



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

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

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

SMART CONTRACTS IN MODERN BUSINESS TRANSACTIONS: EXAMINING THEIR LEGAL ENFORCEABILITY AND COMMERCIAL IMPLICATIONS UNDER INDIAN LAW

RITU MUKHI

ABSTRACT

The growth of blockchain technology has transformed the way commercial transactions are created and performed. One of its most significant innovations is the smart contract. Smart contract is a self-executing agreement that are automated, when the predetermined conditions are fulfilled. While smart contracts offer significant advantages, like greater efficiency because of automation, transparency as it is immutable, and reduced transaction costs by reducing reliance on intermediaries they also challenge traditional legal principles governing contract formation, evidence, liability and dispute resolution. Unlike foreign jurisdictions that have expressly recognised smart contracts through legislation, India does not yet have a dedicated statutory framework for regulation. Their legal validity is therefore determined through existing legislation, particularly, Indian contract Act, 1872, The Information Technology Act, 2000, and the Bhartiya Sakshya Adhiniyam, 2023. This article examines whether these statutes are sufficient to govern blockchain based agreements. It contends that although the present legal regime provides a workable legal foundation for recognising electronic agreements, they do not adequately address issues arising from automated execution, coding defects, decentralised systems, and cross- border transactions. The article further explores issues relating to evidentiary challenges, contractual remedies, regulatory concerns, and the need for legislative reform. It concludes that India should adopt a hybrid legal framework that preserves the flexibility of existing contract law while providing statutory recognition for smart contracts, and establishing clear standards for liability, consumer protection, and dispute resolution.

KEY WORDS: Automation, blockchain, Indian Contract Act, Electronic evidence, Bhartiya Sakshya Adhiniyam, regulatory framework.

INTRODUCTION

India's digital economy has fundamentally changed the way commercial transactions are conducted, supported by initiatives like Digital India and Increasing adoption of blockchain for transparency and efficiency. Traditional contracts rely on written agreements, intermediaries, and judicial enforcement to ensure that parties fulfil their obligations. Although this framework has long provided legal certainty, it is often associated with procedural delays, higher, transaction costs, and administrative inefficiencies. The emergence of blockchain technology has introduced an alternative model through smart contracts, where contractual terms are embedded into computer code and executed automatically once predefined conditions are satisfied. Smart contracts aim to address these issues by embedding terms directly into code, which is immutable runs on automation on a decentralised blockchain ledger.

The concept originated in the 1990s with computer scientist Nick Szabo, who described them as computerised transaction protocols, using the vending machine as a simple analogy. Szabo illustrated that once the required payment is made, the machine automatically dispenses the selected product. Ethereum's launch in 2015 enabled the developers to create self- executing agreements through programmable code.¹

In India, Smart Contracts lacks explicit statutory recognition. Their legal validity must therefore be assessed through existing legislation, creating uncertainty regarding their enforceability and regulation. This raises some legal questions: can a smart contract satisfy the essential requirements of a valid contract under the Indian contract Act, 1872 and how should blockchain based records be treated under Bhartiya Sakshya Adhiyiniyam, 2023? Who bears liability when automated execution fails because of coding defects or inaccurate external data? Which raises the question whether the existing legal remedies effectively address disputes arising from immutable blockchain transaction? Furthermore, should India continue to rely on traditional legal principles or it requires a dedicated legislative framework governing smart contracts.

¹ Stuart D. Levi & Alex B. Lipton, **An Introduction to Smart Contracts and Their Potential and Inherent Limitations**, Harv. L. Sch. F. on Corp. Governance (May 26, 2018), <https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations>

This article critically examines to which extent the current Indian legal framework accommodates blockchain- based contractual arrangements. It analyses the enforceability of smart contract under the existing contract law, evaluates the evidentiary treatment off blockchain records, considers issues of liability and remedies, and explores the need for coordinated regulatory reforms. It seeks to provide a practical legal assessment of smart contracts and contribute to the ongoing discussion on modernising India's contract law for the digital economy.

UNDERSTANDING SMART CONTRACTS AND BLOCKCHAIN TECHNOLOGY

A smart contract is an automated digital agreement, which functions when a predetermined conditions are fulfilled. Unlike conventional contracts which general relies on manual performance by the contracting parties or third- party intermediaries, contractual terms are embedded in computer code that execute smart contracts independently without human intervention.² This automated execution streamlines transactions by reducing delays, lowering administrative costs, and minimising the need for intermediaries such as banks, escrow agents, or broker.

The operation of a smart contract can be understood through three key components: code, blockchain infrastructure and automation. First, the rights and obligations of the parties are translated into programming languages such as solidity, Rust or Vyper, which use coded instructions. These instructions define the specific conditions required before the contractual performance.³

For example, a smart contract governing an insurance policy may automatically release compensation when verified weather data confirms that rainfall has fallen below an agreed threshold. Likewise, an online marketplace may automatically transfer payment to seller once delivery has been verified through a trusted logistic provider. Since the contractual conditions are precisely programmed, the likelihood of ambiguity during execution is considerably reduced. However, this precision also creates difficulties because of any coding error, software

² **What Are Smart Contracts on Blockchain?**, IBM Think, <https://www.ibm.com/topics/smart-contracts> (last visited July 19, 2026).

³ **Understanding the Functionality and Benefits of Smart Contracts for Corporations**, FTI Tech. (May 16, 2023), <https://www.ftitechnology.com/resources/blog/understanding-the-functionality-and-benefits-of-smart-contracts-for-corporations>

bug, or incomplete programming may produce unintended legal consequences, giving rise to contractual disputes.

The second key element underlying the operation of a smart contract is blockchain networks. Blockchain functions as a decentralised digital ledger that records transactions across multiple computers. Every transaction is authenticated through cryptographic techniques and immutably linked to previous records, creating a tamper-resistant chain of information. This structure enhances transparency, security and trust by ensuring that identical copies of transaction records are maintained across the network. It enhances data integrity and promotes trust among participants by eliminating reliance on intermediaries, thereby reducing the possibility of fraud or unauthorised manipulation.

Automation constitutes the third and most distinguishing characteristic of smart contracts. Smart contracts execute contractual obligations automatically once the conditions encoded within the software are fulfilled eliminating the manual human interventions. For example, an Escrow payment may be released immediately upon confirmation of the delivery, or ownership of a digital assets may transfer automatically after the purchase price has been received. The efficiency achieved through automation makes smart contracts particularly attractive for industries requiring rapid and repetitive transactions.

However, the legal position of smart contract in India remains largely dependent upon the interpretation of existing legislation, as no statute expressly defines or regulates blockchain-based agreements. The enforceability is derived from Indian Contract Act, 1872, which prescribes the essential elements of a valid contract under section 10 of the Indian Contract Act, 1872, including a lawful offer and acceptance, lawful consideration, competent parties, free consent, and a lawful object. If a smart contract fulfils these statutory requirements, there is no inherent legal reason why it should be denied contractual validity merely because its terms are expressed through computer code rather than written language.

The section 10 A of the Information Technology Act, 2000, expressly recognises the contracts concluded through electronic means. The provisions demonstrate the legislature's intention to accommodate the evolving methods of digital contracting. The legal challenge, therefore is not whether smart contracts qualify as valid contracts, but whether established principles of contract law adequately address agreements that are automated, decentralised, self-executing irreversible transactions.

A. OFFER AND ACCEPTANCE THROUGH CODE

The validity of smart contracts in India depends on whether they satisfied the essential requirement of a contract under Indian contract Act, 1872. Sections 2(a) and 2(b) of the Indian Contract Act define a proposal and its acceptance. In a blockchain environment, a smart contract deployed on a blockchain network may be viewed as a standing offer. A user who interacts with the code by transferring digital assets or activating a particular function may thereby communicate acceptance through conduct rather than written or spoken words.

Indian courts have already recognised that contracts formed electronically are legally valid. In *Trimex International FZE Ltd. v. Vedanta Aluminium Ltd.*, the Supreme Court held that a binding contract may arise through electronic communications if the essential contractual elements are present.⁴ Although the dispute concerned email correspondence rather than blockchain technology, the Court adopted a functional approach by focusing on the parties' intention instead of the medium through which consent was communicated. The same reasoning may reasonably extend to smart contracts.⁵

Section 10A of the Information Technology Act, 2000 further strengthens this position by providing that contracts shall not be denied legal effect merely because they were concluded electronically. Therefore, Indian law already recognises the validity of electronic agreements; the principal question is whether blockchain transactions satisfy the substantive requirements of contract law.

B. FREE CONSENT AND CONSENSUS *AD IDEM*

While electronic contracting is recognised under Indian law, establishing free consent in smart contract, which operates entirely through computer code. presents greater challenge. Under Sections 13 and 14 of the Indian Contract Act, parties must agree upon the same thing in the same sense and their consent must be free from coercion, undue influence, fraud, misrepresentation, or mistake. Traditional contracts allow parties to read and negotiate contractual clauses before execution. Smart contracts, however, frequently require users to rely upon software interfaces without understanding the underlying programming language.

⁴ *Trimex Int'l FZE Ltd. v. Vedanta Aluminium Ltd.*, (2010) 3 S.C.C. 1 (India).

⁵ Harshita M., **Beyond Self Execution: The Legal Fallout of Smart Contract**, *Indian J. for Rsch. in L. & Mgmt.* (2026).

Most commercial users cannot independently verify Solidity or similar programming languages. Consequently, they rely upon software developers, platform operators, or simplified user interfaces to understand the contractual relationship. This creates a gap between the legal agreement intended by the parties and the technical instructions embedded within the code.

Suppose a coding error causes payment to be released immediately instead of after delivery. The blockchain faithfully executes the programmed instructions even though they do not reflect the parties' actual intentions. In such circumstances, determining consensus *ad idem* becomes considerably more complex because the code executed differs from the agreement the parties believed they had entered into.

Several scholars have therefore suggested adopting a “legal wrapper” or hybrid contract model. Under this approach, parties execute a conventional written agreement alongside the smart contract. The written document records commercial obligations in plain language, while the blockchain code merely automates performance. Such an approach preserves contractual certainty while reducing disputes arising from programming errors.

C. CAPACITY AND CERTAINTY

Another challenge concerns the competency of parties under Section 11 of the Indian Contract Act. Blockchain transactions generally occur through pseudonymous digital wallets rather than verified legal identities. Consequently, a blockchain network cannot independently determine whether a participant is a minor, mentally incapable, or otherwise legally incompetent to contract.

This limitation creates risks absent in conventional contracting. If a minor enters into a blockchain transaction, the agreement may remain technologically executable even though it is legally void. The automated nature of smart contracts therefore cannot replace legal requirements concerning contractual capacity.

Nevertheless, smart contracts also offer certain advantages. Their “if-then” programming structure provides a high degree of certainty regarding contractual performance. Traditional contracts often generate disputes because contractual language is ambiguous. Smart contracts minimise interpretative disputes by executing only those conditions specifically programmed into the code. Thus, automation enhances certainty while simultaneously reducing flexibility.

BLOCKCHAIN RECORDS AS EVIDENCE UNDER THE BHARATIYA SAKSHYA ADHINIYAM, 2023

Even if smart contracts satisfy the requirements of contract formation, they must still be proved before courts in the event of litigation. This raises important questions concerning the evidentiary value of blockchain records.

The Bharatiya Sakshya Adhiniyam, 2023 modernises India's law of evidence by recognising electronic records as documentary evidence. Since blockchain transactions are permanently recorded through cryptographic verification, they possess significant evidentiary value. Every transaction contains a timestamp, digital signatures, cryptographic hash values, and transaction identifiers that collectively establish the authenticity of the recorded information.

Unlike conventional electronic records stored on centralised servers, blockchain records are replicated across numerous network participants. Altering a transaction retrospectively would require simultaneous modification of multiple copies maintained throughout the network, making unauthorised alteration practically impossible. Consequently, blockchain records provide a particularly reliable audit trail.

Nevertheless, certain evidentiary challenges remain unresolved. Existing certification requirements were largely designed for conventional electronic records generated by identifiable computer systems. Decentralised blockchain networks lack a single system administrator capable of issuing certification in the traditional sense. Indian courts may therefore need to interpret the Bharatiya Sakshya Adhiniyam flexibly to accommodate cryptographically authenticated decentralised records.

Expert testimony will also assume increasing importance. Judges may require technical evidence explaining blockchain architecture, hash functions, digital signatures, and oracle mechanisms before determining the evidentiary value of particular transactions.

LIABILITY AND REMEDIES

Automation significantly reduces human intervention, but it does not eliminate legal responsibility. When a smart contract fails because of defective programming, inaccurate external information, cybersecurity attacks, or software vulnerabilities, determining liability becomes difficult. Coding errors may arise from negligent developers, while incorrect data supplied by external “oracles” may trigger unintended execution despite the underlying code

functioning correctly. In other cases, vulnerabilities may be exploited by malicious third parties.⁶

Indian contract law does not presently contain specialised rules allocating liability among developers, platform operators, oracle providers, and contracting parties. Consequently, courts will likely rely upon established principles of contractual interpretation, negligence, professional responsibility, and breach of contractual obligations.⁷

The immutable nature of blockchain further complicates remedies. Traditional contractual remedies include rescission, restitution, specific performance, and damages. However, once a blockchain transaction has been executed and validated, technological reversal is generally impossible.

This does not mean that parties are left without legal remedies. Courts continue to possess jurisdiction to award compensatory damages under Section 73 of the Indian Contract Act. Restitution under Section 65 may also remain available where unjust enrichment has occurred, although repayment will ordinarily occur through off-chain financial settlements rather than reversal of blockchain records. In appropriate circumstances, injunctions, declarations, and equitable relief may also supplement contractual remedies.

Comparative jurisprudence illustrates these challenges. In *Quoine Pte Ltd. v. B2C2 Ltd.*, the Singapore Court of Appeal considered whether automated cryptocurrency transactions executed through computer algorithms could be set aside for unilateral mistake. Although decided under Singapore law, the judgment demonstrates how conventional principles of contract law continue to govern technologically sophisticated transactions.⁸

REGULATORY REFORM AND THE WAY FORWARD

India currently regulates different aspects of digital finance through multiple institutions, including the Reserve Bank of India (RBI), the Securities and Exchange Board of India (SEBI), the International Financial Services Centres Authority (IFSCA), and the Ministry of Electronics and Information Technology (MeitY). While each regulator addresses specific concerns within its jurisdiction, no unified framework presently governs smart contracts. A

⁶ Harshita M., **Unveiling Smart Contracts: The Future of Digital Agreements**, Manupatra Articles, <https://articles.manupatra.com/article-details/Unveiling-Smart-Contracts-The-Future-of-Digital-Agreements>

⁷ Mitali Aditya Patil, **Smart Contracts: The Need of Legal Implications in India**, 7 *Indian J. L. & Legal Rsch.* (2025).

⁸ *Quoine Pte. Ltd. v. B2C2 Ltd.*, [2020] SGCA(I) 2 (Sing.)

fragmented regulatory structure creates uncertainty for businesses seeking to adopt blockchain technology. Clear legislative guidance would encourage innovation while simultaneously strengthening consumer protection, cybersecurity standards, and legal certainty.

Rather than enacting an entirely separate statute governing every aspect of blockchain technology, India should adopt a hybrid regulatory model. Such a framework would expressly recognise smart contracts while continuing to apply the established principles of the Indian Contract Act. Written legal agreements should complement computer code wherever contractual rights or obligations require judicial interpretation. Standardised disclosure requirements, identity verification mechanisms, cybersecurity obligations, and dispute resolution clauses would further reduce uncertainty.⁹

Regulatory sandboxes supervised by RBI, SEBI, and IFSCA may also provide an effective environment for testing blockchain-based commercial applications before their widespread adoption. Such an approach balances technological innovation with regulatory oversight without imposing unnecessary restrictions on emerging technologies.

CONCLUSION

Smart contracts represent an important development in the evolution of digital commerce by combining contractual obligations with automated blockchain technology. Indian law already provides a substantial legal foundation for recognising electronically concluded agreements through the Indian Contract Act, 1872 and the Information Technology Act, 2000, while the Bharatiya Sakshya Adhiniyam, 2023 strengthens the evidentiary recognition of electronic records. However, automation introduces legal issues that traditional contract law was not designed to address, including algorithmic consent, coding errors, decentralised evidence, oracle failures, and the practical impossibility of reversing blockchain transactions.

Existing legal principles remain sufficiently flexible to accommodate many aspects of smart contracts, yet reliance solely upon judicial interpretation may create uncertainty as blockchain adoption increases. India should therefore move towards limited statutory recognition through a hybrid legal framework that integrates traditional contractual principles with technology-specific safeguards. Such an approach would preserve commercial certainty, protect

⁹ **Understanding the Functionality and Benefits of Smart Contracts for Corporations**, FTI Tech. (May 16, 2023), <https://www.ftitechnology.com/resources/blog/understanding-the-functionality-and-benefits-of-smart-contracts-for-corporations>.

consumers, encourage innovation, and ensure that legal accountability evolves alongside technological progress.