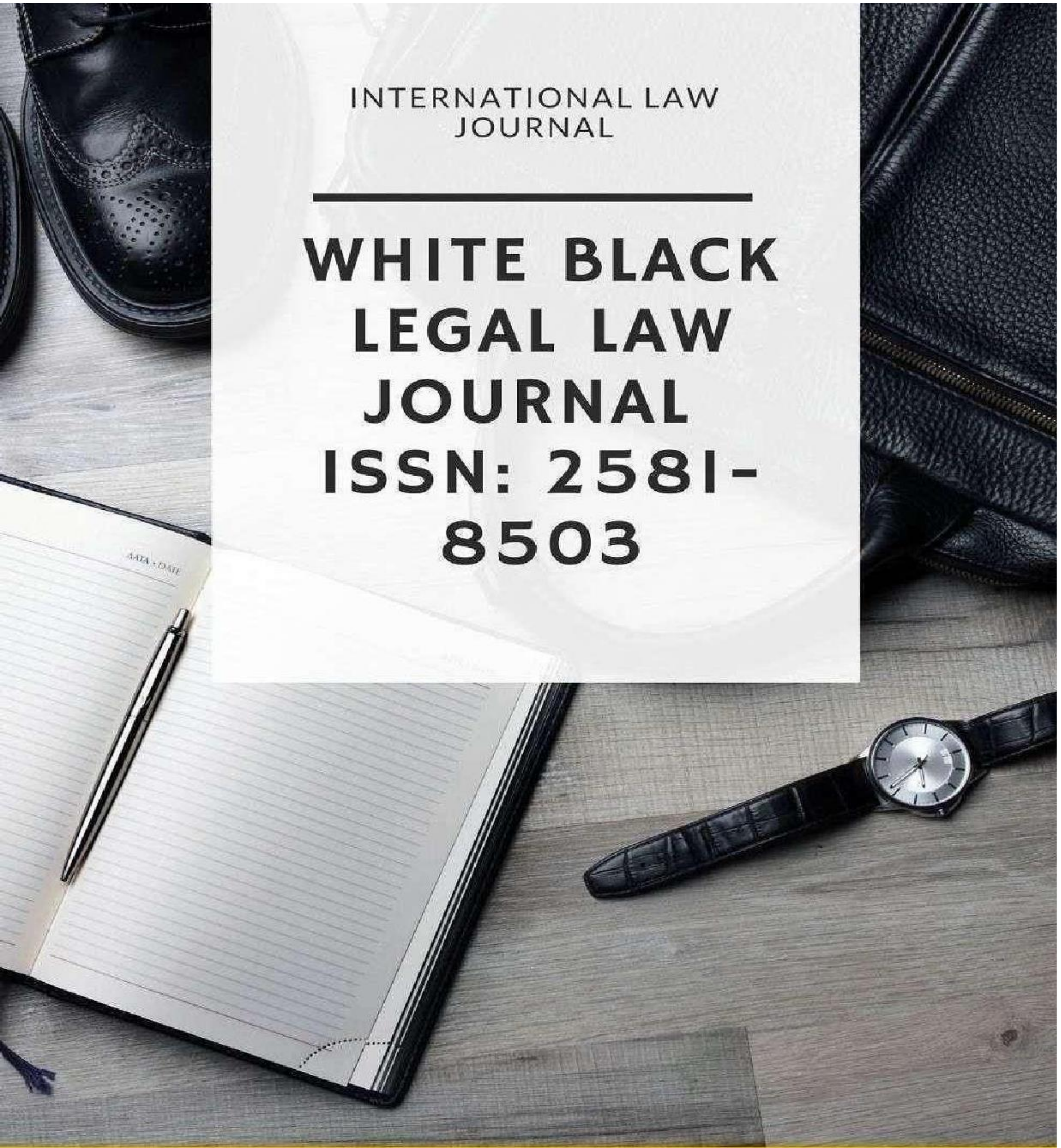
INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503



Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

 ISSN: 2581-8503

INDIA'S LEGAL RESPONSE TO CRYPTOCURRENCY FRAUD

AUTHORED BY - ADV ANOOP MAHOBIA
AFFILIATION - PRSU RAIPUR

Abstract

Cryptocurrency fraud reveals a fundamental flaw in legal systems which have always been built around identifiable intermediaries, territorial transactions and traditional forms of property. The case of India shows this issue clearly. Cryptocurrency activity is not banned in itself nor is it thoroughly regulated by a specific piece of legislation; rather, the legal approach is spread out over criminal law, cyber law, anti-money-laundering rules, taxation, securities regulation, foreign-exchange controls and administrative enforcement. This article critically looks at whether this scattered system is sufficient to prevent, investigate and deal with cryptocurrency fraud. Based on doctrinal legal analysis, case studies and comparative regulatory analysis, it examines the Bharatiya Nyaya Sanhita, 2023, the Information Technology Act, 2000, the Prevention of Money Laundering Act, 2002, the role of the Reserve Bank of India, SEBI, FIU-IND and the Enforcement Directorate, and the constitutional importance of the case Internet and Mobile Association of India v. Reserve Bank of India. It contends that the main issue is not a complete lack of law, but a misalignment between the risks posed by technology and the specific mandates of the institutions involved. The paper also compares the multi-agency enforcement model in the United States, the European Union's harmonised Markets in Crypto-Assets framework and Singapore's licensing and consumer-protection model. It suggests an Indian framework based on risk, featuring a specific digital-asset statute, activity-based licensing of virtual digital asset service providers, unified KYC/AML and travel-rule compliance, a specialised cyber-forensic capability, cross-border cooperation, mandatory cybersecurity and custody standards, and accessible investor redress. The article concludes that effective regulation should shift from the reactive practice of classifying crypto fraud into old legal categories to one of technology-neutral but crypto-aware governance.

Keywords: *Cryptocurrency fraud; Virtual Digital Assets; Bharatiya Nyaya Sanhita; PMLA; IT Act; FIU-IND; Investor Protection; MiCA; VASP; Blockchain Forensics*

1. Introduction

Money has repeatedly changed form in response to technology, social organisation and the needs of commerce. Cryptocurrency represents a particularly disruptive stage in that history because value can be transferred through distributed networks without the conventional intermediation of a central bank or financial institution. The architecture that makes crypto-assets attractive—pseudonymous addresses, decentralised validation, programmable transactions and borderless transferability—also creates new opportunities for fraud. The research manuscript on which this article is based identifies Ponzi schemes, phishing, fake initial coin offerings (ICOs), pump-and-dump manipulation, exchange hacks, rug pulls, money laundering and impersonation scams as recurring forms of abuse in the Indian ecosystem. The underlying problem is therefore not simply whether cryptocurrency is 'legal', but whether the legal system can identify actors, classify conduct, freeze or recover assets, preserve digital evidence, protect victims and allocate responsibility across multiple institutions.

The Indian position has developed through incremental and sometimes contradictory measures. The Reserve Bank of India (RBI) issued a 2018 circular directing regulated entities not to deal with or provide services to businesses dealing in virtual currencies. The Supreme Court subsequently struck down that circular in Internet and Mobile Association of India v. Reserve Bank of India, holding the restriction disproportionate under Article 19(1)(g). The judgment did not create a positive right to an unregulated crypto market; rather, it demonstrated the constitutional limits of a sweeping prohibition and left the legislative question open.

Since then, the regulatory centre of gravity has shifted toward risk containment. Crypto-assets became taxable as virtual digital assets (VDAs), VDA service providers were brought within the anti-money-laundering architecture in 2023, and FIU-IND has increasingly used registration and compliance mechanisms against offshore and domestic service providers. The current position is therefore better described as partial regulation without a comprehensive crypto statute. Importantly, the position has continued to evolve in 2026: the Income-tax Act, 2025 contains dedicated crypto-asset reporting architecture, while FIU-IND continues active enforcement against non-compliant VDA service providers.

This article advances a central proposition: India's problem is a regulatory patchwork rather than a complete legal vacuum. Existing laws can prosecute substantial portions of crypto fraud, but their effectiveness declines where the offence depends on anonymous developers, decentralised protocols, offshore service providers, smart-contract manipulation or rapid movement across multiple wallets and jurisdictions. The resulting gap is institutional as much as doctrinal.

2. Research Questions and Methodology

The article is guided by five questions: (i) how do decentralisation, pseudonymity, irreversibility and borderless transfer challenge the application of Indian criminal law; (ii) whether the BNS, IT Act and PMLA provide an adequate basis for investigation and prosecution; (iii) how institutional fragmentation among RBI, SEBI, FIU-IND, ED and police agencies affects enforcement; (iv) what lessons can be drawn from the United States, European Union and Singapore; and (v) what institutional and legislative reforms can provide investor protection without suppressing legitimate technological innovation?

The methodology is doctrinal and comparative. Primary legal materials include statutes, judicial decisions, regulatory instruments and official government materials. The underlying dissertation also uses case studies of major Indian cryptocurrency frauds, including GainBitcoin, Morris Coin, Bux Coin-related litigation and WazirX-related disputes. The comparative component examines the United States' SEC/FinCEN model, the European Union's Markets in Crypto-Assets Regulation (MiCA), and Singapore's Payment Services Act and related Monetary Authority of Singapore requirements. Because cryptocurrency law is unusually time-sensitive, this article updates the dissertation's 2025 position with official Indian materials available through 11 September 2026.

3. The Technology of Fraud: Why Cryptocurrency Creates a Distinct Legal Problem Decentralisation, pseudonymity and irreversibility

Cryptocurrency transactions are generally recorded on distributed ledgers rather than in a central institutional ledger. A wallet address may reveal the transaction history associated with that address without automatically revealing the natural or legal person controlling it. This is better understood as pseudonymity rather than perfect anonymity. That distinction is legally important: blockchain records may be highly useful as evidence, but the evidentiary bridge between a wallet and a human actor frequently requires exchange records, device evidence, communications, IP information, KYC material or other off-chain evidence.

The relative irreversibility of confirmed transactions creates a second problem. In ordinary payment systems, fraudulent transfers may sometimes be reversed, frozen or recalled through an intermediary. In a public blockchain, a victim who voluntarily transfers assets to a fraudster cannot ordinarily invoke a central operator to reverse the transaction. Legal remedies must therefore depend on identifying the beneficiary, freezing assets when they enter an identifiable service, tracing proceeds, obtaining judicial orders and cooperating with foreign authorities.

4. India's Existing Legal Architecture

4.1 Bharatiya Nyaya Sanhita, 2023

The BNS supplies the general criminal-law foundation for fraud. Section 318 addresses cheating and is relevant where deception induces a victim to part with property or act to his or her detriment. Section 314 addresses dishonest misappropriation of property, while Section 316 addresses criminal breach of trust. Section 111 on organised crime may become relevant where the factual and statutory requirements are satisfied in coordinated, serious criminal activity. These provisions are sufficiently technology-neutral to reach many crypto-fraud transactions.[1]
The difficulty is not that cheating suddenly ceases to be cheating because Bitcoin is used. The difficulty lies in attribution, proof of dishonest intention, the legal characterisation of the digital asset as property, and territorial jurisdiction. In a traditional fraud, investigators may identify the account holder, intermediary and place of transaction comparatively quickly. In a crypto scheme, the promoter may use pseudonymous wallets, overseas exchanges, mixers and decentralised protocols. Thus, the substantive offence may be straightforward while the evidentiary and jurisdictional pathway to the offender is not.

4.2 Information Technology Act, 2000

The IT Act remains important where the fraudulent conduct is technologically mediated. Sections 43 and 66 may apply to unauthorised access and dishonest or fraudulent acts involving computer resources; Section 66C addresses identity theft; and Section 66D addresses cheating by personation using computer resources. These provisions are particularly relevant to phishing, fake exchange interfaces, account takeover, credential theft and hacking of wallets or exchanges.[2]
Its limitation is historical design. The Act predates blockchain-based cryptocurrencies and therefore does not provide a comprehensive law of digital assets, decentralised autonomous

1Bharatiya Nyaya Sanhita 2023, ss 111, 314, 316, 318.
2Information Technology Act 2000, ss 43, 66, 66C, 66D.

organisations, smart-contract liability or crypto-asset custody. The law can often reach the cyber component of a crypto offence, but it does not necessarily regulate the underlying digital-asset business model. This creates a distinction between 'cybercrime involving crypto' and 'fraud inherent in a crypto product or market'.

4.3 Prevention of Money Laundering Act and FIU-IND

The PMLA is the most important example of India adapting an existing financial-crime statute to digital assets. The 2023 notification brought specified VDA activities within the reporting-entity architecture, including exchange between VDAs and fiat currency, exchange between different VDAs, transfer of VDAs, safekeeping or administration, and specified financial services connected with the issue or sale of VDAs. FIU-IND registration therefore provides a compliance gateway even in the absence of a comprehensive crypto licensing law.[3]

This development significantly changes the proposition that India has 'no regulation'. It has regulation, but it is principally activity-based AML/CFT regulation rather than a complete market-conduct and investor-protection regime. FIU-IND's continuing enforcement against offshore VDA service providers demonstrates that the regulatory perimeter is increasingly being asserted on the basis of activity and targeting of the Indian market rather than only physical presence.

The PMLA nevertheless has structural limits. Money laundering is ordinarily parasitic on proceeds of crime; it is not a substitute for a complete substantive law governing every form of crypto fraud. Further, tracing a blockchain transaction does not by itself prove who controlled the relevant wallet or establish the underlying scheduled offence. The effective model must therefore connect blockchain analytics, KYC records, device evidence, banking information and conventional criminal investigation.

4.4 Taxation and the emerging crypto-asset reporting architecture

Tax law has produced an important form of legal recognition without creating legal-tender status. The VDA framework introduced a 30% tax rate on income from transfers of VDAs, subject to the statutory rules, and a 1% TDS regime in specified circumstances. More recently, the Finance Act, 2025 expanded the statutory VDA definition with a crypto-asset limb effective from 1 April 2026 and introduced dedicated reporting architecture for crypto-asset transactions.

3Prevention of Money Laundering Act 2002, ss 3, 5, 8, 12; Financial Intelligence Unit–India, 'Registration of Virtual Digital Asset Service Providers as Reporting Entity under PMLA' (4 July 2023).

Under the Income-tax Act, 2025, Section 509 requires prescribed reporting entities to furnish statements relating to crypto-asset transactions; the 2026 framework also introduced penalties for non-compliance.[4]

These developments are significant because they strengthen the information infrastructure available to the state. They should not, however, be mistaken for comprehensive investor protection. Tax reporting answers the question 'what transaction information must be reported to tax authorities?'; it does not fully answer 'who may operate an exchange?', 'what cybersecurity standard must it meet?', 'what disclosures must a token issuer make?', or 'what remedy does a defrauded consumer receive?'

4.5 SEBI, RBI and institutional fragmentation

SEBI's jurisdiction is strongest where a crypto product or scheme falls within existing securities or collective-investment concepts. The underlying research notes the relevance of Section 11AA of the SEBI Act to pooled investment arrangements. Yet the absence of a general statutory classification of cryptocurrencies as securities limits SEBI's ability to act as a universal crypto regulator.[5]

The RBI occupies a different institutional position. Its monetary and banking mandate gives it substantial authority over regulated financial entities and payment systems, but not a free-standing mandate to regulate every private digital asset. The 2018 circular and its subsequent invalidation illustrate the constitutional boundary: financial regulation must remain proportionate to the demonstrated harm and within statutory authority.

FIU-IND and ED fill important AML and proceeds-of-crime functions, while state police, cyber cells and economic-offence units often handle the originating fraud. The result is a multi-agency ecosystem without a single institution carrying end-to-end responsibility for crypto market integrity. This fragmentation is the central institutional weakness identified by the research.

5. Judicial Response and Case Studies

5.1 Internet and Mobile Association of India v. RBI

The Supreme Court's 2020 judgment is foundational because it demonstrates that regulatory caution cannot automatically justify a total restriction. The Court examined proportionality and

4Income-tax Act 1961, ss 2(47A), 115BBH, 194S; Finance Act 2025.
5Securities and Exchange Board of India Act 1992, s 11AA.

held that the RBI's banking restriction was excessive in light of the evidentiary record. The decision did not declare cryptocurrencies legal tender, nor did it prevent Parliament from legislating. Its deeper lesson for crypto policy is methodological: the state must match the intensity of the regulatory response to demonstrable risk and statutory authority.[6]

5.2 GainBitcoin: the archetype of the crypto-Ponzi problem

The GainBitcoin matter, as analysed in the source research, illustrates how an apparently technological investment proposition can resemble a conventional Ponzi scheme. Investors were promised fixed or unusually high Bitcoin-linked returns, and the scheme allegedly used multi-level structures and subsequent token substitutions. The case exposes the weakness of relying on the novelty of the asset as a defence against ordinary fraud law. The core conduct—inducement by deception and diversion of investor funds—can fit established criminal categories; the difficulty is scale, evidence, asset tracing and coordination.[7]

5.3 Morris Coin: fictitious token, real liability

The Morris Coin case study is particularly valuable because it shows how the 'crypto' label can be used to create an appearance of technical legitimacy. Investors were solicited with promises concerning token issuance, exchange listing and high returns, while the underlying token allegedly did not exist in the promised form. The case illustrates the regulatory gap at the boundary between traditional cheating and unregulated token issuance. It also demonstrates why disclosure, licensing and promoter accountability are necessary before a fraud occurs rather than only after funds disappear.[8]

5.4 Bux Coin litigation and the limits of territorial enforcement

The Bux Coin-related litigation discussed in the research demonstrates the transnational dimension of crypto fraud. A purportedly Dubai-connected enterprise, a digital exchange and investors across multiple Indian states created a jurisdictional mosaic. Courts were required to balance the seriousness of the alleged economic offence with personal liberty, while also imposing conditions designed to prevent recurrence. Such litigation shows that Indian courts can apply existing penal and state-specific depositor laws, but it also shows the cost of doing

6Internet and Mobile Association of India v Reserve Bank of India (2020) 10 SCC 274.
7Ganesh Shivkumar Sagar v State of Gujarat, Special Leave to Appeal (Crl) No 268 of 2023 (Supreme Court materials discussed in the source research).
8Enforcement Directorate, materials concerning the Morris Coin investigation and attachment of assets.

so in the absence of uniform digital-asset legislation.[9]

5.5 WazirX: the consumer-protection gap

The WazirX episode is different from an investment Ponzi because it centres on exchange security and consumer redress. The research records the July 2024 breach involving a very large loss of crypto-assets and the subsequent consumer litigation. The NCDRC's 2025 disposition, as discussed in the source, illustrates the jurisdictional problem created by contractual choice-of-law and the absence of a specialised Indian mechanism for crypto disputes. The case exposes an important policy gap: AML supervision of an exchange does not automatically create a comprehensive regime governing custody, segregation of customer assets, cybersecurity, insurance, or compensation following an exchange failure.[10]

6. Enforcement Challenges

6.1 Attribution and digital evidence

The most persistent enforcement problem is attribution. A public ledger can show the movement of assets but may not identify the person behind a wallet. Investigators therefore need a chain of evidence connecting blockchain addresses to exchanges, devices, communications, bank accounts and persons. This requires technical capacity that is unevenly distributed across India's policing and prosecution systems.

6.2 Mixers, DeFi and technological escalation

Mixing services and privacy-enhancing technologies can obscure transaction trails. DeFi introduces another problem: there may be no conventional intermediary against whom a regulator can immediately impose KYC, governance or cybersecurity duties. Smart contracts can automate transactions, but code does not resolve the legal question of who bears responsibility when a developer intentionally embeds a vulnerability or uses administrative privileges to extract liquidity.

6.3 Jurisdiction and international cooperation

Crypto fraud is structurally transnational. A victim may be in India, the promoter in another jurisdiction, the exchange in a third, and the assets distributed across wallets controlled through

9Divyesh Dhansukhbhai Darji v State of Gujarat, R/Criminal Misc Appl Nos 16743 & 17068 of 2021 (Guj HC).
10Nirod Kumar Das v State of Odisha (OPID), BLAPL No 12151 of 2023 (Orissa HC).

multiple jurisdictions. Mutual legal assistance, exchange cooperation, asset-freezing orders and recognition of digital evidence must therefore operate faster than conventional cross-border litigation. The absence of harmonised rules creates opportunities for regulatory arbitrage.

6.4 Institutional capacity and public awareness

Technical capacity is only one side of the problem. Victims frequently lack knowledge of wallet security, private keys, phishing and the legal risks of unrealistic returns. Public education is therefore a preventive regulatory tool. The research rightly treats investor education not as a peripheral issue but as part of the legal response to fraud.

7. Comparative Regulatory Models

7.1 United States: enforcement power with institutional fragmentation

The United States demonstrates the strengths and weaknesses of a multi-agency model. The SEC addresses crypto-assets and offerings that fall within securities law; FinCEN applies anti-money-laundering obligations to covered financial businesses; the Department of Justice prosecutes criminal offences; and other agencies may assert jurisdiction depending on the asset and activity. The Howey framework has allowed courts and regulators to analyse certain token offerings as investment contracts.[11]

The United States has also begun an institutional clarification process. The SEC established a Crypto Task Force in January 2025 to work toward a clearer regulatory framework and continues public engagement. The American experience demonstrates that strong enforcement cannot fully compensate for classification disputes and overlapping mandates.

7.2 European Union: harmonisation through MiCA

The EU's MiCA model offers a different lesson: instead of relying primarily on case-by-case classification, it creates a dedicated framework for crypto-assets and crypto-asset service providers, with requirements concerning authorisation, disclosure, governance and consumer protection. MiCA distinguishes categories such as asset-referenced tokens and e-money tokens and imposes obligations on service providers.[12]

For India, the major lesson is institutional coherence. A harmonised statutory perimeter can

11US Securities and Exchange Commission, 'Crypto Task Force' materials (2025–2026); Financial Crimes Enforcement Network, Bank Secrecy Act guidance concerning convertible virtual currency and money services businesses.

12Regulation (EU) 2023/1114 on Markets in Crypto-assets (MiCA).

reduce the uncertainty that arises when each regulator attempts to fit a new asset into an old category. The Indian model need not copy MiCA, but it should adopt the principle that crypto-asset activities should be classified by function and risk rather than by technological label.

7.3 Singapore: licensing, AML and consumer safeguards

Singapore's Payment Services Act provides an activity-based licensing structure for digital payment token services, supported by anti-money-laundering and technology-risk requirements. The Monetary Authority of Singapore has also adopted a consumer-oriented approach that includes risk disclosures and restrictions on misleading promotion. The model demonstrates how a jurisdiction can permit innovation while imposing entry, governance and operational standards.[13]

8. Toward an Indian Risk-Based Crypto-Fraud Framework

8.1 Enact a dedicated Digital Asset Regulation Act

India should move from a collection of partial controls toward a dedicated, technology-neutral statute. The statute should not necessarily legalise every crypto product or treat every token as a security. Instead, it should define the regulatory perimeter and allocate responsibilities by activity and risk. It should define digital assets, crypto-asset service providers, custodians, exchanges, issuers, brokers, token promoters and relevant decentralised activities, while expressly preserving the legal status of sovereign currency and CBDC.

8.2 Introduce activity-based VASP licensing

Registration with FIU-IND is an important AML gateway but should be complemented by a licensing regime for market conduct and operational risk. Exchanges, custodians, brokers, transfer providers and token issuers should face proportionate licensing thresholds. Requirements should include fit-and-proper criteria, minimum capital where appropriate, segregation of customer assets, cybersecurity audits, incident reporting, business continuity, record retention and governance.

8.3 Build a specialised crypto-fraud investigation architecture

A national digital-asset fraud coordination mechanism should connect FIU-IND, ED,

13Payment Services Act 2019 (Singapore); Monetary Authority of Singapore, requirements applicable to Digital Payment Token service providers.

cybercrime police, state economic-offence units, RBI, SEBI and tax authorities. The objective should be operational rather than bureaucratic: one complaint should trigger coordinated tracing, rapid preservation of evidence, identification of exchange touchpoints and assessment of whether PMLA, BNS, IT Act, tax or securities provisions apply.

8.4 Make blockchain analytics a standard investigative capability

The underlying research identifies Chainalysis, CipherTrace and Elliptic-type tools and the potential use of machine learning to identify suspicious smart-contract patterns. India should build an accountable public-sector capability rather than rely entirely on private vendors. AI-assisted risk scoring should be used as an investigative lead, not as a substitute for human adjudication. Systems should maintain audit trails, preserve explainability and comply with constitutional privacy and evidentiary requirements.[14]

8.5 Create mandatory consumer-protection standards

A crypto customer should receive clearer legal protection than exists under the present fragmented model. Exchanges should disclose material risks, conflicts of interest, custody arrangements and security incidents. Customer assets should be segregated where appropriate. A specialised ombudsman or digital-asset dispute mechanism should provide low-cost redress for smaller claims. For proven fraud, law should facilitate rapid asset freezing and restitution without prejudging criminal liability.

8.6 Address DeFi without pretending that decentralisation eliminates responsibility

A future statute should distinguish genuinely decentralised protocols from entities that exercise meaningful control over code, treasury, governance, front-end access or user assets. Regulation should focus on functional control and risk creation. A person who can materially alter a protocol, control liquidity or profit from user transactions should not escape regulation merely by describing the project as 'decentralised'. At the same time, open-source software development should not automatically become a regulated financial activity.

8.7 Strengthen international cooperation

India should deepen cooperation through FATF standards, mutual legal assistance, regulator-to-regulator channels and structured exchange of information with major crypto jurisdictions.

14Chainalysis, ‘Crypto Pump and Dump Schemes Make Up 24% of New Tokens’ (2023).

The FATF Travel Rule principle is particularly relevant because it seeks to preserve originator and beneficiary information across VASP transfers. Cross-border asset recovery should become a specialised operational field.[15]

9. Testing the Hypothesis and Answering the Research Questions

The research hypothesis that the existing Indian framework is doctrinally inadequate is supported, but with an important qualification. It would be inaccurate to describe Indian law as incapable of addressing crypto fraud. Cheating, criminal breach of trust, cyber offences, money laundering, tax reporting and certain securities or depositor-protection offences can all be used depending on the facts. The deficiency is systemic: no single framework provides a complete pathway from market entry to prevention, detection, prosecution, asset recovery and consumer redress.

The first research question is answered by identifying pseudonymity, decentralisation, irreversibility and cross-border operation as the main sources of difficulty. The second is answered by showing that BNS, IT Act and PMLA are useful but functionally incomplete. The third is answered through the institutional analysis: overlapping mandates create regulatory seams, while technical capacity varies. The fourth is answered by the comparative section: India can combine the EU's statutory coherence, Singapore's licensing and consumer protection, and the US's specialised enforcement capabilities. The fifth is answered by the proposed risk-based framework.

10. Conclusion

Cryptocurrency fraud should not be treated as a problem created solely by a new form of money. It is a problem created by the collision between new technological infrastructure and legal institutions designed around intermediaries, territoriality and identifiable assets. India has moved beyond a purely prohibitory approach. Yet the regulatory patchwork remains inadequate for the full lifecycle of crypto fraud. A victim of a rug pull needs more than the possibility of prosecuting cheating after the event. A customer of an exchange needs custody and cybersecurity standards before an attack. A token issuer needs disclosure duties before collecting public money. Investigators need rapid access to KYC and blockchain intelligence before assets cross multiple jurisdictions. And courts need a coherent statutory vocabulary for

15Financial Action Task Force, standards concerning virtual assets and virtual asset service providers, including the Travel Rule.

determining rights, duties and remedies.

The appropriate Indian response is therefore neither unconditional prohibition nor laissez-faire. It is risk-based governance. Parliament should establish a clear statutory perimeter; regulators should allocate obligations according to activity and risk; FIU-IND and investigative agencies should operate through interoperable intelligence systems; exchanges and custodians should satisfy measurable governance and cybersecurity standards; and consumers should receive meaningful disclosure and redress. Such a framework would not guarantee the disappearance of crypto fraud—no financial system can—but it would reduce the structural advantages currently enjoyed by fraudsters and improve the capacity of the Indian legal system to identify, disrupt, punish and remediate digital-asset crime.

The deeper lesson is constitutional as well as regulatory. Internet and Mobile Association of India v. RBI demonstrates that disruptive technology must be governed through lawful and proportionate state action. A mature Indian crypto policy should therefore combine financial stability, innovation, privacy, consumer protection, technological competence and the rule of law. The objective should not be to make cryptocurrency risk-free; it should be to make the legal system capable of responding to the risks that cryptocurrency creates.