INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 8 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

CRYPTOCURRENCY AND MONEY LAUNDERING IN INDIA: A STUDY UNDER THE PMLA 2002

AUTHOR – RUDRA VASHISHTH & NANCY SHARMA

STUDENTS AT QUANTUM UNIVERSITY

BEST CITATION – RUDRA VASHISHTH & NANCY SHARMA, CRYPTOCURRENCY AND MONEY LAUNDERING IN INDIA: A STUDY UNDER THE PMLA 2002, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 6 (8) OF 2026, PG. 761-773, APIS – 3920 – 0001 & ISSN - 2583-2344.

Abstract

Cryptocurrencies establish a new financial system which utilizes decentralized blockchain technology for direct peer-to-peer transactions without any need for central banks or financial institutions to act as intermediaries. The increasing use of virtual digital assets in India creates new economic possibilities but also raises regulatory challenges. Their features which include pseudonymity and cross-border transferability and weak regulatory control make them highly suitable for criminals who intend to use these technologies for money laundering activities. The laundering of criminal proceeds stands as the primary target of the Prevention of Money- Laundering Act, 2002 (PMLA) which functions as the main law enforcement tool against this crime. India now shows progress in meeting global anti-money laundering requirements through its new regulations which extend reporting requirements to virtual asset service providers. This research investigates the methods by which criminals use cryptocurrencies to process illegal funds and assesses the PMLA's capacity to counter this risk while assessing enforcement practices and court decisions. The research identifies existing regulatory weaknesses and presents recommendations to improve institutional capacity for Cryptocurrency and Money Laundering in India through PMLA 2002which will increase institutional transparency while maintaining financial security through innovative solutions. The PMLA established basic legal foundations which require a specialized and technology-based regulatory framework to tackle new types of digital financial crime.

Keywords: Cryptocurrency, Money Laundering, PMLA 2002, Virtual Digital Assets, Blockchain, Enforcement Directorate, Financial Intelligence Unit, AML Compliance.

1. Introduction

1.1 Cryptocurrency Overview:

Cryptocurrency represents a category of digital or virtual currencies which employ cryptographic methods to secure their transactions and establish new unit generation controls.[1] Cryptocurrencies use decentralized ledger technology to record transactions through a blockchain system which functions as a distributed network of computers that shares transaction data. The decentralized structure enables users to conduct transactions with each other without needing financial institutions to act as intermediaries. The main cryptocurrencies on the market today include Bitcoin, which stands as the first and most recognized digital asset, Ethereum, which serves as a smart contract platform[2], and numerous stablecoins, which are cryptocurrencies that maintain their value by linking to fiat currencies to decrease price fluctuations. [3]

Cryptocurrencies possess main properties that define their function in digital currency systems which include:

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 8 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

• Decentralization: No central authority controls the network; instead, consensus mechanisms (e.g., Proof of Work, Proof of Stake) validate transactions.

• Pseudonymity: Participants transact using wallet addresses rather than personal identifiers, offering privacy while still leaving digital traces.

• Peer-to-Peer Transfer: Users can send and receive value directly without reliance on traditional financial intermediaries like banks or payment processors.

• Global Reach: Cryptocurrencies enable near-instant, cross-border transfers, transcending national boundaries and conventional regulatory frameworks. The features of these systems support financial innovation and inclusion efforts; however, they create special difficulties for regulatory bodies and criminal justice systems, which arise mainly from their use in illegal financial activities.

1.2 Money Laundering

Money laundering uses **multiple stages** to hide the illegal origins of funds until they look like they come from authentic sources. [4]The practice enables criminals to move their illegal earnings without restriction which results in damage to financial systems. The process is typically conceptualized in three broad stages:

1. The initial introduction of illegally obtained funds into the financial system. This could involve depositing cash into bank accounts, purchasing financial instruments, or converting cash into digital assets.

2. Layering The process uses complex transactions, which create an obscured trail of financial records while simultaneously breaking all connections between the funds and their original criminal source. The techniques of this process involve making multiple financial transfers, which occur between different accounts and across international borders, and through various financial instruments, making it impossible to track the funds.

3. The now-laundered money reenters the legitimate economy through investments, purchases, or consumption, giving the appearance of lawful income. Regulators and law enforcement agencies use various anti-money laundering (AML) tools to monitor and detect all money laundering activities that operate through traditional financial systems.[5] The development of digital asset ecosystems has created fresh methods for money laundering, which present obstacles to existing anti-money laundering (AML) regulatory systems.

1.3 The Indian Context

Cryptocurrency interest and participation in India have experienced rapid growth during the past ten years. Digital assets now serve as investment options and technological solutions which retail investors and tech entrepreneurs and speculative traders have started to use. Estimates suggest millions of Indians hold or trade cryptocurrencies which help develop the digital asset economy. Legitimate adoption exists at present but people worry about dangerous cryptocurrency usage which enables money laundering and tax evasion and terrorist financing and other financial crimes.

The pseudonymous nature of transactions together with cross-border value transfer capabilities which digital assets enable create regulatory and enforcement difficulties in a jurisdiction which lacks developed digital asset regulations. Indian authorities developed their response through multiple approaches which include:

• Judicial intervention through Supreme Court rulings about banking access for crypto businesses.

• Enforcement actions under existing statutes such as the Prevention of Money-Laundering Act 2002 PMLA

• Efforts toward creating a comprehensive regulatory regime for virtual digital assets.[7]

The current situation requires further investigation because existing digital asset practices in India create difficulties which

conflict with traditional anti-money laundering systems. The study aims to provide detailed examination of these issues.

2. Theoretical and Conceptual Framework

The relationship between cryptocurrency and money laundering requires researchers to study three elements which include technological systems, regulatory frameworks, and methods that criminals use to conduct financial crimes. Cryptocurrencies operate as lawful financial instruments because they contain design elements which create opportunities for criminals to conduct illegal financial operations.[8]

(a) Anonymity and Pseudonymity

Cryptocurrency users send digital coins between alphanumeric wallet addresses which do not require users to disclose their real names. The blockchain system enables public access to transaction data; however, the actual identity of a wallet owner remains hidden from public view. The system allows users to conduct transactions without showing their actual identity because all personal information stays hidden until connections arise through exchange platforms or investigation methods. Criminals use this system in places where organizations fail to follow Know Your Customer (KYC) rules because it lets them hide their illegal activities. [9]

(b) Irreversibility of Transactions

Blockchain transactions, which receive validation through distributed ledger technology, become permanent after their validation process and ledger entry. The cryptocurrency system permits users to transfer digital assets but lacks the ability to reverse transactions that occur through their platform, unlike traditional banking systems that enable users to freeze or reverse suspicious transactions. The system creates two results because it makes asset recovery more difficult and decreases the ability of institutions to control their operations.[10]

(c) Ease of Cross-Border Transfers

The framework of international boundaries does not restrict cryptocurrency operations because these digital currencies can be used anywhere in the world. The system enables people to send money between any two locations in the world within a few minutes because it does not depend on existing banking networks, which work with multiple banks nor on currency exchange companies. Criminals can use this method to transfer their illegal assets between different countries because they can avoid controlled financial systems which exist in most countries but they can escape to places where there are fewer regulations against money laundering thus creating difficulties for international agencies to enforce their rules and work together.

(d) Mixers and Tumblers

Cryptocurrency mixers or tumblers are services designed to enhance privacy by pooling and redistributing digital assets among multiple users, thereby breaking the traceable link between sender and recipient. The tools create obstacles for investigators who want to track transactions because they break down single transactions into multiple smaller transactions which are later combined back into one single transaction. The tools exist to fulfill privacy needs but they have become commonly used by criminals who want to hide their illegal activities. [11]

(e) Decentralized Finance (DeFi) Platforms

The term Decentralized Finance (DeFi) describes financial systems which run on blockchain technology without using any centralized financial entities. The system allows users to borrow and lend money while they can trade all types of assets through automated systems which control their operations. The absence of a single governing body in DeFi platforms results in limited customer identification systems which lack essential reporting functions for regulatory compliance. The lack of custodial supervision creates difficulties for law enforcement who need to trace operations back to the proper responsible parties.[12]

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 8 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

(f) Technological Sophistication and Accelerated Innovation

The crypto ecosystem evolves rapidly, introducing innovations such as privacy coins, cross-chain bridges, and tokenized assets. Regulatory frameworks, including anti-money laundering laws, often lag behind technological developments. This regulatory gap creates temporary spaces where illicit actors may exploit legal ambiguities.[13]

2.2 Money Laundering Lifecycle with Cryptocurrency

The traditional three-stage model of money laundering—placement, layering, and integration— remains conceptually applicable to cryptocurrency transactions. However, the methods and mechanisms differ significantly in the digital environment.

Stage	Traditional Financial System	Cryptocurrency Ecosystem
Placement	Depositing illicit cash into banks or purchasing financial instruments	Converting cash into cryptocurrency via exchanges, peer-to-peer platforms, prepaid cards, or offshore platforms
Layering	Complex bank transfers, shell companies, offshore accounts	Using mixers, privacy coins, cross-chain swaps, DeFi lending pools, multiple wallet transfers
Integration	Investing in property, businesses, luxury goods	Converting crypto into fiat currency through exchanges; investing in NFTs, real estate, or legitimate businesses

(a) Placement in the Crypto Context

The first step in the cryptocurrency system brings illegal money into the virtual world. People can purchase cryptocurrencies through exchanges which allow KYC requirements and they can use peer-to-peer trading platforms which enable direct cryptocurrency exchanges or they can turn cybercrime profits into digital currencies. Cybercriminals now require users to make ransomware payments in Bitcoin which allows them to escape traditional money laundering methods.

(b) Layering through Digital Complexity

Digital Complexity enables different methods for executing cryptocurrency transactions which require multiple digital techniques. The process of transferring money requires users to send their assets through multiple wallet addresses. Users employ mixing services to hide their complete transaction records. Users exchange their digital assets through cross-chain swaps. Users of decentralized exchanges (DEXs) maintain their privacy by choosing to operate outside centralized systems. Users employ privacy-protecting digital currencies which enable them to keep their transaction information secret. Investigators need to handle multiple blockchain transactions which need to be handled because blockchain systems maintain records forever. The last step of money laundering involves returning the cleaned money back to the economic system. The process allows users to change their cryptocurrency into traditional currency through regulated exchanges before they make investments in real estate luxury goods startups and online businesses. People in India can report their cryptocurrency profits as trading income which makes their illegal earnings seem legitimate for taxation purposes.

(c) Integration into the Legitimate Economy

The final stage involves reintroducing laundered funds into the formal economy. This may occur by converting cryptocurrency back into fiat currency through regulated exchanges, investing in real estate, luxury assets, startups, or digital ventures. In jurisdictions like India, individuals may declare cryptocurrency gains as trading profits, thereby giving an appearance of

legitimacy to previously illicit proceeds.

3. Legal Framework in India

3.1 Prevention of Money-Laundering Act, 2002 (PMLA)

The Prevention of Money-Laundering Act of 2002 establishes itself as India's main law against money laundering by preventing criminals from converting their illegal earnings into clean money and establishing rules for seizing assets used in these crimes. The Act aligns India's domestic framework with international obligations, particularly those arising under the Financial Action Task Force (FATF) recommendations.[14]

(a) Objective of the Act The primary objectives of the PMLA are:

- To prevent and control money laundering;
- To confiscate and attach property obtained through criminal proceeds;
- To punish offenders involved in laundering activities;
- To implement international AML standards.

The Act criminalizes not merely the possession of illicit proceeds but also activities such as concealment, possession, acquisition, use, or projecting such proceeds as untainted property.

(b) Definition of "Proceeds of Crime"

According to Section 2(1)(u) of PMLA, "proceeds of crime" designates any property that criminals acquire through their illegal activities which involve scheduled offences. The Act defines "property" in a comprehensive manner which encompasses all types of assets including movable things, immovable things, tangible things, and intangible things. This extensive definition establishes that cryptocurrency, as a digital and intangible asset, qualifies as "property" because it possesses value that comes from a scheduled offence. Thus, even though cryptocurrencies are not

recognized as legal tender in India, they may qualify as property capable of attachment under PMLA.

(c) Scheduled Offences

PMLA operates in conjunction with a list of "scheduled offences" provided in its Schedule. The list includes criminal activities which violate laws established through the Indian Penal Code and Narcotic Drugs and Psychotropic Substances Act and Prevention of Corruption Act and other statutes. Money laundering proceedings under PMLA start when financial gains emerge from these base criminal activities. [15]

(d) Attachment and Confiscation

The Act grants authorities the right to provisionally seize assets which they believe belong to money laundering operations according to Section 5. The Central Government can take control of properties after the adjudication process ends. Authorities have obtained the power to Control cryptocurrency operations through these actions:

- The authorities have the ability to Freeze exchange accounts.
- The authorities have the ability to Seize digital wallets

. • The authorities have the ability to Attack virtual assets which are stored by intermediaries.[16]

Law enforcement agencies need to contact exchanges because digital assets exist in online storage to enforce their mandates which include asset seizure and withdrawal limitations.[17]

(e) Punishment

Section 4 of PMLA establishes a sentence range which requires at least three years in prison but allows a maximum of ten years for specific narcotics-related violations. The harsh bail restrictions established by Section 45 prove that lawmakers want to categorize money laundering as a major financial crime.

(f) Enforcement Directorate (ED)

The Enforcement Directorate (ED) serves as the main agency which investigates PMLA violations while enforcing its legal requirements. The agency has authorization to

- Search and seize items

. • Call people to give evidence.

- Seize and confiscate property.
- Prosecute cases in Special Courts.

3.2 Applicability of PMLA to Cryptocurrency

India has not declared cryptocurrency as legal tender; however, the absence of legal tender status does not exempt digital assets from regulatory scrutiny.[18] The PMLA applies to assets which meet its requirements for criminal asset classification instead of using currency status as its determining factor.

The PMLA applies to situations which include the following three scenarios.

(a) Cryptocurrency as Proceeds of Crime

The first scenario involves cryptocurrency which acts as the proceeds from illegal activities. Illicit funds generated from scheduled offences become "proceeds of crime" when they are converted into cryptocurrency digital assets. The assets generated from cyber fraud activities or ransomware attacks and narcotics trafficking operations become subject to PMLA because they represent crypto assets.[19]

(b) Use of Virtual Assets to Conceal Illicit Wealth

Virtual assets serve as tools which criminals use to hide their illegal wealth from authorities. Criminals Use cryptocurrencies to create multiple layers of their money laundering operations. The use of digital assets to hide ownership and disguise origins while showing illicit wealth as legitimate investment returns creates an offence under PMLA Section 3.

(c) Liability of Exchanges and Intermediaries

The regulatory notifications determine whether cryptocurrency exchanges and virtual asset service providers become classified as PMLA reporting entities. The exchange platforms allow users to convert between fiat and crypto because they serve as financial gateways between regulated and unregulated financial spaces.[20] The organization faces enforcement actions and penalties when it fails to conduct due diligence or maintain records or report suspicious transactions.

(d) Extra-Territorial Implications

The PMLA uses its provisions for cross-border offences and overseas property attachment to address the borderless cryptocurrency market. International cooperation mechanisms and mutual legal assistance treaties (MLATs)[21]

3.3 Financial Intelligence Unit – India (FIU-IND)

The Financial Intelligence Unit of India operates as the main national organization that handles suspicious financial transaction information through its processes of receiving, processing, analyzing, and distributing this data.

(a) Reporting Obligations

The PMLA and its associated rules require reporting entities to submit three types of documents which include Suspicious Transaction Reports STRs and Currency Transaction Reports CTRs and Records of identity verification and transaction history. Digital assets have become more important in today's world, which means that cryptocurrency exchanges and service providers now need to follow these reporting requirements.

(b) Monitoring and Analysis

The FIU-IND monitoring system detects suspicious activities by analyzing transaction patterns which include three types of unusual transaction events: high-value crypto conversions and rapid movement of funds across multiple wallets and transactions that do not match the financial profiles of customers.

(c) Coordination with Enforcement Agencies

The FIU-IND organization shares intelligence information with several agencies which include the Enforcement Directorate and the Income Tax Department and other investigative bodies. Blockchain analytics tools enable investigative agencies to trace fund flows in crypto- related cases through their joint use with these agencies.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 8 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

4. Regulatory Developments and Enforcement in India

4.1 RBI and Cryptocurrency

The Reserve Bank of India (RBI) has raised concerns about cryptocurrencies because they endanger consumer protection standards and financial stability and create market volatility and allow capital flight and people are able to use them for money laundering and terrorist financing. [22]The RBI has declared that cryptocurrencies have no actual value since they lack both sovereign backing and intrinsic worth which creates systemic dangers when they enter the regulated banking system. The RBI issued a circular in April 2018 which prohibited all regulated entities including banks and financial institutions from conducting business with customers who engaged in virtual currency transactions. The prohibition created total banking restriction which prevented Indian cryptocurrency exchanges from obtaining any banking services. The Supreme Court received a challenge against the circular which was brought to court. The Supreme Court of India voided the RBI circular in the case of **Internet and Mobile Association of India v. Reserve Bank of India** because it failed to meet the test of proportionality.[23] The Court found that the RBI possessed authority to control virtual currencies yet complete banking prohibition represented an extreme response because which cryptocurrency exchanges showed no evidence that they caused harm. The ruling allowed crypto trading platforms to resume operations in India but businesses remained uncertain about upcoming regulations. The new regulatory framework moved away from complete bans to establish controls which would monitor potential risks through taxation systems and AML compliance activities. The RBI has been working on developing a Central Bank Digital Currency as a regulated alternative to private cryptocurrencies.[24]

4.2 Income Tax and Cryptocurrency

The Income Tax Act of 1961 mandates taxation for cryptocurrency transactions because the government considers virtual digital assets (VDAs) as taxable assets. The Finance Act 2022 established a dedicated tax framework for virtual digital assets which consists of a 30 tax on virtual digital asset transfer profits and an expense deduction prohibition that allows only acquisition costs and a total loss prohibition that prevents crypto trading losses from offsetting other earnings and a TDS requirement for designated crypto transfers that exceed established limits. The taxation framework establishes economic recognition for cryptocurrencies without granting them official currency designation. The tax provisions serve two functions because they enable the government to collect revenue and improve the ability to trace financial transactions. The authorities obtain better access to cryptocurrency trading activities because TDS and reporting requirements necessitate traders to disclose their trading activities which helps monitor anti-money laundering operations under PMLA. [25]

4.3 Enforcement Directorate Actions

The Enforcement Directorate (ED) has increasingly invoked the Prevention of Money-Laundering Act, 2002 in cases involving cryptocurrency transactions linked to scheduled offences such as cyber fraud, illegal betting, narcotics trafficking, and financial scams. The enforcement actions currently operate through two primary methods which include a process that allows authorities to attach cryptocurrency assets stored at exchanges and another method which enables them to freeze accounts of exchanges that the authorities suspect operate as money laundering channels and they operate through an investigation process that targets shell companies which transfer illegal funds into digital assets and the authorities summon exchange representatives because they did not meet anti-money laundering regulations. The ED has treated cryptocurrency as "property" within the meaning of PMLA, enabling provisional attachment and eventual confiscation where linked to proceeds of crime. The enforcement actions show that even in the absence of a

dedicated cryptocurrency statute, existing economic offence laws can be adapted to address digital laundering mechanisms.

5. Challenges in Implementation

5.1 Anonymity and Traceability

Blockchain systems allow users to view all transactions but users cannot determine which individual owns a specific wallet. Real-world identity verification needs The processes which handle KYC records and The process requires exchanges to work together with their customers and The system requires information which needs to be shared between different countries. The process of tracing transactions through decentralized exchanges and peer-to-peer transfers without intermediaries makes the process more difficult to execute.[26] Investigators face challenges from privacy-enhancing technologies which obstruct their ability to conduct forensic examinations.

5.2 Technology and Law Enforcement Gap

To investigate cryptocurrencies law enforcement needs specialized skills which include blockchain analytics and cyber forensics and digital asset tracing capabilities[27]. Many enforcement agencies face .Crypto technology develops at a faster rate than regulatory bodies can manage so the enforcement systems become unbalanced between different encryption technologies which include DeFi and cross-chain systems.

5.3 Global Jurisdictional Issues

Cryptocurrency transactions operate beyond the control of individual nations. Criminal organizations use the ability to move funds between overseas exchanges and wallet platforms in countries that have insufficient anti-money laundering regulations.

This situation creates three major problems which include:

- Difficulties in freezing overseas assets,
- Challenges in enforcing attachment orders,
- Dependence on mutual legal assistance treaties (MLATs).

The existing global regulatory system differences lead to enforcement problems which produce a regulatory loophole that criminal organizations exploit.

6. Judicial Responses

6.1 Supreme Court on Cryptocurrency

The Internet and Mobile Association of India v. Reserve Bank of India [28]case established a crucial legal precedent which changed the crypto regulatory system in India. The Supreme Court applied the doctrine of proportionality and held that while the RBI possessed regulatory authority, the complete restriction on banking services lacked sufficient empirical justification. The judgment recognized cryptocurrency trading as a legitimate business activity, subject to reasonable regulation. The Court recognized money laundering and financial stability risks but permitted future legislative or regulatory measures.

6.2 PMLA Proceedings in Crypto Cases

The Indian judiciary has confirmed that the Enforcement Directorate possesses investigation and crypto asset seizure powers under PMLA when three specific conditions are met. The first requirement mandates a scheduled offence existence. The second requirement states that the digital asset must meet the definition of "proceeds of crime." The third requirement mandates that all Act-required procedures must be followed. The courts have interpreted "property" to encompass all types of digital assets which exist outside the physical realm. The judicial system has examined two aspects because it only assessed whether statutory procedures were followed and not whether PMLA applies to cryptocurrency.

7. Comparative Perspectives

A comparative examination of global regulatory frameworks demonstrates that while jurisdictions differ in classification and regulatory philosophy, most have integrated cryptocurrencies into existing Anti-Money

Laundering (AML) regimes.

Jurisdiction	Crypto-AML Regulation	Reporting Requirements
United States	Cryptocurrencies treated as property; AML governed under the Bank Secrecy Act and enforced through Financial Crimes Enforcement Network (FinCEN) regulations. Virtual Asset Service Providers (VASPs) classified as Money Services Businesses (MSBs).	Mandatory filing of Suspicious Activity Reports (SARs) and Currency Transaction Reports (CTRs); compliance with the Travel Rule; KYC obligations.
European Union	Comprehensive regulation through Markets in Crypto-Assets Regulation (MiCA) and AML directives such as Fifth Anti-Money Laundering Directive.[29]	Customer due diligence, beneficial ownership verification, and application of the Travel Rule for crypto transfers across member states.
Singapore	Regulated under the Payment Services Act, with crypto exchanges licensed and supervised by the Monetary Authority of Singapore.	Mandatory reporting of suspicious transactions; stringent AML/CFT compliance; licensing and audit requirements.

Comparative Analysis

- **United States:** The U.S. model integrates cryptocurrency within existing financial crime statutes rather than creating a separate criminal regime. The authorities treat exchanges just like they treat traditional financial institutions when they assess compliance with anti-money laundering regulations. [30]
- **European Union:** The European Union has established a unified regulatory system which combines market regulations and anti-money laundering rules to safeguard consumer rights while maintaining financial system stability.
- **Singapore:** Singapore provides clear guidelines for crypto business operations through its licensing system but enforces strict compliance requirements. India's Position India depends on taxation laws and Reserve Bank of India advisories together with the Prevention of Money- Laundering Act 2002 enforcement, for its regulatory framework. The country has made progress in bringing crypto service providers into its anti-money laundering reporting requirements but it still needs a separate complete cryptocurrency anti-money laundering law which matches the standards of MiCA and Payment Services Act. The current regulations permit changes instead of formal establishment as permanent rules.

8. Policy Recommendations

India should implement these specific measures to enhance its ability to combat money laundering activities associated with cryptocurrency transactions.

8.1 Clear Regulatory Classification

India needs to establish a specific legal framework which will define the following terms:

- Virtual Digital Assets (VDAs),
- Utility tokens, • Security tokens,
- Non-Fungible Tokens (NFTs).

The process of classifying digital assets through official definitions enables better identification of different asset types which leads to more effective PMLA enforcement.[31] The legal system would establish standards about licensing requirements and measures to protect consumers and procedures for fighting money laundering.

8.2 Mandatory KYC/AML Compliance for All Intermediaries

All cryptocurrency exchanges together with custodial wallet providers and decentralized exchange interfaces that operate in India and all peer-to-peer platforms must perform strict Know Your Customer (KYC) verification.

- Maintain transaction records,
- Implement risk-based AML programs,
- Report suspicious transactions to FIU-IND.

Uniform compliance standards would reduce regulatory arbitrage and close enforcement gaps.

8.3 Establishment of Blockchain Analytics Units

The Enforcement Directorate and Financial Intelligence Unit-India and Cyber Crime Divisions require dedicated blockchain investigation units which need to employ blockchain forensic tools for tracing wallet transactions and discovering user behavior patterns and identifying mixing processes. Continuous technical training is essential to keep pace with technological innovation.

[32]8.4 Strengthened International Cooperation

The borderless nature of digital assets requires India to enhance its Mutual Legal Assistance Treaties (MLATs) through domestic standardization of Financial Action Task Force (FATF) guidelines and its involvement in international asset recovery efforts and its partnerships with worldwide blockchain analytics organizations. International collaboration remains essential for effective control of cross-border crypto laundering operations.

8.5 Public Awareness and Compliance Culture

Effective AML enforcement requires awareness beyond regulatory agencies. Recommended steps include:

- Judicial training programs on digital evidence and crypto tracing
- capacity-building workshops for enforcement officers
- compliance training for financial institutions
- public education campaigns to discourage misuse. [33]

A compliance-driven ecosystem reduces the likelihood of inadvertent facilitation of laundering.

9. Case Studies

9.1 Illustrative Case Study: Laundering through a Crypto Exchange Hypothetical Scenario:

1. **Predicate Offence:** Proceeds generated from illegal narcotics trafficking.
2. **Placement:** Cash converted into cryptocurrency through peer-to-peer platforms or foreign exchanges.
3. **Layering:** Funds transferred through multiple wallet addresses and routed via mixing services to obscure origin.
4. **Cross-Border Movement:** Crypto assets transferred to an offshore exchange in a jurisdiction with weak AML oversight.
5. **Integration:** Converted back into fiat currency and remitted to a shell company registered in India as purported business

income.

6. **Enforcement Action:** The Enforcement Directorate identifies suspicious transactions, traces wallet clusters through blockchain analysis, provisionally attaches crypto assets and related bank accounts under PMLA, and initiates prosecution.

This scenario demonstrates how traditional laundering stages adapt within digital infrastructure while remaining conceptually similar.

9.2 Enforcement Directorate Attachment Cases

In recent years, the Enforcement Directorate has initiated multiple investigations involving cryptocurrency exchanges suspected of facilitating laundering of fraud proceeds and cybercrime earnings. Common patterns include:

- Conversion of scam proceeds into cryptocurrency,
- Use of exchange platforms lacking robust KYC compliance,
- Rapid movement of digital assets across multiple accounts.

Where sufficient evidence establishes linkage to scheduled offences, the ED has provisionally attached crypto holdings under PMLA and pursued adjudication before Special Courts. Courts have generally upheld such actions when procedural safeguards are met and the nexus to proceeds of crime is demonstrated.

10. Conclusion

Modern finance has undergone its most significant transformation through cryptocurrencies which enable decentralized value transfer and deliver efficient technological solutions while promoting financial access and creating fresh economic possibilities. The Indian market shows increasing digital asset trading activity because of growing technological adoption and rising investor interest. The use of cryptocurrencies brings various advantages to users whereas its implementation creates major obstacles for regulatory authorities who need to enforce measures against money laundering activities and terrorist financing operations and cybercrime-related financial transactions and cross-border unlawful financial activities. The Prevention of Money-Laundering Act, 2002 (PMLA) has emerged as the principal statutory mechanism through which Indian authorities address crypto-linked financial crime. The statute permits law enforcement to treat all digital assets as criminal proceeds because it defines "proceeds of crime" using broad terms and defines "property" in an extensive manner. The Enforcement Directorate investigative powers allow authorities to establish temporary prohibition of money traceable to scheduled offences through cryptocurrency seizure and confiscation. The current system lacks a specific regulation for cryptocurrency which creates a situation with undefined rules. Authorities developed their regulatory framework through actual cases which had judicial decisions and tax policies from the Income Tax Act of 1961 and Financial Intelligence Unit-India reporting requirements and international norms established by the Financial Action Task Force (FATF). The existing enforcement structure which includes these elements operates effectively but it has not yet developed into a complete anti-money laundering system for cryptocurrency transactions.

References

1. Prevention of Money-Laundering Act, 2002
2. Internet and Mobile Association of India v. Reserve Bank of India
3. Financial Intelligence Unit – India, AML Reporting Guidelines
4. Financial Action Task Force, International AML/CFT Standards and Recommendations
5. Income Tax Act, 1961 (as amended by Finance Act, 2022 introducing Virtual Digital Asset taxation provisions)
6. Union Budget 2022–23, Government of India (Virtual Digital Asset taxation framework)

7. Prevention of Money-Laundering (Maintenance of Records) Rules, 2005.

8. Ministry of Finance, Government of India, Notification S.O. 1072(E) dated 7 March 2023 (bringing Virtual Digital Asset service providers within the ambit of PMLA reporting obligations).

9. Reserve Bank of India, Circular DBR.No.BP.BC.104/08.13.102/2017-18 (6 April 2018) – Prohibition on dealing in Virtual Currencies.

10. Internet and Mobile Association of India v. Reserve Bank of India, (2020) 10 SCC 274.

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

12. Financial Crimes Enforcement Network, Guidance FIN-2019-G001 on Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies (2019).

13. Bank Secrecy Act, 31 U.S.C. § 5311 et seq.

14. Markets in Crypto-Assets Regulation (Regulation (EU) 2023/1114).

15. Payment Services Act 2019.

16. Enforcement Directorate, Press Releases on Attachment of Cryptocurrency Assets under PMLA (various years).

17. Supreme Court of India, *Vijay Madanlal Choudhary v. Union of India*, (2022) 10 SCC 386 (upholding constitutional validity of key PMLA provisions).

18. International Monetary Fund, *Global Financial Stability Report* (2022–23 editions discussing crypto-asset risks).

19. World Bank, *Cryptocurrencies and Blockchain: Policy Challenges for Developing Countries* (Policy Research Working Paper).

20. NITI Aayog, Discussion Paper on Blockchain Technology: Enabling Trust in the Digital Economy (2020).

21. Ministry of Finance, Government of India, Explanatory Memorandum to the Finance Bill, 2022 (Virtual Digital Asset taxation provisions).

ENDNOTES

1 Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System (2008)

2 Gavin Wood, Ethereum: A Secure Decentralised Generalised Transaction Ledger (2014).

3 Financial Stability Board (FSB), Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements (2020).

4 UNODC, Model Legislation on Money Laundering (2016).

5 FATF, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation (2012, updated 2023).

6Taxation measures specific to digital assets

6 Internet and Mobile Association of India v. Reserve Bank of India, (2020) 10 SCC 274.

7 Ministry of Finance (India), Notifications Bringing Virtual Digital Asset Service Providers under PMLA Reporting Entity Framework (2023).

8 FATF, Virtual Assets and Virtual Asset Service Providers Guidance (Updated 2021).

9 FATF, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation (2012, updated 2023).

10 UNODC, Cryptocurrency Investigation Manual (2022).

11 U.S. Department of the Treasury, Sanctions Review and Actions Relating to Virtual Currency Mixers (2022).

12 Europol, Cryptocurrencies: Tracing the Evolution of Criminal Finances (2022).

13 IMF, Regulating Crypto Assets: Global Challenges and Policy Responses (2023).

14 FATF, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation (Updated 2023).

15 PMLA, 2002, Sec 3 read with Schedule.

16 Enforcement Directorate Press Releases on Crypto Attachments (2022–2024).

17 UNODC, Cryptocurrency Investigation Manual

(2022).

18 Reserve Bank of India, Press Releases on Cryptocurrency (2018–2022).

19 FATF, Money Laundering and Terrorist Financing Risks Arising from Virtual Assets (2019).

20 Ministry of Finance Notification S.O. 1072(E), 7 March 2023.

21 UN Convention Against Transnational Organized Crime (2000); FATF Recommendations.

22 RBI Press Releases on Cryptocurrency Risks (2017–2022).

23 Internet and Mobile Association of India v. RBI, (2020) 10 SCC 274.

24 RBI, Concept Note on Central Bank Digital Currency (2022).

25 Ministry of Finance Notification S.O. 1072(E), 7 March 2023.

26 FATF, International Standards (Updated 2023).

27 UNODC, Cryptocurrency Investigation Manual (2022).

28 Internet and Mobile Association of India v. RBI, (2020) 10 SCC 274.

29 Directive (EU) 2018/843 (Fifth AML Directive); Regulation (EU) 2023/1114 (MiCA).

30 FinCEN Guidance on Virtual Currencies (2013, updated 2019).

31 FATF, Virtual Assets and VASPs Guidance (2021).

32 UNODC, Cryptocurrency Investigation Manual (2022).

33 FIU-IND Annual Report (2023).