 DOI: *https://doi.org/10.63108/IJLMH.12706*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 4

2026

Crimes on Cryptocurrency and Jurisdictional Challenges of Enforceability in India

SWETA PANDA* AND DR. AMRUTA DAS**

ABSTRACT

Cryptocurrency began as a marginal experiment among cypherpunk technologists and has since become an asset class worth trillions of dollars globally, and its rise has been matched by a parallel rise in criminal activity that feeds off the pseudonymity, decentralisation and borderless movement these assets allow. India counts among the countries with the largest populations of crypto holders anywhere, yet Parliament has still not enacted any statute dedicated to virtual digital assets; oversight instead comes piecemeal, through tax provisions, anti-money-laundering notifications and rulings handed down case by case. This article sets out the scale of crypto-related crime worldwide, reviews the current statistics, and examines the jurisdictional and enforcement difficulties that follow from them, with particular attention to how those difficulties play out inside India. India's liability framework is then measured against a handful of foreign models, the Indian judiciary's engagement with the resulting legal gaps is assessed against international standards and model policy approaches, and the article closes by setting out a proposed regulatory framework.

Keywords: *Cryptocurrency, Digital Assets, Jurisdiction, Money Laundering, Blockchain*

I. INTRODUCTION

At its core, cryptocurrency is digital money whose existence and ownership records live on a blockchain: a ledger that no single institution controls, maintained instead by a distributed network of computers acting in consensus. No government stands behind it or guarantees its worth, and value comes purely from scarcity, network agreement and the demand users place on it. Indian law sidesteps the word "currency" entirely, preferring the statutory phrase "virtual digital asset" (VDA), a category built to encompass cryptocurrency, non-fungible tokens and whatever further asset class the Central Government later chooses to notify.[1] The phrasing was chosen deliberately, and the statutory scheme stops well short of treating these assets as legal tender. Paradoxically, the very properties that make cryptocurrency attractive to ordinary users,

* Author is a Student at SOA National Institute of Law, Siksha 'O' Anusandhan (Deemed to be University), Bhubaneswar, Odisha, India.
** Author is an Associate Professor of Legal Studies at SOA National Institute of Law, Siksha 'O' Anusandhan (Deemed to be University), Bhubaneswar, Odisha, India.
[1] Income-tax Act, 1961, § 2(47A) (India) (inserted by the Finance Act, 2022, No. 6 of 2022).

its decentralised structure, its pseudonymity, the speed with which it crosses borders and the fact that transactions cannot be reversed, are exactly what make it useful to criminals.

Criminal exploitation of crypto falls into five broad categories, some of whose boundaries overlap:

(a) crypto used as an instrument in offences already covered by existing law, including drug trafficking, terrorist financing, ransomware payments and sanctions evasion, as well as romance-investment frauds of the kind known as "pig butchering";

(b) crypto used as the payment or laundering channel for the proceeds of other, unrelated offences;

(c) attacks originating within the crypto industry itself, including exchange breaches and wallet thefts, rug pulls, and the exploitation of defective smart contracts;

(d) investment fraud dressed in crypto vocabulary, typically structured as a Ponzi scheme; and

(e) the sale of tokens with no underlying asset or project behind them.

Each of the five categories exploits a single vulnerability. The blockchain ledger is technically open for anyone to inspect, but it is difficult to establish who controls a given address, and once funds move across international borders through mixing services they become tougher still to freeze.[2] The comparative overview below sets out the range of responses different countries have adopted, from outright prohibition to a full licensing system. India is unusual within that group in having no purpose-made regulation for the sector; it is governed instead by tax provisions, separately issued anti-money-laundering notifications and the general criminal law, each of which is examined in turn in the sections that follow.

II. STATEMENT OF THE PROBLEM

Cryptocurrency is no longer confined to a recreational fringe, and its macroeconomic and national-security footprint now warrants close study. Addresses associated with illicit activity received at least US$154 billion in 2025, roughly 162 per cent more than the year before, a rise driven principally by a 694 per cent increase in the value received by sanctioned entities.[3] Stablecoins, which until recently represented only a modest fraction of illicit flows, accounted

[2] FINANCIAL ACTION TASK FORCE, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (Oct. 2021).

[3] CHAINALYSIS, *2026 Crypto Crime Report: Introduction* (Feb. 2026), https://www.chainalysis.com/blog/2026-crypto-crime-report-introduction/.

 [ISSN 2581-5369]

for 84 per cent of them in 2025, a shift traceable to their price stability and to the ease with which they cross borders.[4]

India has felt this trend directly. Cybercrime complaints recorded through the Indian Cyber Crime Coordination Centre (I4C), which operates under the Ministry of Home Affairs, rose by roughly 24 per cent in 2025 compared with the year before, to about 28.15 lakh cases, and reported cyber-fraud losses stood at approximately Rs. 22,495 crore.[5] Investment scams, chiefly fake trading platforms and crypto-linked Ponzi schemes, are estimated to account for more than 75 per cent of that loss figure.[6]

Nothing illustrates the domestic stakes as clearly as the July 2024 breach of WazirX, then one of India's largest exchanges. Attackers compromised a multi-signature wallet arrangement custodied by the Singapore-based firm Liminal and removed digital assets worth an estimated US$230 million, or roughly Rs. 1,900 crore.[7] The blockchain-analytics firm Elliptic attributed the intrusion to the North Korea-linked Lazarus Group on the basis of on-chain fund movements consistent with that group's earlier activity.[8] The episode exposed more than a technical failure. The Enforcement Directorate had already alleged, in 2022, that the exchange's Indian operating company had created a web of agreements with entities in the United States, the Cayman Islands and Singapore that obscured the exchange's beneficial ownership.[9]

Figures on this scale make crypto crime in India a live enforcement problem rather than a speculative one. Private wealth is being extracted faster than enforcement agencies can trace, freeze and recover it.

III. CRYPTOCURRENCY, ITS MARKET AND ITS REGULATORY EFFECTS

Cryptocurrency disrupts financial oversight precisely because it bypasses the machinery regulators have traditionally relied on. Anti-money-laundering and foreign-exchange rules are constructed around intermediaries, banks, wire-transfer companies and payment processors, that authorities can supervise directly, require to identify their customers, and compel to flag

---

[4] CHAINALYSIS, *supra* note 3.
[5] *Cybercrime Saw 24% Spike in 2025: Indians Lost Rs 22,495 Crore, Mainly in Investment Scams*, THEPRINT (Feb. 21, 2026), https://theprint.in/india/cybercrime-saw-24-spike-in-2025-indians-lost-rs-22495-crore-mainly-in-investment-scams/2859930/.
[6] *Cybercrime Saw 24% Spike in 2025*, *supra* note 5.
[7] *WazirX Cryptocurrency Exchange Loses $230 Million in Major Security Breach*, THE HACKER NEWS (July 22, 2024), https://thehackernews.com/2024/07/wazirx-cryptocurrency-exchange-loses.html.
[8] *WazirX Cryptocurrency Exchange Loses $230 Million*, *supra* note 7 (reporting Elliptic's attribution of the intrusion to the Lazarus Group on the basis of on-chain analysis).
[9] *ED Raids Premises of Director of Crypto Firm WazirX, Freezes Rs 64.67 Crore Bank Balance*, THEPRINT (Aug. 5, 2022), https://theprint.in/economy/ed-raids-director-of-crypto-firm-wazirx-freezes-rs-64-67-crore-bank-balance/1070605/.

suspicious behaviour. Crypto networks remove that intermediary layer altogether, moving value from one node to another without any signal passing through a supervised institution. That quietly dismantles the assumption underlying most financial regulation: that a state can supervise financial activity simply by watching the institutions physically located within its borders.

Regulatory friction has done remarkably little to slow Indian adoption. India ranked first on the Chainalysis Global Crypto Adoption Index in both 2023 and 2024.[10] What that friction has done is push activity offshore, and the migration is now measured as a share of trading volume rather than as a count of platforms. Exchanges' own submissions to the Parliamentary Standing Committee on Finance put the offshore share of Indian trading volume at close to ninety per cent,[11] while an industry study drawing on the trading behaviour of more than 670,000 users placed it at 72.66 per cent for the 2024-25 financial year.[12] An earlier study by the Esya Centre estimated that Indian users traded roughly Rs. 2.63 lakh crore on offshore platforms between December 2023 and October 2024, and that web traffic to nine offshore exchanges rose by about 57 per cent over the same period.[13] Those nine exchanges were the same platforms against which the Financial Intelligence Unit had issued show-cause notices in December 2023, asking the Ministry of Electronics and Information Technology to block their web addresses in India.[14] Whichever figure is nearer the mark, offshore migration on this scale places a substantial proportion of Indian trading activity beyond the direct regulatory reach of any Indian authority.

This disruption shows up in three distinct ways, set out below.

First, it weakens the effectiveness of monetary policy and capital controls. Crypto-denominated value can cross into or out of India almost instantly, entirely avoiding the settlement channels the Reserve Bank of India is equipped to watch. The Bank pressed exactly this concern in the

---

[10] CHAINALYSIS, *2024 Global Crypto Adoption Index* (Sept. 2024) (ranking India first among the countries surveyed, as it had in 2023).

[11] *India Parliament Panel Urges Phased Crypto Regulation Under SEBI or RBI*, THE CRYPTO TIMES (July 24, 2026), https://www.cryptotimes.io/2026/07/24/india-parliament-panel-urges-phased-crypto-regulation-under-sebi-or-rbi/ (reporting the exchanges' own figures placed before the Parliamentary Standing Committee on Finance).

[12] KOINX, *India 1% TDS on Crypto Statistics* (Jan. 2026), https://www.koinx.com/stats/india-tds-on-crypto-statistics (recording that 72.66 per cent of the trading volume studied for the 2024-25 financial year was executed on international exchanges).

[13] *Unwelcome Regulations, High Taxes Push More Indians to Offshore Crypto Exchanges*, THE WEEK (Dec. 28, 2024), https://www.theweek.in/news/biz-tech/2024/12/28/bitcoin-tds-regulations-high-taxes-push-more-indians-to-offshore-crypto-exchanges.html (reporting the findings of an ESYA CENTRE study).

[14] *India to Block URLs of 9 Offshore Exchanges Including Binance After Issuing Compliance "Show Cause" Notices*, COINDESK (Dec. 28, 2023), https://www.coindesk.com/policy/2023/12/28/india-issues-compliance-show-cause-notices-to-9-offshore-exchanges-including-binance-and-kucoin.

 [ISSN 2581-5369]

litigation discussed below, warning that the technology leaves room for an effectively parallel and unsupervised payment system to take shape beyond its oversight.[15]

Second, it makes tax compliance and disclosure harder to enforce. A wallet has no built-in connection to a Permanent Account Number or an Aadhaar identity unless it happens to be funded or emptied through a domestic, know-your-customer-compliant exchange. That gap creates an incentive to move to offshore venues or to peer-to-peer trades on which no tax is deducted at source.

Third, it accelerates the professionalisation of fraud. Stablecoins and cross-chain bridges allow offenders to move assets between jurisdictions in minutes, while an Indian investigator relying on mutual legal assistance may need months to obtain the same information. A conventional fraud can usually be reconstructed through a limited number of correspondent banking relationships; a crypto fraud may span years of transactions across several exchanges in several countries, each governed by a different disclosure regime.

IV. CHALLENGES IN ENFORCEABILITY

Offences of this magnitude can be answered only by investigation and prosecution capable both of recovering assets and of establishing a credible deterrent. The structure of the sector works against both objectives. Regulatory authority over crypto is fragmented across institutions, and the rules of liability become concrete only when a particular matter reaches a court or a tribunal.

A. Issues and challenges

Four features of the crypto ecosystem account for most of the difficulty enforcement agencies encounter.

The first is the number of jurisdictions a single scheme can touch. A victim in Mumbai, a wallet provider in Singapore, a custodian licensed in the Cayman Islands and an off-ramp in a jurisdiction that does not cooperate can all feature in one matter, a pattern the WazirX proceedings illustrate.[16] Crypto transactions settle in close to real time and leave no conventional paper trail, which unsettles two assumptions built into Indian criminal procedure: that an offence has an identifiable place of commission, and that the offender can be located. Mutual legal assistance, the formal route for gathering evidence abroad, moves at nothing like that speed.

---

[15] *Internet & Mobile Ass'n of India v. Reserve Bank of India*, 2020 SCC OnLine SC 275 (India).

[16] *ED Raids Premises of Director of Crypto Firm WazirX*, *supra* note 9.

The second is attribution. Blockchain addresses are pseudonymous rather than anonymous, so a chain of transactions can often be traced back to an exchange that holds know-your-customer records. Where no such exchange sits anywhere on the chain, the trail simply ends. The technical journey of stolen digital assets may be fully visible while the real-world identity behind an address remains out of reach, largely because of the substantial share of peer-to-peer trading conducted on platforms in jurisdictions that do not enforce customer-identification obligations, and because of mixers and other privacy tools.[17]

The third is the absence of any single regulator with general oversight of the sector. Several authorities exercise jurisdiction over some aspect of crypto activity in India, but none holds a general power to license virtual digital asset service providers. The resulting gaps can be exploited by sophisticated operators, and they leave a victim genuinely uncertain about which body to approach.

The fourth is uneven investigative capacity. The cyber-forensic and blockchain-analytics skills these cases demand are concentrated in central agencies, while first information reports are registered and initial investigation is carried out at the state and district level, where those skills are scarce.

B. Authorities and governance

No single institution has been granted comprehensive authority over virtual digital assets in India. Jurisdiction sits instead across several bodies, each drawing its powers from a different statute.

The Reserve Bank of India retains residual authority under the Reserve Bank of India Act, 1934, the Banking Regulation Act, 1949, and the Payment and Settlement Systems Act, 2007. The Supreme Court examined that authority and narrowed its exercise, though it did not remove the power itself, in 2020.[18]

Since VDA-related services were brought within the reporting-entity framework of the Prevention of Money-Laundering Act, 2002, by a notification of 7 March 2023, the Enforcement Directorate has become the sector's most active enforcement body.[19] By December 2025 the Ministry of Finance had informed Parliament that the Directorate had attached, seized

[17] FINANCIAL ACTION TASK FORCE, *supra* note 2.
[18] *Internet & Mobile Ass'n of India*, *supra* note 15.
[19] Ministry of Finance (Dep't of Revenue), Notification dated Mar. 7, 2023, issued under § 2(1)(sa)(vi) of the Prevention of Money-Laundering Act, No. 15 of 2003 (India).

or frozen Rs. 4,189.89 crore in crypto-linked proceeds of crime, made 29 arrests and filed 22 prosecution complaints, with one accused declared a fugitive economic offender.[20]

The scope of this reporting-entity framework has itself been tested in litigation. In a decision significant for how it defines an accountable institution, the Delhi High Court held that an entity which provides only a technology interface enabling payment between a payer and a beneficiary is nonetheless a payment system operator, and therefore a reporting entity obliged to furnish transaction information to the Financial Intelligence Unit, although the Court simultaneously quashed the penalty that had been imposed.[21] The reasoning matters for the crypto sector because it attaches the reporting obligation to the function performed rather than to custody of customer funds.

On the taxation side, section 115BBH of the Income-tax Act, 1961 imposes a flat 30 per cent charge on income from the transfer of a virtual digital asset, while section 194S imposes a 1 per cent deduction at source on such transfers.[22] Both are administered by the Central Board of Direct Taxes, which gains a form of indirect oversight simply because each taxable transaction generates its own record.

The Indian Cyber Crime Coordination Centre supplies a further layer of capacity, operational rather than regulatory. Its National Cybercrime Suspect Registry, launched in September 2024, pools suspect identifiers contributed by banks and financial institutions; by December 2025 more than 18.43 lakh identifiers and 24.67 lakh mule accounts had been shared through it.[23] What is still missing is a frontline regulator for VDA exchanges themselves, of the kind the European Union created for crypto-asset service providers under its Markets in Crypto-Assets Regulation.

C. Liability framework

With the institutions identified, the substance of liability can be examined, first by comparison with the regimes of other countries and then through the three overlapping regimes that operate in India.

[20] *ED Attaches Rs 4,190 Cr in Crypto Cases, Declares One as Fugitive Offender*, BUSINESS STANDARD (Dec. 8, 2025), https://www.business-standard.com/india-news/ed-attaches-4-190-cr-in-crypto-cases-declares-one-as-fugitive-offender-125120800468_1.html.

[21] *PayPal Payments Pvt. Ltd. v. Financial Intelligence Unit India*, W.P. (C) No. 138 of 2021 (Delhi H.C. July 24, 2023) (India).

[22] Income-tax Act, 1961, §§ 115BBH, 194S (India).

[23] *Cybercrime Saw 24% Spike in 2025*, *supra* note 5 (reporting MINISTRY OF HOME AFFAIRS figures on the National Cybercrime Suspect Registry).

 [ISSN 2581-5369]

i. Comparative overview

No universal template governs liability for cryptocurrency. Jurisdictions have instead settled on a handful of familiar positions, each reflecting a different view about how much room the technology should be allowed to occupy.

Five jurisdictions are taken here because each sits at a different point on that spectrum. China represents outright prohibition; the European Union represents comprehensive, harmonised licensing already fully in force; the United States represents a fragmented model only now beginning to converge; and the United Kingdom and Singapore, common-law jurisdictions whose courts have already had to characterise cryptocurrency for ordinary private-law purposes, offer the clearest indication of how India's own courts might eventually resolve the property question the Supreme Court left unanswered in 2020.

Comparative practice sorts into three broad regulatory postures.

The prohibitionist model is best represented by China. A notice issued on 24 September 2021 by the People's Bank of China together with nine other authorities declared all virtual-currency-related business activity unlawful, extended that prohibition to offshore exchanges serving mainland residents, and was accompanied by a plan to phase out mining.[24] Prohibition removes liability questions from consideration entirely by leaving no lawful space in which the activity can take place.

The comprehensive licensing model is represented by the European Union's Markets in Crypto-Assets Regulation, applicable in full across the Union since 30 December 2024.[25] It requires a crypto-asset service provider to obtain authorisation from the competent authority of a single member state, an authorisation that can then be passported throughout the bloc, subject to reserve, disclosure and travel-rule obligations. Article 111 of the Regulation obliges member states to arm their competent authorities with maximum administrative fines of at least EUR 700,000 for a natural person and, for a legal person, of at least EUR 5,000,000 or, depending on which group of obligations has been infringed, 3, 5 or 12.5 per cent of total annual turnover; the higher ceiling of EUR 15,000,000 or 15 per cent of turnover is reserved for the market-abuse infringements in Articles 88 to 92.[26]

[24] *China's Central Bank Says All Cryptocurrency Transactions Are Illegal*, FORBES (Sept. 24, 2021), https://www.forbes.com/sites/siladityaray/2021/09/24/chinas-central-bank-says-all-cryptocurrency-transactions-are-illegal/.

[25] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-Assets, 2023 O.J. (L 150) 40, art. 149.

[26] Regulation (EU) 2023/1114, *supra* note 25, arts. 111(2)(d), 111(3), 111(5). Article 112 governs the coordinated exercise of those powers; Articles 113, 114 and 115 concern the right of appeal, the publication of decisions and the reporting of penalties to ESMA and EBA, and confer no power to fine.

The fragmented model is represented by the United States, where liability is divided among securities regulators, commodities regulators and financial-crimes authorities. The GENIUS Act, signed into law on 18 July 2025, is the first federal statute to create a comprehensive framework for payment stablecoins; it requires issuers to hold reserves on a one-to-one basis, to disclose reserve composition monthly, and, for larger issuers, to submit audited annual financial statements.[27] Its architecture points toward greater coordination in future.

The United Kingdom and Singapore add a further layer worth noting. Each has moved toward comprehensive statutory licensing while its courts have independently resolved a question Indian courts have not. The Financial Conduct Authority published final rules for the United Kingdom's cryptoasset regime on 30 June 2026, bringing trading platforms, intermediaries, custodians, stablecoin issuers and staking arrangements within a licensing framework built on the Financial Services and Markets Act 2000; applications for authorisation open on 30 September 2026 and the regime takes full effect on 25 October 2027.[28] The prudential side of that regime was settled at the same time: a cryptoasset that can be prudently valued and is admitted to a qualifying United Kingdom cryptoasset trading platform attracts a single 40 per cent net risk position requirement, while a cryptoasset meeting neither condition is deducted from regulatory capital altogether.[29] The Monetary Authority of Singapore has taken a narrower and more conservative approach, finalising a stablecoin framework in 2023 which requires reserve assets to be held at not less than the full value of coins in circulation, in segregated accounts, subject to monthly independent attestation and annual audit.[30]

Courts in both jurisdictions have also generated the most developed body of common-law authority anywhere on cryptocurrency's legal status. In *AA v. Persons Unknown* the English High Court was satisfied, for the purpose of granting an interim proprietary injunction, that cryptoassets are a form of property under English law.[31] The Court of Appeal in *Tulip Trading Ltd v. van der Laan* moved the law in a different direction, holding that there was a serious issue to be tried as to whether the developers of a bitcoin network owe fiduciary duties to the owners

---

[27] Guiding and Establishing National Innovation for U.S. Stablecoins Act of 2025, S. 1582, 119th Cong. (enacted July 18, 2025).
[28] Financial Conduct Authority, *A New Regime for Cryptoasset Regulation* (final rules published June 30, 2026), https://www.fca.org.uk/firms/new-regime-cryptoasset-regulation.
[29] Financial Conduct Authority, *PS26/12: A Prudential Regime for Cryptoasset Firms* (June 30, 2026), https://www.fca.org.uk/publication/policy/ps26-12.pdf; see also Financial Conduct Authority, *CP25/42: A Prudential Regime for Cryptoasset Firms* (Dec. 16, 2025), https://www.fca.org.uk/publications/consultation-papers/cp25-42-prudential-regime-cryptoasset-firms.
[30] Monetary Authority of Singapore, *MAS Finalises Stablecoin Regulatory Framework* (Aug. 2023), https://www.mas.gov.sg/news/media-releases/2023/mas-finalises-stablecoin-regulatory-framework.
[31] *AA v. Persons Unknown* [2019] EWHC 3556 (Comm) (Eng.).

of assets recorded on it, and allowing the claim to proceed.[32] Singapore's courts have travelled a parallel road. In *Quoine Pte Ltd v. B2C2 Ltd* the Court of Appeal observed that there might be much to commend the view that cryptocurrencies are capable of assimilation into the general concepts of property, but expressly declined to decide the point.[33] The General Division of the High Court supplied the answer in *ByBit Fintech Ltd v. Ho Kai Xin*, holding that crypto assets are things in action capable of being held on trust and declaring a constructive trust over the misappropriated tokens.[34] Taken together, these decisions give litigants in the United Kingdom and Singapore an established evidentiary and remedial toolkit, proprietary injunctions, freezing orders and constructive trusts, that Indian courts have not yet had occasion to develop for themselves.

Notwithstanding these differences, every regime discussed here shares a common baseline drawn from the standards of the Financial Action Task Force, under which any entity that exchanges, transfers, safekeeps or administers virtual assets is treated as a virtual asset service provider subject to the same customer-identification and suspicious-transaction-reporting duties applied to banks, and to the travel rule requiring originator and beneficiary information to accompany transfers.[35]

ii. The Indian legislative framework

India's own strategy neither outlaws users nor leaves service providers untouched. It imposes liability on providers while leaving both them and the courts without a settled legal characterisation of what a virtual digital asset actually is. No statute deals specifically with cryptocurrency. The draft Banning of Cryptocurrency and Regulation of Official Digital Currency Bill, 2019 was never introduced in Parliament, and its successor, the Cryptocurrency and Regulation of Official Digital Currency Bill, 2021, was listed in the Lok Sabha Bulletin twice, in January and again in November 2021, without being introduced on either occasion.[36] Three regulatory pillars therefore operate independently of one another to generate legal liability.

The taxation regime. Section 2(47A) of the Income-tax Act, 1961, inserted by the Finance Act, 2022, defines a virtual digital asset in very wide terms, covering cryptocurrencies, non-fungible tokens and any other asset the Central Government may notify.[37] Section 115BBH taxes income

---

[32] *Tulip Trading Ltd v. van der Laan* [2023] EWCA Civ 83 (Eng.).
[33] *Quoine Pte Ltd v. B2C2 Ltd* [2020] SGCA(I) 02 (Sing.).
[34] *ByBit Fintech Ltd v. Ho Kai Xin* [2023] SGHC 199 (Sing.).
[35] FINANCIAL ACTION TASK FORCE, *supra* note 2 (Recommendation 15 and its Interpretive Note).
[36] LOK SABHA BULLETIN, Part II (Jan. 29, 2021); LOK SABHA BULLETIN, Part II (Nov. 23, 2021) (each listing the Cryptocurrency and Regulation of Official Digital Currency Bill, 2021 for introduction).
[37] Income-tax Act, 1961, *supra* note 1.

arising from the transfer of such an asset at a flat rate of 30 per cent, allows no deduction other than the cost of acquisition, and bars both the set-off and the carry-forward of losses.[38] The design is intended to maximise revenue and to discourage speculative trading, while incidentally advancing enforcement objectives by making compliant transactions traceable. Section 194S requires 1 per cent to be deducted at source on transfers, subject to an annual threshold of Rs. 50,000 for specified persons and Rs. 10,000 for others.[39] Failure to deduct attracts a penalty under section 271C equal to the amount not deducted, while failure to pay deducted tax to the credit of the Central Government can attract prosecution under section 276B.[40] These provisions are fiscal rather than penal in character, but they nonetheless operate as an implicit layer of oversight over crypto transactions.

The anti-money-laundering regime. A Ministry of Finance notification of 7 March 2023, issued under section 2(1)(sa)(vi) of the Prevention of Money-Laundering Act, 2002, brought a wide range of VDA-related conduct within the category of designated business or profession, and so within the definition of a reporting entity: exchange between virtual digital assets and fiat currency, exchange between one or more forms of virtual digital assets, transfer of such assets, safekeeping or administration of such assets or of instruments enabling control over them, and participation in financial services connected with an issuer's offer and sale of a virtual digital asset.[41] A reporting entity must apply know-your-customer norms, maintain records and report suspicious transactions to the Financial Intelligence Unit, while money laundering itself carries rigorous imprisonment of three to seven years together with attachment of property.[42] This breadth comes at a price. The notification is drafted widely enough to reach non-custodial participants such as software developers and node operators who take no real control of user funds, which raises proportionality concerns alongside the expanded powers it confers on the Enforcement Directorate.

The general criminal law. Criminal liability enters the framework through the Bharatiya Nyaya Sanhita, 2023, which replaced the Indian Penal Code with effect from 1 July 2024 and consolidates criminal breach of trust in section 316, cheating in section 318 and forgery in section 336,[43] and through the Information Technology Act, 2000, which covers unauthorised access, data theft and identity fraud of the kind connected with fraudulent crypto schemes,

---

[38] Income-tax Act, 1961, § 115BBH (India).
[39] Income-tax Act, 1961, § 194S (India).
[40] Income-tax Act, 1961, §§ 271C, 276B (India).
[41] Notification dated Mar. 7, 2023, *supra* note 19.
[42] Prevention of Money-Laundering Act, No. 15 of 2003, §§ 4, 12 (India).
[43] Bharatiya Nyaya Sanhita, No. 45 of 2023, §§ 316, 318, 336 (India).

exchange breaches and investment fraud.[44] Because neither statute was drafted with cryptocurrency in view, a prosecutor must first characterise the relevant asset as property or as consideration before the statutory language can apply at all. Courts have accepted that characterisation without difficulty in straightforward fraud cases, but it is considerably harder to sustain where the question is whether a stolen virtual digital asset counts as movable property within the meaning of section 2(21) of the Sanhita for the purposes of theft or misappropriation.

D. Enforcement and asset-recovery roadblocks

A favourable court order or a completed investigation is not, by itself, the end of the story. As an agency moves from a paper finding to a recovered asset, two further obstacles arise, distinct from the structural problems described above.

The first is that a domestic order reaches only so far when the asset sits outside India. An Indian court, or the Enforcement Directorate acting under the Prevention of Money-Laundering Act, can direct a domestic exchange to freeze a customer's holdings because that exchange falls within Indian jurisdiction. The position changes where the exchange is established abroad, or where the suspect controls a wallet without any custodian at all. The Indian party must then obtain a judgment at home, trace the assets through blockchain analysis, and persuade a court in the other country to give that judgment local effect. That sequence stalls where no mutual enforcement arrangement exists between the two states, or where the foreign jurisdiction's own data-protection law prevents an exchange there from disclosing information about its customers.[45]

Cross-border enforcement co-operation does sometimes work, even where it stops short of returning money to victims. In June 2025 the Spanish Guardia Civil, working with Europol and with law-enforcement counterparts in France, Estonia and the United States, dismantled a crypto investment-fraud network that had laundered an estimated EUR 460 million taken from more than 5,000 victims worldwide, arresting five suspects through precisely this kind of coordinated action across several jurisdictions at once.[46] No sum recovered for the victims was reported. Outcomes of that kind remain the product of case-by-case cooperation rather than of an established procedural pathway, and Indian agencies cannot assume that a comparable partnership will be available in every matter they pursue.

---

[44] Information Technology Act, No. 21 of 2000, §§ 43, 66, 66C, 66D (India).

[45] *Understanding Cryptocurrency Forfeiture: A Guide to Digital Asset Seizure*, NAT'L L. REV. (June 26, 2025), https://natlawreview.com/article/understanding-cryptocurrency-forfeiture-guide-digital-asset-seizure.

[46] EUROPOL, *Crypto Investment Fraud Ring Dismantled in Spain After Defrauding 5 000 Victims Worldwide* (June 2025), https://www.europol.europa.eu/media-press/newsroom/news/crypto-investment-fraud-ring-dismantled-in-spain-after-defrauding-5-000-victims-worldwide.

The second difficulty is technological rather than procedural: certain tools are built specifically to defeat the tracing methods on which asset recovery depends. A mixing service, sometimes called a tumbler, takes in cryptocurrency from a large number of unconnected depositors, blends it together, and pays it back out in a way that severs any obvious link between the funds a criminal received and the funds that criminal later withdraws. United States regulators treated the mixer itself, and not only its users, as the wrongdoer when the Financial Crimes Enforcement Network assessed a US$60 million penalty against the operator of the Helix and Coin Ninja services for failing to register as a money services business and for failing to maintain an anti-money-laundering programme.[47] Certain cryptocurrencies go further still by building the same obfuscation into the protocol itself: Monero conceals both the sender and the transaction amount through ring signatures and confidential-transaction cryptography, while Zcash offers an equivalent shielded mode built on zero-knowledge proofs. The difficulty this creates for investigators is not theoretical. The criminal investigation division of the United States Internal Revenue Service offered a bounty of up to US$625,000 in 2020 for a working tool capable of tracing Monero or Lightning Network transactions.[48] Once stolen proceeds pass through a mixer, or are converted into a privacy coin and later converted back into a transparent one, investigators are typically able to pick up the trail again only from the point of reconversion.

Read together with the jurisdictional and attribution problems set out earlier, these two constraints explain why even a diligently investigated Indian crypto-fraud case can conclude not with a victim's money being returned, but with a judgment against an asset that has, by the time the judgment is obtained, become practically unreachable. It is for this reason that the reforms proposed below are framed as much around recovery as around prosecution.

V. Response of the Indian Judiciary

A. The Internet and Mobile Association judgment

The single most important judicial intervention to date is the Supreme Court's decision in *Internet and Mobile Association of India v. Reserve Bank of India*, delivered on 4 March 2020 by a bench comprising Justices R. F. Nariman, Aniruddha Bose and V. Ramasubramanian.[49] A group of cryptocurrency exchanges had challenged a Reserve Bank circular dated 6 April 2018

---

[47] Financial Crimes Enforcement Network, *First Bitcoin Mixer Penalized by FinCEN for Violating Anti-Money Laundering Laws* (Oct. 2020), https://www.fincen.gov/news/news-releases/first-bitcoin-mixer-penalized-fincen-violating-anti-money-laundering-laws.

[48] *IRS Offers $625K Bounty to Break Monero or Lightning Network Privacy*, BeInCrypto (Sept. 2020), https://beincrypto.com/irs-offers-625k-bounty-to-break-monero-or-lightning-network-privacy/.

[49] *Internet & Mobile Ass'n of India*, *supra* note 15.

 [ISSN 2581-5369]

directing regulated entities to withdraw banking services from any person or business dealing in virtual currencies.

The question before the Court was whether cutting off banking services entirely to virtual-currency businesses was a proportionate exercise of the Bank's statutory power over the monetary and credit system, given that no actual harm to any regulated entity had been demonstrated.

The Court held that the Reserve Bank does possess the power to regulate, and in an appropriate case to prohibit, dealings in virtual currencies, tracing that power to sections 45JA and 45L of the Reserve Bank of India Act, 1934, to sections 35A and 36(1)(a) of the Banking Regulation Act, 1949, and to sections 10(2) and 18 of the Payment and Settlement Systems Act, 2007.[50] It nonetheless struck the circular down as a disproportionate exercise of that power. The Bank had produced no material showing that any entity it regulates had suffered, or was likely to suffer, damage from dealings with virtual-currency exchanges, and less intrusive alternatives had gone unconsidered. The circular accordingly failed the proportionality standard applicable to restrictions on the freedom to practise any profession or to carry on any trade or business under Article 19(1)(g) of the Constitution.[51]

What the Court chose not to decide may matter as much as what it did. It declined to rule on the legality of virtual currencies themselves, and it did not characterise them as property, as a commodity or as a currency instrument.[52] India was left regulating an asset whose legal nature remains judicially unsettled. The decision's significance also runs wider than crypto: any sectoral regulator that restricts access to financial services must now satisfy the same proportionality standard, which the judgment establishes as a general requirement of economic regulation.

B. Later jurisprudence

Indian courts and tribunals have been notably cautious since 2020, engaging with crypto questions at their margins rather than at their core.

On the tax side, the Jodhpur bench of the Income Tax Appellate Tribunal held in *Raunaq Prakash Jain v. Income Tax Officer* that bitcoin acquired in 2015-16 and sold in 2020-21, before the virtual digital asset provisions were inserted into the statute, was a capital asset, so that the

[50] *Internet & Mobile Ass'n of India*, *supra* note 15 (holding that the Reserve Bank's powers extend to virtual currencies).
[51] *Internet & Mobile Ass'n of India*, *supra* note 15 (setting the circular aside as a disproportionate restriction under INDIA CONST. art. 19(1)(g)).
[52] *Internet & Mobile Ass'n of India*, *supra* note 15 (declining to decide the legality or legal character of virtual currencies).

resulting gain was taxable as a long-term capital gain and rollover relief under section 54F was available.[53] The ruling governs only the pre-2022 period, but it remains the clearest judicial statement so far that cryptocurrency can be an asset in the ordinary sense.

On the anti-money-laundering side, the Delhi High Court's holding that an entity providing only a payment technology interface is a reporting entity extends an obligation designed for institutions that hold funds to entities through which funds merely move.[54] The reasoning runs in one direction only. It does not follow that every crypto-adjacent business becomes a payment system operator, and the decision should not be read as creating new categories of regulated entity by analogy.

In criminal matters, the largest crypto-linked prosecutions have generated a steady stream of interlocutory litigation without producing appellate authority on the legal character of the assets involved. The Enforcement Directorate has filed prosecution complaints in the GainBitcoin matter, a mining-contract scheme the agency treats as a Ponzi fraud,[55] and has alleged proceeds of crime of roughly Rs. 6,000 crore in the investigation into the Mahadev betting platform, in which cryptocurrency is said to have been one of the channels used to move funds out of India.[56] Both illustrate the practical difficulty of tracing and securing assets at the investigative stage, but neither has yet yielded a ruling on the underlying characterisation question.

What emerges overall is a judiciary attentive to proportionality in regulatory action, and realistic about the practical difficulty of tracing crypto assets, yet one that has stopped short of resolving the most basic question of all: whether cryptocurrency is property, a security, a commodity, or something closer to a currency instrument. It is exactly this gap that the United Kingdom and Singapore case law discussed earlier has already begun to close within those systems.

VI. CONCLUSION AND SUGGESTIONS

Cryptocurrency crime in India reduces to three unresolved problems: the technology is inherently transnational by design; the domestic legal response is scattered across tax law, anti-money-laundering rules and general criminal law without any real coordination; and international-cooperation mechanisms have not kept pace with the speed at which illicit crypto value can move. The Supreme Court's 2020 decision cleared away one obstacle on the

---

[53] *Raunaq Prakash Jain v. Income Tax Officer* (Income Tax App. Trib., Jodhpur Bench, Nov. 28, 2024) (India).
[54] *PayPal Payments Pvt. Ltd.*, *supra* note 21.
[55] *Raj Kundra Summoned by PMLA Court After ED Files Chargesheet in GainBitcoin Case*, OUTLOOK BUSINESS, https://www.outlookbusiness.com/news/raj-kundra-summoned-by-pmla-court-after-ed-files-chargesheet-in-gainbitcoin-case.
[56] *Mahadev Betting Case: Everything Known About the Rs 6,000 Cr Scam So Far*, BUSINESS STANDARD (Dec. 13, 2023), https://www.business-standard.com/india-news/mahadev-betting-case-everything-known-about-the-rs-6-000-cr-scam-so-far-123121300347_1.html.

banking side, but continuing uncertainty over crypto's legal status, neither clearly defined nor supported by investor protection, and answerable to no single regulator, has left India with a regime that imposes surveillance and liability on the sector without offering the corresponding benefits that comparable economies have secured through legislation such as the European Union's Markets in Crypto-Assets Regulation or the United Kingdom's newly finalised authorisation regime.

Several concrete reforms would meaningfully close this gap. Parliament should pass a virtual digital asset statute naming a single lead regulator, the Securities and Exchange Board of India for exchange-traded assets and the Reserve Bank for payment-related matters, with licensing, capital-adequacy and disclosure obligations built around the virtual asset service provider concept, replacing today's patchwork of tax provisions and anti-money-laundering notifications.

India should also scale up its mutual legal assistance and information-sharing arrangements with the jurisdictions that host the major crypto platforms Indian investors actually rely on, and should engage more actively with multilateral instruments such as the Crypto-Asset Reporting Framework of the Organisation for Economic Co-operation and Development, to which more than seventy jurisdictions have now made political commitments, so that cross-border tracing is not confined to bilateral treaty processes too slow to keep up with blockchain settlement speeds.[57]

Investigative capacity has to move away from the centre. Cyber-forensic and blockchain-analytics units, at present concentrated in national agencies, should be extended down to district police forces and trained to work directly with I4C analytics. Settling the legal nature of a virtual digital asset, whether as property, as a security or as a distinct category of asset altogether, would eliminate a recurring source of uncertainty in theft, contract and insolvency proceedings, much as the United Kingdom and Singapore case law discussed earlier has already done for those jurisdictions. Public financial-literacy campaigns of the kind envisaged by the Karnataka Cyber Security Policy, 2024, which places public awareness and skill building among its principal pillars, deserve to be adapted and scaled up nationally,[58] since a meaningful share of ongoing losses traces back to fraudsters reaching investors through social-media advertisements promising unrealistic returns.

---

[57] ORGANISATION FOR ECONOMIC CO-OPERATION & DEVELOPMENT, *Crypto-Asset Reporting Framework: 2025 Monitoring and Implementation Update* (2025), https://www.oecd.org/content/dam/oecd/en/networks/global-forum-tax-transparency/crypto-asset-reporting-framework-monitoring-implementation-update-2025.pdf.
[58] GOVERNMENT OF KARNATAKA, *Karnataka Cyber Security Policy, 2024* (2024) (listing awareness and education, skill building, and partnership for capacity building among its principal pillars).

Cryptocurrency shows no sign of disappearing from India's financial landscape, and the trajectory of global regulation does not point toward prohibition as the preferred response. The more promising path, the one the European Union and, more recently, the United Kingdom and the United States have each pursued in their own way, is to replace today's improvised mix of tax and anti-money-laundering rules with a single, focused and workable framework: one that gives enforcement agencies a clear jurisdictional footing, gives industry the regulatory certainty it needs, and gives investors the protection a maturing asset class demands.

*****