International Journal of Creative and Open Research in Engineering and Management
ISSN: **3108-1754 (Online)**
Volume 02 Issue 04 April-2026 | Impact Factor: 3.5

Smart Contracts in India: Law and Challenges

Dinesh Singh sagar*, Dr. Arun Kumar Singh*

How to Cite this Article:

sagar, D. S. (2026). Smart Contracts in India: Law and Challenges. International Journal of Creative and Open Research in Engineering and Management, 02(04). https://doi.org/10.55041/ijcope.v2i4.103

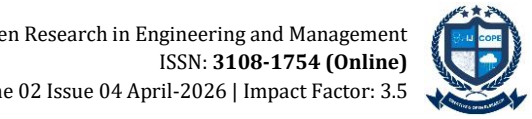
https://doi.org/10.55041/ijcope.v2i4.103

Abstract

Smart contracts, self-executing agreements programmed on blockchain networks, represent a technological innovation with profound implications for contract law. India's existing legal framework, the Indian Contract Act of 1872 and the Information Technology Act of 2000, was not designed to accommodate such digital instruments. This chapter examines the legal recognition and enforceability of smart contracts within this dual framework, identifies significant challenges, and explores emerging prospects for regulatory adaptation. The analysis reveals that while India possesses foundational provisions recognizing electronic contracts and digital signatures, the explicit statutory recognition of smart contracts remains absent. Key challenges include the absence of legal personhood for autonomous smart contracts, liability attribution problems, evidentiary uncertainties and jurisdictional ambiguities. This chapter argues that targeted legislative amendments integrating blockchain technology provisions, coupled with judicial interpretation of existing provisions, could facilitate smart contract recognition while preserving consumer protection standards. This balanced approach offers India an opportunity to position itself as a global leader in fintech innovation, without compromising legal certainty.

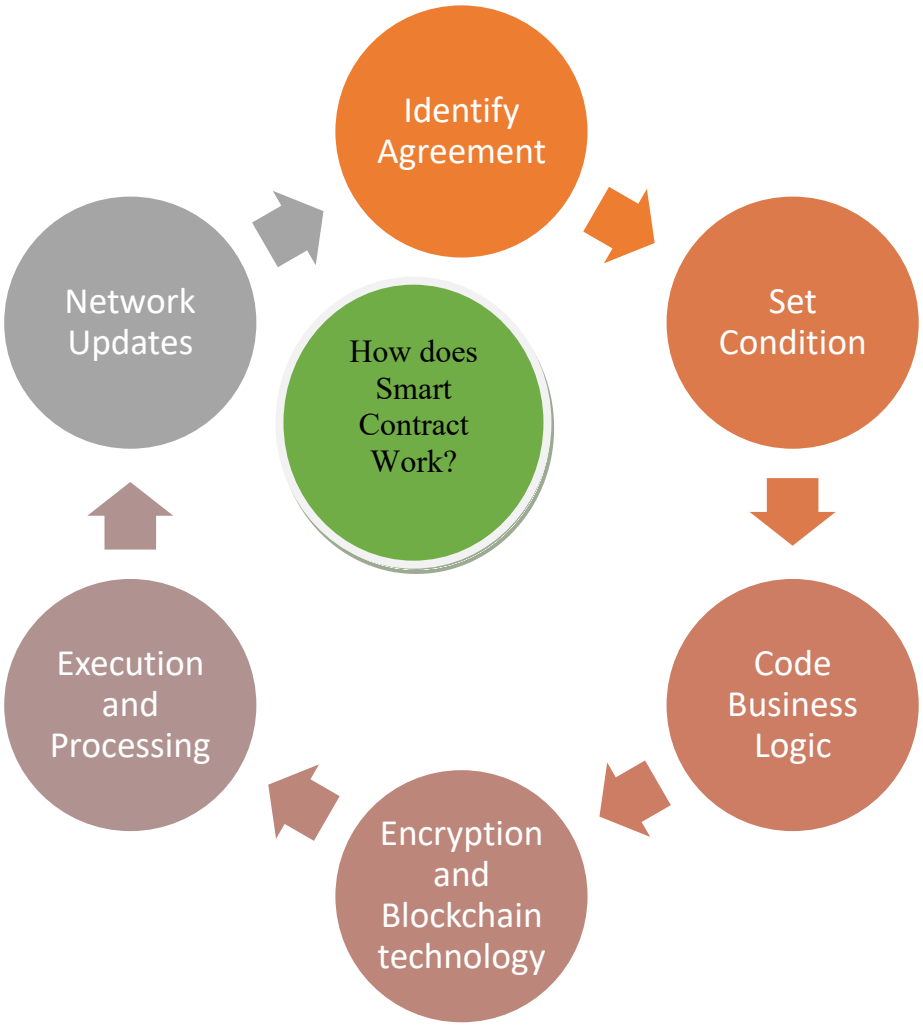
Keywords: smart contracts, blockchain, Indian Contract Act, IT Act, legal recognition, enforceability, fintech

* Assistant professors, school of law. IFTM University, Moradabad
* Assistant professors, school of law. IFTM University, Moradabad



1. Introduction

The emergence of blockchain technology and smart contracts has introduced unprecedented challenges to traditional contract law frameworks. Smart contracts, defined as "self-executing programs where contractual terms are encoded into computer code and automatically executed upon satisfaction of predetermined conditions," represent a fundamental departure from conventional contract formation and execution mechanisms. [1] India's legal infrastructure, while progressively modernized through the Information Technology Act of 2000 and its subsequent amendments, lacks explicit statutory provisions governing smart contracts. The Indian Contract Act of 1872 remains the primary legislation governing contractual relationships, predating digital technologies by over a century. Meanwhile, the IT Act introduced the concepts of electronic contracts and digital signatures but did not anticipate the autonomous execution capabilities of smart contracts, creating significant uncertainty regarding the recognition and enforceability of smart contracts in Indian jurisdictions. The stakes are considerable, as blockchain technology is increasingly employed in supply chain management, financial services, intellectual property administration, and governance applications. [3]



Smart contracts represent one of the most significant technological innovations influencing contemporary commercial and legal transactions. Conceptually, a smart contract is a self-executing digital agreement in which the terms and conditions of a contract are embedded in computer code and automatically enforced through blockchain technology. Unlike traditional contracts that rely on human intervention for performance and enforcement, smart contracts operate on the principle of *"code is law,"* whereby contractual obligations are executed automatically once predefined conditions are fulfilled.

From a functional perspective, smart contracts are not "contracts" in the conventional legal sense drafted in natural language; rather, they are programmable instructions deployed on a decentralized digital ledger. Once deployed, these instructions execute autonomously without the need for intermediaries such as banks, brokers, or escrow agents. This automation significantly reduces transaction costs, minimizes delays, and enhances certainty and efficiency in contractual performance. However, the same features that make smart contracts attractive also raise complex legal and regulatory questions, particularly in jurisdictions like India where contract law is primarily based on traditional notions of offer, acceptance, intention, and enforceability.

The legal nature of smart contracts must be examined through the lens of existing contract law principles. Under Indian law, particularly the Indian Contract Act, 1872, a valid contract requires free consent, lawful consideration, lawful object, and capacity of parties. Smart contracts can potentially satisfy these elements if the parties have agreed—explicitly or implicitly—to be bound by the coded terms. In many cases, smart contracts function as tools for performance and enforcement rather than as standalone contracts. The legally binding agreement may exist off-chain (in written or electronic form), while the smart contract merely automates execution. This distinction is crucial in assessing their enforceability under Indian law.

Another important aspect of the legal nature of smart contracts relates to consent and intention. In traditional contracts, intention to create legal relations is inferred from the conduct and communication of the parties. In smart contracts, intention is often expressed through the act of deploying or interacting with the code. This raises questions about whether parties fully understand the implications of the code they agree to, especially when the contract logic is complex or written in highly technical programming language. Issues of unequal bargaining power, informational asymmetry, and lack of transparency may therefore challenge the validity of consent.

Further, the immutability of blockchain-based smart contracts creates tension with established legal doctrines such as mistake, frustration, coercion, and misrepresentation. Once deployed, a smart contract typically cannot be altered unilaterally, even if an error is discovered or circumstances fundamentally change. While traditional contract law allows for rescission, modification, or judicial intervention, smart contracts may continue to execute regardless of equitable considerations, thereby posing challenges to fairness and justice.

In the Indian context, the legal recognition of smart contracts is still evolving. While electronic contracts are recognized under the Information Technology Act, 2000, there is no explicit statutory framework governing smart contracts. Consequently, their legal nature remains hybrid—partly technological and partly contractual—requiring interpretation through existing legal doctrines. Courts and regulators are thus faced with the task of reconciling automated digital enforcement with human-centric legal principles such as reasonableness, intent, and equity.

In sum, smart contracts represent a paradigm shift in the way agreements are formed, performed, and enforced. Their legal nature cannot be understood in isolation from traditional contract law, nor can they be fully accommodated without doctrinal and regulatory adaptation. Understanding smart contracts as both technological instruments and legally relevant arrangements is essential for addressing the broader legal challenges they pose within the Indian legal system.

1.1.1 Technical Architecture vs. Legal Definition

Smart contracts operate through immutable code deployed on distributed ledger systems and execute transactions automatically when specified conditions are met. Technically, they require no intermediaries and theoretically eliminate the need for third-party enforcement. [4] However, legal recognition requires the translation of technical capabilities into concepts that are comprehensible within existing legal frameworks, such as intention, offer, acceptance, consideration, and legality. The fundamental tension between technological operations and legal requirements emerges immediately. Traditional contract law presumes rational human agents with capacity and intent, whereas smart contracts operate

deterministically according to programmed logic without subjective intent. [5] This creates the first major challenge: whether a smart contract can constitute a legally binding agreement when no human has directly "agreed" to the specific transaction being executed.

2. Current Legal Framework: Gaps and Inadequacies

2.1 The Indian Contract Act, 1872

Section 10 of the Indian Contract Act defines a contract as an agreement that is enforceable by law. Sections 13-14 establish that agreement requires consensus between parties "when one person signifies to another his willingness to do or abstain from doing anything, with a view to obtain the assent of that other to such act or abstinence, he is said to make an offer." The Act contains no provisions distinguishing automated contract execution from traditional offer acceptance paradigms. When a smart contract executes without human intervention upon triggering conditions, courts must determine whether the prior programming constitutes a validly formed agreement or whether automatic execution represents an unauthorized contract modification. [2] Additionally, the Act requires all contracts to comply with Section 10, which specifies that consideration must be given by both parties to the contract. Smart contracts that execute microtransactions at millicond speeds raise questions about whether the traditional consideration doctrine can be applied meaningfully. The doctrine of impossibility (Section 56) may be contested when smart contracts cannot be modified, even when performance becomes impossible.

2.2 The Information Technology Act, 2000

The IT Act represents India's primary legislative response to digital commerce and cybersecurity. Section 2(t) defines "electronic records" as records generated, transmitted, or stored in digital form, explicitly including e-mails and digital documents. Section 2(w) defines an "electronic signature" as an authentication achieved through electronic means that satisfies the legal requirements for signatures. Section 5(a) of the IT Act permits electronic contracts, stating: "Where any law provides that information or any other matter shall be in writing, that requirement shall be deemed to have been satisfied if such information or matter is (a) rendered or made available to a person in electronic form." Critically, Section 5 establishes that information technology can satisfy requirements that typically demand written documentation. However, the IT Act predates blockchain technology by more than two decades. While smart contracts constitute electronic records, they possess qualities of autonomy, immutability, and irreversibility that stretch the Act's framework beyond its original contemplation. [1]

3. Principal Challenges to Smart Contract Recognition

3.1 Challenge 1: Legal Personhood and Attribution of Liability

Traditional contract law attributes contractual obligations and liabilities to identifiable legal persons, such as individuals or corporations. When a smart contract is executed automatically, determining which party bears the liability for non-performance or harmful outcomes becomes conceptually problematic. Consider the following supply chain scenario: a smart contract automatically releases payment upon delivery confirmation from a sensor. If the delivery confirmation is falsified through IoT device compromise, has the smart contract been breached? Has the programmer who coded the contract breached it? Has the platform hosting the contract on its network been breached? Indian contract law lacks a framework for allocating liability in such contexts. Section 43-A of the IT Act addresses unauthorized access and imposes liability for damage caused by unauthorized alterations to computer systems. However, this assumes human agency in unauthorized actions. Vulnerability-based smart contract failures create an interpretive gap. [6]

3.2 Challenge 2: The Evidence and Proof Problem

Section 101 of the Indian Evidence Act, 1872, imposes the burden of proof on the party asserting a fact. Smart contracts, while creating immutable records on blockchains, often abstract the specific contract formation process. The code itself becomes the contract, but interpreting the code requires technical expertise beyond traditional judicial competency. Consider evidentiary requirements: In a typical contract dispute, courts examine correspondence, witness testimony, and documentary evidence to determine the parties' intentions. With smart contracts, the code allegedly reflects this intention; however, the code is often accompanied by extensive comments, variable definitions, and deployment parameters scattered across multiple repositories and versions. The Supreme Court of India, in Bhagwati Prasad Singh v. Pradeep Singh (2002) established that electronic evidence must be authentic and reliable. Smart contracts complicate authenticity determination: a wallet address may have deployed the contract, but identifying the actual individual behind that address requires blockchain forensics foreign to traditional evidence examination.

3.3 Challenge 3: Voidability and Remedies

Sections 15-22 of the Indian Contract Act address the conditions vitiating consent: fraud, misrepresentation, duress, and undue influence. Remarkably, the Act provides remedies: rescission, damages, and restitution. Smart contracts, once deployed and executed immutably on blockchain networks, cannot be rescinded or partially undone without creating conflicting record transactions. An aggrieved party cannot simply ask a smart contract to undo a transaction; the immutability that makes smart contracts trustless also makes them irreversible, and[1] creating a fundamental incompatibility: Indian law presumes that courts can grant relief, but smart contracts operate in an environment where technological relief is impossible.

3.4 Challenge 4: Jurisdiction and Enforcement

Smart contracts are typically executed across distributed networks that span multiple jurisdictions. A smart contract deployed in India may execute transactions involving parties in Singapore and Malaysia, with computations occurring on nodes across Europe and North America. Section 28 of the Indian Contract Act restricts agreements that exclude the jurisdiction of courts; smart contracts create enforcement scenarios that are decentralized, automated, and transnational and predate and supersede traditional jurisdictional frameworks. [3]

4. Prospects: Pathways Toward Recognition

4.1 Judicial Interpretation and Doctrine Evolution

While legislative amendments remain necessary, Indian courts have the capacity to interpret existing provisions expansively. The Supreme Court's progressive stance on technology integration, evident in recent decisions on digital rights and cybersecurity, suggests that judges may treat smart contracts as valid electronic contracts under the IT Act. Courts could invoke Section 5 of the IT Act to recognize smart contracts as satisfying writing requirements, treating the code and blockchain records as analogous to written evidence. The doctrine of consensus ad idem (meeting of minds) could accommodate programming-time agreements, with smart contract execution constituting mere performance of pre-agreed terms rather than fresh contract formation. Indian judicial practice recognizes that technological evolution does not negate established legal principles but rather requires their application in novel contexts. This interpretive flexibility offers a pathway.

4.2 Legislative Amendment: The Smart Contracts Bill

The Information Technology (Amendment) Bill, currently under consultation, represents an opportunity to embed explicit smart contract provisions into the law. The proposed amendments could:

1. Smart contracts are defined as self-executing electronic agreements in which contractual performance occurs through programmed code execution.
2. Liability is allocated by establishing the presumption that original programmers bear responsibility for the smart contract code functionality unless third-party alterations are demonstrable.
3. Create reversibility provisions permitting courts to order contract cancellation and restitution, notwithstanding blockchain immutability, and create parallel legal reversal orders.
4. Establish evidence standards recognizing blockchain records as prima facie evidence while permitting challenges through expert testimony and forensic analysis.
5. Address jurisdictional complexity by establishing India's jurisdiction over smart contracts when either party is domiciled in India or contract performance occurs in Indian territory.

4.3 Regulatory Sandbox and Adaptive Governance

The Reserve Bank of India's fintech regulatory sandbox demonstrates India's commitment to experimental adaptive governance. Extending this framework to smart contracts in specific sectors, such as supply chain, insurance, and securities settlement, could generate practical experience informing future comprehensive legislation. Such sectoral pilots would permit the identification of specific implementation challenges requiring legislative responses, grounded in real-world experience rather than theoretical speculation. The energy sector, particularly renewable energy trading, represents a promising domain for smart contract pilots, given the ongoing interest in blockchain technology for climate financing. [3]

6.Conclusion

Smart contracts present India with a genuine regulatory dilemma: rejection risks marginalizing Indian industries from emerging fintech innovations, while premature acceptance risks legal uncertainty and consumer harm. The evidence suggests a third path: targeted statutory recognition coupled with conservative judicial interpretation until practical experience is accumulated. The Indian Contract Act and IT Act, while not explicitly addressing smart contracts, contain sufficient flexibility for judicial adaptation to new technologies. Section 5 of the IT Act already permits the electronic performance of contracts; courts need only recognize smart contract codes as constituting such performance. Legislative action should focus narrowly on clarifying recognition, allocating liability, and establishing evidentiary standards, rather than attempting comprehensive smart contract regulation, which would inevitably become outdated rapidly. This evolutionary approach permits the use of smart contracts within the existing framework while creating dedicated provisions addressing their unique characteristics, balancing innovation encouragement with legal certainty. India possesses the institutional capacity to become a global leader in responsible blockchain governance. The path forward requires neither revolutionary legal reconstruction nor technophobic rejection but rather the thoughtful integration of emerging technologies into established legal principles adapted to contemporary contexts.

References

1. Alevizos, L. (2024). Automated cybersecurity compliance and threat response using AI, blockchain, and smart contracts. *Journal of Data Science and Technology*.
2. Information Technology Act, 2000,
3. Jain, (2023). Regulation of digital healthcare in India: Ethical and legal challenges. *Healthcare Journal*.
4. World Trade Organization (WTO). (2018). Can blockchain revolutionize international trade?
5. Lynn, T., Mooney, J. G., et al. (2018). Disrupting finance: How blockchain and smart contracts function as innovation catalysts in financial services.
6. Liu, & Papa. (2022). Can BRICS De-dollarize the Global Financial System? Integration of distributed ledger technologies in emerging economies.
7. Wolff, J. (2022). *Cyberinsurance policy*: Liability attribution challenges when autonomous systems cause financial harm.
8. The Indian Contract Act, 1872 (Act IX of 1872)