Minnesota Journal of Business Law and Entrepreneurship

Volume 2026, No. 1

ISSN: 1540-3270

Cryptocurrency Regulation in India: Legal Uncertainty, Financial Stability, and Digital Sovereignty

Ms. Pooja Kumari[1]

Abstract

The rapid global expansion of decentralized cryptoassets has confronted state authorities with complex regulatory, fiscal, and structural challenges.[2] In India, this tension is uniquely pronounced. The state has chosen to navigate private digital innovations by asserting its authority across multiple domains: maintaining structural barriers, implementing rigorous taxation frameworks, and advancing state-controlled alternatives. This research paper evaluates the three-dimensional matrix shaping India's cryptocurrency policy ecosystem: macro-legal uncertainty, systemic risks to financial stability, and the pursuit of digital sovereignty.By analyzing judicial shifts—such as the landmark *Internet and Mobile Association of India (IAMAI) v. Reserve Bank of India* case—alongside contemporary anti-money laundering amendments under the Prevention of Money Laundering Act (PMLA), the strict fiscal regimes established via the Finance Acts, and the parallel rollout of the Digital Rupee (e₹) as a Central Bank Digital Currency (CBDC), this paper demonstrates how India has constructed a de facto containment strategy. It concludes that while this approach has successfully mitigated systemic exposure and curbed capital flight, the persistent lack of an integrated statutory framework leaves retail investors exposed, keeps the domestic web3 ecosystem in legal limbo, and highlights the ongoing friction between private cryptographic protocols and sovereign monetary controls.

Keywords: Crypto Assets, Regulatory, Fiscal, Money laundering, Digital.

1. Introduction

The emergence of public, distributed ledgers and decentralized cryptographic tokens has introduced a profound paradigm shift in global monetary history.[3] By eliminating trusted intermediaries and enabling programmatic, peer-to-peer transfers of value across borders, private cryptocurrencies challenge the state's historical monopoly over the issuance of currency, the collection of seigniorage, and the enforcement of macroeconomic controls.

For an emerging market economy like India, this digital revolution presents an intricate regulatory paradox. On one hand, India boasts a highly sophisticated digital ecosystem, driven by pioneering initiatives in Digital Public Infrastructure (DPI) such as the Unified Payments Interface (UPI).[4] This backdrop has fostered a massive, tech-savvy population eager to participate in decentralized finance (DeFi) markets. On the other hand, the cross-border fluidity, high volatility, and structural anonymity inherent in private cryptoassets pose severe threats to capital control regimes, tax compliance, and monetary policy transmission channels.

The response from Indian authorities has evolved from early skepticism and administrative restrictions to a comprehensive, multi-pronged containment and substitution strategy. Rather than enacting a singular, comprehensive statutory act to explicitly legalize or ban digital assets, the Indian state has built a strict regulatory perimeter. This framework is formed by combining stringent tax policies, anti-money laundering compliance requirements, and traditional central banking directives. Simultaneously, the Reserve Bank of India (RBI) has developed the Digital Rupee (e₹) as a state-controlled alternative designed to capture the structural efficiencies of tokenization while protecting sovereign interests.

---

[1] Assistant Professor (Selection Grade), UPES, School of Law, Dehradun.

[2]Grijalva-Salazar, R. V. (2025). Bridging Regulation and Innovation: A Systematic Review of Cryptocurrency Taxation and Fiscal Policy (2020–2025). MDPI Journal of Risk and Financial Management, 18(12), 720–738. https://www.mdpi.com/1911-8074/18/12/720

[3]Raza, H. (2026). CBDC vs Cryptocurrency: A Comparative Review of Sovereign versus Decentralized Virtual Currencies. EconStor Research Paper Series, 1–34.

[4]Sankritik, A. (2025). Digital Public Infrastructure: Setting Standards with the Hourglass Model. The World Bank Development Report Compendium, 1–28.

This paper provides a detailed legal and economic analysis of this regulatory configuration. Section 2 examines the history of legal uncertainty in India, tracking the journey from administrative bans to judicial oversight and partial regulatory capture. Section 3 evaluates the systemic risks to financial stability that drive the central bank's restrictive stance. Section 4 explores how the interplay between cryptoasset containment and CBDC development serves as a core tool for preserving India's digital sovereignty. Finally, Section 5 discusses the long-term structural implications of this approach for innovation, consumer protection, and state control.

2. The Landscape of Legal Uncertainty and Judicial Intervention

2.1 The Early Administrative Bans and the IAMAI Landmark Ruling

The foundational architecture of cryptocurrency regulation in India was initially shaped by executive and administrative actions rather than statutory legislation. Prior to formalizing a cohesive legislative stance, the state's approach was characterized by systemic risk aversion. Following a series of public advisories issued between 2013 and 2017 warning retail investors of the operational, legal, and economic risks associated with virtual currencies, the Reserve Bank of India (RBI) enacted its most aggressive administrative intervention. On April 6, 2018, the central bank issued its historic Circular No. RBI/2017-18/154.[5]

This administrative directive prohibited all entities regulated by the RBI—including scheduled commercial banks, cooperative banks, non-banking financial companies (NBFCs), and payment system operators—from providing banking rails, clearing services, or maintaining accounts for any individual or business entity dealing with or settling virtual currencies. By cutting off the interface between crypto-asset service providers and the domestic banking system, the circular effectively choked off fiat-to-crypto on-ramps and off-ramps. This institutional blockade forced a severe contraction in domestic trading volumes, crippled local venture inflows, and pushed market participants toward decentralized, peer-to-peer (P2P) trading structures and offshore jurisdictions.

This regulatory blockade was subsequently challenged before the Supreme Court of India in the landmark case *Internet and Mobile Association of India (IAMAI) v. Reserve Bank of India* (2020) 10 SCC 274.[6] The petitioners, comprising domestic cryptocurrency exchanges, software developers, and retail traders, mounted a multi-layered constitutional challenge. They argued that the RBI's circular represented an arbitrary, colorable, and disproportionate exercise of administrative power.

The core of the petitioners' case rested on two primary constitutional pillars:

Article 19(1)(g): They contended that the absolute denial of banking access completely destroyed their business models, thereby violating their fundamental right to practice any profession or carry on any occupation, trade, or business. They argued that while the state can impose "reasonable restrictions" under Article 19(6), a total prohibition via an administrative circular—in the absence of an express Parliamentary statute declaring cryptocurrencies illegal—was unconstitutional.

Article 14: The petitioners asserted a violation of the right to equality and protection against arbitrariness. They argued that the RBI lacked an empirical, evidence-based foundation showing actual, quantifiable harm caused by virtual currencies to the regulated banking system, making the blanket ban a knee-jerk reaction rather than a reasoned regulatory response.

In its detailed judgment delivered in March 2020, a three-judge bench of the Supreme Court utilized the constitutional doctrine of proportionality to set aside the RBI circular.[7] The Court extensively evaluated the statutory boundaries of central banking power. It acknowledged that under the Banking Regulation Act, 1949, the Reserve Bank of India Act, 1934, and the Payment and Settlement Systems Act, 2007, the RBI possesses expansive, plenary powers to manage monetary stability, credit markets, and payment infrastructures. The Court explicitly rejected the petitioners' argument that the RBI had no jurisdiction over virtual assets, ruling that if an

[5]Reserve Bank of India. Circular No. RBI/2017-18/154, dated April 6, 2018. The circular directed all RBI-regulated entities to stop dealing with virtual currencies.

[6]Internet and Mobile Association of India v. Reserve Bank of India, (2020) 10 SCC 274. The Supreme Court struck down the 2018 RBI circular applying the doctrine of proportionality.

[7]The three-judge bench applied the proportionality doctrine derived from Modern Dental College & Research Centre v. State of Madhya Pradesh, (2016) 7 SCC 353 and further developed in K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

unregulated instrument reacts with or threatens the formal monetary system, the RBI is fully empowered to intervene.

However, the Court ruled that the *manner* of the intervention failed the strict test of proportionality. Under Indian jurisprudence, for an administrative action to be proportionate, it must adopt the least restrictive means necessary to achieve its legitimate objective. The bench emphasized that the RBI had failed to demonstrate any direct, measurable empirical damage suffered by its regulated commercial banks or the broader financial ecosystem due to cryptocurrency activities prior to issuing the circular.

Crucially, the Court observed that the RBI had consistently maintained that virtual currencies were not banned by law in India. Therefore, completely denying banking access to an otherwise lawful business activity was an excessively harsh measure that amounted to a fatal blow. The Supreme Court pointed out that less restrictive alternatives—such as introducing rigorous identity verification, strict transaction caps, enhanced due diligence, or conditional banking windows—should have been systematically explored and tested before resorting to a total financial cutoff. By striking down the circular, the *IAMAI* judgment established a vital legal precedent: while the central bank holds vast regulatory authority over macroeconomic security, its enforcement mechanisms must be anchored in empirical necessity and balanced against constitutionally protected economic freedoms.

2.2 The Shift to Anti-Money Laundering Frameworks (PMLA)

While the Supreme Court's *IAMAI* ruling restored nominal banking access to the cryptoasset ecosystem, it did not resolve the broader, systemic question of statutory legality, asset classification, or administrative oversight. Instead of introducing a dedicated, standalone virtual assets bill to govern the sector, the Government of India chose an alternative regulatory path: utilizing its existing, powerful statutory frameworks to bring the entire sector under strict state surveillance and accountability. The most significant legislative step toward formalizing accountability occurred on March 7, 2023, when the Ministry of Finance issued a notification extending the provisions of the Prevention of Money Laundering Act, 2002 (PMLA) to the virtual digital asset (VDA) ecosystem.[8]

Under this sweeping framework, entities operating as Virtual Digital Asset Service Providers (VDASPs)—including centralized cryptocurrency exchanges, custodian wallet providers, peer-to-peer (P2P) trading platforms, and digital asset marketplaces—were formally designated as "Reporting Entities" under Section 2(1)(wa) of the PMLA.[9] This classification completely dismantled the historical pseudonymity and regulatory isolation of the domestic crypto ecosystem, subjecting it to the same strict operational requirements as commercial banks, financial institutions, and stock brokerages.

The designation as a Reporting Entity imposes a comprehensive, non-negotiable matrix of statutory obligations on cryptocurrency service providers. These obligations can be broken down into three core operational layers:

A. Enhanced Customer Due Diligence (KYC Compliance): Under Section 11A of the PMLA and the associated Maintenance of Records Rules, VDASPs are legally required to mandate rigorous customer onboarding via Know Your Customer (KYC) verification protocols. Before an individual or corporate entity can open an account, execute a trade, or deposit/withdraw assets, platforms must verify their true identity using biometric Aadhaar authentication, Permanent Account Number (PAN) validation, and corporate registration documents. This statutory layer completely eliminates unverified, anonymous trading accounts within domestic boundaries.[10]

B. Comprehensive Audit Trails and Record Keeping: Under Section 12 of the Act, every reporting entity must maintain an unalterable, comprehensive record of all transactions—including the nature, value, currency, and parties involved—for a minimum statutory period of five years from the date of the transaction.[11] Additionally, client identity records and account files must be preserved for five years after the business relationship has ended.

---

[8]Ministry of Finance, Government of India. (2023). Notification on Application of the Prevention of Money Laundering Act, 2002 to Virtual Digital Assets, S.O. 1074(E), dated March 7, 2023.

[9]Prevention of Money Laundering Act, 2002, Section 2(1)(wa), as amended by the Finance Act, 2023. See also PMLA (Maintenance of Records) Rules, 2005, Rule 3.

[10]Prevention of Money Laundering Act, 2002, Section 11A read with PMLA (Maintenance of Records) Rules, 2005. Aadhaar-based KYC is additionally governed by the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

[11]Prevention of Money Laundering Act, 2002, Section 12. The five-year retention period aligns with FATF Recommendation 11 on record keeping obligations for financial institutions.

C. Mandatory Reporting of Suspicious Activities: VDASPs are legally bound to monitor transactional behavior continuously and file Suspicious Transaction Reports (STRs) and Cash Transaction Reports (CTRs) directly to the Financial Intelligence Unit-India (FIU-Ind). Under the PMLA guidelines, any transaction that lacks apparent economic rationale, involves unusually high values, or suggests potential links to predicate offenses must be reported within a strict window, typically seven days of forming a suspicion.[12]

The strict enforcement and structural impact of this framework became clear in late 2023 and early 2024. In December 2023, FIU-India issued compliance show-cause notices to nine prominent offshore cryptocurrency exchanges for operating within the Indian market and serving domestic users without registering under the domestic AML framework.[13] Because these platforms had failed to comply with the statutory provisions of the PMLA, the Ministry of Electronics and Information Technology (MeitY), acting on FIU-India's recommendations, placed administrative URL and domain blocks on their web portals and removed their mobile applications from major app stores within Indian jurisdiction. This enforcement action marked a structural turning point for the industry.

Consequently, by integrating VDAs into the PMLA framework, the state achieved two major goals: it aligned its domestic digital asset market with the international compliance standards established by the Financial Action Task Force (FATF),[14] and it shifted the legal status of cryptocurrency from an unmonitored digital asset into a highly scrutinized, visible financial ecosystem where anonymity is no longer a viable feature.

2.3 The Complexities of Categorization: Commodity vs. Currency

A core driver of continued legal uncertainty in India is the lack of a standardized, singular statutory definition for cryptoassets across different regulatory bodies. Instead of establishing a cohesive, uniform classification, different state authorities view digital assets through separate lenses tailored to their specific regulatory mandates. This fragmented approach has led to a split legal environment where the same cryptographic token is categorized as property for tax collection, scrutinized as a potential financial security, and completely rejected as a valid currency.

Regulatory Body / Authority	Framework / Legislation	Asset Categorization	Primary Policy Focus
Reserve Bank of India (RBI)	RBI Act, 1934	High-risk private token (Not recognized as money)	Systemic stability, preserving the sovereign payment monopoly.
Ministry of Finance (CBDT)	Income Tax Act, 1961 (Sec 2(47A))	Virtual Digital Asset (VDA)	Fiscal capture, tracking wealth accumulation, preventing tax evasion.
Securities and Exchange Board of India (SEBI)	Securities Contracts (Regulation) Act, 1956	Hybrid utility/derivative (Proposed)	Protecting retail investors, managing market manipulation risks.

[12]Prevention of Money Laundering Act, 2002, Sections 12 and 13. The Financial Intelligence Unit–India (FIU-IND) operates under the Department of Revenue, Ministry of Finance.

[13]Financial Intelligence Unit–India (FIU-IND). (2023). Show-Cause Notices to Offshore Virtual Digital Asset Service Providers. The nine exchanges included Binance, Kraken, and others. See also Ministry of Electronics and Information Technology (MeitY) blocking orders issued in January 2024.

[14]Financial Action Task Force (FATF). (2021). Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. Paris: FATF. The 2023 PMLA amendment brought India into formal compliance with FATF Recommendation 15.

The Reserve Bank of India maintains that private cryptocurrencies cannot be classified as valid currency or legal tender under the Reserve Bank of India Act, 1934.[15] The central bank's legal reasoning is built on the premise that currency must be backed by a sovereign issuer and represent a direct financial liability of the state. In contrast, the Ministry of Finance's Central Board of Direct Taxes (CBDT) created a pragmatic fiscal category via the Finance Act, 2022, introducing Section 2(47A) into the Income Tax Act, 1961.[16] Concurrently, the Securities and Exchange Board of India (SEBI) has expressed caution regarding the classification of specific utility and governance tokens under the Securities Contracts (Regulation) Act, 1956,[17] as fitting a decentralized, autonomous organization (DAO) into its traditional legal structures remains highly problematic. This lack of a uniform statutory definition prevents the development of stable corporate compliance structures, leaves consumers vulnerable to platform insolvencies, and creates continuous friction between the flexible nature of decentralized networks and the compartmentalized jurisdictions of sovereign regulatory bodies.

3. Macroeconomic Risks and Systemic Threats to Financial Stability

3.1 Capital Flight and Violations of FEMA

The RBI's cautious stance on private cryptocurrencies is rooted in structural concerns regarding India's macroeconomic balance, specifically the management of its capital account. Under the Foreign Exchange Management Act, 1999 (FEMA), India maintains a highly calibrated capital account regime.[18] While current account transactions are largely liberalized, capital account convertibility remains tightly regulated to protect the domestic economy from sudden capital flight, exchange rate shocks, and speculative attacks on the Indian Rupee (INR).

Private cryptocurrencies create alternative, parallel networks for cross-border capital movement that operate entirely outside these authorized banking channels. By utilizing decentralized stablecoins pegged to foreign currencies or public asset ledgers, individuals can shift large amounts of domestic wealth into offshore digital wallets. This process bypasses the caps established by the RBI's Liberalised Remittance Scheme (LRS) and circumvents reporting requirements managed by Authorized Dealer (AD) banks. This structural bypass poses a direct threat to the state's capacity to monitor its balance of payments. If a significant share of domestic savings shifts into cross-border, private digital assets, it limits the central bank's ability to track foreign exchange reserves, manage capital accounts during macro-shocks, and enforce compliance with foreign asset disclosure laws under the Black Money Act of 2015.

3.2 Risks to Monetary Policy Transmission and Seigniorage

The widespread adoption of private cryptocurrencies within a domestic economy can lead to a phenomenon known as "crypto-ization"—the gradual substitution of the sovereign domestic currency with digital private assets for transactions, savings, and accounting purposes.[19] In emerging market economies, crypto-ization presents a severe risk to the transmission of monetary policy. When commercial banks lose deposit volume to decentralized stablecoins or digital asset pools, the central bank's ability to steer liquidity and control inflation via policy rates—such as the Repo Rate under the Reserve Bank of India Act—becomes compromised.

Furthermore, crypto-ization directly threatens a key source of central bank revenue: seigniorage—the economic profit generated by issuing currency, calculated as the difference between the face value of money and its actual production cost. When physical notes or traditional digital bank deposits are replaced by private cryptographic

[15]Reserve Bank of India Act, 1934, Sections 3 and 26. The RBI's core argument is that private cryptoassets fail the legal tender test as they are not backed by sovereign guarantee or state liability. See RBI Annual Report 2022–23, Chapter V.

[16]Income Tax Act, 1961, Section 2(47A), as inserted by the Finance Act, 2022 (No. 6 of 2022). The VDA definition was deliberately broad to capture future asset classes without requiring legislative amendment.

[17]Securities Contracts (Regulation) Act, 1956, Section 2(h). For a comparative analysis of how the Howey Test under U.S. securities law might apply to Indian token structures, see Reddy, J. (2019). The Case for Regulating Crypto-Assets. Indian Journal of Law and Technology, 15, 1–34. https://doi.org/10.55496/gigz6133

[18]Foreign Exchange Management Act, 1999, Sections 6 and 10. The Liberalised Remittance Scheme (LRS), administered under FEMA, permits Indian residents to remit up to USD 250,000 per financial year for permissible capital and current account transactions only.

[19]Reserve Bank of India. (2023). Annual Report 2022–23. The RBI has repeatedly flagged crypto-ization risks in its Financial Stability Reports, particularly FSR December 2021 and FSR June 2023.

tokens, this seigniorage wealth shifts from the state to private, often foreign, network issuers and protocol developers. This shift reduces the fiscal surplus that the central bank can transfer annually to the sovereign government, creating structural imbalances in public finance management.

3.3 The Fragility of the Crypto Ecosystem and Cyber-Enabled Financial Risks

The structural volatility and operational vulnerability of the broader cryptoasset market amplify these systemic risks. Traditional financial systems rely on institutional backstops, clearinghouses, and lender-of-last-resort facilities to manage liquidity runs and credit shocks. The decentralized finance ecosystem possesses no such structural stabilizers. The systemic vulnerabilities of the private digital asset ecosystem are driven by three main factors:

De-Pegging of Stablecoins: Stablecoins function as the primary liquidity bridge between traditional fiat currencies and volatile cryptoassets. However, empirical analysis shows that their stability is fragile, with a significant percentage of stablecoins experiencing de-pegging events and failing to sustain their target value over time.[20] The collapse of algorithmic or under-collateralized stablecoins can trigger rapid contagion across digital asset markets.

Asset-Currency Conflict and Behavioral Volatility: Retail adoption of cryptocurrencies is often driven by speculative motives rather than transactional utility, leading to a structural asset-currency conflict.[21] Price fluctuations trigger valuation anxiety and transaction hesitations, making these assets highly unstable for domestic retail commerce and limiting their utility primarily to speculative cross-border settlements.

Cyber-Enabled Fraud and Exploits: The financial sector has seen an escalation in digital fraud and crypto-related cyber events over the past decade.[22] Without institutional verification layers, public blockchain smart contracts are vulnerable to code exploits, flash-loan attacks, and malicious hacks. When a decentralized protocol is compromised, the transaction irreversibility inherent in cryptographic ledgers means retail investors have no formal statutory recourse or recovery mechanisms.

4. Digital Sovereignty and the State's Containment Strategy

4.1 The Fiscal Perimeter: The Taxation Framework of the Finance Acts

Recognizing that a direct administrative ban faced significant constitutional hurdles following the *IAMAI* ruling, the Government of India implemented a rigorous fiscal strategy via the Finance Act, 2022, introducing Section 115BBH[23] and Section 194S[24] into the Income Tax Act, 1961. This framework created a highly restrictive tax environment for digital assets:

Provision / Section	Tax Treatment / Rule	Key Implication
Flat Income Tax Rate (Sec 115BBH)	30% tax on all positive transfer revenues from VDAs.	High fixed taxation on crypto gains.

[20]Dávalos-Mayorga, E. R. (2026). Stablecoins: financial risks, vulnerabilities, and implications for the future internet — a systematic review. Frontiers in Blockchain, 9(1797659), 1–14. Empirical data from this study shows that a significant percentage of algorithmic stablecoins have failed to maintain their pegs over sustained periods.
[21]Dharumaiyan, A. (2026). Assessing the Viability of Cryptocurrency as a Payment Method: A Consumer Perspective. Doctoral Dissertation, National Louis University, 1–112. The dissertation identifies a structural asset-currency conflict in retail crypto adoption patterns.
[22]Khiaonarong, T., & Shanyuan, Z. (2026). The Rise of Cyber Events and Digital Fraud in the Financial Sector. IMF Working Paper, WP/26/62, 1–45. The paper documents an increase in sophisticated exploit attacks on DeFi protocols.
[23]Income Tax Act, 1961, Section 115BBH, as inserted by the Finance Act, 2022. The 30% flat rate applies regardless of the taxpayer's income slab and without benefit of the basic exemption limit.
[24]Income Tax Act, 1961, Section 194S, as inserted by the Finance Act, 2022. TDS is deductible at 1% by the buyer/exchange on transactions exceeding ₹10,000 per financial year (₹50,000 for specified persons). This created automatic reporting infrastructure.

Loss Offsets & Deductions	Strictly prohibited except for cost of acquisition/purchase.	No deduction of mining, trading, or operational expenses.
Cross-Asset Loss Offsets	Prohibited — losses in one token/asset cannot offset gains in another.	Each VDA taxed independently.
Tax Deducted at Source (Sec 194S)	1% TDS on transactions exceeding the prescribed threshold.	Creates a continuous fiscal audit trail and improves transaction monitoring.

This combination of a flat 30% tax, no loss offsets, and a 1% TDS on every transaction created a highly restrictive fiscal perimeter. The 1% TDS requirement, in particular, turned digital asset exchanges into decentralized tax collection hubs. It forced the institutional recording of every trade, giving the Central Board of Direct Taxes a comprehensive, real-time ledger of domestic digital asset flows. From a policy perspective, this design was intentionally severe. By eliminating the economic incentives for high-frequency day trading and speculative arbitrage, the state successfully reduced speculative domestic volumes, redirected domestic capital back into traditional regulated equities, and contained the growth of private crypto markets without enacting an explicit legal ban.

4.2 The Substitution Strategy: The Digital Rupee (e₹) CBDC

The second core component of India's digital sovereignty strategy is a structural substitution model: replacing private, unregulated cryptoassets with a sovereign alternative. Under the authority of the Finance Act, 2022, which amended the Reserve Bank of India Act, 1934,[25] the RBI launched its pilot projects for the Digital Rupee (e₹) Central Bank Digital Currency (CBDC) in late 2022,[26] expanding it into a core operational priority by 2026. The Digital Rupee is structured across two distinct functional layers:

Wholesale CBDC (e₹-W): Positioned to optimize interbank settlements, wholesale tokenization reduces reliance on traditional clearing arrangements, lowers counterparty risks, and improves efficiency in the secondary market settlement of government securities.

Retail CBDC (e₹-R): Designed as a digital alternative to physical cash, the retail CBDC represents a direct, non-remunerated liability of the Reserve Bank of India, held in digital tokens within wallets provided by authorized commercial banks.

Institution	Category	Purpose / Function
Reserve Bank of India (RBI)	Wholesale e₹ (e₹-W)	Used for interbank settlements and sovereign security clearing.
Reserve Bank of India (RBI)	Retail e₹ (e₹-R)	Functions as a sovereign cash equivalent for household and retail utility.

From an architectural standpoint, the Digital Rupee utilizes distributed ledger technology (DLT) in a controlled, permissioned environment. Unlike public networks like Ethereum or Bitcoin, where consensus is maintained by decentralized, pseudo-anonymous validators, India's CBDC ledger is governed entirely by the central bank. This architecture allows the state to leverage the technical benefits of tokenization—such as instant settlement finality

[25]Reserve Bank of India Act, 1934, Section 22, as amended by the Finance Act, 2022 (clause 1 of the Act). The amendment inserted a definition of 'bank notes' that enables the RBI to issue CBDCs as legal tender.

[26]Reserve Bank of India. (2022). Concept Note on Central Bank Digital Currency (CBDC). Department of Payment and Settlement Systems. The wholesale pilot (e₹-W) launched in November 2022 and the retail pilot (e₹-R) in December 2022.

and programmatic compliance—while retaining full control over supply, ledger access, and transactional visibility. This approach effectively protects sovereign currency systems from the risks of private crypto-ization.[27]

4.3 Data Localisation and National Security

Preserving digital sovereignty requires strict control over financial data infrastructure. The RBI's directives on Storage of Payment System Data (2018) mandate that all electronic payment transaction data must be stored exclusively on physical servers located within the political boundaries of India.[28] If transactions are processed offshore, the underlying data must be permanently purged from foreign databases and brought back to domestic storage within 24 hours.

Private, public-permissionless blockchains operate on decentralized consensus networks where transaction ledgers are copied globally across thousands of independent nodes. This structure makes compliance with data localization mandates and privacy frameworks like the Digital Personal Data Protection (DPDP) Act, 2023,[29] technically impossible. By pushing transactions toward permissioned sovereign ledgers (e₹) and enforcing PMLA reporting on local exchanges, India ensures that its financial intelligence agencies maintain unimpeded access to financial data. This monitoring capability is vital for detecting illicit trade networks, preventing terrorist financing, and defending national security interests against asymmetric digital threats.

5. Structural Implications and the Path Forward

5.1 The Cost of the Compliance Perimeter on Innovation

While India's strategy has effectively contained speculative risks, it has also introduced notable structural challenges for the domestic technology sector. The combination of high tax rates, strict AML reporting requirements, and limited access to traditional banking rails has created a demanding environment for domestic web3 startups, software engineers, and blockchain developers.

This strict regulatory environment has led to a "brain drain" of capital and talent from India to jurisdictions with more accommodative frameworks, such as Dubai (Virtual Assets Regulatory Authority - VARA) and Singapore (Monetary Authority of Singapore - MAS).[30] Indian entrepreneurs frequently set up their holding companies, intellectual property, and primary development teams offshore to avoid domestic regulatory uncertainties. Consequently, while India remains a major provider of global blockchain engineering talent, much of the economic value, equity generation, and intellectual property in the web3 space is being realized in offshore jurisdictions.

5.2 The Regulatory Vacuum in Consumer Protection

The current regulatory model—which relies primarily on tax policy and anti-money laundering enforcement—leaves notable gaps in proactive consumer protection. Because India lacks a dedicated statutory regulator for digital assets, retail investors have limited legal recourse when platforms face insolvency, operational outages, or deceptive marketing practices.

Currently, consumer grievances are managed through general consumer protection frameworks or the advertising guidelines issued by the Advertising Standards Council of India (ASCI), which require mandatory risk disclaimers

[28]Reserve Bank of India. (2018). Circular on Storage of Payment System Data, RBI/2017-18/131. The directive mandates that data related to payment systems must be stored only in India. Non-compliance can attract penalties under the Payment and Settlement Systems Act, 2007.

[29]Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023). The Act creates a framework for the processing of digital personal data within India and applies to data processed outside India if it involves profiling of Indian data principals.

[30] Ahmad, T. (2025). Regulatory Challenges of Crypto-currency (Bitcoin) in India: Legal and Financial Perspectives. Atlantis Press Financial Law Series, 325–339. https://www.atlantis-press.com/article/126019777.pdf. The paper documents the regulatory arbitrage leading to capital and talent migration to Dubai's VARA and Singapore's MAS frameworks.

on VDA promotions.[31] However, these measures do not address complex technical risks, such as exchange insolvency, the commingling of client and corporate assets, or market manipulation on local trading desks. The lack of a clear regulatory authority means that while investors are heavily taxed on their gains, they operate without the structural protections, deposit insurance, and market oversight standard in traditional equity and commodity markets.

5.3 The G20 Synthesis Paper and the Path to Global Harmonization

Recognizing that the decentralized and cross-border nature of private cryptoassets makes unilateral domestic bans or isolated regulatory regimes ineffective, India used its G20 Presidency to champion the creation of an international consensus framework. This effort resulted in the adoption of the G20 Crypto Risk Roadmap, which was guided by a joint Synthesis Paper produced by the International Monetary Fund (IMF) and the Financial Stability Board (FSB).[32]

The IMF-FSB Synthesis Paper outlines clear policy guidelines that explicitly discourage member states from enacting blanket, uncoordinated bans on cryptocurrency activities. Instead, it advocates for an integrated regulatory strategy built on macroeconomic safeguards—implementing clear monetary and fiscal protections to shield emerging market economies from capital flight—and comprehensive regulatory standards applying uniform oversight that subjects VDAs to strict AML and countering the financing of terrorism (CFT) baselines.[33]

For India, this international roadmap provides a structured path toward a comprehensive domestic framework. Moving forward, India's regulatory model is expected to transition from its current system of isolated fiscal controls toward an integrated, statutory registration and supervisory framework. This evolution will likely involve assigning specific market oversight duties to an existing independent regulator, such as SEBI or the RBI, or establishing a dedicated digital assets authority.

6. Conclusion

India's approach to cryptocurrency regulation reflects a calculated policy model focused on containing private digital asset risks while advancing sovereign alternatives. By establishing strict boundaries through the Prevention of Money Laundering Act and implementing a rigorous taxation framework under the Finance Acts, the state has managed to limit speculative retail investment, maintain its capital account protections, and reduce potential vulnerabilities within its traditional financial architecture.

However, this strategy of regulatory containment introduces its own structural trade-offs. The persistent lack of a unified statutory law creates an ambiguous environment for businesses, impacts domestic technological innovation, and leaves retail investors without clear consumer protections. Concurrently, the rollout of the Digital Rupee demonstrates a commitment to using the operational efficiencies of tokenization to reinforce, rather than replace, central monetary authority.

As international regulatory standards align around the IMF-FSB Synthesis Paper, India faces the task of evolving its approach from a system of protective measures into a mature statutory framework. To secure its financial stability and digital sovereignty in the long term, the state must eventually move beyond a policy of containment. The path forward will require enacting comprehensive legislation that provides clear asset definitions, establishes firm market rules, protects consumers, and encourages sustainable technological development within a well-regulated framework.

India's evolving stance on cryptocurrency regulation represents a highly deliberate policy model. Rather than enacting an outright statutory prohibition—which would face significant constitutional hurdles under Article

---

[31] Advertising Standards Council of India (ASCI). (2022). Guidelines for Advertising of Virtual Digital Assets and Related Services. The guidelines require a mandatory disclaimer: 'Crypto products and NFTs are unregulated and can be highly risky.'

[32] Financial Stability Board (FSB) & International Monetary Fund (IMF). (2023). IMF-FSB Synthesis Paper: Policies for Crypto-Assets. G20 Leadership Series. The paper was formally adopted by G20 Leaders at the New Delhi Summit in September 2023.

[33] AlQudah, M. Z. (2025). Systematic and bibliometric reviews of cryptocurrency market regulation: trends, influential contributions, and future directions. Journal of Financial Regulation. https://www.emerald.com/jfrc/article/34/1/1/1252779. The study identifies a global convergence toward AML-CFT based regulatory frameworks.

19(1)(g) and drive transactions into unmonitored shadow markets—the state has constructed a sophisticated containment and substitution strategy. This approach uses existing legal, fiscal, and central banking frameworks to restrict private digital innovations while clearing a path for state-controlled alternatives.

By establishing a strict administrative perimeter through the Prevention of Money Laundering Act (PMLA) and designating service providers as Reporting Entities, the state has eliminated the anonymity of decentralized networks. Simultaneously, the rigorous fiscal framework—specifically the combination of a flat 30% tax under Section 115BBH, the prohibition of loss offsets, and the 1% Tax Deducted at Source (TDS) mechanism under Section 194S—has successfully altered the economic incentives of the market. However, this strategy introduces significant long-term structural trade-offs in innovation, consumer protection, and the tension between sovereign tokenization and decentralization principles.

The path forward requires enacting a comprehensive, standalone legislative framework. This statute must provide clear legal definitions differentiating utility tokens, governance tokens, and stablecoins, establish firm rules for exchange operations, institute clear consumer protection mechanisms, and build an adaptable framework for technological growth. Only by replacing legal ambiguity with a balanced statutory architecture can India protect its macroeconomic environment while capturing the economic and technical benefits of the global decentralized digital economy.

References

[1] Ahmad, T. (2025). Regulatory Challenges of Crypto-currency (Bitcoin) in India: Legal and Financial Perspectives. Atlantis Press Financial Law Series, 325–339. https://www.atlantis-press.com/article/126019777.pdf

[2] AlQudah, M. Z. (2025). Systematic and bibliometric reviews of cryptocurrency market regulation: trends, influential contributions, and future directions. Journal of Financial Regulation. https://www.emerald.com/jfrc/article/34/1/1/1252779/Systematic-and-bibliometric-reviews-of

[3] Bailey, R., & Parsheera, S. (2018). Data Localisation in India: Questioning the Means and Ends. NIPFP Working Paper Series / SSRN Electronic Journal, 242, 1–32. https://doi.org/10.2139/ssrn.3356617

[4] Central Board of Direct Taxes (CBDT), Ministry of Finance, Government of India. The Finance Act, 2022. Gazette of India.

[5] Dávalos-Mayorga, E. R. (2026). Stablecoins: financial risks, vulnerabilities, and implications for the future internet — a systematic review. Frontiers in Blockchain, 9(1797659), 1–14.

[6] Dharumaiyan, A. (2026). Assessing the Viability of Cryptocurrency as a Payment Method: A Consumer Perspective. Doctoral Dissertation, National Louis University, 1–112.

[7] Financial Stability Board (FSB) & International Monetary Fund (IMF). (2023). IMF-FSB Synthesis Paper: Policies for Crypto-Assets. G20 Leadership Series.

[8] Grijalva-Salazar, R. V. (2025). Bridging Regulation and Innovation: A Systematic Review of Cryptocurrency Taxation and Fiscal Policy (2020–2025). MDPI Journal of Risk and Financial Management, 18(12), 720–738. https://www.mdpi.com/1911-8074/18/12/720

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

[10] Khiaonarong, T., & Shanyuan, Z. (2026). The Rise of Cyber Events and Digital Fraud in the Financial Sector. IMF Working Paper, WP/26/62, 1–45.

[11] Ministry of Finance, Government of India. (2023). Notification on Application of the Prevention of Money Laundering Act, 2002 to Virtual Digital Assets, S.O. 1074(E).

[12] Raza, H. (2026). CBDC vs Cryptocurrency: A Comparative Review of Sovereign versus Decentralized Virtual Currencies. EconStor Research Paper Series, 1–34.

[13] Reddy, J. (2019). The Case for Regulating Crypto-Assets. Indian Journal of Law and Technology, 15, 1–34. https://doi.org/10.55496/gigz6133

[14] Reserve Bank of India. (2018). Circular on Storage of Payment System Data, RBI/2017-18/131.

[15] Reserve Bank of India. (2022). Concept Note on Central Bank Digital Currency (CBDC). Department of Payment and Settlement Systems.

[16] Sankritik, A. (2025). Digital Public Infrastructure: Setting Standards with the Hourglass Model. The World Bank Development Report Compendium, 1–28.

[17] Wang, J. (2026). Influencing factors and mechanisms of action on the participation intentions of cryptocurrency investment fraud victims. PubMed Central (PMC). https://pmc.ncbi.nlm.nih.gov/articles/PMC12935255/