International Journal of Advance and Innovative Research
Volume 12, Issue 3: July - September 2025
ISSN 2394 - 7780

MONEY LAUNDERING THROUGH DIGITAL ASSETS AND CRYPTOCURRENCIES: REGULATORY GAPS AND ENFORCEMENT CHALLENGES IN INDIA

SUPRIYA MICHAEL LOPES
PhD Scholar, University of Mumbai, Email: supriyamlopes@gmail.com

ABSTRACT
The rapid rise of cryptocurrencies and other digital assets has transformed the global financial landscape, introducing new modes of decentralised and borderless transactions. These innovations, while fostering financial inclusion and technological advancement, have simultaneously created significant vulnerabilities for misuse in illicit activities, particularly money laundering. Globally, enforcement agencies have identified cryptocurrencies as a preferred medium for laundering illicit proceeds due to features such as pseudonymity, decentralisation, and the ease of cross-border transfers without traditional financial intermediaries.
In the Indian context, the increasing adoption of virtual digital assets (VDAs) has raised serious regulatory concerns. Instances of their misuse in financial crimes, including fraud and terror financing, have highlighted the inadequacy of existing legal frameworks to effectively monitor and control such transactions. The inherent characteristics of cryptocurrencies—anonymity, lack of central authority, and global accessibility—pose unique challenges to conventional anti-money laundering (AML) mechanisms.
India has taken initial regulatory steps by bringing virtual asset service providers within the ambit of the Prevention of Money Laundering Act, 2002 and subjecting them to oversight by the Financial Intelligence Unit-India (FIU-IND). However, these measures remain fragmented and reactive, leaving substantial regulatory gaps in areas such as cross-border enforcement, technological tracking, and jurisdictional coordination.
This paper argues that despite formal inclusion under the PMLA framework, significant lacunae persist in both regulation and enforcement, undermining the effectiveness of anti-money laundering efforts in the digital asset ecosystem. The study adopts a doctrinal and analytical methodology, supplemented by a comparative analysis of international standards, particularly those developed by the Financial Action Task Force (FATF), to assess India's preparedness in addressing emerging challenges in cryptocurrency-based money laundering.

INTRODUCTION

Background
The emergence of cryptocurrencies marks a significant shift in the global financial ecosystem, driven by advancements in blockchain technology and decentralised finance. Cryptocurrencies such as Bitcoin operate on distributed ledger systems that enable peer-to-peer transactions without the need for intermediaries like banks.[1] This technological innovation has introduced efficiency, transparency, and accessibility in financial transactions; however, it has simultaneously created avenues for misuse, particularly in the context of financial crimes.
In India, the adoption of cryptocurrencies has witnessed exponential growth over the past decade, especially among retail investors and technology-driven financial platforms.[2] The rise of cryptocurrency exchanges and digital asset trading platforms has facilitated large-scale participation in virtual asset markets. Despite regulatory uncertainties, including restrictions imposed by the Reserve Bank of India (RBI) and their subsequent relaxation, the crypto ecosystem in India continues to expand rapidly.[3]
This increasing adoption has also transformed traditional methods of money laundering. Conventionally, laundering involved physical cash or banking channels; however, the advent of digital assets has enabled a shift towards more sophisticated methods of laundering. Cryptocurrencies allow rapid, cross-border transactions with limited traceability, thereby making them attractive tools for illicit financial activities.[4]

Conceptual Framework
Money laundering refers to the process by which proceeds of crime are concealed or disguised to appear as legitimate income. It traditionally involves three stages: placement, layering, and integration.[5] Placement refers

"[1] Andreas M. Antonopoulos, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies* 15 (O'Reilly Media, California, 2nd edn., 2017).
[2] Reserve Bank of India, "Report on Trend and Progress of Banking in India" 78 (2022).
[3] *Internet and Mobile Association of India v. Reserve Bank of India*, (2020) 10 SCC 274.
[4] Financial Action Task Force, "Virtual Assets and Virtual Asset Service Providers" 12 (2019).
[5] K.C. Mishra, *Money Laundering: The Indian Experience* 45 (Taxmann Publications, New Delhi, 2018).

ISSN 2394 - 7780

to the introduction of illicit funds into the financial system; layering involves complex transactions to obscure the origin of funds; and integration denotes the re-entry of laundered money into the legitimate economy.
Digital assets and cryptocurrencies have significantly altered these stages. Cryptocurrencies can facilitate layering through multiple wallet transfers, mixing services, and anonymity-enhancing technologies.[1] Moreover, decentralised platforms often operate beyond traditional regulatory oversight, thereby complicating detection and enforcement. The pseudonymous nature of blockchain transactions further enhances the ability of offenders to obscure identities, making cryptocurrencies a preferred medium for laundering illicit proceeds.[2]

Research Problem

The rapid evolution of digital assets has outpaced the development of regulatory frameworks in India. While certain aspects of cryptocurrency transactions are indirectly governed by existing laws such as the Prevention of Money Laundering Act, 2002 and the Information Technology Act, 2000, there is no comprehensive legislation specifically addressing cryptocurrency-related offences.[3]
This regulatory gap creates uncertainty in enforcement and compliance. Authorities face challenges in monitoring transactions, identifying offenders, and asserting jurisdiction over cross-border activities. Furthermore, there exists a fundamental tension between fostering technological innovation and ensuring effective regulation.[4] Excessive regulation may stifle innovation in the fintech sector, whereas inadequate regulation may expose the financial system to significant risks, including money laundering and terrorist financing.

Research Questions

The present study seeks to address the following key questions:

- Whether the existing legal framework in India adequately regulates money laundering through cryptocurrencies?
- What are the major enforcement challenges faced by regulatory authorities in tackling crypto-based laundering?
- How can the existing regulatory gaps be effectively addressed to balance innovation with financial security?

Hypothesis

This research is premised on the hypothesis that the existing legal framework governing cryptocurrencies in India is fragmented and inadequate to effectively address the challenges of money laundering. While laws such as the Prevention of Money Laundering Act, 2002 provide a foundational framework, their application to digital assets remains ambiguous and inconsistent.
Cryptocurrencies, by their very nature, enable laundering through mechanisms such as anonymity, use of mixers and tumblers, and seamless cross-border transfers without regulatory intervention. These features significantly undermine traditional enforcement mechanisms and create substantial challenges for investigative agencies.

LITERATURE REVIEW

Global Perspective

The global regulatory discourse on money laundering through digital assets has been significantly shaped by the Financial Action Task Force (FATF), which introduced comprehensive recommendations concerning Virtual Digital Assets (VDAs) and Virtual Asset Service Providers (VASPs). These recommendations emphasise the "travel rule," customer due diligence, and risk-based supervision to ensure transparency in digital transactions.[5]
The FATF framework reflects a shift from traditional financial surveillance to technologically adaptive regulatory mechanisms capable of addressing the anonymity and decentralisation inherent in cryptocurrencies.[6]

[1] Id. at 52.
[2] Nikolei M. Kaplanov, "Nerdy Money: Bitcoin, the Private Digital Currency, and the Case against Its Regulation" 25 Loyola Consumer Law Review 111 (2012).
[3] The Prevention of Money Laundering Act, 2002 (Act 15 of 2003); The Information Technology Act, 2000 (Act 21 of 2000).
[4] Arner Douglas W., Janos Nathan Barberis and Ross P. Buckley, "FinTech, RegTech and the Reconceptualization of Financial Regulation" 37 Northwestern Journal of International Law & Business 371 (2017).
[5] Financial Action Task Force, "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers" (2019).
[6] Id. at 15.

In the European Union, the regulatory framework has evolved through directives such as the Fifth Anti-Money Laundering Directive (AMLD5), which explicitly includes cryptocurrency exchanges and custodian wallet providers within its ambit.[1] The proposed Markets in Crypto-Assets Regulation (MiCA) further strengthens compliance obligations, aiming to harmonise crypto regulation across member states.[2] Similarly, the United States adopts a fragmented yet robust approach, where agencies like the Financial Crimes Enforcement Network (FinCEN) treat virtual currencies as "money services businesses," thereby subjecting them to anti-money laundering (AML) compliance requirements.[3] Judicial and administrative interpretations in the U.S. have reinforced the applicability of existing financial laws to digital assets, though regulatory overlaps persist.[4]
Scholarly literature highlights that while these jurisdictions have made significant strides in regulating digital assets, challenges remain in enforcing cross-border compliance due to jurisdictional inconsistencies and technological complexities.[5] The global experience underscores the necessity of clear definitions, coordinated enforcement, and international cooperation to effectively combat money laundering through cryptocurrencies.

Indian Scholarship

Indian legal scholarship reflects an evolving yet fragmented understanding of cryptocurrencies and their regulation. One of the most significant concerns identified is the absence of a clear statutory definition of cryptocurrency within the Indian legal framework.[6] While the Reserve Bank of India initially imposed restrictions on virtual currencies, the Supreme Court in *Internet and Mobile Association of India v. Reserve Bank of India* invalidated the circular, thereby reopening the space for crypto transactions.[7]
Subsequently, the regulatory landscape witnessed a significant shift with the extension of the Prevention of Money Laundering Act, 2002 to include Virtual Digital Assets.[8] This brought crypto exchanges and related entities within the ambit of AML obligations such as record maintenance, reporting of suspicious transactions, and verification of client identity.[9] Scholars have analysed this move as a step towards regulatory recognition; however, they argue that the absence of a comprehensive legislative framework continues to create uncertainty.[10]
Academic discussions further point out that Indian enforcement agencies face considerable challenges due to the pseudonymous nature of blockchain transactions and the lack of technical expertise.[11] Moreover, the reliance on executive notifications rather than parliamentary enactments has been criticised for undermining legal certainty and accountability.[12] The interplay between taxation policies on cryptocurrencies and their regulatory treatment under PMLA has also been a subject of scholarly debate.[13]

Identified Gaps in Literature

Despite the growing body of literature on cryptocurrencies and money laundering, several critical gaps remain. A major limitation is the lack of victim-oriented studies that examine the impact of crypto-related financial crimes on individuals and institutions.[14] Most research focuses on regulatory frameworks and compliance mechanisms, often neglecting the human dimension of such offences.
Additionally, there is a notable scarcity of enforcement-based empirical studies that evaluate the effectiveness of existing AML measures in the context of digital assets.[15] The absence of reliable data on investigations, prosecutions, and convictions under the PMLA involving cryptocurrencies further limits the scope of

[1] Directive (EU) 2018/843 of the European Parliament and of the Council (5th Anti-Money Laundering Directive).
[2] European Commission, "Proposal for a Regulation on Markets in Crypto-assets (MiCA)" (2020).
[3] Financial Crimes Enforcement Network, "Application of FinCEN's Regulations to Virtual Currencies" (2013).
[4] Id.
[5] Angela Walch, "The Path of the Blockchain Lexicon" 36 Review of Banking & Financial Law 713 (2017).
[6] Nishith Desai Associates, "Regulating Cryptocurrency in India: Issues and Challenges" (2018).
[7] *Internet and Mobile Association of India v. Reserve Bank of India*, (2020) 10 SCC 274.
[8] The Prevention of Money Laundering Act, 2002 (Act 15 of 2003), Notification dated March 7, 2023.
[9] Id., s. 12.
[10] Arjun Kumar, "Cryptocurrency Regulation in India: A Legal Analysis" 12 Indian Journal of Law and Technology 45 (2021).
[11] Raghav Sharma, "Money Laundering through Cryptocurrencies: Challenges for India" 8 NLUJ Law Review 112 (2022).
[12] Id. at 120.
[13] Surbhi Bansal, "Taxation of Virtual Digital Assets in India" 14 NUJS Law Review 89 (2022).
[14] Kshetri Nir, "Blockchain's Roles in Strengthening Cybersecurity and Protecting Privacy" 15 Telecommunications Policy 102 (2017).
[15] Id.

meaningful analysis.[1] This lack of empirical grounding weakens policy recommendations and hinders the development of evidence-based regulatory strategies.

A central issue emerging from the literature is that the absence of a clear and uniform definition of cryptocurrency creates regulatory ambiguity, leading to inconsistent enforcement practices.[2] This ambiguity affects not only regulatory agencies but also market participants, who operate in an uncertain legal environment. Consequently, the existing scholarship indicates that while India has taken initial steps towards regulating digital assets, a comprehensive and coherent legal framework is essential to address the challenges of money laundering in the digital age.[3]

CONCEPTUAL FRAMEWORK: MONEY LAUNDERING VIA CRYPTO

Mechanisms of Crypto Laundering

Money laundering through cryptocurrencies operates through technologically advanced mechanisms that obscure the origin and movement of illicit funds. One of the most commonly used methods is the use of crypto mixers or tumblers, which pool together cryptocurrencies from multiple users and redistribute them in a manner that breaks the transactional trail, making tracing extremely difficult.[4] These services significantly undermine regulatory efforts aimed at tracking illicit financial flows.

Another prominent mechanism involves the use of privacy-centric cryptocurrencies such as Monero and ZCash, which incorporate advanced cryptographic techniques like ring signatures and zero-knowledge proofs to conceal transaction details, including sender, receiver, and transaction amounts.[5] This enhanced anonymity makes such assets particularly attractive for criminal activities.

Layering, a critical stage of money laundering, is also facilitated through the use of multiple digital wallets. Criminals frequently transfer funds across numerous wallets, exchanges, and jurisdictions to create complex transaction chains that are difficult for enforcement agencies to decode.[6] This digital layering mirrors traditional laundering techniques but is far more efficient due to the global and instantaneous nature of blockchain transactions.

Methods Used by Criminals

Criminals increasingly exploit the dark web to conduct illicit transactions using cryptocurrencies. The dark web provides an anonymous marketplace for illegal goods and services, where cryptocurrencies act as the primary medium of exchange due to their pseudonymous nature.[7]

Another emerging method is NFT-based laundering, where non-fungible tokens are used to artificially inflate asset values. Criminals may buy and sell NFTs among themselves at exaggerated prices to legitimise illicit funds, thereby creating a façade of lawful transactions.[8] This method exploits the lack of valuation standards and regulatory oversight in NFT markets.

Additionally, cryptocurrencies are often converted into real-world assets such as real estate, luxury goods, or fiat currency through exchanges.[9] This conversion completes the integration phase of laundering, allowing illicit funds to re-enter the legitimate economy. The involvement of unregulated or weakly regulated exchanges further exacerbates enforcement challenges.

Key Features Enabling Laundering

Certain inherent features of cryptocurrencies make them particularly susceptible to misuse for money laundering. Anonymity or pseudonymity is one of the most significant factors, as users can transact without revealing their real identities, thereby complicating investigative processes.[10]

---

[1] Enforcement Directorate, "Annual Report 2022–23" (Government of India, 2023).
[2] Supra note 8.
[3] Supra note 1.
[4] Financial Action Task Force, "Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing" (2020).
[5] Paul Vigna and Michael J. Casey, *The Age of Cryptocurrency* 215 (St. Martin's Press, New York, 2015).
[6] Andreas M. Antonopoulos, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies* 180 (O'Reilly Media, California, 2017).
[7] UN Office on Drugs and Crime, "Darknet Cybercrime Threats to Southeast Asia" (2021).
[8] Nadini Srivastava, "NFTs and Money Laundering: Emerging Legal Concerns" 12 Indian Journal of Law and Technology 45 (2022).
[9] Reserve Bank of India, "Report on Trend and Progress of Banking in India" 132 (2022).
[10] Financial Action Task Force, "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers" (2019).

ISSN 2394 - 7780

Decentralization further intensifies this challenge, as cryptocurrencies operate without a central authority or intermediary, limiting the scope of regulatory oversight and control.[1] This absence of centralized governance structures makes enforcement fragmented and jurisdictionally complex.
Moreover, the speed and global reach of cryptocurrency transactions enable rapid movement of funds across borders, often bypassing traditional financial monitoring systems.[2] These characteristics allow criminals to exploit regulatory gaps and jurisdictional inconsistencies effectively.

LEGAL FRAMEWORK IN INDIA

Prevention of Money Laundering Act (PMLA), 2002

The Prevention of Money Laundering Act, 2002 (PMLA) constitutes the primary legislative framework in India to combat money laundering, including offences arising from digital assets and cryptocurrencies.[3] The Act aims to prevent the process of disguising proceeds of crime as untainted property and provides for attachment, adjudication, and confiscation of such assets.[4] Its scope extends to offences listed under the Schedule to the Act, thereby linking money laundering with predicate offences.[5]
A significant development in the context of digital assets is the inclusion of Virtual Digital Assets (VDAs) within the regulatory ambit of the PMLA through a 2023 notification issued by the Ministry of Finance.[6] This notification brought crypto exchanges, wallet providers, and intermediaries under the definition of "reporting entities," thereby mandating compliance with anti-money laundering (AML) obligations such as customer due diligence, record maintenance, and reporting of suspicious transactions.[7] The inclusion marks a shift towards formal recognition of cryptocurrencies as potential instruments of financial crime.
The Financial Intelligence Unit–India (FIU-IND) plays a pivotal role in implementing the PMLA framework by collecting, analysing, and disseminating financial intelligence related to suspicious transactions.[8] It acts as the central national agency responsible for coordinating AML efforts and ensuring compliance by reporting entities.[9] However, the decentralised and pseudonymous nature of cryptocurrencies poses challenges in effective monitoring and tracing of illicit transactions, thereby exposing enforcement limitations.

Other Relevant Laws

Apart from the PMLA, several other statutes contribute to regulating digital financial crimes in India. The Information Technology Act, 2000 provides the legal framework for addressing cyber offences, including hacking, identity theft, and data breaches, which often facilitate cryptocurrency-related crimes.[10] Provisions such as Section 66 (computer-related offences) and Section 43 (damage to computer systems) are frequently invoked in cases involving digital asset fraud.[11]
The Bharatiya Nyaya Sanhita (BNS), which replaces the Indian Penal Code, also plays a role in addressing offences such as cheating, criminal breach of trust, and fraud committed through digital platforms.[12] While not specifically tailored to cryptocurrencies, its provisions are applicable in prosecuting underlying criminal conduct linked to money laundering.
Further, the Foreign Exchange Management Act, 1999 (FEMA) regulates cross-border transactions and foreign exchange dealings, which are highly relevant in the context of cryptocurrencies due to their global and borderless nature.[13] The absence of clear classification of cryptocurrencies under FEMA creates ambiguity in regulating cross-border crypto transactions, thereby contributing to regulatory gaps.[14]

[1] Chris Brummer, *Cryptoassets: The Innovative Investor's Guide to Bitcoin and Beyond* 97 (Yale University Press, New Haven, 2019).
[2] Basel Institute on Governance, "Cryptocurrencies and Money Laundering" (2019).
[3] The Prevention of Money Laundering Act, 2002 (Act 15 of 2003).
[4] Id., s. 3.
[5] Id., sch.
[6] Ministry of Finance, "Notification S.O. 1072(E)" (March 7, 2023).
[7] Id.
[8] Financial Intelligence Unit–India, "Functions of FIU-IND" available at: https://fiuindia.gov.in (last visited on March 17, 2026).
[9] Id.
[10] The Information Technology Act, 2000 (Act 21 of 2000).
[11] Id., ss. 43, 66.
[12] The Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023).
[13] The Foreign Exchange Management Act, 1999 (Act 42 of 1999).
[14] Id.

ISSN 2394 - 7780

Regulatory Authorities

The regulatory landscape governing cryptocurrencies in India involves multiple authorities, each with overlapping and sometimes unclear jurisdictions. The Reserve Bank of India (RBI), as the central banking authority, has consistently expressed concerns regarding financial stability, consumer protection, and systemic risks associated with cryptocurrencies.[1] Although the RBI had earlier imposed a banking ban on crypto transactions, it was later set aside by the Supreme Court.[2]

The Securities and Exchange Board of India (SEBI) has an uncertain role in regulating cryptocurrencies, particularly due to ambiguity regarding whether such assets qualify as "securities."[3] This lack of clarity has led to regulatory fragmentation and jurisdictional overlap.

The Enforcement Directorate (ED) serves as the primary enforcement agency under the PMLA, empowered to investigate offences, attach properties, and initiate prosecution.[4] In recent years, the ED has actively pursued cases involving cryptocurrency exchanges and digital asset transactions linked to money laundering activities.[5] However, enforcement challenges persist due to technological complexities, anonymity, and lack of international cooperation mechanisms.

Judicial Developments

Judicial intervention has played a crucial role in shaping the regulatory framework governing cryptocurrencies in India. In *Internet and Mobile Association of India v. Reserve Bank of India*, the Supreme Court struck down the RBI circular prohibiting banks from dealing with cryptocurrency exchanges, holding it to be disproportionate and violative of Article 19(1)(g) of the Constitution.[6] This landmark judgment recognised the legitimacy of cryptocurrency trade while emphasising the need for a balanced regulatory approach.

The decision highlighted the absence of legislative prohibition on cryptocurrencies and underscored the importance of proportionality in regulatory actions.[7] However, it also left unresolved questions regarding comprehensive regulation, thereby placing the onus on the legislature to formulate a clear legal framework.

REGULATORY GAPS IN INDIA

Absence of Comprehensive Crypto Legislation

India presently lacks a unified and comprehensive statutory framework specifically governing cryptocurrencies and digital assets. While regulatory bodies such as the Reserve Bank of India (RBI) and the Securities and Exchange Board of India (SEBI) have intermittently issued circulars and advisories, there is no dedicated legislation that clearly defines the legal status, classification, and regulatory treatment of cryptocurrencies.[8] This regulatory vacuum creates ambiguity regarding whether such assets are to be treated as commodities, securities, or virtual digital assets (VDAs), thereby complicating enforcement under anti-money laundering laws.

The inclusion of virtual digital assets within the ambit of the Prevention of Money Laundering Act, 2002 (PMLA) through subsequent notifications represents a step towards regulation; however, it remains fragmented and reactive rather than comprehensive.[9] In the absence of a clear legislative framework, enforcement agencies face interpretational challenges, particularly in linking digital assets to predicate offences and establishing culpability.[10] Consequently, the lack of a codified regulatory regime undermines both investor protection and effective anti-money laundering enforcement.

Weak KYC/AML Compliance

Another significant regulatory gap lies in the inconsistent implementation of Know Your Customer (KYC) and Anti-Money Laundering (AML) standards across cryptocurrency exchanges. While domestic exchanges have

[1] Reserve Bank of India, "Statement on Developmental and Regulatory Policies" (April 6, 2018).
[2] *Internet and Mobile Association of India v. Reserve Bank of India*, (2020) 10 SCC 274.
[3] Securities and Exchange Board of India Act, 1992 (Act 15 of 1992).
[4] The Prevention of Money Laundering Act, 2002 (Act 15 of 2003), ss. 48, 49.
[5] Directorate of Enforcement, "Annual Report 2022-23" (2023).
[6] *Internet and Mobile Association of India v. Reserve Bank of India*, (2020) 10 SCC 274.
[7] Id.
[8] Reserve Bank of India, "Statement on Developmental and Regulatory Policies" (Apr. 6, 2018).
[9] Ministry of Finance, "Notification Bringing Virtual Digital Assets under PMLA" (Mar. 7, 2023).
[10] The Prevention of Money Laundering Act, 2002 (Act 15 of 2003).

ISSN 2394 - 7780

increasingly adopted KYC norms in compliance with PMLA obligations, several offshore platforms continue to operate without stringent verification mechanisms.[1] This enables users to bypass domestic regulatory scrutiny by transacting through foreign exchanges that do not adhere to Indian compliance standards.

Furthermore, peer-to-peer (P2P) transactions and decentralized platforms often operate outside the purview of traditional regulatory oversight, making it difficult to trace the identity of transacting parties.[2] The absence of uniform global standards and the lack of coordinated enforcement mechanisms exacerbate these challenges. Reports have indicated that non-compliant exchanges serve as conduits for laundering illicit funds, thereby weakening the overall AML framework.[3]

Jurisdictional Challenges

The inherently borderless nature of cryptocurrencies poses serious jurisdictional challenges for Indian enforcement agencies. Transactions conducted on blockchain networks transcend national boundaries, often involving multiple jurisdictions with varying regulatory standards.[4] This creates difficulties in investigation, evidence collection, and prosecution of offenders involved in cross-border money laundering activities.

Extradition of offenders engaged in cryptocurrency-related crimes further complicates enforcement. Differences in legal frameworks, absence of bilateral treaties, and the lack of recognition of cryptocurrency offences in certain jurisdictions hinder cooperation.[5] Additionally, obtaining data from foreign exchanges often requires navigating complex mutual legal assistance procedures, which are time-consuming and inefficient.[6]

The decentralized architecture of blockchain technology further limits the ability of authorities to assert territorial jurisdiction, thereby creating enforcement lacunae.[7] As a result, jurisdictional ambiguities significantly impede the effective regulation of cryptocurrency-based money laundering.

Technological Loopholes

Technological advancements within the cryptocurrency ecosystem have introduced sophisticated methods for concealing illicit transactions. Tools such as cryptocurrency mixers and tumblers enable users to obfuscate transaction trails by pooling and redistributing digital assets, thereby making tracing extremely difficult.[8] Similarly, the use of Virtual Private Networks (VPNs) allows users to mask their geographical location, thereby evading jurisdiction-specific regulations.[9]

Decentralized exchanges (DEXs), which operate without a central intermediary, further complicate regulatory oversight. These platforms facilitate anonymous trading and do not require users to undergo KYC verification, thereby providing an avenue for laundering illicit funds.[10] Privacy-focused cryptocurrencies such as Monero and Zcash also enhance anonymity by concealing transaction details, posing additional challenges for enforcement agencies.[11]

The rapid pace of technological innovation often outstrips regulatory responses, resulting in a persistent gap between emerging risks and existing legal frameworks.[12] Consequently, enforcement agencies struggle to adapt to evolving laundering techniques within the digital asset ecosystem.

Regulatory Arbitrage

Regulatory arbitrage constitutes another major challenge in the regulation of cryptocurrencies in India. In the absence of uniform global regulations, users and service providers often migrate to jurisdictions with lenient or

[1] Financial Action Task Force, "Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing" (2020).
[2] Id.
[3] Chainalysis, "Crypto Crime Report" (2023).
[4] Financial Action Task Force, "Guidance for a Risk-Based Approach to Virtual Assets and VASPs" (2019).
[5] United Nations Office on Drugs and Crime, "Manual on International Cooperation for the Purposes of Confiscation of Proceeds of Crime" (2012).
[6] Id.
[7] Arner Douglas W., Barberis Janos, et.al., "FinTech and RegTech: Impact on Regulators and Banks" 19 Journal of Banking Regulation 1 (2017).
[8] Financial Action Task Force, supra note 4.
[9] Id.
[10] Angela Walch, "Deconstructing 'Decentralization': Exploring the Core Claim of Crypto Systems" 55 Harvard Journal of Law & Technology 1 (2019).
[11] Paul Vigna and Michael J. Casey, The Age of Cryptocurrency 112 (St. Martin's Press, New York, 2015).
[12] Chris Brummer, Cryptoassets: Legal, Regulatory, and Monetary Perspectives 89 (Oxford University Press, Oxford, 2019).

ISSN 2394 - 7780

non-existent regulatory frameworks to avoid compliance obligations.[1] This practice undermines domestic regulatory efforts and creates an uneven playing field for compliant entities.

Indian users frequently access offshore exchanges that offer greater anonymity and fewer restrictions, thereby circumventing domestic KYC and AML requirements.[2] This not only facilitates money laundering but also exposes users to risks such as fraud, hacking, and lack of legal recourse.[3]

Moreover, regulatory uncertainty within India further incentivises such behaviour, as businesses and investors seek stable and predictable regulatory environments.[4] The absence of harmonised international standards and coordinated enforcement mechanisms exacerbates the problem of regulatory arbitrage.[5]

In sum, the regulatory gaps in India's approach to cryptocurrencies—ranging from legislative ambiguity and weak compliance mechanisms to jurisdictional and technological challenges—significantly hinder the effective prevention of money laundering. Addressing these gaps requires a comprehensive legal framework, strengthened enforcement capabilities, and enhanced international cooperation.[6]

ENFORCEMENT CHALLENGES

Investigation Challenges

The rapid rise of digital assets and cryptocurrencies has posed significant challenges to traditional investigative frameworks in India. One of the foremost issues is the lack of technical expertise among law enforcement agencies. Investigating cryptocurrency transactions requires specialized knowledge of blockchain technology, cryptographic protocols, and digital wallets—skills that are not yet widespread within enforcement bodies such as the Directorate of Enforcement (ED) and local police authorities.[7]

Additionally, blockchain tracing presents inherent complexities. While blockchain transactions are publicly recorded, they are pseudonymous, making it difficult to identify the real individuals behind wallet addresses.[8] Techniques such as mixing services, tumblers, and privacy coins further obscure transaction trails, complicating efforts to trace illicit funds.[9] This technological opacity often delays investigations and reduces the effectiveness of enforcement mechanisms under existing laws such as the Prevention of Money Laundering Act, 2002 (PMLA).[10]

Low Conviction Rates

Another critical challenge is the notably low conviction rate in money laundering cases involving digital assets. Despite an increase in enforcement actions, successful prosecutions remain limited, indicating systemic inefficiencies in investigation and evidence collection.[11] The complexity of proving the linkage between digital assets and predicate offences further burdens prosecution agencies.[12]

The stringent evidentiary requirements under the PMLA, coupled with the technical nature of cryptocurrency transactions, often result in weak cases before courts.[13] Moreover, delays in forensic analysis and lack of standardized investigative protocols contribute to prolonged trials and eventual acquittals.[14] These low conviction rates highlight a gap between enforcement activity and judicial outcomes, raising concerns about the effectiveness of India's anti-money laundering framework.[15]

Institutional Constraints

[1] Financial Stability Board, "Regulation, Supervision and Oversight of Crypto-Asset Activities" (2022).
[2] Id.
[3] Chainalysis, supra note 6.
[4] Nischal Shetty, "India's Crypto Industry and Regulatory Uncertainty" Economic Times, Feb. 15, 2022.
[5] Financial Action Task Force, supra note 7.
[6] Ministry of Finance, "Report of the Committee on Virtual Currencies" (2019).
[7] Financial Action Task Force, "Virtual Assets and Virtual Asset Service Providers" (2019).
[8] Andreas M. Antonopoulos, Mastering Bitcoin 45 (O'Reilly Media, California, 2nd edn., 2017).
[9] Id. at 50.
[10] The Prevention of Money Laundering Act, 2002 (Act 15 of 2003).
[11] Enforcement Directorate, "Annual Report 2022-23" (2023).
[12] Id. at 45.
[13] The Prevention of Money Laundering Act, 2002 (Act 15 of 2003), ss. 3, 24.
[14] K.C. Mishra, "Money Laundering and Challenges in India" 12 Journal of Financial Crime 210 (2021).
[15] Id. at 215.

ISSN 2394 - 7780

Institutional limitations further aggravate enforcement challenges. Multiple agencies, including the ED, Financial Intelligence Unit (FIU-IND), Reserve Bank of India (RBI), and state police authorities, operate within overlapping jurisdictions, often leading to coordination issues.[1] The absence of a unified regulatory framework for cryptocurrencies exacerbates this fragmentation.[2]

Inter-agency communication gaps and bureaucratic delays hinder timely information sharing, which is crucial in cases involving rapidly moving digital assets.[3] Moreover, regulatory uncertainty regarding the legal status of cryptocurrencies in India has created ambiguity in enforcement priorities and strategies.[4] This lack of clarity undermines institutional efficiency and weakens the overall enforcement ecosystem.[5]

Cross-Border Enforcement Issues

Cryptocurrency transactions are inherently borderless, posing serious challenges to jurisdiction and enforcement. Investigations often require cooperation from foreign jurisdictions, especially when exchanges or wallets are located outside India.[6] However, the process of obtaining information through Mutual Legal Assistance Treaties (MLATs) is often time-consuming and inefficient.[7]

Delays in MLAT responses can result in the dissipation of digital assets, as cryptocurrencies can be transferred across multiple jurisdictions within seconds.[8] Furthermore, differences in regulatory approaches across countries complicate enforcement efforts, as some jurisdictions may not recognise certain crypto-related offences.[9] These cross-border challenges significantly limit the ability of Indian authorities to effectively investigate and prosecute money laundering cases involving digital assets.[10]

Practical Case Examples

Recent enforcement actions in India demonstrate the growing misuse of cryptocurrencies in financial crimes. The Directorate of Enforcement has conducted several raids and seizures involving crypto assets linked to frauds, scams, and illegal betting operations.[11] In multiple cases, digital assets were found to be used as a medium for laundering proceeds of crime due to their anonymity and ease of transfer.[12]

For instance, investigations into online fraud schemes have revealed the conversion of illicit funds into cryptocurrencies to evade detection.[13] Similarly, ED actions against certain crypto exchanges have highlighted non-compliance with anti-money laundering norms and inadequate Know Your Customer (KYC) procedures.[14] These enforcement measures underscore the increasing role of digital assets in financial crimes and the urgent need for robust regulatory and investigative mechanisms.[15]

Overall, while enforcement agencies in India have intensified their actions against cryptocurrency-related money laundering, significant structural, technical, and legal challenges persist. Addressing these issues requires capacity building, improved inter-agency coordination, and enhanced international cooperation to ensure effective enforcement of anti-money laundering laws in the digital age.[16]

COMPARATIVE ANALYSIS

USA

The United States has developed one of the most stringent anti-money laundering (AML) frameworks in relation to digital assets and cryptocurrencies. The regulatory approach is characterised by strict compliance requirements imposed under the Bank Secrecy Act (BSA), which has been extended to cover virtual asset

[1] Reserve Bank of India, "Report on Trend and Progress of Banking in India" (2022).
[2] Nirmala Sitharaman, "Cryptocurrency and Regulation in India" The Hindu, Feb. 2, 2022.
[3] Government of India, "Report of the Committee on Virtual Currencies" (2019).
[4] Id.
[5] S. Sahoo, "Regulating Cryptocurrencies in India" 3 Indian Journal of Law and Technology 55 (2020).
[6] Financial Action Task Force, "International Standards on Combating Money Laundering" (2012).
[7] Government of India, "Mutual Legal Assistance Treaties: A Guide" (Ministry of Home Affairs, 2020).
[8] FATF, Supra note 1 at 30.
[9] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (2008).
[10] Id.
[11] Enforcement Directorate, Press Release, "ED Attaches Cryptocurrency Assets in Fraud Case" (2023).
[12] Id.
[13] R. Sharma, "Crypto Frauds and Money Laundering in India" The Economic Times, Aug. 10, 2023.
[14] Enforcement Directorate, Press Release, "Action against Crypto Exchanges for AML Violations" (2022).
[15] Id.
[16] FATF, Supra note 1.

ISSN 2394 - 7780

service providers (VASPs), including cryptocurrency exchanges.[1] The Financial Crimes Enforcement Network (FinCEN) treats such entities as "money services businesses," thereby mandating registration, reporting obligations, and implementation of Know Your Customer (KYC) norms.[2]
Further, the USA adopts a multi-agency regulatory structure wherein agencies such as the Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC) exercise jurisdiction depending upon the nature of the crypto asset.[3] Enforcement has been particularly robust, with authorities actively prosecuting violations relating to illicit transactions and non-compliance with AML norms. This strict approach ensures a higher degree of transparency but has also been criticised for regulatory overlap and uncertainty.

European Union
The European Union has taken a harmonised and forward-looking approach through the introduction of the Markets in Crypto-Assets (MiCA) Regulation, aimed at creating a uniform regulatory framework across member states. MiCA establishes comprehensive rules governing issuance, trading, and supervision of crypto-assets, along with strict AML compliance requirements.[4]
In addition, the EU's AML Directives have progressively incorporated virtual currencies within their scope, requiring enhanced due diligence and reporting obligations. The focus is on balancing innovation with financial stability and consumer protection. The establishment of a single regulatory framework under MiCA reduces fragmentation and ensures legal certainty, which is particularly significant in cross-border transactions involving digital assets.

Lessons for India
A comparative analysis of the USA and EU frameworks highlights critical lessons for India. First, there is a pressing need for a centralised regulatory authority to oversee cryptocurrency transactions and enforce AML compliance. Currently, India's regulatory framework remains fragmented, with overlapping jurisdiction between different authorities such as the Reserve Bank of India and the Enforcement Directorate.
Second, India must adopt a robust compliance framework akin to the USA model, ensuring mandatory registration, KYC norms, and reporting obligations for all virtual asset service providers. Finally, the EU's MiCA model underscores the importance of a unified and codified regulatory regime, which can reduce ambiguity and promote investor confidence.[5]
Therefore, India must strike a balance between regulatory oversight and technological innovation by adopting a comprehensive legal framework that addresses existing gaps while ensuring effective enforcement against money laundering through digital assets.

ROLE OF TECHNOLOGY IN ENFORCEMENT
Technological advancements have become indispensable in combating money laundering through digital assets and cryptocurrencies. Given the pseudonymous and decentralised nature of blockchain-based transactions, traditional enforcement mechanisms are often inadequate. Consequently, enforcement agencies increasingly rely on technological tools to trace, analyse, and detect illicit financial flows.

Blockchain Forensics
Blockchain forensics refers to the use of specialised tools and techniques to analyse blockchain transactions and identify suspicious patterns. Contrary to popular belief, blockchain transactions are not entirely anonymous but are recorded on a public ledger, enabling transaction tracing.[6] Tools such as chain analysis software assist agencies in linking wallet addresses to real-world identities, thereby facilitating investigation and prosecution.
These tools enable authorities to trace the movement of illicit funds across multiple wallets and exchanges, even when layered through complex transactions. However, challenges remain due to the use of privacy coins, mixers, and decentralised exchanges, which obscure transaction trails and hinder effective enforcement.[7]

[1] The Bank Secrecy Act, 1970 (United States), s. 5311.
[2] Financial Crimes Enforcement Network, "Application of FinCEN's Regulations to Virtual Currencies" (2013).
[3] Regulation (EU) 2023/1114 on Markets in Crypto-assets (MiCA).
[4] Id., arts. 5, 6.
[5] Reserve Bank of India, "Statement on Developmental and Regulatory Policies" (2022).
[6] The Prevention of Money Laundering Act, 2002 (Act 15 of 2003).
[7] Financial Action Task Force, "Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing" (2020).

ISSN 2394 - 7780

AI & Machine Learning

Artificial Intelligence (AI) and Machine Learning (ML) play a crucial role in detecting suspicious transactions by analysing vast volumes of financial data in real time. These technologies identify anomalies, behavioural patterns, and high-risk transactions that may indicate money laundering activities. Financial institutions increasingly deploy AI-driven systems to strengthen their Anti-Money Laundering (AML) compliance frameworks.[1]

Advanced analytics significantly enhance the efficiency and accuracy of AML detection mechanisms. However, their effectiveness is constrained by limitations such as inadequate data availability, lack of standardisation, and regulatory uncertainty in the crypto ecosystem. Moreover, the dynamic nature of digital assets requires continuous adaptation of algorithms to address evolving laundering techniques.

CONCLUSION

Cryptocurrencies represent a transformative innovation in the global financial ecosystem, offering efficiency, transparency, and decentralisation. However, they also pose significant challenges, particularly in the context of money laundering and financial crimes. The dual nature of digital assets makes them a "double-edged sword," capable of fostering innovation while simultaneously facilitating illicit activities.

The absence of a comprehensive regulatory framework in India has created substantial gaps in enforcement, allowing misuse of cryptocurrencies for laundering proceeds of crime. The decentralised and borderless nature of digital assets further exacerbates these challenges, making traditional regulatory approaches inadequate.

Judicial and regulatory responses in India have been evolving, but they remain fragmented and reactive rather than proactive. The lack of clarity in legal definitions and enforcement mechanisms contributes to uncertainty and undermines the effectiveness of Anti-Money Laundering measures.

A balanced approach is therefore essential—one that promotes technological innovation while ensuring robust regulatory oversight. Strengthening AML frameworks, enhancing institutional capacity, and integrating advanced technological tools are critical steps in achieving this balance.

Looking ahead, India has the opportunity to emerge as a global leader in crypto regulation by adopting a forward-looking and comprehensive approach. By aligning with international standards and leveraging technological advancements, India can effectively mitigate risks associated with digital assets while fostering a secure and innovative financial ecosystem.

References

1. The Prevention of Money Laundering Act, 2002 (Act 15 of 2003).
2. The Constitution of India.
3. Andreas M. Antonopoulos, *Mastering Bitcoin* (O'Reilly Media, California, 2nd edn., 2017).
4. Financial Action Task Force, "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers" (2019).
5. Financial Action Task Force, "Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing" (2020).
6. Reserve Bank of India, "Master Direction – Know Your Customer (KYC) Direction, 2016" (updated 2023).
7. Reserve Bank of India v. Internet and Mobile Association of India, (2020) 10 SCC 274.
8. United Nations Office on Drugs and Crime, "Cryptocurrencies and Money Laundering" (2017).
9. Arner Douglas, Janos Barberis and Ross Buckley, "The Evolution of Fintech" 47 Georgetown Journal of International Law 1271 (2016).
10. Arner Douglas, Janos Barberis and Ross Buckley, "Fintech and RegTech in a Nutshell" 21 Journal of Banking Regulation 1 (2017).

[1] Arner Douglas, Janos Barberis and Ross Buckley, "The Evolution of Fintech: A New Post-Crisis Paradigm" 47 Georgetown Journal of International Law 1271 (2016)."