INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 6 AND ISSUE 7 OF 2026

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 6 and Issue 7 of 2026 (Access Full Issue on - https://ijlr.iledu.in/volume-6-and-issue-7-of-2026/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 73059 14348 - info@iledu.in / Chairman@iledu.in

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 7 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

"CODE IS LAW" BUT IS CODE A CONTRACT?

SMART CONTRACTS UNDER THE INDIAN CONTRACT ACT, 1872 AND THE INFORMATION TECHNOLOGY ACT, 2000

AUTHOR – KHUSHI PATEL, STUDENT AT UNITEDWORLD SCHOOL OF LAW, KARNAVATI UNIVERSITY

BEST CITATION – KHUSHI PATEL, "CODE IS LAW" BUT IS CODE A CONTRACT? - SMART CONTRACTS UNDER THE INDIAN CONTRACT ACT, 1872 AND THE INFORMATION TECHNOLOGY ACT, 2000, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 6 (7) OF 2026, PG. 409-422, APIS – 3920 – 0001 & ISSN - 2583-2344. DOI - HTTPS://DOI.ORG/10.65393/IJLRV6I746

ABSTRACT

Smart contracts — self-executing agreements expressed in blockchain code — are transacting billions of dollars of value daily, yet their legal enforceability under Indian law remains fundamentally uncertain. This article undertakes a systematic doctrinal analysis of smart contracts against the essential requirements of a valid contract under the Indian Contract Act, 1872 ("ICA") and the authentication and evidentiary framework of the Information Technology Act, 2000 ("IT Act"). The analysis demonstrates that the ICA's core requirements — offer and acceptance, consideration, capacity, free consent, and legality — can each be satisfied in a smart contract interaction when interpreted in light of the blockchain's technical architecture. This article proposes the "Informed Interaction Standard" as a workable judicial test for offer and acceptance. It identifies two critical gaps in the IT Act: the non-recognition of blockchain cryptographic authentication as a valid electronic signature and the inapplicability of the Section 65B evidentiary certificate requirement to blockchain records. To address these gaps, the article proposes three targeted legislative interventions: a new Section 10B (IT Act) expressly validating smart contracts; a Section 3A notification recognising blockchain authentication; and a new Section 65C establishing an alternative evidentiary certification pathway for distributed ledger records. Comparative analysis of England, the United States, Singapore, and the European Union confirms that India is an outlier in its failure to resolve these questions and benchmarks the proposed reforms against best international practice.

Keywords: *smart contracts, Indian Contract Act 1872, Information Technology Act 2000, blockchain law, decentralised finance, digital signatures, Section 65B, electronic contracts, DAO, law reform.*

I. Introduction: The Central Doctrinal Challenge

In the summer of 2016, a vulnerability in the Solidity code governing The DAO — at the time the largest crowdfunding campaign in history, holding approximately USD 150 million — was exploited by an attacker who drained roughly USD 60 million into a child contract before the Ethereum community could respond.[1] The attacker had not violated the smart contract's code. The code had executed exactly as written. When confronted with this observation, a faction within the Ethereum community invoked the slogan that had become a founding ideology of the decentralised finance (DeFi) movement: "code is law." If the code authorises the drain, the attacker did not steal; the attacker simply used the contract.

The Ethereum community ultimately rejected this conclusion, executing a controversial hard fork of the blockchain to reverse the transactions and restore the funds.[2] But the episode exposed, with unusual clarity, the central doctrinal challenge that smart contracts pose to the law of contract: the relationship between what code does and what the parties

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 7 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

intended. In conventional contract law, a discrepancy between what a contract says and what the parties intended is the stuff of rectification, mistake, and misrepresentation. In smart contract law, the discrepancy may be between what the code executes and what the parties believed the code would execute — a gap that conventional doctrine was never designed to address.

This article addresses a question that has become increasingly urgent as smart contract transactions proliferate: are smart contracts "contracts" in the legal sense under Indian law? The answer matters profoundly for commercial practice — smart contracts are used in billions of dollars of transactions every day, and their legal status under Indian law is currently uncertain in ways that create real commercial and legal risk. The article proceeds as follows. Section II surveys the relevant statutory framework. Sections III through VI analyse each essential element of a valid contract. Section VII addresses the IT Act's authentication and evidentiary framework in depth. Section VIII examines remedies for smart contract failure, including the novel problem of irreversibility. Section IX undertakes comparative analysis of four jurisdictions. Section X proposes specific legislative amendments and judicial tests. Section XI concludes.

II. The Statutory Framework

A. Essential Elements of a Valid Contract under Section 10

The Indian Contract Act, 1872 is one of the great codifications of the common law of contract. Section 10 defines the essential conditions of a valid contract: all agreements are contracts if they are made by the free consent of parties competent to contract, for a lawful consideration and with a lawful object, and are not hereby expressly declared to be void. This deceptively simple provision contains five distinct requirements. The first two — free consent and competency — relate to the parties. The third and fourth — lawful consideration and lawful object — relate to the substance of the agreement. To these, the Act's subsequent provisions add the requirements of offer and acceptance (Sections 2(a) and 2(b)) and certainty of terms.[3]

Each of these requirements was designed with human contracting parties in mind — parties who make offers, form intentions, give consents, and have legal capacities governed by the laws of their domicile. The application of these requirements to smart contracts, in which the "parties" may be automated protocols interacting with each other, and in which "consent" may be expressed by the act of sending a transaction to a contract address, requires careful doctrinal reconstruction.

B. The IT Act, 2000: Electronic Contracts and Digital Signatures

The Information Technology Act, 2000 was enacted to give legal effect to electronic records and to facilitate e-commerce. Its central provisions — Sections 3 to 5 — were modelled on the UNCITRAL Model Law on Electronic Commerce (1996) and the Model Law on Electronic Signatures (2001).[4] The Act establishes a Public Key Infrastructure (PKI) system: a subscriber obtains a digital signature certificate from a licensed Certifying Authority (CA); the CA verifies identity; the subscriber signs documents with their private key; and the signature is verified using the CA-certified public key.[5]

This architecture reflects the technology of 2000. It does not reflect the technology of 2024, in which cryptographic authentication is performed by blockchain wallets whose private keys are self-generated, whose public keys are not certified by any CA, and whose authentication is verified by the consensus of the blockchain network. The gap between the IT Act's authentication architecture and the blockchain's is the source of much of the legal uncertainty around smart contracts in India.

C. Section 10A: The Electronic Contract Provision

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 7 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

Section 10A, inserted by the Information Technology (Amendment) Act 2008, provides that where contract formation is expressed in electronic form or by means of an electronic record, the contract shall not be deemed unenforceable solely on that ground.[6] Section 10A has been interpreted broadly by Indian courts to validate email, click-wrap agreements, and online marketplace transactions.[7]

However, Section 10A does not resolve the smart contract question. It addresses the medium of communication but says nothing about the nature of the contracting parties (which in a smart contract interaction may be automated protocols), the authentication of those parties (which in a blockchain context is cryptographic rather than CA-certified), or the enforceability of automatically executed and irreversible performance. These gaps require both judicial interpretation and legislative clarification.

III. Offer and Acceptance in the Age of Self-Executing Code

A. The Classical Doctrine and Its Assumptions

Section 2(a) of the Indian Contract Act defines a proposal as the signification by one person to another of their willingness to do or abstain from doing anything, with a view to obtaining the assent of that other.[8] Section 2(b) defines acceptance as the signification of assent by the person to whom the proposal is made.[9] Together, these provisions require: (i) two identifiable parties; (ii) a communication of willingness by one party; (iii) a communication of assent by the other; and (iv) a meeting of minds — consensus ad idem — on the essential terms.

These requirements encode assumptions about contracting that are so fundamental as to be invisible. An offer is made by a person who has a "will" — a mind capable of forming intentions. A legal system that has never encountered a contracting party that is a piece of code rather than a human being or a legally recognised artificial person has had no occasion to examine these assumptions. Smart contracts force that examination.

B. Three Analytical Models of Smart Contract Formation

1. The Deployment Model

Under the deployment model, the developer's act of deploying the smart contract constitutes a standing offer to any person who interacts with it on the terms specified in the contract code. The user's act of calling a contract function constitutes acceptance. This maps neatly onto the classical doctrine of unilateral contracts, exemplified by [10] and applied by Indian courts subsequently. The Supreme Court's statement in Bhagwandas Goverdhandas Kedia v Girdharilal Parshottamdas[11] that an offer may be directed to the world at large supports the proposition that deployment to a public blockchain constitutes a standing offer. On this model, the contract is formed at the moment the user's transaction is included in a block — the blockchain equivalent of the postal rule's "moment of posting."[12]

The deployment model works well for simple smart contracts in which the developer is identifiable and the contract's terms are clearly stated. It works less well for complex DeFi protocols in which the "deployer" may be an earlier smart contract, and in which the user may not understand the terms to which they were assenting — creating difficulty establishing consensus ad idem.

2. The Interaction Model

Under the interaction model, the contract is formed at the moment of execution, when the smart contract runs and performs the agreed exchange. The exchange itself is both the offer and the acceptance — a simultaneous meeting of minds expressed through performance rather than communication. However, this model dissolves the distinction between contract formation and performance, which the law of remedies crucially depends upon: if formation and performance are simultaneous, there is no

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 7 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

moment at which breach can occur, and therefore no basis for a remedy in damages.

3. The Automated Agent Model

The automated agent model treats the smart contract itself as an agent of the deployer, acting within the scope of its programmed authority. This draws on the doctrine of actual authority: a principal who creates an agent with actual authority to enter into contracts on specified terms is bound by those contracts.[13] This model has been adopted by several US state smart contract statutes, notably Tennessee's and Arizona's, which expressly provide that a smart contract may act as an "electronic agent" for its deployer.[14] It has strong doctrinal attractions in the Indian context: the ICA contains an extensive agency framework (Sections 182–238) that can accommodate a "programmed agent" without fundamental disruption, and Section 2(1) of the IT Act defines an "automated electronic agent" as a computer program designed to act without human intervention.

C. The Informed Interaction Standard: A Proposed Doctrinal Test

None of the three models is fully satisfactory on its own. This article proposes an integrative test — the "Informed Interaction Standard" — calibrated to the requirements of the Indian Contract Act. A smart contract interaction constitutes a valid offer and acceptance under the ICA if and only if:

(a) Identifiable deployer: The smart contract was deployed by an identifiable person or entity. Pseudonymous deployment does not prevent contract formation, but may affect the availability of remedies.

(b) Accessible terms: The terms of the smart contract are accessible to users in a form they can reasonably be expected to understand — through verified source code, a plain-language summary, or a white paper. This requirement is analogous to the notice requirement for exemption clauses in standard-form contracts.[15]

(c) Voluntary interaction: The user's transaction was voluntary, not the result of coercion, technical manipulation, or phishing.

(d) Execution as performance: The moment of acceptance is the moment the user's transaction is broadcast to the network; the moment of performance is the moment the transaction is confirmed on-chain.

This standard integrates the deployment model's recognition of the standing offer, the interaction model's identification of performance as the critical moment, and the automated agent model's attribution of the contract to the deployer. It preserves the essential requirements of consensus ad idem by insisting on accessible terms, while accommodating the automated nature of smart contract performance.

IV. Consideration in Smart Contracts

A. The Doctrine and Its Application

The Indian Contract Act's approach to consideration is, in one important respect, more permissive than English common law. Section 2(d) defines consideration as an act, abstinence, or promise made at the desire of the promisor, by the promisee or any other person.[16] The words "or any other person" — making Indian contract law accept third-party consideration — have practical significance in multi-party smart contract interactions involving liquidity pools, automated market makers, and protocol treasuries, where consideration may flow from a pool of participants rather than a single identified counterparty.

The requirement that consideration be furnished "at the desire of the promisor" is the principal doctrinal challenge where the "promisor" is a smart contract with no desires in any conventional sense. However, on the automated agent model, the deployer is the promisor, and the "desire" is expressed in the code itself: by programming the contract to accept and execute transactions in exchange for specified assets, the deployer has expressed

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 7 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

their desire for precisely that consideration in advance.

B. Token Transfers, Gas Fees, and Reciprocal Obligations

In practice, consideration takes several forms: in a decentralised exchange (DEX) swap, the user transfers Token A to the protocol's liquidity pool and receives Token B; in a lending protocol, the user deposits collateral and receives a loan. The gas fee — the amount paid by the user to compensate the network's validators for processing the transaction — deserves specific attention.[17] Gas fees for complex DeFi transactions can amount to several dollars or more. The gas fee provides a clean doctrinal hook for consideration: even where the substance of the exchange might be analysed as a unilateral transaction, the gas fee ensures that the user has given something of value in exchange for the contract's execution. The combination of the permissive third-party consideration rule, the automated agent model's attribution of "desire" to the deployer, and the gas fee's consideration hook makes it possible to find consideration in the vast majority of smart contract interactions.

V. Capacity, Free Consent, and the Pseudonymity Problem

A. Capacity: The Unknown Contracting Party

Section 11 of the Indian Contract Act provides that every person is competent to contract who is of the age of majority, who is of sound mind, and who is not disqualified from contracting by any law.[18] The age of majority in India is eighteen years under the Indian Majority Act 1875.[19] A contract with a minor is void ab initio — confirmed by the Privy Council in Mohori Bibee v Dharmodas Ghose[20] and never displaced by subsequent legislation.

The pseudonymity of smart contract counterparties creates a genuine capacity problem. A blockchain wallet address reveals nothing about the age, mental state, or legal status of the person controlling it. A minor in India can obtain a cryptocurrency wallet, acquire tokens on a decentralised exchange — which requires no KYC verification — and interact with smart contracts. The self-executing and irreversible nature of smart contract performance means that assets may have already moved by the time incapacity is discovered. The law has three tools to address this: (i) a good-faith defence for deployers who had no reason to know of the incapacity; (ii) a restitutionary remedy that adjusts the parties' positions without voiding already-occurred performance; and (iii) a regulatory requirement for KYC verification at the gateway that limits minors' access to DeFi protocols. All three tools are available under existing Indian law.

B. Free Consent: Coercion, Fraud, Misrepresentation, and Mistake in Code

Section 14 of the Indian Contract Act provides that consent is free if it is not caused by coercion, undue influence, fraud, misrepresentation, or mistake.[21] Each of these grounds raises specific questions in the smart contract context.

Coercion (Section 15). Coercion is the committing or threatening of an act forbidden by the Indian Penal Code, or the unlawful detaining or threatening to detain property.[22] So-called "vampire attacks" in DeFi — where a hostile protocol systematically drains liquidity by offering superior short-term incentives — raise whether such market manipulation constitutes "unlawful detaining of property." The better view is that Section 15 requires a legal wrong directed at a specific person; generalised market competition, however aggressive, does not constitute coercion in the contract law sense.

Fraud (Section 17). Fraud is the suggestion of a fact known to be false, or the active concealment of a fact, with the intention of deceiving.[23] A smart contract that presents a misleading interface — appearing to offer one service while actually performing another — constitutes fraud by the deployer, regardless of the fact that the deception is effected through code.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 7 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

Misrepresentation (Section 18). A protocol's white paper, marketing materials, or user interface that misrepresents the protocol's mechanics could constitute misrepresentation under Section 18,[24] giving the user a right to rescind the transaction — subject to the irreversibility problem discussed in Section VIII.

C. Algorithmic Mistake: A New Category

The most analytically interesting free consent issue is not any of the conventional categories but a new category that might be called "algorithmic mistake" — a mistake not in the parties' understanding of the contract's terms but in the code's implementation of those terms. Consider a developer who writes a smart contract intended to execute an interest rate swap at 5 per cent per annum, but due to a coding error the contract implements a rate of 5 per cent per day. Both parties intended the annual rate; the code executes the daily rate. Section 20 of the Indian Contract Act provides that where both parties are under a mistake as to a matter of fact essential to the agreement, the agreement is void.[25] The coding error scenario is precisely such a mutual mistake. However, because the smart contract has already executed, restitution requires a further on-chain transaction. This analysis points to a gap in Indian law addressed by the proposed Section 10B below.

VI. Legality of Object and Public Policy

Section 23 of the Indian Contract Act provides that the consideration or object of an agreement is unlawful if it is forbidden by law, would defeat the provisions of any law, is fraudulent, involves or implies injury to the person or property of another, or the court regards it as immoral or opposed to public policy.[26] A contract with an unlawful object or consideration is void.

Several categories of smart contract activity raise legality concerns. A smart contract that facilitates gambling — the payment of prizes from a pool of staked assets based on a random outcome — may be void as a wagering agreement under Section 30 of the Contract Act.[27] A smart contract that facilitates the transfer of securities without SEBI registration has an unlawful object. Indian courts have applied the public policy ground broadly in contexts involving regulatory evasion.[28] The general principle is clear: a smart contract whose object is to facilitate a lawful activity is not rendered unlawful by the fact that it operates on a blockchain. Conversely, a smart contract whose object is to facilitate an unlawful activity is void — though the irreversibility of on-chain execution means that the assets may already have moved, making the legal remedy purely remedial rather than preventive.

VII. The IT Act, 2000: Authentication, Electronic Signatures, and Blockchain

A. Digital Signatures and Certifying Authorities: The Mismatch

The IT Act's framework for digital signatures is built around a tripartite relationship: the subscriber, the Certifying Authority (CA), and the relying party.[29] The CA is the trust anchor: it is because the CA has verified the subscriber's identity that the relying party can trust the signature. A blockchain wallet's cryptographic key pair is entirely different: the private key is generated by the wallet software — not by any CA — and there is no identity verification at the point of key generation. Authentication on a blockchain is provided not by a trusted third party but by the mathematics of public-key cryptography and the consensus of the network. The result is a legal asymmetry: a CA-certified digital signature is legally valid under the IT Act; an identical cryptographic signature verified by blockchain consensus is legally uncertain. This asymmetry has no technical justification — the blockchain signature is, if anything, more tamper-resistant — but it has significant legal consequences for the enforceability of smart contracts and the admissibility of blockchain evidence.

B. Cryptographic Authentication as Electronic Signature

Section 3A of the IT Act, inserted by the 2008 Amendment, provides for "electronic signatures" (a broader category than "digital signatures") and empowers the Central Government to prescribe methods of electronic signature by notification.[30] The Central Government has notified two methods: Aadhaar-based e-authentication and digital signatures using CA-issued certificates.[31] Blockchain cryptographic authentication has not been notified. The legislative power exists; what is lacking is the political will to exercise it. The proposed legislative amendments in Section X include a recommendation that the Central Government exercise its Section 3A power to notify blockchain cryptographic authentication as a valid electronic signature method, subject to specified technical standards.

C. The Section 65B Evidentiary Problem: A Deep Analysis

No aspect of smart contract law under Indian law has more practical significance than the admissibility of blockchain records as evidence in Indian courts. Section 65B of the IT Act, as interpreted by the Supreme Court in Anvar PV v PK Basheer[32] and confirmed in Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal,[33] requires the production of a certificate from the person responsible for the computer system that produced the electronic record.

The problem is that a blockchain is managed collectively by thousands of independent nodes, no single one of which can claim to be the "person responsible for the computer system." The blockchain is, by design, the precise opposite of the kind of centrally administered computer system that Section 65B contemplates. The consequences are severe: a party seeking to enforce a smart contract in an Indian court will need to produce evidence of the contract's terms (the smart contract code), its execution (the transaction record on the blockchain), and the parties' interactions (their wallet addresses' transaction history). All of this evidence is stored on the blockchain. If it is inadmissible for want of a Section 65B certificate, the entire evidentiary foundation of smart contract claims collapses.

Recent judicial developments have introduced some flexibility. In Shafhi Mohammad v State of Himachal Pradesh,[34] the Supreme Court appeared to hold that the certificate requirement could be dispensed with in certain circumstances, though this was subsequently limited by Arjun Panditrao. The High Court of Delhi has shown increasing willingness to admit electronic records where authenticity can be demonstrated by other means.[35] However, these are judicial accommodations in the face of an inadequate statutory framework. Legislative action is required.

D. Proposed Statutory Solution: Section 65C (New)

The following is the proposed text of a new Section 65C to be inserted into the Information Technology Act, 2000:

65C. Admissibility of Distributed Ledger Records — (1) For the purposes of Section 65B, a record stored on a Recognised Distributed Ledger (as defined by notification under Section 3A) shall be treated as a computer output produced in the ordinary course of the operation of that Distributed Ledger. (2) The authenticity of a Distributed Ledger record may be certified by any of the following persons: (a) a blockchain forensics analyst accredited by a body notified by the Central Government; (b) a licensed exchange or custodian that maintains a copy of the relevant blockchain; or (c) an expert witness who demonstrates, to the satisfaction of the court, familiarity with the operation of the relevant Distributed Ledger. (3) A certificate produced under sub-section (2) shall, for the purposes of Section 65B, satisfy the requirements of that section. (4) In any proceeding in which the authenticity of a Distributed Ledger record is in question, the burden of proof shall lie on the party challenging authenticity to demonstrate, on a

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 7 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

balance of probabilities, that the record has been tampered with or is otherwise unreliable.

The proposed Section 65C addresses the evidentiary gap directly by creating an alternative certification pathway. Its key features are: (i) the recognition of the blockchain itself as a "computer system" for Section 65B purposes, without requiring a single responsible person; (ii) three alternative certification routes appropriate to the decentralised nature of blockchain evidence; and (iii) a presumption of reliability that places the burden of challenging authenticity on the party denying the record — a presumption justified by the blockchain's cryptographic tamper-resistance.

VIII. Remedies for Smart Contract Failure: The Problem of Irreversibility

A. Damages, Specific Performance, and Injunction

Section 73 of the Contract Act entitles the party who suffers loss from a breach to receive compensation for all losses which naturally arose from the breach or which the parties knew, at the time of making the contract, to be its probable result.[36] The Hadley v Baxendale[37] foreseeability principle, incorporated in Section 73, applies in the smart contract context. The principal complication is identifying the defendant: if the deployer is pseudonymous, the judgment may be impossible to enforce.

Section 10 of the Specific Relief Act provides that specific performance may be enforced when compensation would not afford adequate relief.[38] Smart contracts raise a novel question: can a court order "specific performance" of a smart contract transaction — ordering a new on-chain transaction to replicate one that failed? In principle, yes: the court can order the defendant to execute a transaction from their wallet achieving the same economic result as the failed performance. The ability of a court to grant an injunction against the operation of a smart contract is, in practice, very limited. An injunction operates against a person, not against code. A court can order the deployer to take down the smart contract's user interface, or to upgrade the contract where upgradeable proxy patterns are in use. It cannot order the blockchain to stop executing the contract's code.

B. Unjust Enrichment and Restitution

Where a smart contract executes incorrectly and transfers assets in circumstances that neither party intended, the recipient is unjustly enriched at the expense of the transferor. Indian law recognises a general obligation to make restitution for unjust enrichment under Section 70 of the Contract Act and under the equitable doctrine of unjust enrichment applied in a range of contexts.[39] The restitutionary remedy is particularly important in the smart contract context because it does not require proof of a binding contract: it is available wherever one party has been enriched at the expense of another in circumstances the law regards as unjust. The blockchain's transparency provides a significant advantage over conventional unjust enrichment cases: the flow of assets is publicly traceable, and blockchain analytics tools can, in many cases, identify the ultimate recipient of improperly transferred assets even where the initial transaction was between anonymous wallet addresses.

C. Developer Liability for Bugs: The Negligence Framework

One of the most practically significant and legally underdeveloped questions is the liability of developers for bugs in their code. The DeFi ecosystem has suffered billions of dollars in losses from smart contract vulnerabilities — re-entrancy attacks, integer overflow errors, logic bugs, and oracle manipulation — and the legal framework for attributing those losses to identified defendants is underdeveloped. The negligence framework offers the most doctrinally coherent basis. Under Indian tort law, as developed under the Law of Torts and the Consumer Protection Act 2019, a person who creates a product causing loss to a user may

be liable in negligence if: (i) they owed a duty of care; (ii) they breached that duty by failing to exercise reasonable care; and (iii) the breach caused the user's loss.[40]

Donoghue v Stevenson[41] established that a manufacturer owes a duty of care to the ultimate consumer of their product, even without a contractual relationship. Applied to smart contracts, a developer who deploys a smart contract for public use owes a duty of care to users of that contract. The emerging industry standard of independent smart contract auditing provides a useful benchmark for what constitutes "reasonable care."

D. Oracle Failure: Misrepresentation by Automated Data Feed

An oracle that supplies incorrect data to a smart contract effectively makes a false representation to every user whose transaction is affected by that data. Where the oracle's error causes a user to lose money — for example, by triggering a liquidation at an artificially low price — the user may have a claim against the oracle operator for misrepresentation under Section 18 of the Contract Act. The chain of causation is somewhat attenuated — the plaintiff relies on the protocol, which relies on the oracle — but it is not different in kind from product liability chains in which a defective component supplied by a sub-contractor ultimately causes loss to an end consumer.

IX. Comparative Analysis: How Other Jurisdictions Treat Smart Contracts

A. England and Wales: The LawTech Delivery Panel Report

In November 2019, the UK Jurisdiction Taskforce published its Legal Statement on Cryptoassets and Smart Contracts,[42] providing the most authoritative analysis of smart contract law in any common law jurisdiction. The Legal Statement concluded that smart contracts are capable of satisfying the requirements of a valid contract under English law. On offer and acceptance: deployment to a public blockchain constitutes an offer to the world capable of acceptance by interaction, on the analogy of a unilateral contract. On consideration: provision of crypto assets, gas fees, or other value in exchange for the smart contract's performance constitutes good consideration. On certainty and intention: smart contracts are capable of being sufficiently certain and of evidencing an intention to create legal relations.[43]

The Legal Statement's conclusions are broadly applicable to Indian law given the shared common law heritage. Where Indian law differs — notably in its more permissive approach to third-party consideration and its codified framework — those differences generally make smart contract enforceability easier to establish in India than in England.

B. United States: State-Level Smart Contract Statutes

The United States has seen a proliferation of state-level legislation recognising smart contracts. Arizona's Electronic Transactions Act amendments (2017) were among the first, providing that smart contracts may exist in commerce and that a contract may not be denied legal effect solely because it contains a smart contract term.[44] Similar provisions have been enacted in Tennessee, Nevada, Wyoming, and Illinois, among others.[45]

The US state statutes share a common design: they do not attempt to resolve all doctrinal questions raised by smart contracts, but establish a baseline principle of non-discrimination — a contract shall not be denied enforcement solely because it is a smart contract or contains smart contract terms. This is analogous to, but goes slightly beyond, India's Section 10A. The US statutes also typically provide that the blockchain record of a smart contract transaction constitutes an electronic record for evidentiary purposes — addressing, at the statutory level, the problem that Section 65B creates in India.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 7 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

C. Singapore: B2C2 Ltd v Quoine and Judicial Engagement

Singapore has produced the most sophisticated judicial engagement with smart contract law in any common law jurisdiction, in B2C2 Ltd v Quoine Pte Ltd.[46] The case arose from a series of cryptocurrency trades executed by an algorithmic trading program on the Quoine platform. Due to a software malfunction, Quoine's matching engine executed trades at prices approximately 250 times the market rate. Quoine subsequently reversed the trades; B2C2 sued for breach of contract. The Singapore International Commercial Court held that each trade constituted a valid and binding contract, formed by the automated matching of B2C2's bot's offer and Quoine's engine's acceptance, without any human intervention on either side. The Court held that the unilateral mistake doctrine required knowledge or constructive knowledge by B2C2 of Quoine's mistake, which was not established on the facts.[47]

B2C2 v Quoine is directly applicable to the Indian smart contract context: it establishes judicial authority for the proposition that automated programmes can form binding contracts, that the contracts thus formed are subject to ordinary rules of offer and acceptance, and that mistake arguments do not automatically succeed simply because the transaction was executed automatically at an unexpected price. Indian courts should regard this decision, and its affirmation by the Singapore Court of Appeal, as highly persuasive authority.

D. European Union: MiCA and eIDAS

The eIDAS Regulation[48] establishes a legal framework for electronic signatures and seals across the EU. Under eIDAS, a "qualified electronic signature" produced using a qualified signature creation device has the same legal effect as a handwritten signature.[49] Like India's IT Act, eIDAS contemplates centrally-certified electronic signatures, not blockchain-based cryptographic signatures. However, the European Commission's 2021 eIDAS 2.0 proposal[50] explicitly contemplates the use of distributed ledger technology for electronic identity and trust services. India should monitor and potentially follow this development in any revision of the IT Act.

E. Comparative Synthesis

Table 1: Comparative Smart Contract Law — Key Issues Across Jurisdictions

Issue	India (Current)	England & Wales	USA (State)	Singapore	India (Proposed)
Smart contract validity?	Uncertain; no express provision	Yes — LawTech Legal Statement	Yes — state statutes	Yes — B2C2 v Quoine	Yes — proposed s 10B IT Act
Blockchain authentication ?	No — CA model only	Not expressly; courts flexible	Yes — state e-sign laws	Yes — ETA	Yes — proposed s 3A notification
Blockchain records admissible?	Uncertain — s 65B gap	Yes — electronic records legislation	Yes — e-records legislatio n	Yes — ETA ss 8-10	Yes — proposed s 65C
Developer liability for bugs?	Uncertain; negligence applicable	Negligence; duty of care	Varies by state	Negligence ; Consumer Protection	Negligence + statutory audit duty

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 7 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

Issue	India (Current)	England & Wales	USA (State)	Singapore	India (Proposed)
Oracle failure liability?	Uncertain; misrepresentation possible	Misrepresentation; negligence	Varies	Negligence (obiter)	Proposed misrepresentation rule
Irreversibility / remedies	No bespoke provision; general remedies	General remedies; restitution	Varies	General remedies	Proposed restitution provision

Table 1: Comparative analysis of smart contract law across five jurisdictions. "India (Proposed)" reflects the legislative package proposed in Section X.

The comparative analysis confirms that India is an outlier in its failure to resolve the smart contract enforceability question. Every other jurisdiction examined has moved — through legislation (US states), judicial decision (Singapore, England), or regulatory guidance (EU) — towards clear recognition of smart contract enforceability. India's combination of an uncertain Section 10A, a broken Section 65B evidentiary framework, and no judicial authority directly on point leaves Indian smart contract users in a position of significant and unnecessary legal uncertainty.

X. Proposed Legislative Amendments and Judicial Tests

Drawing on the analysis in Sections III through IX, this section proposes a package of legislative amendments and judicial tests to resolve the principal legal uncertainties around smart contracts under Indian law. The package has four components: (1) a new Section 10B in the IT Act recognising smart contracts as valid contracts; (2) a notification under Section 3A of the IT Act recognising blockchain cryptographic authentication as a valid electronic signature; (3) the proposed Section 65C from Section VII above; and (4) the Informed Interaction Standard for determining whether a smart contract interaction constitutes a valid offer and acceptance under the ICA.

A. Proposed Section 10B, Information Technology Act 2000 (New)

10B. Validity of Smart Contracts — (1) A smart contract — being a self-executing agreement whose terms are expressed in code deployed on a Recognised Distributed Ledger — shall not be denied legal effect or enforceability solely on the ground that: (a) the agreement is expressed in code rather than natural language; (b) the agreement is performed automatically by the execution of code without further act of either party; (c) the parties to the agreement interacted with the code using cryptographic wallet addresses rather than legally registered identities; (d) the performance of the agreement is irreversible by reason of the immutability of the Recognised Distributed Ledger; or (e) the agreement was deployed or executed by an automated electronic agent acting within the scope of its programmed authority on behalf of an identified principal. (2) For the purposes of this section, a smart contract shall be treated as satisfying the requirements of the Indian Contract Act, 1872 as to offer and acceptance if: (a) the code of the smart contract was publicly accessible at the time of the interaction; (b) the user's transaction to the smart contract address was voluntary; and (c) the terms of the smart contract were accessible to the user in a form that could reasonably be understood. (3) Where a smart contract contains an error in its code that causes performance contrary to the shared intention of the parties, the aggrieved

party shall be entitled to restitution equivalent to the loss caused by the erroneous performance, recoverable as a debt due from the party unjustly enriched by the erroneous performance. (4) A developer who deploys a smart contract for public use on a Recognised Distributed Ledger shall owe a duty of care to users of that contract to take reasonable steps to ensure that the code performs as described in any accessible documentation, including by commissioning an independent technical audit of the code before deployment where the total value locked in the contract exceeds such threshold as the Central Government may prescribe.

B. Proposed Section 3A Notification — Blockchain Cryptographic Authentication

In exercise of the powers conferred by Section 3A of the Information Technology Act, 2000, the Central Government hereby notifies the following method of electronic signature as having the same legal effect as an electronic signature under the Act: Blockchain Cryptographic Signature — the use of a private cryptographic key associated with a publicly verifiable blockchain wallet address to generate a digital signature on an electronic record, where: (a) the signature is verifiable using the corresponding public key associated with the wallet address; (b) the wallet address and the corresponding signature are recorded on a Recognised Distributed Ledger at the time of signing; and (c) the technical standards for the cryptographic algorithms used comply with the specifications published by the Ministry of Electronics and Information Technology. A blockchain cryptographic signature so verified shall constitute an electronic signature for all purposes of this Act, except in relation to documents for which a handwritten signature is required by law.

Together, the proposed Section 10B, the Section 3A notification, and the proposed Section 65C from Section VII constitute a comprehensive smart contract recognition package for Indian law. They address: the validity of smart contracts as contracts; the authentication of blockchain-based signatures; the admissibility of blockchain records as evidence; the liability of developers for code errors; and the restitutionary remedy for erroneous execution. Collectively, they remove the principal legal obstacles to the enforcement of smart contracts in Indian courts.

XI. Conclusion

This article has established that smart contracts can and should be recognised as valid contracts under Indian law. The Indian Contract Act's essential elements — offer, acceptance, consideration, capacity, free consent, and legality — can each be satisfied in a smart contract interaction, provided that the analysis is conducted with appropriate sensitivity to the technical architecture of blockchain systems. The Informed Interaction Standard proposed in Section III provides a workable doctrinal test for offer and acceptance that preserves the Act's requirement of consensus ad idem while accommodating automated execution. The consideration analysis shows that token transfers and gas fees provide adequate consideration in the vast majority of smart contract interactions. The capacity and free consent analysis identifies specific problem categories — pseudonymous contracting, algorithmic mistake — that require targeted legislative solutions.

The IT Act's framework for electronic contracts and digital signatures contains two significant gaps: the failure to recognise blockchain cryptographic authentication as a valid electronic signature, and the failure of the Section 65B certificate requirement to accommodate blockchain evidence. Both gaps have been addressed by targeted legislative proposals — the Section 3A notification and the proposed Section 65C — that can be enacted without any structural amendment to the IT Act. The remedial analysis reveals a category of problems unique to smart contracts — irreversibility, developer liability for bugs, oracle failure — that require doctrinal development

through the application and extension of existing remedies.

The comparative analysis confirms that India is behind the curve. England, Singapore, the United States, and the European Union have each developed clearer frameworks for smart contract enforceability than India currently possesses. The proposed legislative package in Section X is calibrated to bring India into alignment with best international practice while remaining faithful to the structure and principles of Indian contract law. The resolution of smart contract enforceability is not merely a technical legal question: it is a prerequisite for India's participation in the global decentralised finance ecosystem on terms of legal certainty and commercial confidence.

Conflicts of Interest and Funding

The author declares no conflicts of interest. No external funding was received for this research.

Footnotes

1. Phil Daian, "Analysis of the DAO Exploit" (Hacking Distributed, 17 June 2016).

2. Vitalik Buterin, "On the Ethereum Hard Fork" (Ethereum Blog, 17 July 2016).

3. Indian Contract Act 1872, ss 2(a), 2(b); Bhagwandas Goverdhandas Kedia v M/s Girdharilal Parshottamdas & Co AIR 1966 SC 543.

4. UNCITRAL, Model Law on Electronic Commerce (United Nations 1996); UNCITRAL, Model Law on Electronic Signatures (United Nations 2001).

5. Information Technology Act 2000, ss 3–5, 24–42 (Certifying Authorities).

6. Information Technology (Amendment) Act 2008, inserting s 10A into the IT Act 2000.

7. Trimex International FZE Ltd v Vedanta Aluminium Ltd (2010) 3 SCC 1; Bharat Sanchar Nigam Ltd v Motorola India Pvt Ltd (2009) 2 SCC 337.

8. Indian Contract Act 1872, s 2(a).

9. ibid s 2(b).

10. Carlill v Carbolic Smoke Ball Company [1893] 1 QB 256 (CA); applied in India in Great Eastern Shipping Co Ltd v Ministry of Shipping AIR 1980 Cal 79.

11. Bhagwandas Goverdhandas Kedia v M/s Girdharilal Parshottamdas & Co AIR 1966 SC 543.

12. Adams v Lindsell (1818) 1 B & Ald 681.

13. Indian Contract Act 1872, ss 182–238; Narandas Morardas Gaziwala v S P Bhagwat & Co AIR 1943 Bom 168.

14. Arizona House Bill 2417 (2017), amending Arizona Revised Statutes § 44-7003; Tennessee Code Annotated § 47-10-202 (2018).

15. Thornton v Shoe Lane Parking [1971] 2 QB 163 (CA); LIC of India v Consumer Education and Research Centre (1995) 5 SCC 482.

16. Indian Contract Act 1872, s 2(d); Chinnaya v Ramayya (1882) ILR 4 Mad 137.

17. Ethereum Foundation, Gas and Fees (Ethereum.org, 2024).

18. Indian Contract Act 1872, s 11.

19. Indian Majority Act 1875, s 3.

20. Mohori Bibee v Dharmodas Ghose (1903) 30 IA 114 (PC).

21. Indian Contract Act 1872, s 14.

22. ibid s 15.

23. ibid s 17.

24. ibid s 18.

25. ibid s 20.

26. Indian Contract Act 1872, s 23.

27. ibid s 30; Public Gambling Act 1867 (as amended by states).

28. Central Inland Water Transport Corp Ltd v Brojo Nath Ganguly AIR 1986 SC 1571.

29. Information Technology Act 2000, ss 2(1)(ta), 3, 24–42.

30. ibid s 3A (inserted by Information Technology Amendment Act 2008).

31. Ministry of Electronics and Information Technology, Gazette Notification dated 27 October 2015.

32. Anvar PV v PK Basheer (2014) 10 SCC 473.

33. Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal (2020) 7 SCC 1.

34. Shafhi Mohammad v State of Himachal Pradesh (2018) 2 SCC 801.

35. Dharambir v Central Bureau of Investigation (2008) 3 CompLJ 336 (Del).

36. Indian Contract Act 1872, s 73; Firm Srinivas Ram Kumar v Mahabir Prasad AIR 1951 SC 177.

37. Hadley v Baxendale (1854) 9 Exch 341.

38. Specific Relief Act 1963, s 10.

39. State of Rajasthan v Basant Nahata AIR 2005 SC 3949; Indian Contract Act 1872, s 70.

40. Consumer Protection Act 2019, s 2(7); M/s Spring Meadows Hospital v Harjol Ahluwalia (1998) 4 SCC 39.

41. Donoghue v Stevenson [1932] AC 562 (HL); adopted in India in Smt Savita Garg v Director, National Heart Institute (2004) 8 SCC 56.

42. UK Jurisdiction Taskforce, Legal Statement on Cryptoassets and Smart Contracts (LawTech Delivery Panel, November 2019).

43. ibid [20]–[28] (offer and acceptance); [29]–[34] (consideration); [35]–[41] (certainty and intention).

44. Arizona Revised Statutes § 44-7061 (2017).

45. Tennessee Code Annotated § 47-10-201 (2018); Nevada Revised Statutes § 719.096 (2017); Wyoming Statutes § 34-29-106 (2019); Illinois Electronic Commerce Security Act (amended 2021).

46. B2C2 Ltd v Quoine Pte Ltd [2019] SGHC(I) 03; [2020] SGCA(I) 02.

47. ibid [2020] SGCA(I) 02, [101]–[115].

48. Regulation (EU) No 910/2014 [2014] OJ L257/73 (eIDAS).

49. ibid art 25(2).

50. European Commission, Proposal for eIDAS 2.0, COM(2021) 281 final.

INSTITUTE OF LEGAL EDUCATION

(Managed by L TO J LAW ASSOCIATES)

NO. 08, ARUL NAGAR, SEERA THOPPU,
MARUDHAANDA KURICHI, SRIRANGAM - 620102,
TAMILNADU, INDIA.

ISSN 2583-2344