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

VOLUME 6 AND ISSUE 10 OF 2026

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

Published by

Institute of Legal Education

https://iledu.in

BEYOND TRADITIONAL CONTRACTS: SMART CONTRACTS AND THE TRANSFORMATION OF INDIAN COMMERCIAL LAW

AUTHOR – BAIBHABA CHINHARA, LLM STUDENT, G.M. LAW COLLEGE, SRI VIHAR, PURI

BEST CITATION – BAIBHABA CHINHARA**,** BEYOND TRADITIONAL CONTRACTS: SMART CONTRACTS AND THE TRANSFORMATION OF INDIAN COMMERCIAL LAW, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 6 (10) OF 2026, PG. 81-100, APIS – 3920 – 0001 & ISSN - 2583-2344. DOI - https://doi.org/10.65393/IJLRV6I1011

ABSTRACT

The digital transformation of commerce has introduced smart contracts—self-executing, code-based agreements on blockchain infrastructure—that challenge traditional legal doctrines by automating performance and minimizing intermediaries. While gaining global traction across finance and supply chains, their legal status within Indian commercial law remains doctrinally fragmented. This article critically examines whether existing Indian statutory frameworks, particularly the Indian Contract Act, 1872, and the Information Technology Act, 2000, can accommodate these blockchain-enabled arrangements. It interrogates foundational legal questions surrounding automated offer and acceptance, algorithmic consent, the enforceability of self-executing obligations, and the evidentiary admissibility of decentralized records. Furthermore, the study analyzes the technological anatomy of smart contracts, distinguishing between legal contracts expressed in code and autonomous software protocols, to highlight legal complexities that conventional doctrines fail to address. Through a comparative examination of regulatory developments in the US, UK, Singapore, EU, and UAE, the article highlights an international movement toward the formal recognition of blockchain contracting. Against this backdrop, it argues that India's existing legal framework, though interpretively flexible, is structurally inadequate for resolving the jurisdictional, liability, and consumer protection challenges posed by algorithmic transactions. The study concludes that smart contracts necessitate a paradigm shift in commercial jurisprudence. India must move beyond mere interpretive accommodation and develop a coherent legislative architecture that balances technological innovation with legal certainty, contractual fairness, and commercial accountability.

Keywords: *Smart Contracts; Indian Contract Law; Blockchain Technology; Algorithmic Transactions; Commercial Jurisprudence; Digital Contracts.*

1. INTRODUCTION

Commercial law has historically evolved in response to transformations in modes of economic exchange. From oral mercantile bargains and handwritten agreements to formally drafted written contracts and digitally executed e-contracts, the legal conception of contractual obligations has continually adapted to changes in commercial practice. The twenty-first century digital economy, however, presents a qualitatively distinct challenge. The emergence of blockchain-enabled smart contracts does not merely alter the medium through which agreements are expressed; rather, it fundamentally reconfigures the mechanisms through which contractual obligations are created, verified, and enforced. Traditional contract law rests upon identifiable human agency, mutual assent, interpretive flexibility, and institutional enforcement through courts or arbitral mechanisms. Smart contracts, by contrast, operate through executable code capable of autonomously performing contractual obligations upon satisfaction of

predefined conditions. Instead of relying upon subsequent legal enforcement, such arrangements often integrate performance directly into the architecture of the agreement itself. In effect, execution becomes technologically embedded rather than judicially contingent. This transformation raises profound jurisprudential questions. Can a sequence of coded instructions constitute a legally valid contract? Does automated execution satisfy the doctrinal requirements of contractual intention and consent? How should courts interpret contractual obligations embedded in software architecture rather than textual language? Who bears liability when algorithmic execution causes unintended commercial harm? Can immutable blockchain records satisfy evidentiary requirements under conventional procedural law? These questions lie at the heart of contemporary commercial legal discourse.

India presents a particularly compelling jurisdiction for examining these issues. As one of the world's fastest-growing digital economies, India has embraced electronic commerce, digital payments, fintech innovation, and platform-based commercial ecosystems at remarkable speed. Government-led initiatives promoting digital governance, paperless transactions, and electronic authentication have accelerated the migration of commercial activity into technologically mediated spaces. The Supreme Court of India has progressively recognized this shift, noting in cases like *Trimex International FZE v. Vedanta Aluminium Ltd.*[190] that once a contract is concluded digitally, formal execution is merely a formality. Yet Indian contract law remains rooted in nineteenth-century legislative architecture, albeit supplemented by modern electronic transaction legislation.

Although the Indian Contract Act, 1872 and the Information Technology Act, 2000 recognize conventional and electronic contracts, neither explicitly addresses blockchain-based smart contracts. While smart contracts promise greater efficiency, transparency, reduced costs, and automation in commercial transactions, they also raise concerns regarding consumer protection, liability, jurisdiction, and enforceability. This article examines whether Indian commercial law is adequately equipped to regulate smart contracts while preserving the fundamental principles of fairness, justice, and legal certainty in a rapidly evolving digital economy.

2. CONCEPTUAL FOUNDATION OF SMART CONTRACTS

The term "smart contract" has often been used loosely, leading to considerable conceptual confusion in both technological and legal discourse. Despite its widespread popularity, the expression is arguably misleading. Smart contracts are not necessarily "smart" in the sense of possessing intelligence, nor are they invariably "contracts" in the conventional legal sense.

The conceptual origins of smart contracts are generally traced to computer scientist Nick Szabo, who in the 1990s described them as computerized transaction protocols that execute the terms of a contract.[191] Szabo envisioned technological systems capable of automating commercial exchanges by embedding contractual obligations directly into programmable architectures. His often-cited vending machine analogy illustrates the concept effectively: once payment is inserted and conditions are satisfied, performance occurs automatically without requiring human intervention.

Modern smart contracts differ significantly from this early conceptualization because of blockchain integration. Blockchain technology provides decentralized infrastructure within which smart contract code can execute with transparency, immutability, and distributed verification. This enables autonomous contractual performance without centralized

[190] *Trimex International FZE v. Vedanta Aluminium Ltd.*, (2010) 3 SCC 1 (India).

191 Szabo, N. (1996). Smart contracts: Building blocks for digital markets. Extropy: The Journal of Transhumanist Thought, (16), 50-58.

intermediaries. From a technical perspective, a smart contract is essentially executable code deployed on a distributed ledger network. The code specifies conditional logic—typically expressed in "if-then" architecture—under which predefined events trigger automated actions. For example:

- If payment is received, then transfer digital asset ownership.
- If shipment confirmation is verified, then release escrow funds.
- If insurance conditions are satisfied, then initiate compensation payment.

This operational structure creates deterministic execution. Once coded conditions are met, performance occurs automatically according to program instructions. Legally, however, important distinctions must be made. A smart contract may fall into several categories:

(a) Code Supporting a Traditional Legal Contract

In this model, parties enter into a conventional legal agreement, while certain operational obligations are automated through code.

- **Example:** A written commercial supply agreement provides that payment shall automatically release upon delivery confirmation through blockchain verification.

Here, the legal contract remains textual; smart execution merely facilitates performance.

(b) Entire Contract Expressed Through Code

In this model, contractual obligations themselves are represented exclusively in software code.

- **Example:** A decentralized lending transaction where loan issuance, collateral locking, interest calculation, and liquidation operate entirely algorithmically.

This raises significant legal interpretation challenges because traditional legal language is absent.

(c) Autonomous Software Protocol Without Legal Intent

Some blockchain applications merely automate transactional behaviour without evidencing legal contractual intention.

- **Example:** Decentralized exchange token swaps executed through protocol interaction.

Not every automated digital interaction necessarily creates enforceable legal obligations.

This distinction is doctrinally critical because contract law depends upon legal intention, not merely functional automation. A technically automated transaction does not automatically qualify as a legally enforceable contract.

3. HISTORICAL EVOLUTION: FROM TRADITIONAL CONTRACTS TO DIGITAL COMMERCIAL AGREEMENTS

Contract law has evolved with commerce, progressing from oral agreements based on trade customs to written contracts that ensured certainty and enforceability. Industrialization increased contractual complexity, while the digital era introduced electronic agreements, including click-wrap and browse-wrap contracts, reflecting the law's adaptation to technological and commercial developments.

Indian law accommodated this shift through the Information Technology Act, 2000, which recognized electronic records and digital authentication mechanisms. The judiciary further cemented this in cases such as *Tamil Nadu Organic Private Ltd. v. State Bank of India*[192], affirming that electronic records satisfy the requirement of a written contract. Yet digital

192 Tamil Nadu Organic Private Ltd. v. State Bank of India, AIR 2014 Mad 103 (India).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 10 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

contracts largely preserved traditional legal structure:

- Human parties
- Express consent
- Textual terms
- Institutional enforcement

Smart contracts represent a deeper rupture. Traditional contracts separate agreement formation from performance enforcement.

- **Example:** Two parties execute an agreement → obligation exists → performance may occur voluntarily or through judicial compulsion.

Smart contracts collapse this separation. Agreement architecture itself contains execution mechanisms. This shifts contract law from:

Promise + legal enforcement

to:

Code + automated performance

The transformation is not merely procedural but philosophical. Traditional contract law tolerates ambiguity, contextual interpretation, equitable adjustment, and judicial intervention. Smart contract systems prioritize precision, determinism, automation, and computational certainty.

Law traditionally asks: *What did the parties intend?*

Code asks: *What instructions were programmed?*

This creates profound jurisprudential tension between interpretive legal reasoning and machine determinism.

4. TECHNICAL ARCHITECTURE OF SMART CONTRACTS: UNDERSTANDING THE TECHNOLOGICAL BACKBONE

Smart contracts combine contractual obligations with automated execution through blockchain technology. Unlike traditional agreements, they embed performance directly into programmable code that executes when predefined conditions are met. Understanding their technological architecture is therefore essential for assessing their legal validity, enforceability, and broader implications.

4.1 Blockchain Infrastructure

Blockchain is a distributed ledger technology that records transactions across multiple interconnected nodes rather than storing information in a centralized database. Each transaction is grouped into blocks, cryptographically linked to preceding blocks, thereby forming an immutable chain.

The principal characteristics of blockchain include:

- decentralization;
- immutability;
- transparency;
- cryptographic verification;
- distributed consensus;
- resistance to unauthorized alteration.

These features are commercially significant because they reduce reliance upon centralized intermediaries such as banks, escrow agents, clearing houses, registrars, and payment processors.

From a legal perspective, however, decentralization introduces accountability complexities. In conventional commercial systems, liability can typically be traced to identifiable institutional actors. Blockchain ecosystems may distribute operational control across anonymous or pseudonymous participants, making responsibility allocation more difficult.

4.2 Executable Code

Smart contracts function through software code written in programming languages such as Solidity (commonly used on Ethereum networks), Rust, or other blockchain-compatible coding environments. This code contains operational logic.

- **Example:**
  - if payment is received, release digital goods;

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 10 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

- if collateral value falls below threshold, liquidate assets;
- if shipment confirmed, transfer escrow funds.

Unlike traditional contractual clauses, these instructions are machine-readable rather than human readable. This distinction is jurisprudentially important. Legal interpretation traditionally depends upon language, intention, contextual meaning, and judicial construction. Code operates with strict syntactic precision and deterministic execution. Courts may interpret ambiguous words; software does not interpret intention beyond coded instruction. Thus, where legal understanding diverges from software execution, disputes become inevitable.

4.3 Distributed Consensus Mechanism

Blockchain transactions are validated through consensus protocols. Common consensus systems include:

- Proof of Work;
- Proof of Stake;
- Delegated consensus variants.

Consensus determines whether network participants accept a transaction as valid. Legally, this raises an important question: Can decentralized network validation be treated as legally reliable authentication?

Traditional legal systems recognize institutional verification mechanisms such as notarization, certification, banking authentication, and digital signature frameworks. Blockchain consensus operates differently, relying on cryptographic trust rather than centralized legal authority. Indian law has yet to directly clarify this issue.

4.4 Cryptographic Signatures and Wallet Authentication

Blockchain transactions usually require cryptographic key authentication. A participant typically controls:

- a public key (visible identifier);
- a private key (confidential authorization mechanism).

Transactions are authorized through private key signatures. Functionally, this resembles authentication. Legally, however, equivalence with recognized electronic signatures remains uncertain. Under Indian law, electronic authentication is regulated under the Information Technology Act, 2000, but blockchain wallet authentication does not always neatly fit statutory digital signature frameworks. Thus, technological authorization may not automatically equal legally recognized consent.

4.5 Oracles

A smart contract cannot independently access external real-world information unless connected through external data feeds known as "oracles." Examples include:

- weather data for insurance triggers;
- market price feeds for financial liquidation;
- shipment confirmations for logistics;
- identity verification systems;
- banking payment confirmations.

If an insurance smart contract pays compensation upon rainfall crossing a threshold, it must rely upon external weather data. This creates legal risk. The blockchain itself may be tamper-resistant, but oracle inputs may be inaccurate, manipulated, delayed, or fraudulent. If a smart contract executes based on incorrect oracle data, liability attribution becomes legally contentious. Potential responsible actors may include:

- oracle providers;
- software developers;
- contracting parties;
- intermediaries;
- platform operators.

Indian jurisprudence has not yet comprehensively addressed this issue.

4.6 Immutability

One of blockchain's most celebrated features is immutability. Once deployed, smart contract code may become difficult or impossible to alter. Commercially, this enhances

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 10 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

predictability. Legally, immutability creates substantial concerns. Traditional contract law allows:

- rectification;
- rescission;
- modification;
- discharge;
- judicial intervention;
- equitable relief.

Immutable smart contracts may frustrate these remedies. For example: A coding error transfers funds incorrectly. Under conventional law, courts may intervene. Under blockchain execution, reversal may be technologically impossible. This creates a tension between legal reversibility and technological finality.

5. INDIAN CONTRACT ACT, 1872 AND SMART CONTRACTS: ENFORCEABILITY ANALYSIS

The principal question confronting Indian commercial law is whether smart contracts satisfy the legal requirements of valid contract formation under the Indian Contract Act, 1872. Section 10 of the Indian Contract Act provides:

"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 framework remains technologically neutral in language. Therefore, the absence of explicit reference to blockchain does not automatically exclude smart contracts. The real issue is doctrinal compatibility.

5.1 Offer and Acceptance

A valid contract requires lawful offer and acceptance. Under traditional doctrine:

- one party makes a proposal;
- the other communicates unconditional assent.

Sections 2(a) and 2(b) define proposal and acceptance. The landmark case of *Bhagwandas Goverdhandas Kedia v. Girdharilal Parshottamdas and Co.*[193] established that a contract is complete only when the acceptance is clearly communicated to the offeror. Smart contract environments complicate this process.

Scenario 1: Traditional Interface with Smart Execution

Example: A digital platform presents terms. User clicks acceptance. Blockchain automates execution.

This resembles recognized electronic contracting. Indian courts have generally accepted electronic manifestations of assent.

Scenario 2: Autonomous Blockchain Interaction

Example: A user interacts directly with decentralized code. No textual negotiation occurs. Execution occurs automatically.

Here, identifying offer and acceptance becomes difficult.

- Is deployment of code the offer?
- Is wallet interaction acceptance?
- Is machine response valid assent?

Traditional doctrine assumes legally communicative human intent. Purely algorithmic environments challenge this assumption.

5.2 Consensus ad Idem (Meeting of Minds)

Contract formation requires mutual understanding. Consent must be real, informed, and directed toward common terms, a principle affirmed in *Tarsem Singh v. Sukhminder Singh*[194]. Smart contracts create serious difficulties here. Code may be incomprehensible to ordinary users. A party may functionally interact with software without understanding its operational consequences. This creates a conceptual distinction between:

- procedural interaction;
- substantive contractual understanding.

193 Bhagwandas Goverdhandas Kedia v. Girdharilal Parshottamdas and Co., AIR 1966 SC 543 (India).

194 Tarsem Singh v. Sukhminder Singh, (1998) 3 SCC 471 (India).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 10 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

If a user cannot interpret executable code, can genuine contractual consensus exist? Indian doctrine traditionally protects parties against misunderstanding, fraud, coercion, mistake, and misrepresentation. Algorithmic opacity threatens these protections.

5.3 Free Consent

Section 14 recognizes free consent. Consent is not free when caused by:

- coercion;
- undue influence;
- fraud;
- misrepresentation;
- mistake.

Smart contracts raise novel questions.

- **Fraud through Code:** Malicious smart contracts may conceal exploitative logic. Users may unknowingly authorize harmful transactions.
- **Mistake:** Coding bugs may produce unintended contractual outcomes. If code diverges from intended agreement, is there mutual mistake?
- **Misrepresentation:** Platforms may inaccurately describe smart contract functionality. This creates defective consent.

Thus, technological automation does not eliminate classical consent defects.

5.4 Competency of Parties

Section 11 requires contractual competency. Parties must:

- be majors;
- be of sound mind;
- not be disqualified by law.

As established in the seminal case of *Mohori Bibee v. Dharmodas Ghose*[195], agreements with minors are *void ab initio*. Blockchain transactions frequently occur pseudonymously. Identity verification may be absent. This creates practical enforceability problems. If contractual participants are unidentified:

- age verification becomes impossible;
- legal capacity cannot be assessed;
- enforcement becomes uncertain. Commercial certainty suffers.

5.5 Lawful Consideration

Section 2(d) recognizes consideration. Smart contract transactions typically involve:

- cryptocurrency transfers;
- tokenized assets;
- digital exchange obligations;
- automated service delivery.

Legal uncertainty arises where consideration consists of digital assets with uncertain regulatory status. Even where technological exchange exists, legal characterization matters. If consideration is unlawful or legally uncertain, enforceability may fail.

5.6 Lawful Object

Section 23 invalidates agreements with an unlawful object. Smart contracts are technologically neutral. They may facilitate legitimate commerce or unlawful activity. Potential problematic uses include:

- illicit transfers;
- unregulated financial schemes;
- sanctions evasion;
- fraudulent token transactions.

Thus, legality depends on underlying purpose, not technology itself.

5.7 Certainty

Section 29 invalidates uncertain agreements, a principle rigorously upheld by Indian courts, such as in *Kovuru Kalappa Devara v. Kumar Krishna Mitter*[196]. Traditional legal drafting often contains ambiguity, interpreted contextually. Smart contracts arguably enhance certainty because code specifies deterministic actions.

195 Mohori Bibee v. Dharmodas Ghose, (1903) 30 IA 114 (PC) (India).

196 Kovuru Kalappa Devara v. Kumar Krishna Mitter, AIR 1945 Mad 10 (India).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 10 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

However, certainty in code does not guarantee legal certainty. Software precision may conceal conceptual uncertainty.

- *Example*: Code triggers payment upon "delivery confirmation." But what legally counts as delivery? The code may assume one interpretation. Law may adopt another.

Thus, computational certainty may coexist with legal ambiguity.

5.8 Possibility of Performance

Contracts impossible to perform may fail (Section 56, Doctrine of Frustration, referenced in *Satyabrata Ghose v. Mugneeram Bangur & Co.*[197]). Smart contracts execute automatically when conditions are satisfied. However:

- oracle failure;
- network congestion;
- software malfunction;
- protocol collapse;
- cyberattack

may frustrate performance. Thus, technological dependence introduces novel impossibility scenarios.

6. SMART CONTRACTS AND BREACH: CAN THERE BE BREACH IN SELF-EXECUTING AGREEMENTS?

A central conceptual question is whether breach remains meaningful when performance is automated. Traditional contracts contemplate voluntary or involuntary non-performance. Section 73 of the Indian Contract Act, 1872 deals with compensation for loss or damage caused by a breach of contract, a principle comprehensively elucidated by the Supreme Court in cases like *Kailash Nath Associates v. Delhi Development Authority*[198].

Smart contracts reduce conventional breach by automating execution. Yet breach does not disappear. It transforms. Possible breaches include:

- defective coding;
- wrongful triggering;
- malicious deployment;
- inaccurate oracle input;
- concealed exploit mechanisms;
- premature execution;
- failure of external dependencies.

Thus, breach shifts from refusal-to-perform toward design-failure and system-failure models. Legal doctrine must adapt accordingly, re-evaluating whether damages can be claimed against the programmer, the platform, or the counterparty when automated logic misfires.

7. SPECIFIC RELIEF AND JUDICIAL REMEDIES

Indian law permits remedies including:

- damages;
- injunction;
- rescission;
- specific performance;
- rectification.

The Specific Relief (Amendment) Act, 2018 transformed specific performance from an equitable, discretionary remedy into a statutory mandate, as observed by the courts in *Sushil Kumar Agarwal v. Meenakshi Sadhu*[199]. Smart contracts complicate these remedies.

Example: Funds automatically transferred irreversibly. A court may declare the transaction wrongful. But technological reversal may be impossible.

This creates enforcement asymmetry: legal remedy exists in principle but not in operational reality. Commercial law must reconcile normative rights with technical constraints.

8. SMART CONTRACTS AND THE INFORMATION TECHNOLOGY ACT, 2000: ELECTRONIC LEGAL RECOGNITION IN INDIA

The Information Technology Act, 2000 provides legal recognition to electronic transactions and forms the basis for assessing smart contract enforceability in India. However,

197 Satyabrata Ghose v. Mugneeram Bangur & Co., AIR 1954 SC 44 (India).
198 Kailash Nath Associates v. Delhi Development Authority, (2015) 4 SCC 136 (India).
199 Sushil Kumar Agarwal v. Meenakshi Sadhu, (2019) 2 SCC 241 (India).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 10 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

enacted before blockchain technology emerged, it contains no explicit provisions on decentralized, self-executing contracts. Consequently, applying the Act to smart contracts depends largely on judicial interpretation rather than statutory clarity.

8.1 Legal Recognition of Electronic Records

Section 4 of the Information Technology Act provides legal recognition to electronic records. It establishes that where any law requires information to be in writing or in printed form, such requirement is satisfied if the information is rendered or made available in electronic form and remains accessible for subsequent reference.

This provision is technologically significant. Smart contracts exist in digital environments. Their contractual logic, transactional records, deployment history, execution pathways, and associated interactions are electronically recorded. Therefore, at a foundational level, the mere electronic nature of smart contracts should not invalidate them.

However, legal complexity emerges because blockchain smart contracts differ from conventional electronic documents.

Traditional electronic records:

- are readable;
- are modifiable;
- are institutionally controlled;
- are stored within centralized systems.

Blockchain records:

- are distributed;
- may be immutable;
- may exist in executable rather than human-readable code;
- may be pseudonymous.

Thus, although Section 4 supports broad digital recognition, its practical application to blockchain remains interpretively uncertain.

8.2 Electronic Signatures and Authentication

Authentication presents a more difficult issue. Section 5 grants legal recognition to electronic signatures where statutory requirements are satisfied. Indian digital authentication frameworks historically focused on:

- digital signatures;
- asymmetric cryptographic systems;
- certifying authority verification.

Blockchain smart contracts generally rely upon wallet-based cryptographic authorization rather than state-recognized digital certification systems. A user interacting with blockchain technology typically authorizes transactions through private key signatures. Technologically, this constitutes authentication.

Legally, however, the question is whether such authentication falls within recognized statutory parameters. Potential issues include:

- absence of certifying authority involvement;
- decentralized verification;
- pseudonymous identity structures;
- lack of conventional electronic signature infrastructure.

If Indian courts adopt a purposive interpretation, blockchain authentication may be recognized functionally. If courts insist upon strict statutory conformity, legal uncertainty may persist. Thus, formal authentication remains a contested issue.

8.3 Electronic Contract Formation

Section 10A of the Information Technology Act is particularly significant. It provides that contracts formed through electronic means shall not be deemed unenforceable merely because electronic communication was used. The courts have upheld this in cases like *M/s. P.R. Transport Agency v. Union of India*[200], where an e-auction acceptance via email was deemed a valid, binding contract. This provision strongly

200 M/s. P.R. Transport Agency v. Union of India, AIR 2006 All 23 (India).

supports digital contracting legitimacy. Applied broadly, it suggests:

electronic communication ≠ legal invalidity.

Accordingly, where smart contract arrangements reflect genuine contractual intention, electronic formation alone should not defeat enforceability. Yet important limitations remain. Section 10A contemplated conventional e-commerce arrangements:

- emails;
- digital acceptance;
- online purchase transactions;
- electronic procurement systems.

It did not explicitly contemplate:

- autonomous execution;
- decentralized blockchain protocols;
- code-native contracting;
- machine-mediated contractual logic.

Thus, while Section 10A offers persuasive support, its direct application to autonomous smart contracts remains legally unresolved.

9. INDIAN EVIDENCE LAW AND BLOCKCHAIN RECORDS

Even if smart contracts are legally recognized, enforceability depends heavily upon evidentiary admissibility. Commercial disputes require proof. The evidentiary status of blockchain records therefore becomes critical.

9.1 Electronic Evidence Framework

Indian evidentiary law recognizes electronic evidence. The framework historically developed through provisions relating to digital records and electronic documentation, most notably Section 65B of the Indian Evidence Act, 1872 (now Section 63 of the Bharatiya Sakshya Adhiniyam, 2023). The Supreme Court of India in *Anvar P.V. v. P.K. Basheer*[201] and later clarified in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*[202], made the certification of electronic records a mandatory condition precedent for their admissibility. Blockchain records may potentially include:

- deployment logs;
- wallet transactions;
- execution history;
- timestamped transfers;
- cryptographic verification trails;
- transactional metadata.

These features enhance evidentiary reliability. Blockchain timestamps may offer stronger auditability than ordinary digital databases. However, evidentiary admissibility is not automatic. Courts must assess:

- authenticity;
- integrity;
- attribution;
- relevance;
- legal reliability.

9.2 Evidentiary Strength of Blockchain

Blockchain offers several evidentiary advantages:

- **Immutability:** Tampering becomes significantly more difficult.
- **Timestamp Integrity:** Transaction chronology becomes traceable.
- **Distributed Verification:** Records are not dependent upon single-party custody.
- **Auditability:** Historical transaction pathways remain visible.

These features may strengthen evidentiary credibility.

9.3 Attribution Problems

A serious challenge concerns authorship and identity. Blockchain addresses may not reveal legal identity. A transaction may show *wallet X transferred digital asset Y.* But legal proceedings require: *who controlled wallet X?*

Without attribution, evidentiary usefulness weakens. Commercial litigation requires person-specific accountability.

9.4 Practical Evidentiary Difficulties

Additional issues include:

- interpretation of machine-readable code;

201 Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473 (India).

202 Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1 (India).

- expert dependency;
- translation of blockchain architecture into judicially comprehensible evidence;
- foreign network infrastructure concerns;
- decentralized record authentication complexities.

Courts may increasingly rely upon technical expert testimony. This raises procedural burdens.

10. SMART CONTRACTS AND JUDICIAL INTERPRETATION: CODE VS LEGAL LANGUAGE

One of the deepest jurisprudential challenges lies in interpretation. Traditional contracts are interpreted through legal language. In *Bangalore Electricity Supply Co. Ltd. v. E.S. Solar Power Pvt. Ltd.*[203], the Supreme Court emphasized that courts must seek to give effect to the plain, literal, and grammatical meaning of the contractual language.

Courts examine:

- intention;
- context;
- conduct;
- commercial purpose;
- implied obligations;
- equitable considerations.

Smart contracts disrupt this framework. Code operates differently from legal drafting. Law tolerates ambiguity. Code rejects ambiguity. Legal drafting may say: *"reasonable efforts shall be undertaken."* Code cannot operationalize vague normative concepts without explicit computational definitions. Thus, smart contracts privilege mechanistic certainty over interpretive flexibility.

10.1 The Code-Is-Law Problem

A prominent conceptual claim in blockchain discourse suggests: *"Code is law."*

This proposition means software architecture itself governs behaviour. Execution occurs automatically. No judicial intervention is needed for performance.

However, from legal jurisprudence, this claim is problematic. Law is not merely execution. Law includes:

- fairness;
- interpretation;
- justice;
- equitable correction;
- public policy;
- remedial discretion.

Code may enforce instructions. Law evaluates legitimacy. Thus: **code may implement obligations, but law determines enforceability.**

10.2 Interpretation Conflicts

Suppose:

- written agreement states one intention.
- smart contract code executes differently.

Which prevails? Possible approaches:

- **Textual Primacy:** Legal agreement governs. Code is an implementation tool.
- **Code Primacy:** Operational execution reflects actual agreed intent.
- **Hybrid Interpretation:** Courts evaluate both.

Indian jurisprudence lacks definitive guidance on this intersection, and commercial uncertainty follows.

11. COMMERCIAL TRANSFORMATION: SECTOR-WISE APPLICATIONS IN INDIA

Smart contracts are not theoretical abstractions. They possess transformative commercial implications across multiple sectors.

11.1 Banking and Financial Services

Banking involves payments, settlement, escrow, collateral, syndicated lending, and trade finance.

The legality and commercial reality of digital assets driving these smart contracts were significantly affirmed by the Supreme Court in *Internet and Mobile Association of India v.*

203 Bangalore Electricity Supply Co. Ltd. v. E.S. Solar Power Pvt. Ltd., (2021) 6 SCC 718 (India).

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

VOLUME 6 AND ISSUE 10 OF 2026

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

Published by

Institute of Legal Education

https://iledu.in

Reserve Bank of India[204], which struck down the RBI's circular banning banks from dealing with cryptocurrency entities, keeping the door open for decentralized fintech. Smart contracts may automate:

- payment release;
- compliance triggers;
- collateral enforcement;
- loan servicing;
- settlement finality.

Potential benefits include reduced intermediaries, lower transaction costs, faster settlement, transparency, and fraud reduction. Risks include coding errors, unauthorized triggers, regulatory non-compliance, and consumer vulnerability.

11.2 Insurance

Insurance smart contracts may automate claims.

- *Example*: parametric crop insurance. If rainfall data falls below threshold, payout occurs automatically.

Advantages: speed, transparency, reduced claims disputes, administrative efficiency.

Risks: oracle manipulation, inaccurate trigger logic, exclusion unfairness, lack of human review.

11.3 Supply Chain and Logistics

Supply chains require shipment verification, customs confirmation, payment release, and document validation. Smart contracts may automate escrow release, delivery confirmation, inventory triggers, and procurement workflows.

Benefits include traceability, anti-fraud mechanisms, and faster execution. Challenges involve real-world verification dependency, oracle reliability, and jurisdictional fragmentation.

11.4 Real Estate Transactions

Potential applications include title transfer workflows, escrow automation, payment verification, and lease execution. However, Indian real estate involves formal registration compliance. Property law imposes statutory procedural requirements. Under Section 17 of the Registration Act, 1908, read with the Supreme Court's ruling in *Suraj Lamp & Industries Pvt. Ltd. v. State of Haryana*[205], the transfer of immovable property legally requires a registered deed. Thus, smart contract automation cannot independently replace registration law.

11.5 Securities and Capital Markets

Capital market applications include settlement automation, tokenized securities, dividend distribution, and compliance monitoring. Benefits include faster clearing, reduced settlement delays, and operational efficiency. Risks include regulatory incompatibility, investor protection concerns, and systemic software failure.

11.6 E-Commerce

Digital commerce may use smart contracts for escrow, milestone payments, automated refunds, licensing, and digital goods distribution. Advantages include frictionless transactions and reduced disputes, though consumer risks remain significant.

11.7 International Trade

Cross-border commerce particularly benefits from automation. Traditional trade suffers from documentary complexity, payment delays, intermediary dependency, and jurisdictional friction. Smart contracts may streamline letters of credit, customs compliance workflows, shipping verification, and escrow execution. However, international legal harmonization remains incomplete.

12. CONSUMER PROTECTION CONCERNS

Consumer law introduces heightened scrutiny. Under the Consumer Protection Act, 2019, the inclusion of "unfair contracts" allows courts and commissions to strike down terms that are severely skewed against the consumer,

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

205 Suraj Lamp & Industries Pvt. Ltd. v. State of Haryana, (2012) 1 SCC 656 (India).

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

VOLUME 6 AND ISSUE 10 OF 2026

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

Published by

Institute of Legal Education

https://iledu.in

as reiterated in *Pioneer Urban Land and Infrastructure Ltd. v. Govindan Raghavan*[206]. Smart contracts may produce asymmetrical power structures. Risks include:

- opaque coding;
- non-negotiable automated terms;
- hidden execution consequences;
- defective consent;
- lack of dispute flexibility;
- algorithmic unfairness.

A consumer may technically "agree" without meaningful understanding. This resembles but may exceed traditional click-wrap asymmetry. Automation should not become a mechanism for circumventing fairness protections.

13. JURISDICTIONAL CHALLENGES AND CONFLICT OF LAWS IN SMART CONTRACT DISPUTES

One of the most formidable legal difficulties posed by smart contracts lies in jurisdiction. Traditional commercial disputes are ordinarily anchored to identifiable territorial connections. Courts determine jurisdiction by examining factors such as the place where the contract was executed, the place of performance, the location of parties, the situs of property, or the territorial nexus of the dispute. Smart contracts destabilize these conventional principles because blockchain transactions frequently transcend territorial boundaries, operate through decentralized networks, and may involve pseudonymous participants whose legal identity or physical location remains uncertain. The jurisdictional question becomes especially problematic in international commercial transactions where parties located in different legal systems interact with blockchain infrastructure distributed across multiple countries. Consider a hypothetical transaction:

- Party A located in India deploys a smart contract.
- Party B located in Singapore interacts with it.
- The blockchain validators are distributed globally.
- Payment occurs through digital assets.
- Oracle data originates from a European service provider.
- The software developer is based in the United States.

In such circumstances, fundamental jurisdictional questions arise:

- Where was the contract formed?
- Where was acceptance communicated?
- Where did performance occur?
- Which court possesses territorial competence?
- Which legal system governs interpretation?

Traditional legal frameworks struggle with these questions because blockchain environments resist geographic localization.

13.1 Place of Contract Formation

Under classical contract law, identifying the place of contract formation assists in determining jurisdiction. Smart contracts complicate this. If deployment of code constitutes offer and blockchain interaction constitutes acceptance, where does acceptance occur? Possibilities include:

- the location of the accepting party;
- the network node recording the transaction;
- the jurisdiction where code was deployed;
- the location of wallet control;
- the jurisdiction specified in associated documentation.

No settled Indian jurisprudence currently resolves this.

13.2 Place of Performance

Jurisdiction may also depend upon performance location. Yet smart contracts execute digitally. Automated payment transfers do not occur in conventional territorial spaces. Execution occurs across decentralized

206 Pioneer Urban Land and Infrastructure Ltd. v. Govindan Raghavan, (2019) 5 SCC 725 (India).

computational architecture. This creates legal ambiguity.

13.3 Governing Law

Commercial certainty ordinarily depends upon governing law clauses. In *National Thermal Power Corp. v. Singer Company*[207], the Supreme Court emphasized the principle of party autonomy, allowing parties to choose the governing law. However, purely decentralized interactions may lack express legal choice provisions. This creates uncertainty regarding contractual interpretation, remedies, enforceability, consumer protections, and regulatory compliance. Absent express legal architecture, courts may face significant interpretive complexity.

13.4 Arbitration as a Commercial Solution

Commercial actors may increasingly rely upon arbitration. Advantages include jurisdictional flexibility, contractual autonomy, international enforceability, and procedural adaptability. The conceptualization of the "seat" of arbitration is pivotal in international commercial law, as laid down in *Bharat Aluminium Co. v. Kaiser Aluminium Technical Services Inc. (BALCO)*[208].

Smart contract ecosystems may even integrate arbitration triggers (such as decentralized dispute resolution protocols). However, arbitration presupposes identifiable legal parties and enforceable procedural consent. Purely decentralized ecosystems remain problematic in effectively binding anonymous nodes to an arbitral award.

14. LIABILITY IN SMART CONTRACT ECOSYSTEMS

A central legal question concerns responsibility when smart contracts malfunction, misfire, or produce unintended consequences. Traditional contracts typically involve identifiable human actors. Smart contract ecosystems involve multiple stakeholders:

- contracting parties;
- software developers;
- blockchain platform operators;
- oracle providers;
- interface designers;
- custodial intermediaries;
- auditors;
- third-party service providers.

Allocating liability becomes significantly more complex in a decentralized environment where traditional doctrines of privity of contract and negligence must be stretched to accommodate new technological realities.

14.1 Developer Liability

If defective code causes financial harm, should software developers be liable? Under the Indian law of torts, establishing a duty of care is paramount, as elucidated by the Supreme Court in cases like *Rajkot Municipal Corporation v. Manjulben Jayantilal Nakum*.[209]

Arguments supporting liability:

- foreseeable commercial reliance;
- negligent coding;
- defective architecture;
- hidden vulnerabilities.

Counterarguments:

- developers merely provide infrastructure;
- users assume protocol risk;
- decentralized systems reduce centralized responsibility.

Liability may depend upon factual circumstances, representations, and contractual architecture. If a developer releases open-source code without commercial warranties, imposing strict liability may stifle innovation. However, if a developer commercializes a proprietary smart contract platform, consumer protection laws and standard negligence principles will likely apply.

207 National Thermal Power Corp. v. Singer Company, (1992) 3 SCC 551 (India).
208 Bharat Aluminium Co. v. Kaiser Aluminium Technical Services Inc., (2012) 9 SCC 552 (India).
209 Rajkot Municipal Corporation v. Manjulben Jayantilal Nakum, (1997) 9 SCC 552 (India).

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

VOLUME 6 AND ISSUE 10 OF 2026

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

Published by

Institute of Legal Education

https://iledu.in

14.2 Oracle Liability

Oracles create major legal vulnerability. If a smart contract executes based upon inaccurate external data: *who bears responsibility?* Potential candidates:

- oracle provider;
- contracting parties;
- software integrator;
- platform operator.

This remains legally unresolved in India. However, under Section 73 of the Indian Contract Act, if the oracle provider was contractually obligated to provide accurate data and failed, they could be liable for consequential damages, provided the damages naturally arose in the usual course of things (*Hadley v. Baxendale* principles, strictly followed in India).

14.3 Platform Liability

If users interact through centralized interfaces, platform operators may attract liability. Possible grounds:

- misrepresentation;
- consumer deception;
- negligent security;
- inadequate disclosures;
- defective integration.

Under Indian law, a critical defense for platforms is the "safe harbor" provision under Section 79 of the Information Technology Act, 2000. However, the Delhi High Court in *Christian Louboutin SAS v. Nakul Bajaj*[210] held that if an e-commerce platform actively participates in the transaction rather than acting merely as a passive conduit, it loses its safe harbor protection. Decentralized Finance (DeFi) platforms that curate, promote, or actively manage smart contracts may face similar judicial scrutiny.

14.4 Party Liability

Contracting parties themselves may remain liable where:

- they knowingly deploy defective logic;
- conceal contractual risks;
- manipulate execution architecture;
- exploit vulnerabilities.

Technology does not erase human accountability. The corporate veil may still be pierced if the smart contract is used as an instrument of fraud, echoing the principles in *State of U.P. v. Renusagar Power Co.*[211]

15. CYBERSECURITY RISKS AND COMMERCIAL VULNERABILITY

Smart contracts may enhance automation but also create concentrated technical risk. Code vulnerabilities may produce catastrophic financial consequences. Common risks include:

- re-entrancy attacks;
- integer overflow vulnerabilities;
- access control failures;
- oracle manipulation;
- private key compromise;
- phishing exploitation;
- governance takeover attacks.

Commercial law traditionally addresses breach, fraud, and negligence. Smart contract environments introduce technologically specialized risk profiles.

15.1 The DAO Incident: Global Significance

One of the most influential historical examples involved the DAO exploit on the Ethereum network. A vulnerability in smart contract architecture enabled the diversion of substantial digital assets. The incident demonstrated:

- code can fail;
- automation can magnify defects;
- immutability may worsen harm;
- technological trust is not absolute.

The episode fundamentally challenged simplistic "code is law" assumptions, proving that human intervention (via a network hard fork) is sometimes necessary to rectify algorithmic catastrophes.

210 Christian Louboutin SAS v. Nakul Bajaj & Ors., (2018) 253 DLT 728 (India).

211 State of U.P. v. Renusagar Power Co., (1988) 4 SCC 59 (India).

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

VOLUME 6 AND ISSUE 10 OF 2026

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

Published by

Institute of Legal Education

https://iledu.in

15.2 Indian Commercial Implications

Indian businesses adopting smart contracts may face:

- operational disruption;
- asset loss;
- reputational harm;
- litigation exposure;
- regulatory scrutiny.

Under Section 43A of the Information Technology Act, bodies corporate are liable to pay damages if they are negligent in implementing reasonable security practices, leading to wrongful loss. Smart contract operators in India must adhere strictly to these cybersecurity governance mandates.

16. PRIVACY AND DATA PROTECTION CHALLENGES

Blockchain architecture creates severe privacy tensions. Commercial law increasingly intersects with data governance. The enactment of India's Digital Personal Data Protection Act (DPDP Act), 2023, fundamentally shifts the compliance landscape. Rooted in the landmark Supreme Court decision of *Justice K.S. Puttaswamy (Retd.) v. Union of India*[212], which recognized privacy as a fundamental right, the DPDP Act introduces strict obligations for "Data Fiduciaries." Potential concerns include:

- transaction traceability;
- metadata exposure;
- pseudonymous re-identification;
- cross-border data flows;
- immutable personal information storage.

Privacy law generally contemplates correction, deletion, and regulatory accountability. Section 12 of the DPDP Act, 2023 grants data principals the **Right to Erasure** (the right to have personal data deleted when it is no longer needed or consent is withdrawn). Blockchain immutability directly frustrates this statutory expectation. Where personal or commercially sensitive information becomes permanently embedded in a decentralized ledger, the legal tension between immutable tech and erasable data rights intensifies.

17. ARTIFICIAL INTELLIGENCE AND SMART CONTRACTS

A new phase of contractual transformation emerges when smart contracts integrate artificial intelligence. Conventional smart contracts execute predefined logic. AI-enhanced systems may:

- adapt dynamically;
- analyze data;
- optimize decision pathways;
- trigger autonomous commercial responses.

Examples include dynamic pricing, automated claims assessment, predictive compliance execution, and autonomous lending risk management. This raises significantly deeper legal issues.

17.1 The Consent Problem

Traditional contract law presumes predictable obligations. AI adaptation may alter execution behaviour over time. If contractual performance evolves dynamically based on algorithmic learning, did the parties truly consent? The Indian Contract Act requires a "consensus ad idem," which becomes elusive if the contract's parameters change post-execution without human oversight.

17.2 Explainability

Legal accountability requires interpretability. Black-box AI systems may resist explanation. Commercial disputes require understandable reasoning to assess breach or negligence. Opacity undermines this accountability.

17.3 Liability Attribution

If an AI makes a harmful or discriminatory commercial decision, who is responsible? Possible actors:

- deployer;

212 Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 10 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

- software architect;
- data provider;
- operator;
- commercial principal.

Since Indian law does not recognize an AI as a juristic person, liability must necessarily trace back to a human or corporate entity.

18. COMPARATIVE INTERNATIONAL LEGAL APPROACHES

Examining comparative jurisdictions offers insight into regulatory possibilities.

18.1 United States

The United States has seen significant experimentation. Certain states (like Arizona and Tennessee) have expressly recognized blockchain-based contractual validity in their statutes. Commercial discourse increasingly treats smart contracts as enforceable where conventional contractual elements exist. However, regulatory fragmentation across states remains substantial.

18.2 United Kingdom

The UK legal approach has generally been technologically adaptive. The UK Jurisdiction Taskforce published a highly influential legal statement indicating that smart contracts can be legally enforceable under existing common law doctrine. The focus remains functional rather than formalistic.

18.3 Singapore

Singapore has embraced legal innovation and fintech development. Its commercial legal ecosystem supports technologically sophisticated dispute resolution mechanisms, making it an important comparative model for accommodating decentralized assets.

18.4 European Union

EU legal discourse emphasizes consumer protection, data rights (GDPR compliance), accountability, and digital governance. Its regulatory approach, including the Markets in Crypto-Assets (MiCA) regulation, is more rights-centric than purely innovation-driven models.

18.5 UAE / Dubai

Dubai has actively positioned itself as a blockchain-forward commercial jurisdiction. Its regulatory experimentation, particularly within the Dubai International Financial Centre (DIFC), offers insight into proactive legal modernization.

19. NEED FOR INDIAN LEGISLATIVE REFORM

India's current framework is adaptable but incomplete. Existing laws were not designed specifically for:

- decentralized contracting;
- autonomous execution;
- blockchain authentication;
- oracle dependency;
- code-native agreements.

Judicial interpretation alone may prove insufficient. Legislative reform should address:

- **Statutory recognition:** clear acknowledgment of smart contract legality.
- **Authentication rules:** blockchain-compatible authorization frameworks.
- **Liability allocation:** responsibility among ecosystem actors.
- **Dispute resolution:** smart contract-specific adjudicatory mechanisms.
- **Consumer safeguards:** mandatory fairness protections.
- **Technical compliance:** security and audit obligations.
- **Data governance compatibility:** privacy-aligned operational rules reconciling the DPDP Act, 2023 with blockchain immutability.

20. CAN INDIAN COMMERCIAL LAW TRULY ACCOMMODATE SMART CONTRACTS?

Smart contracts present a fundamental challenge to Indian commercial law by replacing traditional contractual interpretation with automated, code-based execution. Although the Indian Contract Act, 1872 and the Information Technology Act, 2000 provide a flexible framework for electronic agreements, they were

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 10 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

not designed for autonomous, decentralized transactions. The key issue is not whether smart contracts can satisfy conventional contractual requirements, but whether existing legal principles adequately regulate their unique features while preserving doctrinal consistency, commercial certainty, and effective legal oversight in an increasingly digital economy..

20.1 The Conceptual Mismatch Between Legal Intention and Computational Execution

Contract law fundamentally rests upon consensual obligation. The juridical inquiry traditionally asks:

- What did the parties agree?
- What was their intention?
- Was consent informed?
- Were obligations understood?
- Was enforcement fair?

Smart contracts shift the operative inquiry toward:

- What did the code execute?
- Were conditions technically triggered?
- Did computational logic complete performance?

This creates conceptual divergence. Law privileges intention. Code privileges execution. A legally imperfect but equitable contract may still receive judicial interpretation. A computationally precise but substantively unfair smart contract may execute mercilessly. This tension cannot be dismissed as merely technical; it strikes at the philosophical core of contract jurisprudence.

20.2 Automation Does Not Eliminate Legal Complexity

A persistent misconception suggests that automation removes legal uncertainty. In reality, automation merely redistributes uncertainty.

Traditional contractual disputes often concern non-performance, delay, interpretation, and breach. Smart contract disputes increasingly concern coding defects, oracle failures, authentication ambiguity, protocol exploitation, algorithmic opacity, and software negligence. Thus, uncertainty does not disappear. It mutates. Commercial law must therefore evolve rather than retreat.

20.3 The Problem of Immutability vs Justice

Blockchain immutability is frequently celebrated as a commercial virtue. Predictability undeniably benefits commerce. Yet law has never treated finality as an absolute value. Legal systems preserve corrective doctrines precisely because rigid enforcement may produce injustice. Indian law recognizes:

- rescission;
- rectification;
- injunction;
- restitution;
- mistake doctrines (*e.g., ITC Limited v. George Joseph Fernandes*[213]);
- equitable intervention.

Immutable execution may frustrate these safeguards. A technologically irreversible transaction may remain legally wrongful. This creates a dangerous asymmetry: rights exist theoretically, but remedies become practically ineffective. Commercial justice cannot depend upon technological architecture alone.

20.4 Consumer Vulnerability

Commercial adoption of smart contracts raises particularly acute consumer concerns. Sophisticated institutional actors may understand technical risk. Ordinary users may not. The doctrine of freedom of contract presupposes informed participation. Opaque code undermines this assumption. Consumers may:

- authorize transactions unknowingly;
- misunderstand consequences;
- encounter irreversible execution;
- lack meaningful negotiation power;
- face inaccessible dispute mechanisms.

If unchecked, smart contracts may become instruments of automated exploitation rather than efficient commerce. Indian

213 ITC Limited v. George Joseph Fernandes, (1989) 2 SCC 1 (India).

commercial modernization must not sacrifice consumer justice.

21. RECOMMENDATIONS FOR A COHERENT INDIAN REGULATORY FRAMEWORK

India requires a deliberate and structured legal response. A fragmented interpretive approach would generate prolonged uncertainty. The following reforms merit serious consideration.

21.1 Statutory Recognition of Smart Contracts

A legislative amendment should expressly clarify that smart contracts are not invalid merely because contractual obligations are expressed or executed through code-based systems. Recognition should remain conditional upon satisfaction of substantive contractual requirements. Technology should not displace doctrine.

21.2 Blockchain-Compatible Authentication Standards

Indian electronic signature frameworks should evolve to address decentralized cryptographic authentication. The law should clarify:

- when blockchain wallet authorization constitutes valid consent;
- evidentiary presumptions regarding authenticated transactions;
- identity attribution standards.

21.3 Mandatory Disclosure Standards

Commercial platforms deploying smart contracts should provide intelligible disclosures. Users must understand contractual consequences, execution triggers, reversibility limitations, technological dependencies, and dispute resolution pathways.

21.4 Smart Contract Audit Requirements

High-value commercial smart contracts should undergo security auditing. Mandatory compliance standards could reduce coding vulnerabilities, exploit risk, and systemic instability.

21.5 Oracle Governance Framework

Because oracles represent critical trust dependencies, regulatory guidance should address reliability standards, liability allocation, audit requirements, and data integrity expectations.

21.6 Consumer Protection Safeguards

Consumer-facing smart contracts should attract heightened protection. Possible safeguards include cancellation rights, disclosure obligations, cooling-off mechanisms, unfair term review, and dispute escalation procedures.

21.7 Specialized Dispute Resolution Mechanisms

Judicial systems may struggle with deeply technical disputes. India should consider specialized commercial tribunals, technical expert panels, and blockchain arbitration mechanisms.

21.8 Data Governance Alignment

Smart contract deployment must remain compatible with privacy and data governance principles. Technical design must align with regulatory obligations under the DPDP Act, 2023, exploring solutions like "off-chain" data storage to preserve the Right to Erasure.

22. CONCLUSION

Commercial law has continually evolved alongside economic change, and smart contracts represent its latest transformation. Unlike traditional agreements, smart contracts integrate contract formation and execution through automated blockchain technology, offering benefits such as reduced transaction costs, faster settlements, transparency, and operational efficiency. However, they also create legal challenges concerning consent, interpretation, jurisdiction, liability, cybersecurity, privacy, and enforcement. While the Indian Contract Act, 1872 and the Information Technology Act provide a limited legal foundation, they are insufficient for decentralized automated transactions. India requires

legislative modernization that integrates technological innovation with established legal principles, ensuring automation strengthens rather than replaces justice.

REFERENCES

1. *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473 (India).
2. *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1 (India).
3. *Bangalore Electricity Supply Co. Ltd. v. E.S. Solar Power Pvt. Ltd.*, (2021) 6 SCC 718 (India).
4. *Bhagwandas Goverdhandas Kedia v. Girdharilal Parshottamdas and Co.*, AIR 1966 SC 543 (India).
5. *Bharat Aluminium Co. v. Kaiser Aluminium Technical Services Inc.*, (2012) 9 SCC 552 (India).
6. *Christian Louboutin SAS v. Nakul Bajaj & Ors.*, (2018) 253 DLT 728 (India).
7. Consumer Protection Act, 2019, No. 35 of 2019, Acts of Parliament, 2019 (India).
8. Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament, 2023 (India).
9. Indian Contract Act, 1872, No. 9 of 1872, Acts of Governor-General in Council, 1872 (India).
10. Information Technology Act, 2000, No. 21 of 2000, Acts of Parliament, 2000 (India).
11. *Internet and Mobile Association of India v. Reserve Bank of India*, (2020) 10 SCC 274 (India).
12. *ITC Limited v. George Joseph Fernandes*, (1989) 2 SCC 1 (India).
13. Jain, M. P. (2018). *Indian constitutional law* (8th ed.). LexisNexis.
14. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).
15. *Kailash Nath Associates v. Delhi Development Authority*, (2015) 4 SCC 136 (India).
16. *Kovuru Kalappa Devara v. Kumar Krishna Mitter*, AIR 1945 Mad 10 (India).
17. *M/s. P.R. Transport Agency v. Union of India*, AIR 2006 All 23 (India).
18. *Mohori Bibee v. Dharmodas Ghose*, (1903) 30 IA 114 (PC) (India).
19. *National Thermal Power Corp. v. Singer Company*, (1992) 3 SCC 551 (India).
20. *Pioneer Urban Land and Infrastructure Ltd. v. Govindan Raghavan*, (2019) 5 SCC 725 (India).
21. Pollock, F., & Mulla, D. F. (2019). *The Indian Contract Act, 1872* (15th ed.). LexisNexis.
22. *Rajkot Municipal Corporation v. Manjulben Jayantilal Nakum*, (1997) 9 SCC 552 (India).
23. Reed, C. (2012). *Making laws for cyberspace*. Oxford University Press.
24. *Satyabrata Ghose v. Mugneeram Bangur & Co.*, AIR 1954 SC 44 (India).
25. Singh, A. (2020). *Law of contract and specific relief* (13th ed.). Eastern Book Company.
26. Specific Relief (Amendment) Act, 2018, No. 27 of 2018, Acts of Parliament, 2018 (India).
27. *State of U.P. v. Renusagar Power Co.*, (1988) 4 SCC 59 (India).
28. *Suraj Lamp & Industries Pvt. Ltd. v. State of Haryana*, (2012) 1 SCC 656 (India).
29. Szabo, N. (1996). Smart contracts: Building blocks for digital markets. *Extropy: The Journal of Transhumanist Thought, (16)*, 50-58.
30. *Tamil Nadu Organic Private Ltd. v. State Bank of India*, AIR 2014 Mad 103 (India).
31. *Trimex International FZE v. Vedanta Aluminium Ltd.*, (2010) 3 SCC 1 (India).
32. UK Jurisdiction Taskforce. (2019). *Legal statement on cryptoassets and smart contracts*. LawTechDP.
33. United Nations Commission on International Trade Law. (2017). *UNCITRAL Model Law on Electronic Transferable Records*. United Nations.
34. Werbach, K. (2018). *The blockchain and the new architecture of trust*. MIT Press.
35. World Economic Forum. (2020). *Bridging the governance gap: Agenda for blockchain accountability*. World Economic Forum White Paper.