

---

# **BLOCKCHAIN-ENABLED SMART CONTRACTS: LEGAL STATUS, CHALLENGES, AND THE WAY FORWARD IN INDIA - A COMPARATIVE STUDY**

---

Shruti Vasani & Priyanka Vanvari, NMIMS'S Kirit P Mehta School of Law, Mumbai

## **ABSTRACT**

This paper looks at the issue of legality for smart contracts which are based on blockchain technology within the Indian context. We look at how they are enforced under present contract, IT, and evidence laws and also see how India does or does not align with other foreign jurisdictions. We identify what the legal gaps are and put forth proposals for reform which will in turn provide certainty and accountability.

## **Introduction**

21<sup>st</sup> Century can be defined as the century of innovations, as we are moving forward, we are welcoming many new technological advancements. Blockchain technology is one of the most significant technological innovations that has emerged and affected the data, transactions and contractual relations are executed and recorded. Blockchain is basically a shared, immutable ledger which records business transactions, assets etc. within the network allowing for a single source of truth. Unlike traditional systems, the blockchain technology lacks the need of an intermediary, mostly depending on the cryptographic techniques and consensus mechanisms to record and verify the records. This structure enhances trust, minimizes manipulation and ensures data validity.

Emerged from this block chain technology is the smart contracts, these contracts rely on algorithmic execution and lacks human intervention. This is very different from traditional notion of contract formation. These contracts are automatically executed when terms of contracts are met. These mostly work on "IF/When condition" like releasing funds to the appropriate parties, registering a vehicle, sending notifications or issuing a ticket. These contracts have particularly gained traction in the recent years due to their ability to automate

contractual performance in a trust less environment. They increase certainty by eliminating the need for third party oversight, reduced transportation cost and faster execution.

Despite their large scale adoption, it has certain lacunas which pose considerable challenge to the existing legal framework. Since smart contracts increasing work on code and lacks human execution it might raise considerable questions on issues such as consent, mistake, liability for coding errors, jurisdiction, and admissibility of blockchain records as evidence. The Indian Contracts Act 1872 and Information Technology Act, 2000 while are foundational for recognizing electronic contracts, they were not drafted keeping in mind the automated nature of smart contracts.

Against this backdrop, the research presented here tries to examine the legality of the automated smart contracts, analysing whether the present laws are adequate and addressing their challenges and compare India's approach with Europe and US. It also aims to identify the legal gaps and propose reforms that will ensure certainty, accountability, and effective regulation of smart contracts in the evolving digital economy.

### **Research Question**

This research paper tries to address the following central question

**Whether the existing provisions are adequate in enforcing the blockchain based automatic smart contracts?**

To further examine the issue, the study also explores the following sub – questions

1. Does the provisions of Indian Contract Act 1872, adequately accommodate the formation and execution of smart contracts?
2. Is the Information Technology Act, 2000 ready to address blockchain-based transactions and electronic agreements?
3. What are challenges to the admissibility of the Smart Contracts especially under the Indian evidence Act, 1872?
4. What are the lacunas in the Indian Statutory Framework in relation to others like US and Europe?

## Hypothesis

The study proceeds on the hypothesis that

**While some provisions of Indian legal framework recognize Electronic Contracts and digitized transactions, it fails to particularly regulate the block chain based automatic smart contracts.**

It is further hypothesised that:

This absence of clear provisions creates uncertainty in the enforcement, liability, and evidentiary value, thereby there is a need for legislative clarification and judicial interpretation informed by comparative legal developments.

## Literature Review

The legal implications of block chain technology and smart contracts has gained a lot of traction among scholars and legal practitioners particularly in contract law, technology law, and regulatory studies. Existing literature does agree that while smart contracts are efficient and automated, but they also disrupt traditional legal concepts rooted in human intention, interpretation, and institutional oversight.

A significant portion of the literature examines the validity of smart contracts whether it meets requirements of offer acceptance, and consideration, provided there is clear consent and intention of the parties. However, concerns were raised regarding rigidity and deterministic nature of code, and limits addressing mistake, frustration, or equity-based relief.<sup>1</sup>

Another group of scholars focus on the evidentiary and enforcement challenges. While the block chain technology is transparent, it has been noted that there are several challenges for admitting blockchain records under existing evidence laws especially emphasizing on Section 65B of the Indian Evidence Act, 1872.

Comparative studies help us understand the statutory frameworks in other jurisdictions and their approach to smart contracts. literature analysing the United States points to the supportive role of the Uniform Electronic Transactions Act and the E-SIGN Act, while European

---

<sup>1</sup> Sannidhi Agrawal, *Smart Contracts: Functioning and Legal Enforceability in India* (2023)

scholarship examines the eIDAS Regulation as a harmonised framework for electronic identification and trust services.

The Indian works on smart contracts remains largely doctrinal. Existing writings talk about Indian Contract Act, 1872 and the Information Technology Act, 2000 especially in relation to their lack of provisions to expressly address decentralised or autonomous technologies. The literature therefore identifies a regulatory gap concerning enforceability, liability, and evidentiary standards.

This research builds on the existing scholarship by analysing case laws, and comparative statutory provisions to evaluate the adequacy of Indian framework in regulating block chain based smart contracts and suggest paths of reforms.

## Conceptual & Legal Framework

### Concept of Smart Contracts

Smart Contracts are basically information stored in the block chains that automatically put the obligations in motion once the conditions are satisfied. This term was first coined by Nick Szabo defining them as “**self-executing agreements with terms directly written into code, automating transactions without intermediaries**”.<sup>2</sup> From a legal perspective we can see a smart contract as a traditional contract with just the means of enforcement being technological. They mainly function through if – when logic that means it is embedded with code about a future event and fulfilment of that event lead to the direct enforcement of the contract. These actions might include releasing funds to the appropriate parties, registering a vehicle, sending notifications or issuing a ticket.<sup>3</sup> The blockchain is then updated when the transaction is completed. This ensures that the transactions are not changed and only the granted parties can see the results. To establish the terms, participants must determine how transactions and their data are represented on the blockchain, agree on the “if/when...then...” rules that govern those transactions, explore all possible exceptions and define a framework for resolving disputes. Then, a developer programs the smart contract. However, organizations that use blockchain for

---

<sup>2</sup> Nick Szabo, *Smart Contracts: Building Blocks for Digital Markets*, Nick Szabo's Essays and Papers (1996), [http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart\\_contracts\\_2.html](http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html).

<sup>3</sup> *What are Smart Contracts?*, IBM Think (Feb. 3, 2026), <https://www.ibm.com/think/topics/smart-contracts>.

business increasingly provide templates, web interfaces and other online tools to simplify structuring smart contracts.

The main differentiation lies in the enforcement and execution. Traditional contracts are written or oral agreements interpreted and enforced by courts or arbitral bodies, which does allow for interpretation and relief. Smart Contracts however are automatically enforced by the courts leaving little room for execution and modification. While traditional contracts rely on trust and institutional enforcement, smart contracts rely on technological certainty and automation. This however raises significant questions about consent, mistake and remedies and accountability in cases of unintended outcomes.

### **Blockchain as a Legal Tool**

Blockchain is the technology which forms the basis of smart contracts and acts as a potential legal tool especially for record keeping and verification. Blockchain technology began with the introduction of Bitcoin in 2008, created by an anonymous figure or group known as Satoshi Nakamoto. It acts as a public ledger, thus securing all transactions and preventing double spending. With the development of platforms like Ethereum in 2015, blockchain began to support smart contracts—digital contracts stored on a blockchain that are automatically executed when predetermined terms and conditions are met. All of this enhances trust, security and efficiency.<sup>4</sup>

While these provide significant advantage, it also raises complex legal concerns. Decentralization complicates the identification of responsible parties, making it difficult to attribute liability in the event of system failure or unlawful execution. The Immutability though beneficial for record integrity, conflicts with the major principles of rectification, reversal, or equitable relief in cases of fraud or mistake. Transparency though does enhance trust raises concerns regarding data privacy, particularly in case of sensitive information.

Thus the use of blockchain as legal tool challenges conventional legal frameworks that are built around centralised authority, human discretion, and post-facto adjudication. All this call for re-evaluation of existing frameworks to make it much more inclusive especially for regulation of

---

<sup>4</sup> Stephanie Susnjara & Ian Smalley, *What is Blockchain?*, IBM Think (Feb. 3, 2026), <https://www.ibm.com/think/topics/blockchain>.

smart contracts.

## **Indian Legal Framework Governing Smart Contracts**

The legal validity of a smart contract in India can be tested through the application Indian Contract Act, 1872, the Information Technology Act, 2000, and the Indian Evidence Act, 1872. The point to be noted is that all these legislations have not expressly addressed smart contracts and block chain technology. However, their provisions can form the primary legal framework within which such agreements may be assessed.

### **Indian Contract Act, 1872**

This provision regulates the validity and enforceability of Contract in India. Section 10 of this provision talks about a valid contract and how it requires free consent of parties competent to contract, lawful consideration, and a lawful object.<sup>5</sup> Smart contracts which are enforced through code may satisfy these elements, provided that it was through mutual consent of the parties.<sup>6</sup>

Offer and Acceptance is usually done online, either by interacting by blockchain platform or by agreeing to coded terms embedded in the contract. Consideration is usually cryptocurrency, digital assets or an act or omission.<sup>7</sup> Challenges do arise due to the automated and irreversible execution of smart contracts, as this defeats the doctrines of mistake, coercion, or frustration. Thus, this rigid application of code may not align with the actual intention of the parties

### **Information Technology Act, 2000**

This provision provides statutory recognition of electronic records and electronic contracts in India. It Legally accepts electronic records thereby taking the first step towards the acceptance of smart contracts.<sup>8</sup> Digital signatures and electronic authentication mechanisms make it much more easier to authenticate smart contracts.<sup>9</sup>

---

<sup>5</sup> Indian Contract Act, No. 9 of 1872, § 10.

<sup>6</sup> Sannidhi Agrawal, *Smart Contracts: Functioning and Legal Enforceability in India*, 7 Int'l J. L. & Soc. Sci. 6 (2021).

<sup>7</sup> *Smart Contracts in India*, Obhan & Associates: Blog (Feb. 3, 2026), <https://www.obhanandassociates.com/blog/smart-contracts-in-india/>.

<sup>8</sup> Information Technology Act, 2000, § 10A.

<sup>9</sup> Information Technology Act, 2000, §§ 3, 4.

However the IT Act was created for centralized technologies and does not properly address the concerns of decentralized technologies like blockchain. Smart contracts deployed on distributed ledgers raise issues regarding identification of parties, authentication of consent, and attribution of liability in the absence of a central authority. This lack of specific provisions creates a legal and regulatory gap which needs to be fulfilled.

### **Indian Evidence Act, 1872**

The admissibility of any record is checked by the Indian Evidence Act, 1872, particularly Section 65B, which deals with electronic evidence. Block chain contracts can though qualify as electronic record but the compliance requirements presents significant challenges due to the decentralised nature of blockchain systems.

Judicial Precedents has emphasized time and again the significance of Section 65B for admissibility of electronic records. Identifying a “Person in Control” of a blockchain system for certification purposes is often difficult, thereby complicating the use of blockchain records in court proceedings. Thus, while blockchain enhances reliability, the legal provisions may limit judicial acceptance of such records.<sup>10</sup>

### **Indian Cases Emphasizing Blockchain Technology In Smart Contracts**

As we have seen, Blockchain technology is mainly used in the field of cryptocurrency, and is spreading to other areas also. One of the fields where the use of Blockchain Technologies is widely used in law is in Smart Contracts. The computer programs are executed in the blockchains establishing a collection of clauses between the participating parties which they agree to interact with and they are executed automatically at the moment in which these clauses are fulfilled. As it is a computer code, both the client and the service provider cannot misinterpret the agreed clauses, facilitating and verifying the agreement of the contract. Though there is no direct case in the India as such till now about smart contracts various other cases form the basis of their validity.

---

<sup>10</sup> *Understanding Blockchain Evidence in Indian Courts: Admissibility and Section 65B*, Vidhi Sastras: Blog (Feb. 3, 2026), <https://vidhisastras.com/blog/understanding-blockchain-evidence-in-indian-courts-admissibility-and-section-65b/>.

## **Trimex International FZE Ltd. v. Vedanta Aluminium Ltd**

### **Facts of the Case**

Trimex International FZE Ltd and Vedanta Aluminium Ltd. entered into negotiations for the sale of bauxite. The negotiations took place through emails and fax communications. The parties agreed on essential terms such as quantity, price, delivery schedule, and payment conditions. However in this case we did not see a formal written contract between the parties. Also at a later date Vedanta pulled out of the transaction which they put forth saying that no contract was in fact agreed upon as a formal agreement never took place. Trimex filed a claim for breach of contract which in turn initiated arbitration proceedings.<sup>11</sup>

### **Issues of the Case:**

Issues raised were related to whether a valid and binding contract may be established through email and fax communications, and whether absence of a formal written contract does not preclude that of a concluded contract.

### **Decision:**

The Supreme Court determined that a valid and final contract was present. That which is agreed upon in principle terms and which the parties intend to be bound by may pass as a contract which need not be in writing.

### **Direct Link to Blockchain-Based Smart Contracts:**

This judgment sets the stage for smart contracts on the blockchain. As with emails and faxes in the Trimex case which were accepted as proof of consent, smart contracts report offer and acceptance via code and blockchain transactions. The case reports that physical signatures and formal documents are not a requirement which in turn supports the enforceability of self-executing blockchain contracts which via electronic records and the immutable nature of the blockchain serve as proof of agreement and performance.

---

<sup>11</sup> *Trimex Int'l FZE Ltd. v. Vedanta Aluminium Ltd.*, (2010) 3 SCC 1.

## **Anwar P.V. v. P.K. Basheer (2014)**

### **Facts Of the Case :**

In the case out of an election dispute the Appellant used electronic records which included CDs of speeches and songs to present a case of corrupt electoral practices by the Respondent. These electronic records were produced without complying with the statutory requirements prescribed under the Indian Evidence Act, 1872.<sup>12</sup>

### **Issue:**

Whether electronic records such as CDs, videos, and digital files can be admitted as evidence in court without complying with the conditions laid down under Section 65B of the Indian Evidence Act, 1872.

### **Decision**

The Supreme Court ruled out that which electronic evidence is presented only if it meets the criteria of Section 65B of the Evidence Act. We went against past decisions which had allowed electronic evidence to be put forth under the aegis of secondary evidence. We made it clear that Section 65B stands as a separate entity for the purpose of admission of electronic records.

### **Relevance to Smart Contracts and Electronic Evidence**

Smart contracts create what we see as transaction logs, timestamps, and coded instructions in blockchains. In issues related to the performance, violation, or responsibility under smart contracts, such records will put forth electronic evidence. Although the tech is reliable and unchangeable that which is put on the blockchain, we still see requirement for compliance to Section 65B which includes certification. That creates a practical issue as decentralized block chain systems do not have a clear authority to issue such certificates which in turn makes the admissibility of smart contract evidence a very complex legal issue.

### **Foreign Case Laws**

#### **Feldman v. Google Inc. (2007)**

---

<sup>12</sup> *Anwar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.

Jurisdiction:

United States – U.S. District Court for the Eastern District of Pennsylvania

Legal Principle Laid Down:

The Court held that clickwrap agreements (online contracts where users click “I agree” to terms and conditions) are valid and enforceable, provided that the user is given reasonable notice of the terms and an opportunity to review them before acceptance. The Court emphasized that digital consent expressed through affirmative action (such as clicking a button) satisfies the requirement of free consent under contract law.<sup>13</sup>

Relevance to Enforceability of Electronic or Automated Contracts:

This case is significant because smart contracts and electronic contracts rely on digital modes of assent rather than handwritten signatures. The judgment establishes that Consent in an electronic environment is legally valid, Physical signatures are not mandatory for enforceability, Automated systems can create binding contractual obligations. This supports the enforceability of smart contracts where parties agree to terms through digital interaction with a blockchain platform.

### **Specht v. Netscape Communications Corp. (2002)**

Jurisdiction:

United States – U.S. Court of Appeals, Second Circuit

Legal Principle Laid Down:

The Court held that an electronic contract is not enforceable if the user is not given reasonable notice of the terms and has not clearly manifested consent. Merely downloading software without explicit acknowledgment of terms does not amount to acceptance. The judgment drew a distinction between browse wrap and clickwrap agreements, holding that passive acceptance is insufficient.<sup>14</sup>

---

<sup>13</sup> *Feldman v. Google Inc.*, 513 F. Supp. 2d 229 (E.D. Pa. 2007).

<sup>14</sup> *Specht v. Netscape Commc'ns Corp.*, 306 F.3d 17 (2d Cir. 2002).

### Relevance to Enforceability of Electronic or Automated Contracts:

This case highlights a key limitation on automated and electronic contracts: Automation alone does not guarantee enforceability and clear communication of terms and explicit consent are essential. For smart contracts, this means that if users interact with automated code without understanding or agreeing to the encoded terms, enforceability may be challenged. Transparency and informed consent remain fundamental even in automated systems.

## **Comparative Legal Analysis With Other Countries**

### **Recognition of Electronic Contracts**

#### **India:**

Section 10 of the Indian Contract Act, 1872 as integrated with the Information Technology Act, 2000, confirms the legality of Electronic contracts. In the case of *Trimex International v. Vedanta Aluminium* (2010), contracts via email were judicially recognized. Although there is no explicit definition of smart contracts, they can be enforced indirectly if the elements of a contract are met.

#### **United States:**

The E-SIGN Act (2000) and the Uniform Electronic Transactions Act provide a clear recognition of electronic contracts and electronic signatures. In interstate commerce, smart contracts are recognized, and several states have recognized smart contracts on a blockchain.<sup>15</sup>

#### **European Union:**

EU contract law recognizes the legality of electronic contracts as they are recognized by the eIDAS regulations. The legal validity of electronic signatures, whether advanced or qualified, is clear. Existing legal structures recognize and regulate smart contracts with caution.<sup>16</sup>

### **Evidentiary Standards**

#### **India:**

---

<sup>15</sup> Electronic Signatures in Global and National Commerce Act, 15 U.S.C. §§ 7001–7031 (2000).

<sup>16</sup> Regulation (EU) No. 910/2014 of the European Parliament and of the Council (eIDAS Regulation).

Electronic evidence falls under Section 65B of the Indian Evidence Act. The case of Anvar P.V. v. P.K. Basheer (2014) ruled that electronic records are admissible as long as they are properly certified. This requirement applies to both blockchain and smart contract records.

### **United States:**

Electronic evidence is governed by the Federal Rules of Evidence. Courts are more relaxed and evaluate evidence in terms of authenticity, reliability, and don't require evidence to be certified. Due to its immutability, blockchain evidence is accepted more and more as self-authenticating.

### **European Union:**

EU evidence law emphasizes reliability and integrity of electronic data. Courts assess authenticity based on technical safeguards. Blockchain records are admissible if they ensure data integrity and traceability, without rigid procedural formalities like India.

### **Regulatory Clarity**

#### **India:**

India does not have a dedicated statutory framework for smart contracts. Legal recognition is given through interpretation of present contract and IT laws which in turn causes some uncertainty in implementation and enforcement.

#### **United States:**

The U.S. has high regulatory clarity which includes federal and state level actions regarding blockchain and smart contracts.

#### **European Union:**

The EU has a uniform yet careful approach. While we have see growth in regulation of electronic contracts, smart contracts are put forward by digital, consumer protection, and data laws. Regulation is in a state of evolution but is the same across member states.

### **Conclusion:**

While all three countries recognize e-contracts, India adopts a conservative evidentiary

approach, the US follows a flexible, innovation-friendly model, and the EU balances legal certainty with regulatory caution. These differences significantly impact the enforceability and evidentiary treatment of blockchain-based smart contracts.

### **Legal Issues & Challenges**

Blockchain and we see in smart contracts a way for decentralized and automated transactions but also they bring out very large legal issues. We see that issues of enforcement, jurisdiction, liability and data protection are put forward which in turn point out that present legal structures are insufficient. As to the issue of what makes a smart contract enforceable we see it is in the compliance with traditional contract laws. What we find is that although execution is automated via code which is the beauty of it, we also see issues arise when what is put into the code does not reflect what the parties intended, the code is ambiguous, or performance becomes non-reversible. Also we see that courts may have a hard time in trying to sort out these algorithm based agreements with our present day contract laws. As for the issue of which laws apply which is the issue of jurisdiction we see great difficulty with the decentralized and border less nature of block chain. That often times we do not have a governing law or a jurisdiction clause in smart contracts which leads to claims that conflict, enforcement issues and an increase in litigation in cross border disputes. Liability of coding errors and system failures is a gray area. Smart contracts run by themselves which in turn puts at question which parties are responsible developers, platforms or the parties that enter into the contracts. At present Indian law does not have a clear structure in which to pass out liability for technical failures. We see issues of data privacy and security in the use of blockchains' immutability and transparency which in fact goes against principles of data minimization and the right to be forgotten. By putting personal data on immutable ledgers we may be in violation of privacy laws which in turn leaves us open to legal action. As a whole while smart contracts do what the code says they do and not what the law says, legal input is still very much a requirement. In the void of clear statutory regulation smart contracts will continue to have large scale legal issues.

### **Normative Solutions**

To deal with the legal issues that surround smart contracts in the blockchain space a multi-pronged approach is put forth. First out of which is for the smart contracts in the blockchain space to be recognized by law either through changes to the Information Technology Act, 2000 or through issue of instructions that clarify their standing in present contract law. This will in

turn reduce the issue of enforceability and what is and is not valid. Also within this is the need to modernize what we see as the evidential procedures.

We must see a change or adaptation of the certification requirements as put forth in Section 65B of the Indian Evidence Act, 1872 for use with block chain records which in turn will increase the courts' acceptance of tech based evidence.

Third we should see the development of clear liability models which determine responsibility between developers, platform providers and contract parties in the case of smart contract deployment. This will put in place a system of accountability for issues like coding mistakes or automated failure.

Also we see the implementation of regulatory sandboxes and investment in judicial capacity which will support the controlled roll out of blockchain tech and at the same time allow courts and regulatory bodies to develop experienced based interpretive practices. As a whole these actions will encourage growth in the field of innovation at the same time as they secure legal certainty and protection of rights.

## **Conclusion**

Blockchain-based smart contracts have created a significant shift in the manner in which contractual obligations are created and executed. While Indian law does not explicitly recognise smart contracts, under the Indian Contract Act, 1872 and the Information Technology Act, 2000 but they provide a foundational basis for their validity. challenges though remain relating to automated execution, allocation of liability, and admissibility of blockchain records under the Indian Evidence Act, 1872 which reveal gaps in the current legal framework.

The study finds that smart contracts are not recognized under Indian contract law, and this absence of explicit statutory regulation creates legal uncertainty. Comparative analysis with foreign jurisdictions demonstrates that regulatory clarity and interpretative guidance play a crucial role in facilitating the lawful adoption of smart contracts. The research therefore concludes that targeted legislative reforms and judicial interpretation are essential to ensure legal certainty, accountability, and effective integration of smart contracts within India's evolving digital economy.