

# INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

---

Volume 9 | Issue 3

---

2026

© 2026 International Journal of Law Management & Humanities

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

---

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact [support@vidhiaagaz.com](mailto:support@vidhiaagaz.com).

---

**To submit your Manuscript** for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to [submission@ijlmh.com](mailto:submission@ijlmh.com).

---

# Without Law: Smart Contracts, Statutory Incompatibility, and the Case for Legislative Reform under the Indian Contract Act, 1872

---

ENAKSHI MOHINI\*

## ABSTRACT

*This paper examines the enforceability of smart contracts in India, arguing that the Indian Contract Act, 1872, the Information Technology Act, 2000, and the Bharatiya Sakshya Adhiniyam, 2023 are incompatible with their code-based, self-executing architecture. Because smart contracts rely on blockchain immutability, automatic execution, and cryptographic authentication, it is unclear what Indian law requires in terms of consent, whether records may be used in court, and what should be done after a breach.*

*The paper employs a comparative doctrinal methodology to juxtapose India's legislative inaction with the United Kingdom's common law adaptability, specific U.S. state legislation, and Singapore's technology-agnostic framework. It demonstrates that these jurisdictions facilitate smart contracts without compromising legal certainty, whereas India lacks a corresponding statutory framework. The paper suggests three changes: a legal "wrapper" to tie smart contracts to ordinary contract law; a mutability-based regime for high-risk contracts to keep the courts involved in cases of fraud, mistake, or coercion; and fiduciary responsibility for oracle providers to ensure that execution triggers work. These steps are anticipated to make blockchain automation and enforceable legal protection function together in India.*

**Keywords:** Smart Contracts, Blockchain Immutability, Cryptographic Authentication, Legal Enforceability, Oracle Integration.

## I. INTRODUCTION

### A. The Research Objectives

This study pursues three objectives: to determine whether smart contract execution, in contrast to merely formal electronic contracting, complies with Indian contract doctrine at the moment of creation and performance; to determine whether blockchain evidence can be admitted in Indian courts without distorting the certification framework of Sections 63 and 65 of the Bharatiya Sakshya Adhiniyam, 2023; and to determine whether India requires explicit statutory

---

\* Author is a Student at University of Petroleum and Energy Studies, Dehradun, Uttarakhand, India.

amendment to address oracle dependence, immutable execution, and the lack of workable reversal options.

### **B. Research Questions**

The study addresses three questions. First, how do the Indian Contract Act's requirements of free consent and consensus ad idem apply to automated execution in smart contracts, particularly where performance takes place without human interaction at the time of execution? Second, given blockchain's decentralised architecture, can blockchain records used to demonstrate the creation or operation of smart contracts meet India's electronic evidence certification criteria under the BSA? Third, are the current doctrines of rescission and restitution structurally sufficient, and what legal remedy does Indian law offer when a smart contract runs irrevocably on-chain notwithstanding error, misrepresentation, or oracle error?

### **C. Research Hypothesis**

Because the legislative framework assumes human-mediated agreement, centralised evidential certification, and reversible performance, smart contracts in their current blockchain form are not entirely enforceable under Indian law. To bring Indian law into compliance with the technical architecture of smart contracts, explicit legislative modifications are required, rather than mere judicial interpretation.

### **D. Methodology**

This study examines the structural incompatibility between Indian statute law and smart contract design using a doctrinal comparative technique. Primary legal sources, including the Indian Contract Act, 1872, the Information Technology Act, 2000, the Bharatiya Sakshya Adhiniyam, 2023, and the Digital Personal Data Protection Act, 2023, are examined in relation to the technical aspects of blockchain implementation, cryptographic authentication, and oracle integration. In order to identify India's legislative deficit and develop a detailed, three-part reform proposal, this study compares India to the frameworks of the United States, Singapore, and the United Kingdom.

## **II. SMART CONTRACTS AND THE LIMITS OF EXISTING LEGAL FRAMEWORKS**

Smart contracts are programmatic contracts that execute automatically on a blockchain network. First conceptualised by Nick Szabo, who described them as digitally defined promises that include performance protocols, they operate through distributed consensus mechanisms and automatically take predetermined actions when all conditions are satisfied, without any mediator or enforcement of action after a breach. Their cryptographic design ensures

transactional integrity, immutability, and transparency of execution. Smart contracts are either purely code-based tools or hybrids of on-chain logic and traditional legal language.<sup>1</sup>

Their commercial incentive is significant: they can do away with intermediaries and enable near-instantaneous, tamper-proof execution of transactions, lowering transaction costs significantly. Nevertheless, this architecture is causing acute legal tension in India. The code is expressed in cryptographic programming languages, making contractual terms machine-executable rather than judicially interpretable.<sup>2</sup> Although the IT Act, 2000 defines an electronic contract as one concluded through electronic means in Section 10A, it does not specifically address self-executing blockchain contracts, nor the question of their enforceability. Smart contracts are thus technically functional but doctrinally ungrounded in Indian law.

By contrast, the Law Commission of the United Kingdom (2021) has found that smart legal contracts can be established under existing English law without statutory reform, and states such as Arizona and Tennessee in the United States have passed legislation treating blockchain-based contracts as legally enforceable. The analysis that follows is organised into three broad fault lines: enforceability under the Indian Contract Act, 1872; evidentiary admissibility under the Bharatiya Sakshya Adhiniyam, 2023; and the sufficiency of available statutory remedies. The eventual goal of this paper is to bridge this asymmetry through specific legislative reform.

### III. MECHANISM OF FUNCTIONING: BLOCKCHAIN TECHNOLOGY AND ITS IMPLICATIONS FOR LEGAL ENFORCEABILITY

#### A. Nodes, Consensus, and Hash Chaining

A blockchain is a distributed registry duplicated exactly across a network of participating computer nodes, each of which holds a continuously synchronised copy of the transactional record without any central administrator. A consensus algorithm determines the validity of each transaction, so that only network-wide consensus can permanently inscribe it. This decentralisation is what makes the ledger trustworthy, and at the same time it is the cause of its initial incompatibility with the law. There is no identifiable central node-operator, making it structurally impossible to meet the requirements of Sections 63 and 65 of the Bharatiya Sakshya Adhiniyam, 2023, which require certification by a responsible official. In *Arjun Panditrao*

---

<sup>1</sup>Stuart D. Levi & Alex B. Lipton, *An Introduction to Smart Contracts and Their Potential and Inherent Limitations*, HARV. L. SCH. F. ON CORP. GOVERNANCE (May 26, 2018), <https://corpgov.law.harvard.edu>; Alok Vajpeyi & Gauri Bharti, *The Enforceability of Smart Contracts in India*, MONDAQ (Dec. 13, 2019), <https://www.mondaq.com/india/contracts-and-commercial-law/874892>.

<sup>2</sup>G.A. Atiyah, Abdul Manap & Ahmed Ismael Ibrahim, *Legal Issues Faced by Smart Contracts from the Perspective of Conventional Contracts*, 16 UUM J. LEGAL STUD. 34, 34-53 (2025).

*Khotkar v. Kailash Kushanrao Gorantyal*, the Supreme Court determined this prerequisite to be non-waivable; no node in a blockchain network can satisfy it, rendering blockchain records inadmissible in Indian courts as a matter of judicial mandate.<sup>3</sup>

The cryptographic hash of every block is stored in the next, creating an immutable chain, so that any change in a single block renders all the following ones invalid at once and subsequent manipulation is computationally infeasible. This immutability is the very essence of the technology's integrity, and it therefore directly precludes the remedial architecture of the Indian Contract Act, 1872. Sections 14 to 19 give courts the power to rescind a contract where consent has been vitiated by misrepresentation, coercion, or mistake. A rescission decree against a blockchain ledger is, however, an order issued against mathematics: the executed transaction is irreversible, the transferred assets cannot be recalled, and no court order can reverse a cryptographically sealed entry.<sup>4</sup>

### **B. Smart Contract Lifecycle, Deployment, and Hyperledger Fabric**

A smart contract is written in executable code (usually in Solidity, with state variables and executable functions) that activates itself on a triggering condition. To deploy it, one must pay a computational fee (gas) in cryptocurrency, which is sent to all nodes for consensus validation and permanently written to a unique address. Upon deployment, the contract becomes unalterable and independent: it cannot be changed by any party, court, or regulator, nor undone once executed. The Indian Contract Act establishes corrective recourse, namely rescission and restitution, all of which assume a live, revocable obligation. That supposition is entirely eliminated in a smart contract once it is executed, and Indian courts have no jurisdictional or technical means to intervene.<sup>5</sup>

In permissioned enterprise implementations such as Hyperledger Fabric, used in the execution flows of the BankChain consortium in India, cryptographic certificates and an ordering service are used, but there is no human mediator in the execution logic. Participants are identified by cryptographic keys rather than as legal persons. Section 11 of the Indian Contract Act states that contracting parties must be of legal majority and sound mind, but this check is not carried out by the protocol. A person of unsound mind or a minor may hold a key in the same way as a

---

<sup>3</sup>Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 S.C.C. 1; Swati Suman & Sheersadeb Das, *Smart Contracts & Indian Law: Legally Binding or Technically Blinded*, 11 INT'L J.L. 68, 69 (2025).

<sup>4</sup>The Indian Contract Act, 1872, No. 9, Acts of Parliament, 1872 (India), §§ 14-19; Liu Yang et al., *An Overview of Blockchain Smart Contract Execution Mechanism*, SCIENCE DIRECT (Aug. 2024), <https://doi.org/10.1016/j.sysarc.2024.102452>.

<sup>5</sup>The Indian Contract Act, 1872, *supra* note 4, §§ 56, 62, 65; Kevin Werbach & Nicolas Cornell, *Contracts Ex Machina*, 67 DUKE L.J. 313, 345 (2017).

competent adult, and although anything done by such an individual would be void ab initio under the Act, it would remain irrevocably written on the chain.<sup>6</sup> Furthermore, autonomous code-governed execution severs the link between performance and human volition that consensus ad idem under Section 13 presupposes: the ledger records that something was done, but cannot record that the parties meant to do it in the legally cognisable sense the Act demands.<sup>7</sup>

### C. If/When-Then Logic and Oracle Integration

Every smart contract is programmed with a single set of conditional grammar: once a triggering condition is met, it runs automatically, immediately, and without interpretive judgment. This literalism of code-governed performance excludes the equitable tools Indian courts use, such as the doctrine of contra proferentem and the implication of terms, all of which assume a human interpreter. No Indian tribunal has the technical capability or legal authority to intervene in smart contract execution on a real-time basis. Because blockchains are isolated systems, real-world triggering data is supplied by oracles and middleware that source, verify, and transmit off-chain inputs to the contract. Contractual liability thus rests on oracle-delivered information rather than on any action of the parties. Yet under Section 63 of the BSA, which mandates certification for electronic records, and the Supreme Court's ratio in *Anvar P.V. v. P.K. Basheer*, electronic records require certification by a responsible person who can attest to their accuracy, a standard no oracle operator currently satisfies, meaning that the foundational input on which the contract executed cannot be admitted as evidence in Indian litigation.<sup>8</sup>

The closed loop, namely a real-world trigger, oracle-verified input, self-sovereign on-chain execution, and immutable record, is both the commercial promise of the technology and a cascade that no Indian law can regulate. Decentralisation defeats admissibility; immutability defeats rescission; autonomy defeats consensus; and oracle openness defeats evidence. Every technical characteristic map to a statutory gap, and the overall result is a legal framework incapable of verifying the signature on the contract, admitting the records, rectifying the execution, or safeguarding the information it permanently stores.

---

<sup>6</sup>The Indian Contract Act, 1872, *supra* note 4, § 11; LINUX FOUND. DECENTRALIZED TRUST, HOW WALMART BROUGHT UNPRECEDENTED TRANSPARENCY TO THE FOOD SUPPLY CHAIN WITH HYPERLEDGER FABRIC (2019), <https://www.lfdecentralizedtrust.org/case-studies/walmart-case-study>.

<sup>7</sup>The Indian Contract Act, 1872, *supra* note 4, § 13; A. Yusuf & R. Martinez, *Smart Contracts and Legal Enforceability: Decoding the Political Philosophy of Code as Law*, 4 INTERDISC. STUD. SOC'Y, L. & POL. 292, 296 (2025).

<sup>8</sup>*Anvar P.V. v. P.K. Basheer*, (2014) 10 S.C.C. 473; The Bharatiya Sakshya Adhiniyam, 2023, No. 47, Acts of Parliament, 2023 (India), § 63.

#### IV. WHAT SMART CONTRACTS DO THAT TRADITIONAL CONTRACTS DO NOT: MECHANISM, CASE STUDIES, AND INDUSTRIAL IMPERATIVE

##### A. The Functional Differential

A traditional contract operates on the basis of deferred trust: parties record a promise in natural language and rely on voluntary performance or judicial compulsion in the event of breach. Enforcement depends on courts, arbitral tribunals, and institutional apparatus that are slow, costly, and territorially constrained, and their language is deliberately flexible to accommodate human contingency through interpretation. Smart contracts invert this model. They encode an obligation that is performed autonomously, instantly, and without the possibility of non-performance the moment a predefined on-chain condition is satisfied.<sup>9</sup>

A further distinction lies in the inherently transnational character of blockchain transactions. Traditional contracts ordinarily identify a governing law, territorial nexus, and adjudicatory forum at the time of formation. Smart contracts, by contrast, may execute across multiple jurisdictions simultaneously through distributed nodes and oracle-supplied data streams, making the localisation of contractual performance increasingly difficult. The Supreme Court in *Trimex International FZE Ltd. v. Vedanta Aluminium Ltd.*<sup>10</sup> recognised that commercial contracts formed through electronic communications can create binding obligations notwithstanding geographical separation between the parties. While the decision reflects judicial willingness to accommodate technologically mediated contracting, it nevertheless presupposes identifiable parties, ascertainable intention, and a discernible legal framework governing performance. Smart contracts complicate each of these assumptions, particularly where oracle providers, blockchain validators, and contracting parties operate across different jurisdictions, thereby generating uncertainty regarding applicable law, jurisdiction, and enforcement.

Five structural differentials define this inversion: performance certainty, since the code executes regardless of any post-formation change of intention; disintermediation, since banks, escrow agents, and notaries are rendered redundant by the distributed consensus network; real-time tamper-proof audit trails, which sit in uneasy relationship with the electronic-record certification framework under Sections 63 and 65 of the Bharatiya Sakshya Adhiniyam, 2023; self-enforcement without judicial recourse, since the remedy is structural rather than adjudicative, eliminating both the delay and the equitable safeguards of Indian contract law;

---

<sup>9</sup>Atiyah, Manap & Ibrahim, *supra* note 2, at 36; Suman & Das, *supra* note 3, at 69.

<sup>10</sup>*Trimex International FZE Ltd. v. Vedanta Aluminium Ltd.*, (2010) 3 S.C.C. 1.

and complex programmability, namely multi-step conditional logic that traditional drafting cannot match for speed or precision.<sup>11</sup> Each differential is commercially compelling, and each simultaneously aggravates the legal gaps identified above.

### **B. Case Studies: Technical Execution and Indian Legal Exposure**

**Walmart Canada: DL Freight (DLT Labs).** Walmart Canada worked with roughly 70 third-party freight carriers that generated hundreds of thousands of invoices annually, of which about 70% were disputed owing to data mismatches across fragmented ERP systems, a structural failure of the traditional contractual model rather than of good faith<sup>12</sup>. Partnering with DLT Labs on a Hyperledger Fabric permissioned blockchain, smart contracts were programmed to calculate freight costs from pre-agreed encoded terms, generate invoices on verified delivery confirmation, and settle payment without human intervention. The result was real-time settlement and the near-elimination of invoice disputes; the smart contract functioned precisely as its architecture promised.

The Indian legal gap this case exposes is structural rather than technical. The deployment was nested within an off-chain conventional legal agreement that provided an interpretive and remedial wrapper for the on-chain execution. India possesses no framework mandating or even recognising this hybrid architecture: Section 10A of the IT Act validates electronic contract formation but is silent about self-executing code, and Sections 63 and 65 of the Bharatiya Sakshya Adhiniyam, 2023 pose significant admissibility obstacles for any blockchain evidence produced in court.<sup>13</sup>

**SBI, BankChain, and IBBIC.** The State Bank of India was a founding member of BankChain, a 27-bank consortium that deployed blockchain smart contracts for KYC verification and Letter of Credit processing, later consolidated under the Indian Banks' Blockchain Infrastructure Company (IBBIC), comprising fifteen banks with a combined capitalisation of ₹75 crore<sup>14</sup>. The smart contracts automated KYC data-sharing across institutions and compressed LC processing from four to seven days to near-instantaneous settlement, addressing both the duplicative

---

<sup>11</sup>Levi & Lipton, *supra* note 1; S.N. Khan et al., *Blockchain Smart Contracts: Applications, Challenges, and Future Trends*, PEER-TO-PEER NETWORKING & APPLICATIONS (2021), <https://doi.org/10.1007/s12083-021-01127-0>.

<sup>12</sup>Kate Vitasek et al., *How Walmart Canada Uses Blockchain to Solve Supply-Chain Challenges*, HARV. BUS. REV. (Jan. 5, 2022), <https://hbr.org/2022/01/how-walmart-canada-uses-blockchain-to-solve-supply-chain-challenges>.

<sup>13</sup>The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India), § 10A; The Bharatiya Sakshya Adhiniyam, 2023, *supra* note 8, § 63.

<sup>14</sup>GRANT THORNTON INDIA, IBBIC: PAVING WAY FOR BLOCKCHAIN ADOPTION BY INDIAN BANKS (2021), <https://www.grantthornton.in/insights/blogs/ibbic-paving-way-for-blockchain-adoption-by-indian-banks/>; Sudin Baraokar, *BankChain in Action: SBI Will Start Using Blockchain for Smart Contracts and KYC*, INC42 (Nov. 20, 2017), <https://inc42.com/buzz/bankchain-sbi-blockchain-kyc/>.



documentation burden and the document-fraud-driven NPA accumulation that had damaged the sector.

Three principal legal vulnerabilities arise. First, blockchain-generated hash-based signatures are not issued by a Certifying Authority under Section 35 of the IT Act, so every BankChain KYC record is authenticated by a mechanism Indian law does not recognise and would be inadmissible under the *Khotkar* standard if contested.<sup>15</sup> Second, where LC smart contracts execute on oracle-delivered data that is fraudulent or erroneous, they transfer assets irreversibly; rescission under Sections 17 and 18 of the Indian Contract Act requires judicial intervention, but the blockchain will not respond to a court order reversing a transaction confirmed across 27 nodes. Third, the BankChain KYC records, namely names, addresses, identity numbers, and photographs, are permanently immutable on-chain, making it technically impossible to honour the right to correction and erasure under Section 12 of the Digital Personal Data Protection Act, 2023. On this analysis, on-chain immutability may make compliance difficult<sup>16</sup>.

### C. The Industrial Imperative

These are not isolated deployments. Corporate entities including Bajaj, Mahindra, Hindustan Unilever, and HDFC Bank are already using smart contracts for payments and supply-chain management, and the global blockchain in banking and financial services market was valued at US\$6.98 billion in 2024, projected to reach US\$10.65 billion in 2025<sup>17</sup>. India's Digital India initiative, UPI architecture, and emerging DeFi ecosystem will accelerate this adoption further. The question is not whether smart contracts will be used in India, since they already are, at institutional scale, but whether the legal system can adjudicate disputes, allocate liability, and protect vulnerable parties when they go wrong. The Indian Contract Act was not designed for self-executing obligations; the law of evidence struggles to accommodate decentralised records; the IT Act validates electronic formation but cannot address autonomous execution; and the DPDP Act conflicts structurally with blockchain immutability. The industrial imperative is real, present, and accelerating, while the legislative response is absent, and that asymmetry is the central crisis this paper addresses.<sup>18</sup>

---

<sup>15</sup>The Bharatiya Sakshya Adhinyam, 2023, *supra* note 8, §§ 63, 65.

<sup>16</sup>The Information Technology Act, 2000, *supra* note 13, § 35; Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, *supra* note 3; The Indian Contract Act, 1872, *supra* note 4, §§ 17-18; The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India), § 12.

<sup>17</sup>*The Role of Blockchain in Reshaping Financial Markets*, INT'L J. RSCH. FIN. & MGMT., <https://www.allfinancejournal.com/article/view/563/8-2-48>; *Overview on Smart Contract: Indian Law Perspective*, LEGAL SERV. INDIA, <https://www.legalserviceindia.com/legal/article-8128> (last visited Mar. 1, 2025).

<sup>18</sup>Megha Ravindranath, *Legality of Blockchain and Smart Contracts in India*, 6 INT'L J. FOR MULTIDISCIPLINARY RSCH. 1, 5 (2024); Raghav Pathak, *Interoperability, Legal Interpretation and Application of Smart Contracts*, ONLINE J. INT'L BANKING L. & REG. (2024), [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4964942](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4964942).

## V. WHERE CODE MEETS LEGAL VACUUM: MAPPING INDIA'S FIVE STATUTORY INCOMPATIBILITIES

The central doctrinal difficulty does not turn on whether smart contracts are novel, but on whether they are structurally incompatible with the legal infrastructure of Indian contract law. Their value lies in autonomous execution, yet that very autonomy creates statutory friction at the stage of enforceability. The result is not an incidental gap but an incongruity between code-based performance and a framework designed for human mediation.<sup>19</sup>

### A. Authentication

Smart contracts verify participation through cryptographic private keys, but Section 35 of the Information Technology Act, 2000 recognises digital signatures only when issued by a licensed Certifying Authority. The consequence is direct: the method by which blockchain systems establish identity falls outside the form of authentication that Indian law formally validates.<sup>20</sup>

### B. Admissibility

Sections 63 and 65 of the Bharatiya Sakshya Adhiniyam, 2023 prescribe the conditions governing the admissibility of electronic records and continue the requirement of certification for electronic evidence, while *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* confirms the mandatory nature of such compliance. Yet a permissionless blockchain has no responsible official, no central operator, and no identifiable person capable of certifying the entirety of the network.<sup>21</sup> The practical effect is severe: the very evidence required to establish the execution and operation of a smart contract may face admissibility challenges at the threshold. This concern is reinforced by *Anvar P.V. v. P.K. Basheer*<sup>22</sup>, which held that electronic records are admissible only when accompanied by the statutory certificate and rejected the admission of secondary electronic evidence through ordinary evidentiary rules. The Court emphasised that the certification requirement is a condition precedent to admissibility, making authenticity and traceability central to the evidentiary value of electronic records. Where records are generated collectively through decentralised consensus rather than maintained by a single identifiable operator, compliance with this framework becomes inherently problematic, so that even where a smart contract has executed flawlessly on-chain, proving its existence and operation before an Indian court may encounter significant evidentiary obstacles.

---

<sup>19</sup>The Indian Contract Act, 1872, *supra* note 4, §§ 13-19, 56, 62, 65.

<sup>20</sup>The Information Technology Act, 2000, *supra* note 13, §§ 5, 24, 35.

<sup>21</sup>*Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, *supra* note 3; The Bharatiya Sakshya Adhiniyam, 2023, *supra* note 8, § 63.

<sup>22</sup>*Anvar P.V. v. P.K. Basheer*, *supra* note 8.

### C. Consent

Indian contract law proceeds on the basis of human consent, but smart contracts execute automatically once their coded conditions are triggered. Singapore has resolved this problem expressly by recognising contracts formed through automated message systems under Section 15 of its Electronic Transactions Act; India has enacted no equivalent provision.<sup>23</sup> As a result, smart contracts operate in a legal grey zone where performance occurs autonomously but the doctrinal basis for attributing continuing contractual assent remains unsettled. The reasoning in *Shreya Singhal v. Union of India*<sup>24</sup>, which distinguished human agency from the passive functioning of technological intermediaries, further highlights the difficulty of locating legally cognisable consent where contractual performance is triggered solely by pre-programmed code rather than an active human decision at the moment of execution.

### D. Remedial

The Indian Contract Act provides rescission, restitution, and discharge when a contract fails, but these remedies assume that performance can be reversed. Blockchain architecture denies that possibility. Once execution is complete, the transaction is permanent, and judicial relief is reduced to a personal action against a counterparty who may be pseudonymous, inaccessible, or outside the jurisdiction.<sup>25</sup>

### E. Privacy

Section 12 of the Digital Personal Data Protection Act, 2023 gives data principals the right to correction and erasure, but blockchain records are designed to be immutable. A system built on permanent storage thus conflicts directly with a statute built on revocable data rights, and the incompatibility is structural and cannot be cured by interpretation alone.<sup>26</sup> The United Kingdom, by contrast, has accepted that existing law can support smart legal contracts, while states such as Arizona and Tennessee have enacted targeted legislative recognition; India has neither express statutory validation nor a judicial framework that squarely addresses blockchain-based enforceability.<sup>27</sup>

---

<sup>23</sup>Electronic Transactions Act 2010, § 15 (Sing.).

<sup>24</sup>*Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1.

<sup>25</sup>The Indian Contract Act, 1872, *supra* note 4, §§ 56, 62, 65.

<sup>26</sup>The Digital Personal Data Protection Act, 2023, *supra* note 16, § 12.

<sup>27</sup>LAW COMM'N, SMART LEGAL CONTRACTS: ADVICE TO GOVERNMENT (2021) (U.K.); Ariz. H.B. 2417, 53d Leg., 1st Reg. Sess. (2017); Tenn. Pub. Ch. 591 (2018).

## VI. PROPOSED LEGISLATIVE REFORMS

India's smart contract problem is neither unfamiliarity with the technology nor an absence of commercial adoption, both of which are already present at institutional scale. The existing legal framework fractures across five critical dimensions, namely authentication, admissibility, consent, remediation, and data protection, while comparative jurisdictions demonstrate that precise, targeted legislative drafting can close these gaps without compromising the efficiency that blockchain automation promises.<sup>28</sup> Three structural correctives are therefore proposed.

### A. Legitimising Blockchain Authentication and Reforming the Evidentiary Standard

Section 35 of the IT Act, 2000 should be amended to extend validity to cryptographic blockchain signatures on a functional-equivalence basis, recognising them upon reliable establishment of identity and contractual intention, without disturbing the Certifying Authority framework for conventional digital signatures. This would preserve the Act's central concern with authenticity while accommodating blockchain identity. In the same spirit, the electronic-evidence framework under Sections 63 and 65 of the Bharatiya Sakshya Adhiniyam, 2023 should be amended to permit certification by a technically competent person in respect of distributed ledger systems, replacing the "responsible official" standard with a blockchain-specific evidentiary rule.<sup>29</sup>

### B. Codifying Automated Consent and Mandating the Legal Wrapper

Addressing consent and reversibility, a new statutory provision, modelled on Section 15 of Singapore's Electronic Transactions Act but adapted to Indian contract doctrine, should affirm that a contract is not void or unenforceable merely because performance was carried out by an automated system without human intervention at execution.<sup>30</sup> Such a provision would substitute for the implied human-assent assumption embedded in Section 13 of the Indian Contract Act, 1872. At the same time, high-value smart contracts should require a legal wrapper, namely an off-chain agreement identifying the parties, governing law, and dispute forum, so that the code remains enforceable within a recognisable legal framework.

### C. Resolving the Immutability-Erasure Conflict Under the DPDP Act, 2023

Finally, the DPDP Act should be aligned with blockchain's immutability by preserving privacy through substitutes for deletion, such as cryptographic masking or off-chain storage of personal

---

<sup>28</sup>LAW COMM'N, *supra* note 27; Electronic Transactions Act 2010, *supra* note 23, § 15.

<sup>29</sup>The Bharatiya Sakshya Adhiniyam, 2023, *supra* note 8, §§ 63, 65; Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, *supra* note 3.

<sup>30</sup>Electronic Transactions Act 2010, *supra* note 23, § 15.

data.<sup>31</sup> Comparative experience in the United Kingdom, Arizona, and Singapore indicates that smart contract law works best when legislation operates in functional rather than purely formal terms.<sup>32</sup>

Evaluated cohesively, these three correctives do not dismantle the existing infrastructure of commercial obligations in India; rather, they bridge the immediate statutory gaps identified across authentication, admissibility, consent, remediation, and data privacy. By introducing targeted legislative wrappers, blockchain-specific evidentiary rules, and functional privacy carve-outs, the Indian legal ecosystem can update its statutory capacities without diluting foundational legal protections.

## VII. CONCLUSION

Smart contracts are not a distant legislative concern; they are operational, institutionally embedded, and generate legal consequences that Indian law is presently unequipped to resolve. This paper has demonstrated that the incompatibility between blockchain architecture and Indian statutory law is not incidental but infrastructural, manifesting across authentication, evidentiary admissibility, contractual consent, remedial adequacy, and data protection in a sequence that no single judicial interpretation can adequately address.

The comparative evidence is unambiguous: while the United Kingdom has relied on common law flexibility and Arizona, Tennessee, and Singapore have enacted targeted legislative recognition, India has responded with silence, a silence that grows increasingly untenable as institutional adoption accelerates and disputes become inevitable.

The three proposed reform mechanisms, namely cryptographic authentication, statutory codification of automated consent coupled with a mandatory legal wrapper, and a privacy-preserving resolution of the immutability-erasure conflict, do not aim at dismantling existing Indian contract law; rather, they extend it to a form of contracting its drafters could not have anticipated. India needs the legislative precision to extend its existing framework accordingly.

\*\*\*\*\*

---

<sup>31</sup>The Digital Personal Data Protection Act, 2023, *supra* note 16, § 12.

<sup>32</sup>Ariz. H.B. 2417, *supra* note 27; Tenn. Pub. Ch. 591, *supra* note 27; LAW COMM'N, *supra* note 27.