# INTEGRATION OF BLOCKCHAIN'S 'TRUST LESS' SYSTEM INTO LEGAL CONTRACTS

Mohamed Zayd, School of Excellence in Law, Chennai

**ABSTRACT**

Blockchain technology, which Satoshi Nakamoto (2008) first introduced with the paper titled 'Bitcoin: A Peer-to-Peer Electronic Cash System,' talks about digital transactions from one person to another without the involvement of any financial body. The system works on proof of work and hash timestamps so that any contract made on the chain is publicly accessible and cannot be altered after the contract has been made. It is a completely decentralised and non-trust placing system which ignores any third-party involvement. This paper discusses blockchain and the future of Indian contracts along with it. Bringing this technology to our legal system will largely benefit the populace, as legal contracts made using blockchain will not only rid society of the manipulation of records, breach of contracts with no evidence, and the time at which the contract was made, but it can also be used as evidence in the court of law to prove the validity of the contract. Areas such as real estate transactions, property registration, insurance, and employment are more susceptible to contract manipulation. In modern-day India, contracts between two parties are governed by the Indian Contract Act of 1872. Four major steps are involved in forming a legally valid contract between two parties under the Indian Contract Act of 1872: Offer, Acceptance, Consideration, Consent. This paper will critically analyse how blockchain smart contracts are applicable under the Indian Contract Act of 1872, discussing their legality and whether courts recognise them. It will also examine the validity of contracts created on the blockchain and explore potential solutions to issues such as the lack of regulatory clarity, legal recognition of blockchain addresses, and enforcement challenges in cases of code-based errors or fraud. In the conclusion of this paper, the author has also provided provisions to healthily integrate blockchain into our system, and the author has also discussed how the issues in the passage can be resolved.

**Keywords:** Blockchain, Smart contracts, Indian Contract Act, Consensus, Decentralised.

## 1. Introduction

Blockchain technology was first introduced by Satoshi Nakamoto (2008) in a paper titled 'Bitcoin: A Peer-to-Peer Electronic Cash System,' where he introduced 'Bitcoin,' a digital currency that is not linked with any banks or central authority. Almost all financial transactions on the internet rely on banks and other financial institutions, which don't deliver much on trust. Bitcoin operates on a decentralised trustless verification system using cryptography and math, eliminating the need for central authorities like banks or governments, allowing transactions between two individuals directly, without placing trust in each other or other third-party applications.

## 2. Communal Ledgers and Digital Signatures

To clearly understand how this 'trustless' system works, let us take the example of a digital communal Ledger where people of a dorm store the information about their financial Transactions in the form of a message like, 'Josh owes Cindy $40'. Here, the problem with having a communal Ledger like this is that you can never tell which transaction is legitimate. What's stopping Cindy from adding a False transaction to her benefit?

To prevent such malicious transactions, we add digital signatures beside the message, indicating that Josh or any individual has approved this transaction. To make these digital signatures unique to a particular user, each is provided with a public key and a private key (secret key) (Narayanan et al., 2016). A public key, as the name suggests, is public and visible to everyone, whereas a private key is known only by the user. Unlike normal signatures, which are the same everywhere, digital signatures vary for different messages; therefore, they cannot be easily replicated.

Signing a message is a function of both the message and the private key. This ensures that the signature comes from only you and that the signature cannot be copied by anybody else.

*Sign (Message, Private Key) = Signature*

The verification of the signature is a function of the message, signature and the Public Key that returns either True or False, meaning if the Private Key used to sign the message doesn't match its corresponding Public Key, then it might be a fraudulent signature.

*Verify (Message, Signature, Public Key) = True/False*

These signatures usually come in the form of 256-bit 1s and 0s and are very secure. To try to bypass these signatures, one must try $2^{256}$ combinations of 1s and 0s. This number is astronomically large and is impossible to guess, meaning if a signature is found to be True, you know it's genuine and comes from the user.

## 3. Cryptography, Hash Functions and Proof of Work

Now in our Ledger System, we have authentic Digital signatures along with each message, but a question arises that can Cindy not just duplicate the same message with the digital signature multiple times?

Who decides which transaction must go in the Ledger and which one must not?

This is where cryptography**,** hash functions**,** and proof of work come in. Together, these tools help build a system that can function securely without relying on trust or a central authority. The very definition of a *trustless* system. (Narayanan et al., 2016)

### *3.1 Hash Functions*

A hash function is a mathematical algorithm that takes any input and gives out a fixed-length string of characters. This output is known as the hash or digest. For example, consider a hash function called SHA-256, which, when given the input 'Josh owes Cindy £40', returns a fixed-length string of characters. (Antonopoulos, 2017).

*Input:*

*'Josh owes Cindy $40'*

*Output: 51c54a2e2b1a7d735973b9cbd82659a58e301dbb1e124f24cb646bbf2a1d23ec*

This string of characters is unique for every single input, so even a small change in the input will produce a completely different hash. The hash created for an input is irreversible; it cannot be reverse-engineered from an output, so it is a very secure way of encrypting messages. Every hash has a timestamp, so you know when that hash was made on the Ledger. This makes hash functions ideal for data integrity checks. In blockchain, every transaction and block is hashed, meaning any change to the data alters the hash and is instantly detectable.

*Output for a slightly different input:*

*Input:*

*'Josh owes Cindy 40$'*

*Output:*

*df34766df2d22a515721a5d81b011ea758448662ab45b8489585746299870ffb*

Now, in further addition of Hash Functions, to our trustless Ledger System, let's allow everyone on the block to have a copy of the Ledger of their own, and when any transaction is made, they broadcast it to all the other 'Ledger Holders' to add to the Ledger as same. Now, to prevent anyone from adding a fraudulent transaction to their ledger, we must arrange the whole ledger into blocks of transactions, where each block contains the hash of the previous block, a list of verified transactions, a timestamp and the hash created from all this data. These blocks are arranged in order, or in a '**Chain**', hence the term '***Blockchain***'.

This structure creates a critical consequence: changing a single block invalidates all subsequent blocks, because their hashes would no longer align. This mechanism guarantees immutability. Once data is entered into the blockchain and verified, it becomes computationally infeasible to alter. A crucial property when implementing legal contracts, financial records, or government documentation.

Hence, Blockchain technology is nothing but a ledger-based system where all the transactions made on the block are verified through Digital Signatures and Hashing. But how do we figure out if a particular block added to the chain is genuine or not?

### *3.2 Proof of Work*

Let's say that each block contains a special number that, when put through SHA-256, gives an output with 30 0's in the beginning. To find that special number, an individual must have had a lot of 'work' done, as a 256-bit number with 30 0's in the beginning has a 1 in a billion chance of being found. This is the same concept Satoshi talks about in his paper (Nakamoto, 2008; Narayanan et al., 2016). To add a block to the chain, an individual or a 'miner', as we call it, must complete some intense computational work or provide 'Proof of Work'. Changing a transaction in the block even slightly will result in the user having to find a totally different Proof of Work. This ensures that whatever block is added to the chain is tied with a proof of work and that the block is otherwise considered invalid if it doesn't contain a proof of work.

This structure creates two key outcomes:

1. Security through energy expenditure: Attacking the blockchain would require enormous computing power and electricity.

2. Decentralised trust: No single miner controls the network. A consensus emerges from the computational effort.

PoW matters in Technologies like Blockchain because it assures users that no tampering has been done to the chain, and even if it has been done, it will branch the chain into two, creating two chains. The genuine chain is usually the longest, as most of the miners will be working on cryptographical problems to add blocks to that chain.

## 4. Legal Significance of Smart Contracts in India.

Now that we've established that Blockchain technology has the potential to promote non-centralised transfer of funds and data, let us discuss the implementability of Blockchain into legal contracts made in India.

Adding Blockchain to our inventory enables us to reduce our reliance on central institutions

and place less trust in them.

- Smart contracts allow for the speedy execution of contracts.
- Once on the block, they cannot be altered.
- By getting rid of intermediaries like brokers, notaries and other third-party delays, smart contracts allow for direct communication between the two signing parties.
- Reduces the cost of executing a contract.
- Operating on Blockchain technology provides transparency and Trust between two parties.
- The Hash Timestamps allow the recording of when the contract was made, which makes this contract foolproof.

Certain laws in India dictate how a contract is considered either lawful or void. We will now see how each of these laws is relevant to smart contracts.

***Indian Contract Act of 1872:***

This law forms the basis of Indian contracts and sets out the guidelines that must be followed for a lawful agreement. Self-executing digital contracts stored on a blockchain are known as smart contracts. The traditional principles of the Indian Contract Act determine their enforceability. According to Sections 10–12, a contract must satisfy the requirements for validity, including that the parties are competent, that consent is free, and that consideration is legal (Indian Contract Act, 1872). Sections 73 & 74 provide compensation and liquidated damages in case of breach of contract, even though the contracts are automated; if the conditions are not met, the contract may be deemed void by the courts.

***Information Technology Act, 2000 (IT ACT):***

The IT Act of 2000 makes smart contracts legal and recognisable by the courts as a valid means to create a contract under section 4 (Singh & Narayan, 2022). Digital Signatures made on said contracts are legally valid under section 5 and can be used as evidence of commitment to the contract (Information Technology Act, 2000). Although the Act does not explicitly regulate

blockchain, these sections collectively establish a foundation for digital contract enforceability and protection, providing courts a statutory reference for resolving disputes.

While these laws may provide provisions to accept Smart contracts as a valid way for parties to go into a contract, they have many regulatory issues that need to be addressed.

## 5. **Challenges of implementing Smart Contracts in India.**

### *5.1 Legal Recognition:*

According to the Indian Contract Act of 1872, for a contract to be valid, there must be an offer, acceptance, consideration and consent, with consent being the enabling factor of going into a contract. With Digital Contracts, the age of the two parties cannot be determined as they remain anonymous, therefore making it difficult for the Indian Law to find validity of the contract.

In the court's eyes, you also cannot determine whether the parties were in clarity of mind during the execution of the contract, as this is a self-executing contract with no third party involved.

Furthermore, under section 14 of the Indian Contract Act, the applicability of 'free consent' becomes a problem. (Indian Contract Act, 1872). In the traditional way of signing a contract, there are ways in which you can prove that consent was taken under pressure, coercion or by force, but in Smart contracts, once executed, you have no way to find out if the signee had given consent without the interference of other parties, though being efficient, smart contracts lack this quality.

### *5.2 Digital Signature Validity:*

According to the IT Act, 2000, the digital signatures must be issued by a certifying authority, but the hashing of Blockchain doesn't permit this.

Section 35 of the IT Act states that – *(1) Any person may make an application to the Certifying Authority for the issue of an electronic signature Certificate in such form as may be prescribed by the Central Government* (Information Technology Act, 2000). This becomes a problem as in Blockchain, digital signatures work on the principle of self-generating key pairs. This creates a legal grey area.

### *5.3 Jurisdiction:*

With Smart Contracts, you can execute them across borders. This causes problems as laws may not apply to problems relating to contracts made in this way, as it doesn't come under our Jurisdiction (Chakraborty & Mehta, 2022). Blockchain Technology spans globally, and it introduces a complex legal problem of, 'which country's laws should it abide by?'.

### *5.4 Coding Errors and Security Issues:*

When executing a Smart contract, if the programmer makes a coding error, the contract gets executed regardless of the programmer's intent. One such example of this is the 2016 DAO hack, where 60 million dollars were lost to coding errors. Our Indian Laws have no liability framework for coding errors that affect how a contract performs. (Siegel, 2017).

### *5.5 Scalability:*

Blockchain, in its current state, has scalability issues. Bitcoin processes almost 7 transactions/second, Ethereum 15, while UPI handles 2000+ (NITI Aayog, 2021). While this low output for high consumption of power conflicts with India's 2070 carbon neutrality goal, the high gas fees or fees for using the particular Blockchain limit its use for high-value cases.

## 6. Provisions And Solutions To Integrate Blockchain into Our Legal System

### *6.1 Legislative Reforms:*

To fully utilise Blockchain in its entirety, we need to make some major reforms in our legal system. For example, adding a comprehensive 'Digital and Automated Contracts' section in our Contract Act, 1872, that entails all the details regarding Smart Contracts and detailed information about the fulfilments required to perform a Smart Contract (Sharma & Desai, 2023). Some of the provisions that must be included in this section are:

- Definition of Smart Contracts.
- Establishment of Digital Identity Verification Methods
- Recognising cryptographic consent mechanisms

- Create a liability framework for all stakeholders.

### *6.2 Regulatory Infrastructure:*

Establishing a 'Blockchain Regulation Authority" or BRA for short, under MeitY that handles all matters related to Blockchain. This Regulatory Body must be able to license platforms where transactions are conducted, conduct audits for high-value contracts and put down some due process that needs to be followed to ensure the righteous use of this technology (RBI, 2020).. For example, they could create a national "Smart Contract Registry" for transparency and dispute resolution. Regulatory sandboxes should allow controlled testing of innovative applications.

### *6.3 Judicial Awareness:*

With the introduction of new technology into our legal system, we must put up initiatives so that the Judges and other members of the court who have been familiar only with the paper form of contracts for decades can learn about this new way of forming contracts. We can set up certain 'Technology Courts' in metropolitan cities like Mumbai, Bangalore and Chennai, where these cases might usually come up. These courts require judges who actually understand the technology and can comprehend the logic it uses. The National Judicial Academy can bring courses related to Blockchain so that it teaches them at least the basics of Smart contract code.

Right now, there is a need for standardised procedures related to Blockchain evidence. If someone brings in a Blockchain transaction as proof, there is no guideline for verifying it. Therefore, a step-by-step guideline is to be established for checking transaction authenticity and understanding smart contract execution logs.

### *6.4 Addressing Privacy Concerns:*

"*What goes on the block, stays on the block."*

This phrase is commonly thrown around when using Blockchain terminology to highlight the fact that whatever enters the chain stays there. It's permanent. This might cause some privacy issues for people, as they may want to handle their own personal data the way they want (MeitY, 2021).

To ensure safe use of Smart contracts, people handling personal data must follow a 'Privacy by Design' principle from day one. Don't collect more data than you need, assess privacy risks before deployment, and build in protection mechanisms from the start rather than trying to add them later.

### *6.5 Building The Right Foundation:*

India, as of now, is not ready for Blockchain Technology, as it does not have the right foundation needed for it to flourish. It features revolutionary contract technology, but it cannot meet our demand. As we discussed earlier, Bitcoin can handle 7 transactions/second, while Ethereum handles 15. This is barely enough to sustain our population of 1.4 billion people (NPCI, 2023; Ethereum Foundation, 2022).

Integrating a 'National Blockchain Infrastructure Grid' might sound ambitious, but it is exactly the kind of policy that will boost attention and sustainability of this Technology. Using energy-efficient systems, powering them with renewable energy, creating a reliable foundation for government and critical private sector contracts, etc.

Bringing a 'National Blockchain Infrastructure Grid' is not a way to control, but rather a way to streamline the introduction of Blockchain and ensure the infrastructure can handle the load when smart contracts go mainstream.

## 7. Conclusion:

In conclusion, implementing Blockchain technology into our legal systems comes with both challenges and hurdles, but if done right, it can exponentially increase people's trust in our system. It brings forth a shift. A shift into trustless systems where transparency, timestamps, and security all combine to deliver a totally decentralised way of forming legal contracts.

Revising laws written in the Victorian Era might be a good start. Our Contract Laws are. Ones that were written in the 1870s, a lot of technological advancements have occurred. Blockchain is an important indicator that there is an immediate need to revise our laws, as it doesn't fit into the relevance of our laws.

Bringing into action the policies mentioned above might invigorate people's curiosity to look further into Blockchain and learn about it. Legislation like the Information Technology Act,

2000, and the more recent Digital Personal Data Protection Act, 2023, provides a digital legal framework, they do not yet directly address the legal nature or enforceability of blockchain-based contracts.

Ultimately, blockchain does not make the law obsolete; instead, it requires the law to adapt to stay relevant. The shift towards a trustless contractual system should not be seen as a rejection of legal norms but as a chance to modernise them. As India aims to become a global leader in technology and innovation, aligning its legal framework with blockchain's possibilities is not just desirable, it's essential. The future of Indian contract law may well depend on how effectively it bridges the gap between code and conscience.

**Bibliography:**

Antonopoulos, A. M. (2017). *Mastering Bitcoin: Programming the open blockchain* (2nd ed.). O'Reilly Media.

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. https://bitcoin.org/bitcoin.pdf

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton University Press.

The Indian Contract Act, No. 9 of 1872, India Code (1872).

The Information Technology Act, No. 21 of 2000, India Code (2000).

Chakraborty, D., & Mehta, S. (2022). Blockchain and jurisdictional ambiguity: A global legal challenge. *Journal of International Cyber Law*, 14(1), 33–49.

Gupta, R., & Tyagi, S. (2021). Legal validity of smart contracts under Indian law: A blockchain perspective. *Indian Journal of Law and Technology*, 17(2), 101–123.

Sharma, A., & Desai, R. (2023). Rethinking the Indian Contract Act for the age of smart contracts. *Indian Journal of Legal Innovation*, 8(1), 45–62.

Singh, A., & Narayan, V. (2022). Regulatory challenges in implementing blockchain-based smart contracts in India. *Journal of Cyber Law & Policy*, 9(1), 45–67. [Journal not verified]

Ethereum Foundation. (2022). *Ethereum scalability and performance metrics*. https://ethereum.org/en/roadmap

European Commission. (2022). *Data Act proposal: Enhancing privacy by design in digital applications*. https://digital-strategy.ec.europa.eu

Ministry of Electronics and Information Technology. (2021). *National strategy on blockchain*. Government of India. https://www.meity.gov.in

National Payments Corporation of India. (2023). *UPI product overview*. https://www.npci.org.in

NITI Aayog. (2021). *India's roadmap to net zero emissions by 2070*. Government of India. https://niti.gov.in

Reserve Bank of India. (2020). *Enabling framework for regulatory sandbox*. https://www.rbi.org.in

Vijaya Bhaskar (2022). Re-entrancy, Still a significant threat? https://medium.com/coinsbench/re-entrancy-still-a-significant-problem-e8e1b6fabec1