International Journal of Global Research Innovations & Technology (IJGRIT)
ISSN : 2583-8717(Online), Impact Factor: 6.972, Volume 03, No. 04, October-December, 2025, pp 273-282

A Critical Analysis of Digital Assets and Criminal Liability in India with Special Reference to Cryptocurrency-Enabled Cyber Offences

Adarsh Singhal[1] | Dr. Mahendra Kumar Jangir[2*]

[1]Research Scholar, Maharaj Vinayak Global University, Jaipur.
[2]Associate Professor, Maharaj Vinayak Global University Jaipur.

*Corresponding Author: iim.mhndra@gmail.com

Citation: Singhal, A., & Jangir, M. (2025). A Critical Analysis of Digital Assets and Criminal Liability in India with Special Reference to Cryptocurrency-Enabled Cyber Offences. International Journal of Global Research Innovations & Technology, 03(04), 273–282. https://doi.org/10.62823/IJGRIT/03.04.8566

ABSTRACT

The rapid proliferation of digital assets — encompassing cryptocurrencies, non-fungible tokens (NFTs), and related virtual instruments — has generated a parallel ecosystem of sophisticated financial crime that challenges the structural architecture of India's legal order. This article provides a critical, multidimensional analysis of the intersection between digital assets and criminal liability in India, with a specific focus on cryptocurrency-enabled cyber offences. Drawing on statutory interpretation, judicial precedent, and comparative regulatory analysis, the article examines the definitional evolution of 'virtual digital assets' under the Income Tax Act, 1961; the extension of the Prevention of Money Laundering Act, 2002 (PMLA) to virtual asset service providers in March 2023; the application of the Information Technology Act, 2000; the transitional criminal jurisprudence introduced by the Bharatiya Nyaya Sanhita, 2023 (BNS); and the Enforcement Directorate's growing arsenal of investigative tools. The article further analyses landmark case law including Internet and Mobile Association of India v. Reserve Bank of India (2020), and the recent WazirX security breach (2024) and its regulatory aftermath. Finally, it critically evaluates the persistent lacunae in India's legal framework — including the absence of dedicated cryptocurrency legislation, low conviction rates, jurisdictional challenges in cross-border offences, and the threat posed by decentralised finance (DeFi) protocols — and proposes a comprehensive reformative agenda rooted in the principles of legal certainty, technological neutrality, and international cooperation.

***Keywords**: Virtual Digital Assets, Cryptocurrency, Cyber Crime, Laundering, Ransomware, Dark Web, Enforcement Directorate, Digital Assets Regulation, Financial Intelligence Unit.*

Introduction

The emergence of blockchain technology and its principal application — cryptocurrency — has fundamentally altered the architecture of global finance. Bitcoin, introduced via Satoshi Nakamoto's seminal white paper in 2008, inaugurated a new era of peer-to-peer, decentralised financial transactions that operate without the intermediation of central banks or traditional financial institutions.[1] In the decade and a half since, thousands of cryptocurrencies have been created, non-fungible tokens (NFTs) have disrupted conventional notions of intellectual property and ownership, and decentralised finance (DeFi) platforms have challenged the very foundations of regulated financial markets.

India's encounter with this phenomenon has been turbulent. The Reserve Bank of India (RBI) attempted to excise cryptocurrency from the banking ecosystem by circular in 2018, only to have the Supreme Court strike down that prohibition in 2020 on grounds of disproportionality.[2] The government's response was characteristically cautious: rather than legalising or banning crypto outright, it chose to acknowledge virtual digital assets (VDAs) through the tax statute — imposing a punitive 30% tax on

[1] Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (2008), available at bitcoin.org/bitcoin.pdf.
[2] Internet and Mobile Association of India v. Reserve Bank of India (2020) 10 SCC 274.

gains — while simultaneously deploying anti-money laundering machinery to surveil the space.[1] As of March 2023, the PMLA formally brought all VDA service providers within its ambit, transforming cryptocurrency exchanges into 'reporting entities' with KYC and suspicious transaction reporting obligations equivalent to banks.[2]

Against this backdrop of regulatory improvisation, the criminal exploitation of digital assets has expanded dramatically. India recorded 86,420 cybercrime cases in 2023 — a 31.2% increase from the 65,893 cases registered in 2022 — with fraud-related offences accounting for 68.9% of all reported cases.5 Financial losses to cyber fraud stood at approximately ₹22,812 crore in 2024 alone.6 Ransomware operators demand Bitcoin; dark web marketplaces transact exclusively in Monero or Zcash; cryptocurrency mixers launder the proceeds of organised crime; pump-and-dump schemes defraud retail investors through manipulated altcoin markets. Yet India lacks a dedicated cryptocurrency statute, its IT Act of 2000 was designed for a pre-blockchain world, and the conviction rate for cyber offences languishes below 3%.[3]

This article undertakes a systematic legal examination of these challenges. Part II analyses the definitional and taxonomic framework for digital assets under Indian law. Part III maps the existing criminal law architecture applicable to cryptocurrency-enabled offences across the IT Act, PMLA, BNS, and FEMA. Part IV examines specific categories of cryptocurrency-facilitated cybercrime. Part V evaluates landmark judicial and regulatory precedents. Part VI conducts a comparative analysis with international models. Part VII identifies the critical gaps in India's legal framework and Part VIII proposes legislative and institutional reforms

The Definitional and Taxonomic Framework for Digital Assets Under Indian Law

- **The Genesis of the 'Virtual Digital Asset' Definition**

Prior to 2022, India's legal vocabulary contained no statutory definition of cryptocurrency or any cognate concept. The RBI's 2018 circular referred to 'virtual currencies' without defining them; courts, regulators, and litigants worked from ad hoc characterisations that oscillated between treating crypto as currency, commodity, property, or mere data.

The definitional vacuum was partially addressed by the Finance Act, 2022, which inserted Section 2(47A) into the Income Tax Act, 1961. Under this provision, a 'virtual digital asset' means: 'any information or code or number or token (not being Indian currency or foreign currency), generated through cryptographic means or otherwise, by whatever name called, providing a digital representation of value exchanged with or without consideration, with the promise or representation of having inherent value, or functions as a store of value or a unit of account including its use in any financial transaction or investment, but not limited to investment schemes. The definition further encompasses non-fungible tokens and any other token of similar nature, subject to the Central Government's power to specify or exclude assets by notification.

This definition, though grounded in tax law rather than criminal or regulatory statute, has assumed systemic importance. It is the definition adopted by reference under the PMLA notification of 2023, effectively transplanting a fiscal concept into the anti-money laundering framework. The definition's breadth — extending to any cryptographically generated representation of value — captures Bitcoin, Ethereum, stablecoins, governance tokens, and most DeFi instruments. However, it has significant limitations from a criminal law standpoint: it does not address the property-law status of VDAs (whether they constitute movable property, actionable claims, or sui generis assets), and this ambiguity has consequences for the prosecution of theft, fraud, and misappropriation offences involving digital assets.

- **Taxonomic Distinctions and Their Legal Significance**

Treating all VDAs as a homogenous category obscurelegally significant distinction. From a criminal law perspective, at least four categories of digital asset merit separate analysis. First, payment cryptocurrencies such as Bitcoin and Litecoin function primarily as a medium of exchange and store of value; they are the instrument of choice for ransomware operators, dark web purchases, and cross-border illicit remittances owing to their pseudo-anonymity and irreversibility. Second, utility tokens derive value from access rights to a specific blockchain-based platform or service; they have been used as instruments of fraud in Initial Coin Offering (ICO) scams where the promised utility never materialises.

[1] Finance Act, 2022, inserting Section 2(47A) and Section 115BBH into the Income Tax Act, 1961.
[2] Ministry of Finance, Gazette Notification No. G.S.R. 178(E) dated 7 March 2023 (PMLA VASP Notification).
[3] Citizens for Justice and Peace, 'Cybercrime and the Crisis of Digital Justice: India's invisible victims online' (2025): citing NCRB 2023 data — only 22% of cybercrimes led to charge sheets and less than 3% resulted in convictions.

Third, security tokens represent ownership stakes in assets and carry characteristics of investment contracts; their fraudulent issuance may engage both the IT Act and provisions of the SEBI Act. Fourth, NFTs — unique, indivisible digital assets linked to digital or physical objects — have emerged as instruments of art fraud, intellectual property theft, money laundering, and marketplace manipulation.

- **Legal Status: The Continuing Ambiguity**

Cryptocurrencies are neither legal tender nor prohibited under Indian law — they occupy an uncertain middle ground that the Supreme Court, in Internet and Mobile Association of India v. Reserve Bank of India (2020),[1] acknowledged but did not resolve. The Court struck down the RBI's banking prohibition as disproportionate but expressly did not rule on the broader question of cryptocurrency's legal status. This constitutional silence has cascading implications for criminal jurisprudence: if VDAs are not 'property' for the purposes of the Bharatiya Nyaya Sanhita (formerly IPC), the conventional offences of theft, misappropriation, and criminal breach of trust may not readily apply to their unauthorized taking.

The National Consumer Disputes Redressal Commission (NCDRC) in the WazirX case (April 2025) observed that cryptocurrencies 'may be considered goods under the Consumer Protection Act' while simultaneously characterising the governance regime as 'nebulous,' illustrating the contradictions that pervade judicial engagement with digital assets.10 In May 2025, the Supreme Court questioned the absence of comprehensive cryptocurrency legislation, signalling judicial impatience with the legislative vacuum.[2]

The Criminal Law Architecture Applicable to Cryptocurrency-Enabled Offences

- **The Information Technology Act, 2000: The Primary Statute**

The Information Technology Act, 2000 (IT Act) constitutes India's principal legislative instrument for addressing computer-related crimes. Enacted before the Bitcoin protocol existed; the Act has been applied to cryptocurrency offences through interpretive stretching rather than targeted design. The following provisions are most frequently invoked.

Section 43 of the IT Act imposes civil liability of up to ₹1 crore upon persons who, without the permission of the owner of a computer system, access, download data, introduce computer contaminants, or damage data.12 While Section 43 is remedial rather than penal, it establishes the civil foundation upon which criminal provisions are layered. Section 66 criminalises acts under Section 43 performed 'dishonestly or fraudulently,' punishable with imprisonment up to three years or a fine up to ₹5 lakh, or both. This provision has been applied to the hacking of cryptocurrency wallets and exchange platforms.

Section 66C criminalises identity theft in electronic form, prescribing imprisonment up to three years and a fine up to ₹1 lakh.13 In the cryptocurrency context, this provision covers the fraudulent use of another person's private keys or seed phrases to access and transfer their digital assets — an increasingly prevalent form of crypto theft. Section 66D addresses cheating by personation using computer resources, carrying equivalent penalties, and has been applied to phishing attacks that target cryptocurrency exchange account credentials.

Section 66E penalises violation of privacy through the capture, publication, or transmission of the private area of any person — a provision relevant to sextortion schemes where offenders demand cryptocurrency in exchange for not publishing intimate images. Section 67B criminalises child pornography in electronic form, and ransomware operators who threaten to publish such material as a coercive mechanism add a layer of IT Act liability to their extortion.

Section 72 addresses breach of confidentiality and privacy by persons who have secured access to electronic records in the course of official duty — relevant to cases where cryptocurrency exchange employees leak customer data to external fraudsters. The penalty is imprisonment up to two years or a fine up to ₹1 lakh, widely regarded as inadequate given the scale of harm that data

- **The Prevention of Money Laundering Act, 2002: The PMLA Framework**

The extension of the PMLA to VDAs by the Ministry of Finance Gazette Notification dated 7 March 2023 represents the most consequential regulatory development in India's approach to

[1] Internet and Mobile Association of India v. Reserve Bank of India (2020) 10 SCC 274; see also Bhatt & Joshi Associates, 'Legality of Virtual Digital Assets in India' (December 2025).

[2] Shankari IAS Parliament, 'Virtual Digital Asset (VDA) Regulations in India' (June 2025): noting that the Supreme Court questioned the absence of comprehensive crypto regulation in India in May 2025.

cryptocurrency crime.[1] The notification designates as 'reporting entities' under Section 2(1)(sa) of the PMLA all entities providing financial services in connection with: the exchange of VDAs with fiat currencies; the exchange of one or more forms of VDA; the transfer of VDAs; the safekeeping or administration of VDAs; and the participation in and provision of financial services related to the offer and sale of VDAs.

The substantive offence of money laundering under Section 3 of the PMLA covers ‘every process or activity connected with the proceeds of crime, including its concealment, possession, acquisition, or use, and projecting or claiming it as untainted property.’ This broad formulation extends to any cryptocurrency transaction suspected of being connected with scheduled offences. The scheduled offences include crimes under the IPC/BNS, the IT Act, the Customs Act, the Narcotic Drugs and Psychotropic Substances (NDPS) Act, and others. Accordingly, Bitcoin used to purchase narcotics on the dark web, or Ether received as ransomware payment, potentially constitutes 'proceeds of crime' subject to PMLA attachment and prosecution.

The punishment for money laundering under Section 4 of the PMLA is rigorous imprisonment of not less than three years, extendable to seven years, plus a fine. Where the predicate offence relates to narcotics, the maximum imprisonment extends to ten years. The Enforcement Directorate (ED), the principal investigative authority under the PMLA, has substantially expanded its cryptocurrency-focused enforcement since 2023. By January 2023, the ED had attached proceeds of crime worth approximately ₹936 crore related to cryptocurrency.[2]

As reporting entities, VDA service providers must nowverify the identity of clients and beneficial owners (KYC); maintain records of all cash transactions exceeding ₹10 lakh and report suspicious transactions to the Financial Intelligence Unit-India (FIU-IND); implement internal controls and appoint a Principal Officer for AML compliance; and file cash and suspicious transaction reports in prescribed formats.

- **The Bharatiya Nyaya Sanhita, 2023: Modernisation and Its Limits**

The Bharatiya Nyaya Sanhita, 2023 (BNS), which replaced the Indian Penal Code, 1860 with effect from 1 July 2024, introduced certain cyber-specific amendments while largely preserving the inherited IPC framework. The most significant addition is the inclusion of cybercrimes within the new offence of 'organised crime' under Section 111 of the BNS, which recognises the organised and syndicated nature of contemporary cybercriminal enterprises. The Act also extended the scope of the offence of publishing obscene material to include 'contents in electronic form,' correcting an earlier lacuna.

Several established IPC provisions, now recodified under the BNS, remain applicable to cryptocurrency-enabled offences. Section 318 of the BNS (formerly Section 420 IPC) — cheating — applies where a person by deceit fraudulently induces another to deliver property. Cryptocurrency fraud schemes — including fake exchange platforms, Ponzi investment schemes, and ICO frauds — fall squarely within this provision. In Rafeeq Ahmad v. State of Karnataka (2015), the court convicted the accused under Section 420 IPC (now Section 318 BNS) in conjunction with Section 66 of the IT Act for hacking banking accounts and fraudulently transferring funds.[3]

Section 303 of the BNS (formerly Section 378 IPC — theft) criminalises the dishonest taking of movable property without consent. The applicability of this provision to cryptocurrency depends on the property-law characterisation of VDAs as movable property — a question courts have not definitively resolved. Section 314 of the BNS (formerly Section 403 IPC — dishonest misappropriation) has been applied to situations where hackers gain unauthorized access to digital wallets and misappropriate cryptocurrency.

Section 319 of the BNS (formerly Section 415 IPC — cheating) and Section 340 (formerly Section 468 IPC — forgery for the purpose of cheating) apply to the creation of fraudulent smart contracts and forged blockchain records used to deceive counterparties. The use of the BNS's extortion provision (Section 308, formerly Section 383 IPC) has been argued in ransomware cases where operators demand cryptocurrency as a condition for restoring encrypted data — a compelling characterisation that has yet to be tested at the appellate level.

---

[1] Ministry of Finance, Gazette Notification No. G.S.R. 178(E), 7 March 2023; Oxford Law Blogs (OxBLB), 'Digital Assets & the Indian

[2] Ministry of Finance Press Release, February 6, 2023: 'ED has attached proceeds of crime worth nearly INR 936 crores related to cryptocurrency under PMLA as on January 31, 2023.'

[3] Rafeeq Ahmad v. State of Karnataka (2015), cited in Lex Orbis, 'Cybersecurity Laws and Regulations India 2025' (2025).

- **The Foreign Exchange Management Act, 1999 (FEMA)**

FEMA occupies an important but under-examined role in the regulation of cross-border cryptocurrency transactions. While FEMA does not explicitly reference VDAs, the RBI treats any foreign asset transfer — including transfers of cryptocurrency to or from overseas wallets — as a foreign exchange transaction subject to regulatory scrutiny. The acquisition of cryptocurrency from foreign exchanges without RBI approval may constitute an unauthorised foreign exchange transaction, exposing individuals to civil penalties under Section 13 of FEMA (up to three times the sum involved) and, in severe cases, criminal prosecution under Section 13(1A) for contraventions involving sums exceeding ₹1 crore.[1] The ED has authority to investigate FEMA violations and has exercised this jurisdiction in cryptocurrency cases where funds have been transferred offshore through crypto channels.

Categories of Cryptocurrency-Enabled Cybercrime in India

- **Ransomware and Extortion**

Ransomware — malicious software that encrypts a victim's data and demands cryptocurrency payment for the decryption key — represents one of the most economically destructive manifestations of cryptocurrency-enabled crime. Bitcoin's irreversibility and pseudo-anonymity make it the preferred payment rail for ransomware operators. In India, ransomware attacks surged during the post-pandemic period: in the first half of 2024, India recorded 39 ransomware incidents, with critical infrastructure — particularly healthcare — emerging as a high-value target.[2]

From a criminal law standpoint, ransomware operators face prosecution under Section 66 (hacking) and Section 43 of the IT Act; Section 308 of the BNS (extortion); Section 318 of the BNS (cheating); and potentially Section 4 of the PMLA (money laundering) for the receipt and laundering of ransom cryptocurrency.

- **Cryptocurrency Fraud and Investment Scams**

Investment fraud involving cryptocurrency has emerged as India's most volumetrically significant cryptocurrency crime category. The National Crime Records Bureau (NCRB) 2023 report recorded 86,420 cybercrime cases, of which fraud accounted for 68.9% of cases — many involving cryptocurrency investment schemes.[3] The FIU-IND estimates that between July 2022 and December 2023, Indians traded over ₹1.03 trillion worth of VDAs on non-compliant platforms, creating fertile ground for unregulated fraud.[4]

Cryptocurrency investment fraud takes several forms. Ponzi schemes — where returns to existing investors are funded by contributions from new investors, with promoters siphoning funds via crypto — have proliferated because cryptocurrency's complexity obscures the absence of any genuine underlying investment. Fake exchange platforms mimic legitimate exchanges to steal deposited funds and login credentials. Pump-and-dump schemes involve coordinated purchase of low-capitalisation altcoins, artificial inflation of prices through social media promotion, and rapid sale at peak, leaving retail investors with depreciated holdings. Initial Coin Offering (ICO) frauds involve the creation of fictitious blockchain projects, public fundraising via token sales, and subsequent disappearance of promoters.

The prosecution of these offences engages Section 318 (cheating) and Section 319 (cheating by personation) of the BNS, Section 66D of the IT Act (cheating by personation using computer resources), and Section 3 of the PMLA where the proceeds are laundered through subsequent cryptocurrency transactions.

- **Money Laundering Through Cryptocurrency**

Cryptocurrency's technical features — pseudonymity, border lessness, irreversibility, and the availability of privacy-enhancing tools such as mixers, tumblers, and privacy coins — have made it a preferred instrument for layering and integrating the proceeds of crime. India's money laundering architecture has historically focused on fiat currency flows through the banking system; the migration of laundering activity to blockchain networks has tested this framework's analytical and investigative capabilities.

---

[1] Foreign Exchange Management Act, 1999, Section 13; RBI Guidelines on Foreign Asset Transfers.

[2] IRJMETS, 'Cybercrime Trends in India' (2024): CERT-In India Threat Landscape Report 2024 — 593 cyberattacks, 388 data breaches, 107 data leaks, and 39 ransomware incidents in the first half of 2024.

[3] NCRB, 'Crime in India 2023': fraud-related offences accounting for 68.9% or 59,526 of total cybercrime cases.

[4] Shankari IAS Parliament, 'Virtual Digital Asset (VDA) Regulations in India' (June 2025): citing estimates that between July 2022 and December 2023, Indians traded over Rs. 1.03 trillion worth of VDAs on non-compliant platforms.

Common cryptocurrency money laundering techniques identified in Indian enforcement actions include: 'chain hopping' (converting the proceeds of crime from one cryptocurrency to another across multiple blockchains to obscure the audit trail); the use of cryptocurrency mixers that aggregate and redistribute tokens to break the transaction chain; the utilisation of peer-to-peer (P2P) trading platforms — outside the purview of KYC-compliant exchanges — to convert between fiat and cryptocurrency anonymously; and the exploitation of DeFi protocols where smart contracts execute transactions automatically, without human intermediaries who could be compelled to provide transaction records.[1]

- **Dark Web Marketplace Transactions**

The dark web — websites hosted on the Tor network, inaccessible through conventional browsers — hosts marketplaces where narcotics, weapons, forged documents, stolen financial credentials, and malware are traded using cryptocurrency. India's position in these markets is multidimensional: as a source of pharmaceutical narcotics and counterfeit medicines (exploiting India's large pharmaceutical manufacturing base); as a market for imported narcotics; and increasingly as a market for the purchase of stolen Indian financial data and identity documents.

Enforcement actions targeting dark web activity require coordination between the Narcotics Control Bureau (NCB) under the NDPS Act; the Enforcement Directorate under the PMLA; and the Cyber Crime Cells of state police forces under the IT Act. The case of the Silk Road marketplace (international) demonstrated that even ostensibly anonymous cryptocurrency transactions can be traced when combined with traditional investigative techniques. India's law enforcement agencies have begun developing similar capabilities, though the pace of institutional development lags significantly behind the sophistication of criminal operators.[2]

- **NFT-Related Fraud and Intellectual Property Crime**

Non-fungible tokens (NFTs) — cryptographically unique digital assets representing ownership of digital or physical objects — have generated novel fraud typologies. Copyright infringement through the minting of NFTs from others' artwork without authorisation has proliferated on open platforms like Open Sea. NFT marketplaces wash trading — simultaneous buying and selling of the same NFT between connected wallets to inflate price history — constitutes market manipulation. 'Rug pulls' — where NFT project creators raise funds, list the NFT collection, and then abandon the project while retaining investors' funds — have extracted hundreds of millions globally.

India's legal framework is poorly equipped to address NFT-specific crimes. The Copyright Act, 1957 protects original creative works but does not specifically address the minting of NFTs from copyrighted works without authorisation. The BNS's cheating provisions apply to the intent-to-deceive element of NFT scams but require courts to navigate complex factual matrices of blockchain technology and smart contract mechanics. A dedicated regulatory and criminal framework for digital art markets and NFT platforms is absent.

- **Cryptojacking and Unauthorised Mining**

Cryptojacking — the unauthorised use of a victim's computing resources to mine cryptocurrency — represents a property crime with a distinctly novel character: the victim's hardware is exploited, their electricity consumed, and their device performance degraded, all without their knowledge. Unlike ransomware, cryptojacking is designed to be covert. Malicious scripts embedded in websites or downloaded as malware execute mining algorithms in the background, with the mined cryptocurrency credited to the attacker's wallet.

Section 43 and Section 66 of the IT Act cover the unauthorised introduction of a computer contaminant (the mining script) and the dishonest exploitation of computing resources. The criminal element — given the difficulty of establishing the quantum of financial harm and the covert nature of the offence — makes prosecution challenging. CERT-In's India Threat Landscape Report identified cryptojacking as an emerging threat across Indian corporate networks in 2024.[3]

- **Terrorism Financing and Cryptocurrency**

The use of cryptocurrency to finance terrorist activities raises issues at the intersection of the Unlawful Activities (Prevention) Act, 1967 (UAPA) and the PMLA. The FATF's recommendations on virtual assets specifically address the terrorism financing risk posed by cryptocurrency's speed and

[1] Outlook India, 'How Does India Plan To Fight Against Crypto Money Laundering' (April 2025).
[2] IRJMETS, 'Cybercrime Trends in India 2018-2024 (2024).
[3] Cyble / Cyber Express, 'India Sees Sharp Rise In Cybercrime, NCRB Data Reveals' (December 2025).

border lessness. India, as a FATF member, has committed to implementing the Travel Rule — requiring VASPs to pass originator and beneficiary information along with cryptocurrency transfers — as a counter-terrorism financing mechanism. However, implementation of the Travel Rule across Indian VDA service providers remains incomplete.[1]

Landmark Judicial and Regulatory Precedents

- **Internet and Mobile Association of India v. Reserve Bank of India (2020)**

The Supreme Court's judgment in Internet and Mobile Association of India v. Reserve Bank of India, reported in (2020) 10 SCC 274[2], is the foundational constitutional precedent in India's cryptocurrency jurisprudence.[3] The Court, by a three-judge bench comprising Justice R.F. Nariman, Justice Aniruddha Bose, and Justice V. Ramasubramanian, struck down the RBI's April 2018 circular that prohibited banks from providing services to entities dealing in virtual currencies.

The Court applied the doctrine of proportionality — derived from its earlier jurisprudence on constitutional limitations on fundamental rights — to hold that the RBI's circular, which effectively imposed a blanket ban on cryptocurrency businesses without demonstrating actual harm to the regulated banking system, was disproportionate to the regulatory objective pursued. Crucially, the Court affirmed the RBI's inherent regulatory powers over virtual currencies but held that those powers must be exercised in proportion to identified harm.

The judgment's implications for criminal jurisprudence are considerable. By affirming that trading in cryptocurrency is legally permissible (in the absence of legislative prohibition) and by establishing the principle of proportionality as a constraint on regulatory action, the Court created a framework within which subsequent regulatory and enforcement actions are assessed.

- **The WazirX Security Breach (2024) and Its Regulatory Aftermath**

On July 18, 2024, the WazirX cryptocurrency exchange suffered a security breach resulting in the unauthorized withdrawal of approximately $233 million (approximately ₹1,946 crore) — roughly 45% of the exchange's total asset holdings. The breach targeted one of WazirX'sMult signature wallets, with losses concentrated in Ether and other ERC-20 tokens. The sophistication of the attack, which involved the manipulation of multi-signature authorization procedures through social engineering and malware, pointed to a state-affiliated threat actor, with cybersecurity analysts attributing the breach to the Lazarus Group, a North Korean cyber threat actor.

WazirX suspended all withdrawals following the breach, preventing users from accessing remaining funds. A class action before the NCDRC filed by 40 aggrieved investors was dismissed in April 2025 on jurisdictional grounds, with the Commission acknowledging cryptocurrency's status as 'goods' under the Consumer Protection Act while characterising the regulatory framework as 'nebulous.

The WazirX case crystallises several systemic problems in India's approach to cryptocurrency crime. First, the absence of mandatory insurance requirements or investor protection funds for cryptocurrency exchanges leaves consumers without guaranteed remedies in insolvency or security breach scenarios. Second, the attribution of the breach to a state-sponsored actor highlights the geopolitical dimension of cryptocurrency crime and the limitations of purely domestic enforcement responses. Third, the NCDRC's jurisdictional diffidence — dismissing the case rather than adjudicating on the merits — reflects the broader judicial reluctance to engage with cryptocurrency disputes in the absence of a clear statutory framework

- **The Shreya Singhal Case and Its Crypto-Adjacent Legacy**

While Shreya Singhal v. Union of India (2015) did not directly address cryptocurrency, its invalidation of Section 66A of the IT Act — which had been used to criminalise online speech — established the principle that cyber-specific penal provisions must satisfy the constitutional tests of specificity, proportionality, and intelligible differentia. This principle has implications for cryptocurrency-related penal provisions: any future statutory criminalisation of cryptocurrency activities must satisfy the Shreya Singhal standard of constitutional precision, which provides a check on overly broad legislative responses to cryptocurrency crime.

---

[1] Comply Cube, 'Cryptocurrency Regulation in India in 2024' (February 2025): noting that the Travel Rule, a global standard set by FATF, forms part of India's AML initiative21

[2] (2020) 10 SCC 274

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

Critical Gaps in India's Legal Framework

- **The Absence of a Dedicated Cryptocurrency Statute**

The most fundamental gap in India's legal framework is the absence of dedicated cryptocurrency legislation. The Cryptocurrency and Regulation of Official Digital Currency Bill, 2021 — which proposed to ban private cryptocurrencies while establishing a Central Bank Digital Currency framework — was introduced in the Lok Sabha's agenda but never debated in Parliament and has not progressed. The subsequent approach of regulating through the PMLA notification and the Income Tax Act's VDA definition is pragmatically useful but structurally inadequate: it leaves criminal law provisions scattered across multiple statutes designed for different purposes, without the coherent definitional, jurisdictional, and procedural architecture that a dedicated statute would provide.

- **Low Conviction Rates and Institutional Capacity Deficits**

The NCRB's 2023 data reveals that only 22% of cybercrime cases resulted in charge sheets, and fewer than 3% resulted in convictions.44 This abysmally low conviction rate reflects multiple intersecting deficits: inadequate technical training of investigating officers who lack expertise in blockchain forensics and cryptocurrency investigation; evidentiary challenges in proving digital asset offences (especially where cryptographic tools have obscured transaction trails); judicial unfamiliarity with cryptocurrency technology and its legal characterisation; and the frequent cross-jurisdictional dimension that complicates prosecution.

- **Jurisdictional Challenges in Cross-Border Offences**

The cross-border nature of most sophisticated cryptocurrency crime creates layered jurisdictional challenges that India's legal framework is not designed to address. The IT Act's extraterritorial reach is limited; the PMLA's jurisdiction extends to activities connected with money laundering of proceeds generated within India, but the evidence necessary to establish that connection may be located in servers abroad. Section 1(4) of the BNS (formerly Section 3 IPC) provides for the application of Indian criminal law to acts committed beyond India by persons subject to Indian law, but enforcement against foreign nationals abroad depends on extradition treaties or voluntary cooperation, both of which are uncertain in the cryptocurrency crime context.[1]

The proliferation of cryptocurrency exchanges headquartered in jurisdictions with minimal regulatory oversight — sometimes characterised as regulatory havens — enables criminal operators to establish apparent corporate legitimacy while evading the investigative reach of Indian authorities. The FIU-IND's December 2023 compliance notices to nine major offshore exchanges represented a significant assertion of regulatory authority, but the practical enforceability of those notices against exchanges that choose not to comply remains limited.

- **The DeFi Challenge**

Decentralised Finance (DeFi) protocols — automated smart contract systems that replicate financial services (lending, trading, derivatives, insurance) without centralised intermediaries — present a challenge that existing regulatory frameworks are fundamentally ill-equipped to address. FIU-IND's activity-based approach to VASP definition attempts to capture DeFi within the PMLA framework, but DeFi protocols that are genuinely decentralised — with no single entity capable of exercising control, receiving instructions, or maintaining customer records — cannot realistically comply with KYC and suspicious transaction reporting obligations.[2]

- **Privacy Coins and Anonymity-Enhancing Technologies**

Privacy coins — including Monero (XMR) and Zcash (ZEC) — deploy advanced cryptographic techniques (ring signatures, stealth addresses, zero-knowledge proofs) that provide genuine transaction anonymity, as opposed to Bitcoin's pseudonymity. Unlike Bitcoin transactions, which are recorded on a publicly auditable blockchain and can be traced through blockchain forensic tools, privacy coin transactions cannot be definitively traced even with state-of-the-art analytics. The use of privacy coins in ransomware payments, dark web transactions, and money laundering creates a category of cryptocurrency crime where India's investigative arsenal is effectively neutralised.

---

[1] Lex Orbis, 'Cybersecurity Laws and Regulations India 2025': Section 1(4) of BNS (formerly Section 3 IPC) provides extraterritorial application of Indian criminal law

[2] Global Legal Insights, 'Blockchain & Cryptocurrency Laws & Regulations 2026: India' (October 2025): 'A DeFi protocol's claim to be decentralised is not conclusive. The degree of decentralisation must be demonstrated in practice.

Conclusion and Suggestions

India stands at an inflection point in its engagement with digital assets and the criminal pathologies they enable. The country leads globally in grassroots cryptocurrency adoption — with NASSCOM reporting $6.6 billion in retail investor participation[1] — yet its legal framework remains fractured, improvised, and systematically inadequate to the challenge of cryptocurrency-enabled cybercrime. The regulatory achievements of 2022-2023 — the VDA tax framework and the PMLA notification — represent meaningful but partial progress. The BNS's modernisation of India's criminal code, while symbolically significant, did not address the substantive gaps in cyber-specific criminal law. Conviction rates remain near negligible; institutional capacity is strained; the DeFi challenge is unaddressed; privacy coins represent an analytical frontier beyond current enforcement capabilities; and the Budapest Convention's architecture remains inaccessible to Indian investigators.

India's response must be proportionate to the scale of the challenge: a dedicated Digital Assets Act providing legal certainty and targeted criminal provisions; accession to or approximation of the Budapest Convention's international cooperation framework; a specialised enforcement institution with genuine technical expertise; consumer protection infrastructure for exchange customers; and sustained investment in judicial and law enforcement training. The alternative — continued regulatory improvisation as the blockchain ecosystem accelerates — is neither legally defensible nor socially acceptable. India's digital future demands a legal architecture built for it.

Suggestions

- **Enact a Dedicated Digital Assets and Cryptocurrency Act**

The legislative priority must be the enactment of a comprehensive Digital Assets Act that provides statutory definitions of different categories of digital assets; the legal characterisation of VDAs as a sui generis category of movable property under Indian law; licensing requirements for cryptocurrency exchanges and VDA service providers with conditions integrating AML/CFT obligations; specific criminal offences for blockchain-based crimes (wallet fraud, smart contract exploitation, NFT fraud, crypto Ponzi schemes); an Investor Protection Fund financed by exchange licensing fees; and extraterritorial jurisdiction provisions modelled on the Budapest Convention's approach.

- **Establish a Dedicated Cryptocurrency Crime Investigation Unit**

The government should establish a Cryptocurrency Crime Investigation Unit (CCIU) within the ED or as a standalone body under the Ministry of Home Affairs, staffed with personnel possessing expertise in blockchain forensics, smart contract analysis, and cryptocurrency exchange operations.

- **Implement the FATF Travel Rule Across All Compliant VASPs**

India should mandate full implementation of the FATF Travel Rule — requiring VDA service providers to collect and transmit originator and beneficiary information for cryptocurrency transfers — within a defined statutory timeline. The technical interoperability protocols for Travel Rule implementation (including Verifiable Credentials and Trust Frameworks) should be standardised through CERT-In guidelines, creating a common infrastructure that enables compliance without imposing disproportionate costs on smaller providers.

- **Create a Consumer Protection Regime for Cryptocurrency Markets**

In the wake of the WazirX breach and the NCDRC's jurisdictional vacillation, India requires a clear consumer protection framework for cryptocurrency market participants. This should include mandatory segregation of customer cryptocurrency assets from exchange proprietary assets; mandatory cold storage requirements for a minimum percentage of customer assets; mandatory insurance against security breaches; clear liability allocation for losses arising from exchange insolvency or security failure; and a designated dispute resolution forum with technical expertise in cryptocurrency transactions.

References

1. Information Technology Act, 2000
2. Prevention of Money Laundering Act, 2002
3. Bharatiya Nyaya Sanhita, 2023
4. Bharatiya Nagarik Suraksha Sanhita, 2023

[1] Shankari IAS Parliament, 'Virtual Digital Asset (VDA) Regulations in India': citing NASSCOM report that Indian retail investors poured $6.6 billion into crypto assets.

5. Digital Personal Data Protection Act, 2023
6. Foreign Exchange Management Act, 1999
7. Income Tax Act, 1961 (as amended by Finance Act, 2022).
8. Unlawful Activities (Prevention) Act, 1967.
9. Consumer Protection Act, 2019.
10. National Crime Records Bureau, 'Crime in India 2023' (Ministry of Home Affairs, 2024).
11. FATF, 'Virtual Assets: Guidance for a Risk-Based Approach' (2021).
12. Oxford Law Blogs (OxBLB), 'Digital Assets & the Indian Anti-Money Laundering Regime(July 2023).
13. Global Legal Insights, 'Blockchain & Cryptocurrency Laws & Regulations 2026: India' (October 2025).
14. ICLG, 'Cybersecurity Laws and Regulations Report 2025 India' (November 2024).
15. Law Blend, 'Cyber Crime Laws in India: A Comprehensive Analysis' (March 2025).
16. IMPRI, 'The New Age of Crypto: India's 2024 Regulatory Framework Unveiled' (September 2024).
17. LexOrbis, 'Cybersecurity Laws and Regulations India 2025 (2025).
18. LawPret, 'Cyber Crime in India: A Comprehensive Report' (July 2025).
19. Citizens for Justice and Peace, 'Cybercrime and the Crisis of Digital Justice' (November 2025).
20. ComplyCube, 'Cryptocurrency Regulation in India in 2024 (February 2025).
21. Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (2008).
22. European Union, Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCA).
23. Singapore, Payment Services Act 2019, Cap. 222A.
24. Bhatt & Joshi Associates, 'Legality of Virtual Digital Assets in India: Private Key & Seed Phrase Extraction' (December 2025).
25. IRJMETS, 'Cybercrime Trends in India 2018-2024 (2024).