



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

BLOCKCHAIN TECHNOLOGY AND LAW: OVERVIEW OF THE EMERGING LEGAL AND REGULATORY FRAMEWORK IN INDIA

~ Niharika Uniyal

I. INTRODUCTION

Blockchain technology is a distributed, tamper-proof ledger system that records transactions across a decentralized network of nodes. It has rapidly moved from financial experimentation to the forefront of national policy debate. While the technology first gained public attention as the infrastructure supporting Bitcoin, its applications have since expanded to supply chains, land records, judicial documentation, healthcare and governance. For India, a country concurrently grappling with digital transformation ambitions and regulatory caution, blockchain presents a dual challenge, harnessing its transformative potential while constructing a clear legal architecture capable of addressing its novel risks.

India's legal response to blockchain has been neither uniform nor comprehensive. Instead, it has proceeded in fragments, through taxation legislation, anti-money laundering notifications, judicial observations on electronic evidence and ministerial strategy documents. The Ministry of Electronics and Information Technology (MeitY) released a National Strategy on Blockchain in 2021, laying out a vision for deploying blockchain across forty-four identified sectors.¹ Building upon this, the government formally launched the National Blockchain Framework (NBF) in September 2024, with a budgetary allocation of ₹64.76 crore, providing indigenous, modular Blockchain-as-a-Service (BaaS) infrastructure deployed across National Informatics Centre (NIC) data centres.² Yet, despite this institutional momentum, India continues to lack a

¹Ministry of Electronics and Information Technology (MeitY), National Strategy on Blockchain (2021).

²National Blockchain Framework, MeitY (Sept. 4, 2024). [Home - National Blockchain Framework](#)

combined blockchain law and a series of critical legal questions relating to smart contracts, evidence admissibility, data protection and virtual asset regulation, remain only partially resolved.

II. THE GOVERNING LEGAL FRAMEWORK

India does not possess a dedicated blockchain statute. Instead, the technology is regulated through a variety of existing laws whose applications to distributed ledger technology are often imperfect. Scholars have identified this as a significant structural gap: Indian law urgently needs to confirm that smart contracts carry legal effect and to establish a specialized regulatory body with technical expertise.³ In the absence of bespoke legislation, practitioners and adjudicators must reason by analogy from the *Indian Contract Act, 1872*, the *Information Technology Act, 2000* (IT Act), the *Indian Evidence Act, 1872* and more recent enactments targeting virtual assets.

SMART CONTRACTS AND CONTRACT LAW

A smart contract is a self-executing program stored on a blockchain that automatically performs predefined obligations when specified conditions are satisfied. The foundational question in India is whether such arrangements qualify as valid contracts under the *Indian Contract Act, 1872*. Section 10 of that Act requires that an agreement be made by parties of free consent, competency and for a lawful consideration and object. Commentators have generally concluded that smart contracts satisfy these criteria.⁴ Furthermore, Section 10A of the IT Act explicitly recognizes the validity of contracts formed through electronic means, while Sections 3 and 4 validate digital signatures and electronic records.⁵

However, a complication persists. The IT Act requires that valid digital signatures be issued by government-designated Certifying Authorities. Blockchain-based cryptographic signatures are self-generated and thus fall outside this authorized framework.⁶ This creates a potential authentication deficit, courts asked to assess a breach of a smart contract may find themselves

³ Ajay Patel, *Advance Analyzes for Blockchain Legal Issues in India*, 24 Computer Research & Development (2024).

⁴ Vijay Pal Dalmia et al., *Blockchain and Smart Contracts – Indian Legal Status*, Mondaq (Feb. 5, 2020).

⁵ Megha Ravindranath, *Legality of Blockchain and Smart Contracts in India*, Int'l J. for Multidisciplinary Research (2024).

⁶ Shilpa J, Prajakta K, *Smart Contracts and Blockchain: Legal Issues and Implications for Indian Contract Law*, ResearchGate (Nov. 9, 2021).

unable to presume the validity of the digital mechanism through which the agreement was executed. One academic analysis drawing on comparative jurisprudence, including Arizona's legislative amendment explicitly recognizing smart contract enforceability has urged India to introduce specific statutory provisions rather than continue relying on analogical interpretation.⁷ Until such reforms arrive, smart contracts occupy an ambiguous legal space, technically valid as electronic agreements but procedurally vulnerable in judicial proceedings.

EVIDENCE LAW AND ADMISSIBILITY

Section 65B of the *Indian Evidence Act, 1872* provides for the admissibility of electronic records when accompanied by a certificate of authenticity. Blockchain data is, by design, immutable and cryptographically verifiable, properties that in principle, should, strengthen its evidentiary standing. Yet Indian courts have yet to develop a comprehensive legislation on the authentication of blockchain records. Under the *Indian Evidence Act*, courts will not presume the credibility of the sender of an electronic contract, nor will they assume that the authority verifying a digital signature is a certified agency as prescribed by the IT Act.⁸ Scholars have called for dedicated amendments to the Evidence Act that would establish simplified authentication procedures for blockchain records, acknowledging the technology's inherent integrity mechanisms while maintaining appropriate judicial oversight. The National Judicial Academy has initiated preliminary programmes on digital evidence, with plans to expand blockchain-specific judicial training.⁹

III. VIRTUAL DIGITAL ASSETS: TAXATION AND ANTI-MONEY LAUNDERING

The most significant legislative intervention to date has been the introduction of a tax regime for Virtual Digital Assets (VDAs) through the *Finance Act, 2022*. Inserting Section 115BBH into the Income Tax Act, 1961, Parliament imposed a flat 30% tax on all income arising from the transfer of VDAs, with no distinction between long-term and short-term gains and no

⁷Swati S, Sheersshadeb D, *Smart Contracts & Indian Law: Legally Binding or Technically Blind?*, International Journal of Law (2025).

⁸Bhasker Vishwajeet, *Smart Contracts and the Indian Perspective*, LIVE LAW (Mar. 28, 2022, 9:17). [Smart Contracts And The Indian Perspective](#)

⁹Ritik Agrawal, *Blockchain and Evidence Law: Legal Recognition and Admissibility Challenges in India*, Jus Scriptum Law (July 22, 2025). [Blockchain and Evidence Law: Legal Recognition and Admissibility Challenges in India](#)

allowance for deductions beyond the cost of acquisition.¹⁰ Additionally, Section 194S was introduced to mandate 1% Tax Deducted at Source (TDS) on VDA transactions, ensuring a compliance trail even when the underlying transactions are pseudonymous. Losses from VDA transfers may not be set off against other income, nor carried forward to future years, a deliberate design aimed less at regulating than to deter speculative activity while generating fiscal revenue.¹¹

Parallel to the taxation framework, the Ministry of Finance on 7 March 2023 formally extended the *Prevention of Money Laundering Act, 2002* (PMLA) to cover Virtual Digital Asset Service Providers (VDA SPs), treating them as reporting entities subject to Know Your Customer (KYC) obligations, transaction monitoring and suspicious transaction reporting to the Financial Intelligence Unit-India (FIU-IND).¹² This notification brought India's AML framework into closer alignment with Financial Action Task Force (FATF) recommendations on virtual assets. In December 2023, FIU-IND issued show-cause notices to several major international exchanges, including Binance, KuCoin, Kraken and others for operating in the Indian market without compliance registration, resulting in URL-blocking orders against non-compliant platforms.¹³ In June 2024, FIU-IND issued a detailed penalty order against Binance for operating without registration and failing to meet KYC and AML obligations, marking one of the most significant enforcement actions in India's nascent crypto regulatory history.¹⁴

IV. BLOCKCHAIN IN GOVERNANCE: POLICY AND PRACTICE

Beyond cryptocurrency, the Indian government has actively piloted blockchain technology for public administration. The NBF supports multiple operational proof-of-concept deployments. Its Property Chain maintains immutable ownership histories and has verified over 34 crore property-related documents. It also includes a GST Chain for real-time tax monitoring and a

¹⁰Finance Act, 2022, No. 6, Acts of Parliament, 2022 (India); see also Shahid Khan, *A Taxing Time for Crypto Assets*, India Business L.J. (July 5, 2022).

¹¹Neha K., Pitresh K., Shashank P., *Blockchain Technology and Legal Framework in India: A Systematic Review*, ResearchGate (Sept. 19, 2023).

¹²Prevention of Money Laundering Act, 2002, No. 15, Acts of Parliament, 2003 (India); Ministry of Finance Notification, Mar. 7, 2023 (extending PMLA to VDA service providers).

¹³Probir C., *Blockchain 2025 – India*, JSA Advocates & Solicitors (June 12, 2025). [Blockchain 2025 - India | Global Practice Guides | Chambers and Partners - JSA](#)

¹⁴FIU-IND Order against Binance (June 2024) (on file); see also Reddy K, Athif A, Aabha D, Armaan M, *Blockchain & Cryptocurrency Laws & Regulations 2026 – India*, Global Legal Insights (Oct. 21, 2025).

Judiciary Chain under ICJS, with over 39,000 judicial records and 665 documents validated on-chain. Karnataka's *Aushada* platform employs blockchain to trace pharmaceutical supply chains from manufacturer to hospital, reducing counterfeit drug risks.

MeitY has also invested significantly in institutional capacity. Over 21,000 government officials have been trained across 214 programmes in blockchain architecture, cybersecurity and governance application design. The National Informatics Centre (NIC) has established a Centre of Excellence (CoE) in Blockchain Technology, collaborating with platforms such as Hyperledger Fabric and Ethereum. The government has further introduced sandbox environments allowing startups and academic institutions to prototype blockchain applications using smart contract templates in governance domains. These initiatives reflect a careful policy of deep embedding blockchain in public infrastructure, even as the legal regime governing private blockchain-based transactions falls behind.

V. DATA PROTECTION AND THE BLOCKCHAIN PARADOX

The *Digital Personal Data Protection Act, 2023* (DPDP Act) introduces a consent-based framework for the processing of personal data, establishing rights of erasure and data portability for data principals.¹⁵ Blockchain's defining feature which is its immutability sits in structural tension with these rights. Once personal data is recorded on a public blockchain, it cannot be deleted or modified, fulfilling an erasure request becomes technically impossible without compromising the integrity of the entire chain. The DPDP Act carves out an exception for personal data that has been made publicly available by the data principal, meaning that public keys and voluntarily disclosed blockchain data may fall outside the Act's scope.¹⁶ However, this exception is narrow and does not address personal data unintentionally stored on blockchain records, including metadata that may be re-identified. Legal scholars have proposed that India adopt technical solutions such as off-chain storage of personal data with on-chain hashes or cryptographic deletion techniques like key destruction to reconcile blockchain immutability with data protection obligations.

¹⁵Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

¹⁶Sudipta S., *The necessity of data protection laws in India and the role of blockchain technology in enhancing data security and legal compliance*, International Journal of Law (2024).

VI. OUTSTANDING CHALLENGES AND THE PATH FORWARD

India's blockchain legal landscape is categorized by three interrelated flaws.

1. First, there is a jurisdictional deficit. Because blockchain transactions are borderless and decentralized, traditional notions of territorial jurisdiction sit uneasily with enforcement. The PMLA extends to VDA SPs serving Indian users, but its application to decentralized DeFi platforms without identifiable operators remains unclear.
2. Second, there is a regulatory fragmentation problem. No single authority is vested with comprehensive oversight of blockchain-based activities. The Reserve Bank of India (RBI) holds concerns about monetary policy implications. The Securities and Exchange Board of India (SEBI) has proposed a multi-regulatory framework for crypto assets and the FIU-IND exercises AML supervision. This overlapping jurisdiction, without clear demarcation, creates compliance uncertainty for industry participants.
3. Third, there is a legislative gap regarding smart contract enforceability. Courts currently rely on general contract and IT laws to resolve blockchain-related disputes, creating significant interpretive uncertainty. The Law Commission of India's forthcoming report on evidence law reform is expected to address aspects of this gap and scholars have urged that India follow the example of jurisdictions like Arizona and Wyoming in the United States, which have enacted targeted statutory provisions affirming smart contract validity.

VII. CONCLUSION

India stands at a turning point in its relationship with blockchain technology. The state has embraced the technology's potential with notable enthusiasm, embedding it in land records, judicial infrastructure, supply chains and public health logistics. Yet the legal structure necessary to govern blockchain-based private activity remains incomplete and internally inconsistent. The current approach, patching existing laws onto a technology that challenges foundational legal concepts of identity, jurisdiction and record integrity is unlikely to sustain the next generation of blockchain applications.

A comprehensive legislative response should achieve at least three objectives:

First, explicit statutory recognition of smart contracts, resolving the digital signature authentication anomaly

second, amendments to evidence law providing a clear procedural pathway for the admission of blockchain records

Third, the designation of a lead regulatory authority with technical expertise to harmonize the presently fragmented oversight of virtual assets, smart contracts and distributed ledger technology.

India's National Blockchain Framework provides an encouraging institutional foundation. The task now is to match it with a legal architecture that is equally deliberate, coherent and forward-looking.