THE INDIAN EXPRESS, https://indianexpress.com/article/india/chinese-loan-apps-case-ed-searches-freezes-payment-gateways-8155398/?utm_source=chatgpt.com (last visited Dec 02, 2025)

[5] TIMES OF INDIA, https://timesofindia.indiatimes.com/india/chinese-behind-most-crypto-loan-app-rip-offs-ed-report/articleshow/124886084.cms?utm_source=chatgpt.com (last visited Dec 02, 2025)

[6] THE INDIAN EXPRESS, https://www.newindianexpress.com/states/kerala/2022/Jan/12/rs-1200-crore-crypto-fraud-pulled-off-by-keralite- with-just-a-website-2405723.html?utm_source=chatgpt.com (last visited Nov 29, 2025)

ED initiated money laundering investigation under the Prevention of Money Laundering Act, 2002 based on the FIRs registered by police in various districts of Kerala. As of January 2022, ED attached assets worth 36.72 crore including balances in bank accounts belonging to Nishad K and his companies, immovable property of associates, and even rupee equivalent holdings of cryptocurrencies acquired from the proceeds of crime. In July 2022, ED attached further properties and assets with around 14 crore, including bank balances of the accused firms and real state. Investigations revealed that the investment promised wee fraudulent, the ICO was fake, and the funds were misused. several search operations were conducted at premises linked to the accused, and incriminating documents were seized. On March 24, 2022, ED arrested one of the min stockist / promoters under money laundering charges. The case was registered as cheating and money laundering.[7] As per ED's press release dated 08.09.2023 assets with
3.43 crore (movable and immovable) linked to the same were provisionally attached.[8]

4. Legal and Enforcement Measures in India

India currently lacks a specialised law specifically tailored for cryptocurrencies. The nation has sought to manage crypto-related financial offences by enforcing the existing financial and anti-money laundering regulations. The major milestone occurred in March 2023, when the government formally subjected virtual digital asset (VDA) transactions to the Prevention of Money Laundering Act (PMLA), 2002. This signified a transition from a lenient regulatory environment to a compliance-focused structure.

1. Prevention of Money Laundering Act, 2002

The inclusion of cryptocurrency under PMLA means that:

- Crypto exchanges and intermediaries are now treated as "reporting entities"[9]
- They must conduct KYC, maintain records of transactions, and
- Report suspicious transactions to FIU-IND.

This amendment provides strong enforcement leverage because money laundering offences now apply even if transactions happen on digital platforms outside the traditional banking system. However, the system is still evolving, and not all exchanges have achieved full compliance especially foreign platforms that operate without physical presence in India. Therefore, the legal recognition is strong in theory, but effective implementation depends on monitoring and cross border cooperation.

2. Financial Intelligence Unit - India (FIU-IND)

FIU-IND keeps an eye on financial transactions to look for unusual activities. After crypto platforms became reporting entities, FIU-IND began issuing:

- Compliance notices
- Penalties
- Public suspension orders against non-compliant entities

Although accountability has increased as a result of FIU's engagement, enforcement remains reactive rather than proactive. Exchanges generally comply only after show-cause notices, which emphasizes the need for more proactive monitoring and clearer operating requirements.[10]

3. Enforcement Directorate (ED) Action under PMLA

ED has emerged as the main enforcement body investigating crypto-related laundering. Through:

- Searches
- Bank and wallet freeze orders
- Attachment of proceeds of crime
- ED has played a key role in avoiding dissipation of illicit assets.

ED's ability in tracking money through multilayer transactions illustrates that classic anti-laundering technologies can be modified for crypto. Yet, final recovery often remains incomplete when laundering involves overseas exchanges, mixers, or decentralised platforms. Enforcement capability improves when domestic exchanges collaborate — but decreases dramatically when inquiries involve jurisdictions with lax or ambiguous crypto legislation.

[7] NDTV, https://www.ndtv.com/india-news/cryptocurrency-fraud-man-arrested-in-kerala-ponzi-linked-rs-1-200-crore-cryptocurrency-fraud-2849694?utm_source=chatgpt.com (last visited Nov 28, 2025)

[8] https://enforcementdirectorate.gov.in/sites/default/files/latestnews/PRESS%20RELEASE_Morris%20Coin%20Scam%20Attachment-8.09.2023_0.pdf

[9] Government of Mizoram, https://udpa.mizoram.gov.in/uploads/attachments/2023/02/166b44088949248f6dce2f133085fce4/pmla-guidelines-real-estate-agent.pdf, (last visited Dec 01, 2025)

[10] Financial Intelligence Unit - India, https://fiuindia.gov.in/files/AML_Legislation/pmla_2002.html, (last visited Dec 01, 2025)

4. RBI and Banking Restrictions

The RBI has consistently kept a cautious attitude on cryptocurrency due to dangers linked to volatility, fraud, and informal value transfer. The RBI's policy approach has concentrated on limiting banking exposure to virtual assets, even though cryptocurrency trading is not prohibited in and of itself. In Internet and Mobile Association of India v. RBI (2020),[11] the Supreme Court reversed the RBI's 2018 order prohibiting banks from offering services to cryptocurrency firms. RBI altered its approach following the ruling. Instead of blocking access outright, the central bank now gives instructions to banks to implement:

- Enhanced due diligence for crypto linked accounts
- Reporting suspicious transactions related to crypto investments
- Monitoring of high value transfers between bank accounts and crypto exchanges

Some banks have gone further by voluntarily:

- Imposing transactions caps for crypto trading
- Restricting Credit cards for crypto purchases
- Flagging or freezing accounts used for P2P payments associated with crypto

By discouraging the use of banks for money laundering, the RBI's strategy makes financial institutions cautious and compels customers to adhere to KYC and documentation requirements more openly. However, the drawback is that banking regulations do not prohibit off-bank laundering methods, such as:

- Crypto-to-crypto transfers
- Transactions using decentralised wallets
- Using foreign exchanges that don't adhere to Indian KYC regulations

Therefore, while RBI measures helps reduce misuse through traditional banking channels, they do not directly tackle laundering within the the blockchain ecosystem.

5. Taxation Rules on Virtual Digital Assets

The Union Budget 2022 created a special tax structure for cryptocurrencies and similar assets. Among the provisions are:

- Flat 30% tax on all crypto income — regardless of holding period
- No set-off allowed for losses from one VDA against income from another
- 1% TDS on crypto transfers, applicable on every transaction regardless of profit or loss
- Taxation applicable on gifting of crypto assets

The government explained that although taxation does not automatically confer legal status on crypto,

these rules serve two functions:

- Generate state revenue
- Build a transaction-level traceability framework

Every time crypto is sold or transferred, the 1% TDS deductor captures the seller's PAN and provides transaction details to the Income Tax Department. This allows:

- Identification of frequent traders operating outside registered exchanges
- Tracking wallet-to-wallet transfers via Indian platforms
- Detection of unexplained investment patterns in bank accounts

The tax regime is innovative because it indirectly strengthens AML surveillance. When a user attempts to avoid TDS by shifting suddenly to foreign or unregistered platforms, the behaviour itself becomes a red flag for authorities. Income tax, FIU, and ED can cross share such patters during investigations. [12]

However, this method has structural weaknesses:

Many investors have been forced to join unofficial trading groups on Telegram and WhatsApp because to the 1% TDS charge on each transaction.In order to evade tax deductions, it encourages the adoption of P2P agreements and offshore exchanges. In such areas, documentation and identity traces disappear, making AML monitoring difficult.

As a result, the taxing system serves as a filter for compliance, but it also runs the danger of discouraging consumers from using regulated platforms, which could compromise the goals of enforcement.

5. Recommendations

India has taken significant steps toward integrating cryptocurrencies under the anti–money laundering (AML) framework, particularly with the application of PMLA to virtual digital assets. However, proactive rather than reactive enforcement tactics are needed due to the rapidly changing nature of digital finance. The following recommendations attempt to increase the legal and institutional response to crypto-enabled laundering:

[11] Internet and Mobile Association of India v. RBI (2020), MANU/SC/0264/2020

[12] Abhishek Kumar, *A Study of the Impact of Crypto Currency on the Indian Payment system,* Vol. 12, AJM, 310, 315, (2021)

Stronger Exchange and KYC Regulation

Make KYC required across all crypto platforms and require complete transaction logs for audits.

Mandatory VDA Reporting to FIU-IND

High-value and suspicious transactions must be reported directly to FIU by all cryptocurrency exchanges.

Blockchain Forensics & Tracking Tools

Provide ED, FIU and Cyber Crime sections with specific blockchain-analytics tools to trace wallets and mixers.

Cross-Border Enforcement Agreements

Investigate transactions that are routed through international exchanges by establishing organized collaboration with foreign agencies.

Public Awareness & Investor Education

Frequent awareness campaigns concerning Ponzi crypto schemes, unlawful apps and fraudulent investment platforms.

Below are some recommendations and safety precautions for cryptocurrency owners and investors.

1) Always verify a Web wallet's address, and avoid following dubious connections to an Internet bank or Web wallet.

2) Before transacting, always double-check the recipient's address, the amount entered, details of transaction fees and other costs.

3) Prepare a fallback option to retrieve forgotten account passwords and other credentials as well as keep them safe and confidential.

4) Crypto-investment are dangerous. So standard practices must be followed while investing such diversified investment, reliability of the suppliers and a strong mind-set to deal with unforeseen occurrences.

5) Use cryptocurrency hardware wallets and paper wallets is encouraged.

Use strong antivirus tools to secure the PCs and devices used to access crypto-wallets, and other activities involving virtual currency.[13]

6. Conclusion

Cryptocurrency has introduced a transformative financial innovation, but its anonymity and decentralised nature have simultaneously opened new channels for money laundering in India. Recent investigations by the ED and FIU show that virtual assets are increasingly used to layer and transfer illicit funds through exchanges, wallets and cross- border transactions. While the PMLA amendment of 2023 and SEBI/Finance Ministry interventions mark strong progress, enforcement continues to face challenges due to technological complexity, limited tracing capability and global jurisdictional barriers.

To properly handle crypto-based laundering, India needs boost regulatory clarity, enhance forensic capacity and promote international cooperation while still promoting innovation. A balanced approach—neither over-restrictive nor unregulated—remains vital to guarantee that the crypto ecosystem grows securely without becoming a safe harbour for financial crime.

7. References

1. Achraf Guidara, Cryptocurrency And Money Laundering: *A Literature Review,* Volume 4, Issue 2, CORPORATE LAW & GOVERNANCE REVIEW, *36, 36, (2022)*

2. Ranjith Karat, *Impact of Money Laundering Activities on Indian Economy,* Vol 2, EEL, 111, 114-115, (2022)

3. NDTV, https://www.ndtv.com/india-news/cryptocurrency-fraud-man-arrested-in-kerala-ponzi-linked-rs-1-200-crore-cryptocurrency-fraud-2849694?utm_source=chatgpt.com (last visited Nov 28, 2025)

4. https://enforcementdirectorate.gov.in/sites/default/files/latestnews / PRESS%20RELEASE_Morris%20Coin%20Scam%20Attachment-8.09.2023_0.pdf

5. THE INDIAN EXPRESS, https://indianexpress.com/article/india/chinese-loan-apps-case-ed-searches-freezes- payment-gateways-8155398/?utm_source=chatgpt.com (last visited Dec 02, 2025)

6. THE INDIAN EXPRESS, https://www.newindianexpress.com/states/kerala/2022/Jan/12/rs-1200-crore-crypto- fraud-pulled-off-by-keralite-with-just-a-website-2405723.html?utm_source=chatgpt.com (last visited Nov 29, 2025)

7. NDTV, https://www.ndtv.com/india-news/cryptocurrency-fraud-man-arrested-in-kerala-ponzi-linked-rs-1-200-crore-cryptocurrency-fraud-2849694?utm_source=chatgpt.com (last visited Nov 28, 2025)

[13] Paras Vishwakarma1, Mr. Zohaib Khan2, Dr. Taruna Jain, *Cryptocurrency, Security Issues and Upcoming Challenges to Legal Framework in India,* Vol 05, IRJET, 212, 214, (2018)

8. https://enforcementdirectorate.gov.in/sites/default/files/latestnews / PRESS%20RELEASE_Morris%20Coin%20Scam%20Attachment-8.09.2023_0.pdf

9. Government of Mizoram, https://udpa.mizoram.gov.in/uploads/attachments / 2023/02/166b44088949248f6dce2f133085fce4/pmla-guidelines-real-estate-agent.pdf, (last visited Dec 01, 2025)

10. Financial Intelligence Unit - India, https://fiuindia.gov.in/files/AML_Legislation/pmla_2002.html, (last visited Dec 01, 2025)

11. Internet and Mobile Association of India v. RBI (2020), MANU/SC/0264/2020

12. Abhishek Kumar, *A Study of the Impact of Crypto Currency on the Indian Payment system,* Vol. 12, AJM, 310, 315, (2021)

13. Paras Vishwakarma1, Mr. Zohaib Khan2, Dr. Taruna Jain, *Cryptocurrency, Security Issues and Upcoming Challenges to Legal Framework in India,* Vol 05, IRJET, 212, 214, (2018)