BRIDGING CODE AND LAW: THE LEGAL LANDSCAPE OF SMART CONTRACTS

Kashish Mamnani, Jigeesha Vaishnav & Akshara Dubey, Institute of Law,
Nirma University

ABSTRACT

Smart contracts are of the nature of self-executing contracts that are programmed on blockchain platforms, represents a revolutionary change in online transactions. This research piece critically analyses the legalities of smart contracts in the Indian legal framework. It also deals with their legal enforceability under the Indian Contract Act, 1872, evidentiary admissibility under the Bharatiya Sakshya Adhiniyam, 2023 and the challenges posed by their intrinsic immutability.

The technical framework of smart contracts is the subject of this article, with a distinction between strong (fully autonomous) and weak (hybrid) types and their nexus with traditional legal concepts such as offer, acceptance, and consideration. Smart contracts are capable of satisfying basic contractual requirements, but it has loopholes, particularly in the use of cryptocurrency as consideration, given the regulatory confusion in India concerning digital assets.

One of the main concerns is the tension between the immovability in blockchain and the flexibility required by legal doctrines such as rescission, restitution, and amendment. The decentralized nature of blockchain and the reliance on cryptographic keys rather than state-authorized digital signatures create additional problems under the Information Technology Act, 2000 and for certification as evidence under the Bharatiya Sakshya Adhiniyam, 2023.

This article also reflects a comparative approach by comparing progressive regulatory strategies of various nations such as EU, the U.S. and the UK, which offer technology-neutral frameworks for the recognition of smart contracts. Such insights are utilized to compare and suggest reforms in the Indian context.

The article ends with the determination of major legal loopholes and prescribing statutory acknowledgment of cryptographic signatures, certification protocols specific to blockchain and judicial "legal overlays" to accommodate modification of the contract in extraordinary situations. The article seeks to offer a roadmap for harmonizing smart contract innovation with India's core legal principles.

INTRODUCTION

In a world where technology continues to shape every aspect of human life, the law is faced with new challenges that earlier systems were never formulated to address. Among the most interesting developments in the technology and law, smart contracts that are autonomous contracts written in code and uploaded on decentralized blockchain networks. These contracts eliminate intermediaries like lawyers, notaries or brokers and instead depend on cryptographic trust and automated enforcement. The prospect of transparency, efficiency and tamper-resistance has attracted huge interest in smart contracts as a vehicle for contemporary commerce.

However, although the smart contract technology architecture offers unprecedented security and certainty, their legal status is by no means clear. In India, with the enactment of the Bharatiya Sakshya Adhiniyam, 2023 (BSA), very important questions arise as to whether such blockchain-based instruments are capable of being accepted and enforced as evidence in courts. In the first stage, their admissibility is subject to the requirements specified in Section 63 of the BSA under which computer outputs are treated as electronic records on condition of fulfilling certain requirements. Subsequently admitted, the talk reaches the presumptions made available under Sections 85, 86, and 87 regarding electronic agreements, safe electronic records, and electronic signature certificates. Whether smart contracts are able to properly take advantage of these assumptions is an open but urgent question, considering that they are decentralized and based on cryptographic as opposed to certifying authority–generated signatures.

Globally, however, the picture is more progressive. The European Union, through regulations such as MiCA, and jurisdictions such as the United States and the United Kingdom have increasingly recognized the enforceability of smart contracts. In these systems, courts have adopted a technology-neutral approach, emphasizing that the absence of a traditional written form does not negate legal obligations, provided that party intent is clear. Some jurisdictions have even developed mechanisms allowing judicial intervention to correct the rigidity of code in cases of fraud, mistake, or overriding public policy concerns. These comparative experiences highlight the gap between technological innovation and legal adaptation in India, and the urgent need to rethink traditional approaches to evidence and contract law.

This research article critically explores the admissibility of smart contracts in India under the BSA, analyzing both their technological foundations and their treatment under Indian evidence law. It also examines how similar challenges are addressed globally, and what lessons India can adopt from international best practices. The objective is to provide a holistic picture of the present challenges and to suggest reforms that can harmonize the immutable certainty of blockchain technology with the flexibility required by justice and fairness in legal proceedings.

SMART CONTRACTS: TECHNOLOGY AND LEGAL FOUNDATIONS

A. Technical Mechanics: Code Execution, Immutability, and Contract Typologies

Smart contracts are codes written as contracts, autonomous programs with pre-programmed rules, activated when predetermined conditions are fulfilled.[1] Generally installed on blockchain platforms such as Ethereum or Solana, these contracts reduce the roles of intermediaries like lawyers, notaries, or brokers. Once activated, they autonomously perform terms agreed upon between parties with no further human interaction. This automated aspect provides efficiency and trust, especially in situations where various parties interact without necessarily trusting or knowing one another.

An identifying feature of smart contracts is immutability, once a contract is posted on the blockchain, neither its code nor its execution record can be changed unilaterally.[2] This immutability guarantees integrity and tamper-resistance and hence fraud or unauthorized alteration becomes almost impossible. But this technical aspect, while providing safety, imposes a serious legal restriction: the inability to make corrections or modify the contract to changing circumstances after deployment.[3] Therefore, smart contracts are need to be written with precision and foresight, lest their inflexibility may produce results neither party had originally intended.

Classification-wise, smart contracts can be categorized broadly as strong and weak. Strong smart contracts are completely autonomous, each condition, term, and penalty

[1] SANNIDHI AGRAWAL, 'Smart Contracts: Functioning and Legal Enforceability in India' (2021) 7(1) INT'L J. L. & SOC. SCI. 1.
[2] A. NARANG, 'Smart Contracts: Potential and Legal Status', SEMANTIC SCHOLAR [https://www.semanticscholar.org/paper/Smart-Contracts:-Potential-and-Legal-Status-Narang].
[3] VIDUSHI VATS & SHASHI BHUSHAN, 'Smart Contracts and Legal Enforceability' INT'L J. ADVANCED LEGAL RESEARCH.

are inherent in the code. They are appropriate for clearly defined deterministic transactions, like automatic transfer of payments on confirmation of delivery. While weak smart contracts are based to some extent on off-chain elements, needing human effort or subjective interpretation to complete or enforce some terms. While this hybrid model is more flexible and closer to real-world realities, it reintroduces trust-based dependencies, thus negating some of the blockchain's charm.

B. Legal Characterization under Indian Law

1. Contract Formation: Indian Contract Act, 1872

Based on Indian law, the basis of any enforceable contract is the Indian Contract Act, 1872 which requires certain key elements like offer, acceptance, legal consideration, intention to create a legal relationship and free consent.[4] For smart contracts, jurists and scholars started researching the fit between the old requirements and digital and automated constructs.

An offer can be read as a posting of smart contract code onto a public blockchain, a public call to engage on terms stated. Acceptance is made when a second party engages with this code, most commonly by launching a transaction that activates the contract. Consideration is there too, usually in the form of cryptocurrency or tokens. But here there is a significant challenge. While the Supreme Court in ***Internet and Mobile Association Of v Reserve Bank of India,***[5] invalidated the RBI's ban on cryptocurrency transactions, the broader regulatory treatment of crypto assets in India remains ambiguous. If cryptocurrencies were to be declared illegal tender or banned again, this could jeopardize the enforceability of smart contracts involving such consideration.

Yet another serious issue is posed by the principle of mutuality. Indian contract law stipulates that both parties must give something of value; unilateral smart contracts like donation contracts or automatic grants might not meet this criterion,[6] even if they are flawlessly executed in code. This leaves a gap between what is technically executed and

[4] SATYANSH SINGH PARMAR & LAVANYASHREE RAJE PARMAR, 'Legal Examination of Smart Contracts under Indian Law', WHITE BLACK LEGAL.
[5] *Internet & Mobile Ass'n of India v. Reserve Bank of India*, AIR 2021 SC 2720.
[6] KHURANA & KHURANA, 'Revisiting the Concept of Consideration' (2022) WHITE BLACK LEGAL RESEARCH PAPER (Mar. 1, 2022).

what is legally enforceable, leading to conclude that enforceability cannot be assumed just because execution was possible.

2. Legal Validity of Electronic Contracts: IT Act, 2000

The Information Technology Act, 2000, particularly Sections 3, 5 and 10A, gives legal validity to electronic records and digital signatures which form the basis of electronic contracts.[7] Section 10A states that contracts made in electronic form cannot be rejected legal validity on the ground of having been made in electronic format alone. But this doesn't necessarily mean legal validation of smart contracts, which employ cryptographic keys and public-private key pairs in place of signatures authenticated by state-authorized persons under the IT Act's framework of digital signatures.

This technical-legal inconsistency poses a possible chokepoint. Though blockchain signatures provide security and authentication of identity, they are not "digital signatures" within the meaning of the Indian IT Act unless signed by a certifying authority.[8] Their validity in formal legal process or arbitration, particularly when authentication becomes adversarial, is doubtful. In the absence of legislative guidance, the courts might be reluctant to consider such signatures as irrefutable evidence of contract formation or agreement.[9]

3. Comparative Jurisprudence: International Views

Across the world, legal frameworks are changing to adapt to the intricacies of smart contracts. The EU's MiCA Regulation and the U.S. Uniform Electronic Transactions Act (UETA) both have expansive legal definitions of electronic contracts and stress enforceability, especially where digital assets and cryptographic authentication are involved.[10] Such tools encourage technological neutrality, where contracts entered into

[7] NAYA LEGAL, 'Digital Contracts and Smart Contracts: Legal Validity and Enforceability' [https://www.nayalegal.com/digital-contracts-and-smart-contracts-legal-validity-and-enforceability] (last visited Sept. 7, 2025).
[8] AZB & PARTNERS, 'Smart Contracts in India: An Overview' [https://www.azbpartners.com/bank/mondaqs-comparative-guide-to-blockchain-india/] (accessed 7 September 2025).
[9] HARSHITA RAJ, 'On Application of Arbitration and Smart Contracts: An Indian Perspective' (2022) 1(1) CMR U. J. DISP. SETTLEMENT & ARB. 86.
[10] UK JURISDICTION TASKFORCE, Legal Statement on Cryptoassets and Smart Contracts (2019), [https://lawtechuk.io] (accessed 7 September 2025) .

by means of automated processes may be treated equally as traditional ones, as long as the intent of the parties is manifest.

The UK Jurisdiction Taskforce (UKJT), in its historic 2019 legal statement clearly acknowledged smart contracts as having the ability to form binding legal obligations, regardless of the lack of conventional written form. Furthermore, jurisdictions such as Arizona and Tennessee within the U.S. have enacted laws providing for judicial repair or override of a smart contract where fraud, mistake, or public policy are concerned. These jurisdictions are headed towards "legal overlays" which is unified legal frameworks that enable courts to intrude on otherwise immutable code to preserve central legal principles.

ENFORCEABILITY: IRREVOCABILITY VS. RESCISSION AND RESTITUTION

A. Common Law Doctrines: Rescission and Restitution

One of the fundamental principles of Indian as well as common law is that, even if a contract is validly entered into, it may be rescinded or corrected on certain grounds like fraud, misrepresentation, mistake, or undue influence. When a contract is rescinded, the intention is to restore both parties to their positions prior to entering into the contract, i.e., restitution1. Such principles are based on equity and are utilized as remedies so that there will not be unjust enrichment or exploitation of any of the party to the contract.

But the self-enforcing and irrevocable character of smart contracts represents a nascent challenge to these doctrines. When a smart contract runs on a blockchain, the transaction is irreversible, and absent pre-coding a rollback or contingency provision by the parties, the system does not allow retraction. This inflexibility creates serious questions in situations where a contract was induced through misrepresentation or contained an unsuspected programming flaw.

B. Immutability vs. Judicial Override: The Legal-Tech Tension

The doctrine of immutability is in direct conflict with judicial maxims that are predicated upon the discretionary powers of the courts to correct or invalidate unfair contracts. Such conflict is best demonstrated by the 2016 DAO hack on the Ethereum

blockchain. Using a bug in the code, a hacker stole millions of Ether. Because the smart contract allowed such a move technically, it was not illegal in code but was most definitely unfair according to the law. Ethereum's remedy, a hard fork to undo the transactions was a decision made through consensus of the community, not via legal recourse. This example illustrates the need for legal solutions to override code-level execution where fairness requires.

C. Emerging Solutions: Designing Legally Adaptive Smart Contracts

Progressive jurisdictions are testing combined legal design to bridge these gaps. The UK Jurisdiction Taskforce (UKJT) has promoted legal overlays, where legal terms are added to smart contracts specifically authorizing judicial intervention in fraud or mistake cases. Overlays serve to bridge between immutable code and the equitable requirements of contract law.

Along the same lines, Arizona has enacted "smart contract repair" provisions that vest statutory powers to amend contracts if technical failure results in unforeseen consequences. This is in recognition that code, just like language, is imperfect and open to misinterpretation. Incorporating repairability in the legal framework bridges technology with justice.

Another new innovation picking up steam is the application of hybrid contracts, in which the self-executing aspect is restricted to deterministic elements (i.e., payment on delivery), but subjective or discretionary elements (i.e., dispute resolution) are addressed through conventional legal mechanisms, including arbitration and mediation provisions. These hybrids have the efficiency of automation combined with legal protection.

D. India's Regulatory Position and Pathways for Reform

India is at a junction. Although the Indian Contract Act is broad enough to encompass digital transactions, it does not directly deal with the special architecture of smart contracts. The absence of statutory recognition, particularly with regard to blockchain immutability and crypto-based consideration, creates a vast amount of uncertainty for courts and parties. Furthermore, the IT Act's narrow focus in accepting non-certified

cryptographic signatures under its own system makes it more problematic.

As opposed to proactive jurisdictions, India lacks regulatory clarity, particularly on legal remedies in the event of disputes resulting from smart contract execution. Consumer protection legislation also remains quiet on redress mechanisms whenever harm is caused due to autonomous code execution.

In order to progress, legislative change is needed. The Indian Contract Act and IT Act need to be revised to specifically acknowledge smart contracts, determine their legal limits and allow courts to step in where appropriate. Creating regulatory sandboxes, restricted environments for experimenting with smart contracts and legal recourse may also act as innovation incubators without exposing consumers to full risk.

India may also learn from international models to frame an equilibrium regulatory framework that recognizes the efficiency of smart contracts while keeping them within the scope of legal examination and judicial fairness. Failing this reform, India will find itself lagging in the international race towards blockchain-based legal innovation.

Admissibility of Electronic Evidence

The admissibility of electronic records, including smart contracts, in Indian courts is governed by the Bharatiya Sakshya Adhiniyam. The key provisions are Section 63, which talks about admissibility of electronic records and Sections 85, 85 & 87, which provide presumptions regarding electronic agreements, records and digital signatures. The Information Technology Act, 2000, further backs these provisions by defining terms like Digital signatures and records.

Admissibility of Electronic Records under section 63 of Bharatiya Sakshya Adhiniyam

"Computer output" is defined in Section 63(1) of the BSA, 2023 as a variety of electronic records, such as printouts, saved files, and digital copies.[11] The Information Technology Act of 2000, which acknowledges computer-processed output as authentic

[11] BHARATIYA SAKSHYA ADHINIYAM, 2023, § 63(1), No. 45, Acts of Parliament, 2023 (India).

electronic records, is also in compliance with this.

Whether smart contracts are computer output and, if so, whether they are acceptable evidence under Section 63 of the BSA, 2023, are the points of contention here. The output of a smart contract is produced by a computer system, such as the nodes of the block chain, hence it can be categorized as "computer output" since smart contracts are computer programs with computer-made outputs.

Transaction records entered into a blockchain ledger of this kind can be considered electronic records. A hash value, which is a digital fingerprint of a file, is necessary to guarantee that the electronic form or output corresponds to the original document. However, with a smart contract, the original electronic record is the hash value or code that is on the chain record. This smart contract's hash value confirms its integrity, allowing courts to compare the alleged smart contract code or transaction with the authenticity of the on-chain hash rather than comparing a copy with the original.

This section additionally specifies that, if the four requirements outlined in section 63(2) are satisfied, the data found in an electronic record created by a computer, or "computer output," is admissible as evidence.[12] In order to examine how these conditions are applied in the context of smart contracts, let's start with the fact that, once implemented, smart contracts are always active and callable, with nodes processing transactions, validating blocks, and updating ledgers continuously. It is common practice to process information on the blockchain network.

Furthermore, nodes in smart contracts are always processing transactions, validating blocks, and updating ledgers. Once deployed, smart contracts remain active. For instance, on Ethereum, nodes execute hundreds of smart contract transactions daily. The blockchain network that powers smart contracts is therefore frequently used for information processing.

Third, the hash function, which cryptographically connects the blocks in the blockchain, instantly rejects any tampering or malfunction. As a result, smart contracts are impervious to manipulation or malfunction, which has no bearing on accuracy.

[12] BHARATIYA SAKSHYA ADHINIYAM, 2023, § 63(2), No. 45, Acts of Parliament, 2023 (India).

Fourth, the results of smart contracts are generated solely by running the code with the input supplied by the user and are based on transaction logs or hash values. The outcome is the same as the input because blockchain nodes run deterministic code. Thus, the output or information is derived from input that is normally fed into the computer.

Smart contracts may therefore be accepted as evidence. The problem here is that, in order for the evidence to be admitted in court, section 63(4) requirements that it be accompanied by a certificate. Whereby the certificate must be signed by the person in charge of the computer or device that produced the computer output.[13] However, in smart contracts which are decentralized blockchain-based and operate without human intervention, no single person in charge of the computer system has the authority to sign the certificate.

All smart contract transactions occur on blockchain nodes, which are distributed across countries, but the certificate also requires device information to produce the computer output. Jurisdictional confusion occurs in blockchain since a single server or computer cannot be established as the source. Courts may not find blockchain records reliable or admissible since they are pseudonymous, which hides user's identities behind cryptographic addresses. This certification assesses the reliability of certain computer systems and promotes human accountability for the people who operate them.

Therefore, BSA's requirements pertaining to electronic evidence pay close attention to both the electronic evidence and the computer system or equipment that generates it in order to prevent any tampering or alteration. These protections under section 63 of the BSA are intended to guarantee the authenticity and source of electronic records, as was decided in the instance of ***Anvar P.V. v. P.K. Basheer.***[14] The entire trial based on electronic record proof can be a farce of justice if protections are not in place because electronic records are more vulnerable to tampering, alteration, transposition, excision, etc.

In the world of blockchain technology, which powers smart contracts, there is no challenge or reason for fear because the primary objective of the safeguard mechanism under section 63 is to guarantee that justice is served and that tampering, altering,

[13] BHARATIYA SAKSHYA ADHINIYAM, 2023, § 63(4), No. 45, Acts of Parliament, 2023 (India).
[14] *Anvar P.V. v. P.K. Basheer,* (2014) 10 SCC 473.

transposition, and other such actions do not take place. Nonetheless, it is concerning since smart contracts' immutability will make Section 63 compliance challenging. In lieu of requiring a certificate under section 63(4), the court may ask technical specialists to confirm smart contracts or a new interpretation or law that is adaptable enough to incorporate decentralized technology, like cryptographic proof, which will be highlighted and recognized as reliable evidence.

Presumptions as to regularity, authenticity and intention of electronic agreements, records and signatures

When a smart contract passes the admissibility test under Section 63 of the Bharatiya Sakshya Adhiniyam, the next thing to consider is how Sections 85, 86, and 87 presumptions apply. The reason these presumptions are so important is that they lower the burden of proof by enabling courts to accept certain electronic documents, signatures, and certifications as authentic until proven otherwise.

According to section 85 of BSA, courts may assume that a document that is presented as an electronic record and contains digital or electronic signatures was reached by the individuals involved.[15] The IT ACT, 2000 defines digital signatures as a mechanism of authenticating electronic records through an electronic technique or procedure in accordance with the act's provisions.[16] The IT Act of 2000 specifies in Sections 3 and 3A the methods for authenticating electronic records: first, digital signatures; and second, electronic signatures. These signatures can only be legally recognized as electronic signatures if they are certified by a licensed Certifying Authority.[17]

The smart Contracts use asymmetric cryptography, parties sign using their private keys to create a cryptographic signature that is comparable to a digital signature. The problem is that, as stated in the IT Act of 2000, these are self-generated and not issued by any certifying authority.

The digital signatures under the IT Act and cryptographic signing of transactions in blockchain have comparable characteristics, smart contracts may be covered by section

[15] BHARATIYA SAKSHYA ADHINIYAM, 2023, § 85, No. 45, Acts of Parliament, 2023 (India).
[16] INFORMATION TECHNOLOGY ACT, 2000, § 2(1)(p), No. 21, Acts of Parliament, 2000 (India).
[17] INFORMATION TECHNOLOGY ACT, 2000, §§ 3 & 3A, No. 21, Acts of Parliament, 2000 (India).

85 of the Bharatiya Sakshya Adhiniyam. The automatic assumption of security that legally recognized digital signatures enjoy, however, might not apply to cryptographic signatures in smart contracts if they are not validated by a certifying authority. Section 85 of the BSA states that in 2023, courts will need more proof to help authenticate electronic records, which smart contracts cannot provide.[18]

Section 86 of the BSA, 2023, as interpreted by that court, assumes that a legitimate electronic signature is intact and has been signed with good purpose, as well as that a secure electronic record has not been altered. Thus, blockchain technology, which stores and runs smart contracts, is immutable and therefore unchangeable. Therefore, courts have a reasonable presumption that a smart contract maintained on a blockchain has not been changed since it was deployed. Cryptography works similarly to digital signatures in that it guarantees authenticity and non-repudiation. However, the only difficulty that emerges is with CA, which calls for authentication.[19]

For smart contracts to be regulated by Indian law, section 87 of the BSA, 2023, where the court accepts the validity of CA certificates, should be made flexible to allow for the inclusion of cryptographic signatures, much like on smart contracts. Since no identification is required, CA may be hesitant to validate these cryptographic transactions since, although they demonstrate control, these smart contract cryptographic keys cannot reveal the identity of the parties involved.[20]

Modifying and Terminating Smart Contracts: Legal Challenges and Innovative Solutions

A. Legal Hurdles in Smart Contract Modification

The foremost legal challenge facing modification of a smart contract is the contradiction between the immutability of a blockchain and contract law principles. In traditional contract law, there are developed systems for modifying a contract which include mutual agreement, change of circumstances, or a modification by the court. These principles of law face smart contracts because of their automated, irreversible nature.

[18] BHARATIYA SAKSHYA ADHINIYAM, 2023, § 85, No. 45, Acts of Parliament, 2023 (India)..
[19] BHARATIYA SAKSHYA ADHINIYAM, 2023, § 86, No. 45, Acts of Parliament, 2023 (India).
[20] BHARATIYA SAKSHYA ADHINIYAM, 2023, § 87, No. 45, Acts of Parliament, 2023 (India).

There is a lack of specific laws that deal with smart contracts which leads to a considerable legal risk. There are states like Arizona and Tennessee that have passed laws validating smart contracts, but the rest of the legal world is still behind in dealing with these programmable contracts. Take the Indian Contract Act of 1872, it advanced long before the blockchain was invented, so there were no provisions made for automated execution of contracts.

Another legal hurdle arising from the definitional ambiguity surrounding smart contracts themselves. Courts must be careful while determining whether smart contracts constitute traditional legal contracts or merely technological tools for contract execution.[21] The lack of subjective intent in performing smart contracts undermines the key idea of "meeting of minds" that is crucial for forming contracts.[22]

The recent landmark decision in ***Van Loon v. Department of the Treasury*** illustrates these definitional challenges. The Court of Appeals distinguished between mutable and immutable smart contracts, holding that truly immutable smart contracts cannot be considered "property" under federal law because they are incapable of ownership or control.[23] This ruling demonstrates how traditional legal categories struggle to accommodate the unique characteristics of blockchain-based agreements.[24]

1. The Immutability Paradox

The technical inflexibility of smart contracts creates a fundamental tension between blockchain's core value proposition and legal system requirements. On one hand immutability provides security and trust lessness but on the other it eliminates the flexibility that is essential for effective contract governance.[25] This paradox is particularly acute when unforeseen events necessitate contract changes, or when errors

[21] ANETTA (UNIV. OF ZÜRICH), Legal Challenges and Frameworks of Smart Contracts in Blockchain Technology (GoTranscript, Sept. 28, 2024).
[22] APOORVA MEHTA, 'Smart Contracts: Navigating Legal Waters in the Digital Age' (2023) LEGAL DESIRE MEDIA & INSIGHTS.
[23] DANIEL J. DAVIS & ALEXANDER C. KIM, '"Smart Contracts" Ruling Forces a Blockchain Development Rethink' MONDAQ (Feb. 10, 2025).
[24] *Van Loon v. Dep't of the Treasury,* No. 23-50669 (5th Cir. Nov. 26, 2024).
[25] JEREMY M. SKLAROFF, 'Smart Contracts and the Cost of Inflexibility' (2017) 166 U. PA. L. REV. 263.

in coding need to be corrected.[26]

Research indicates that approximately 80% of smart contracts contain serious vulnerabilities that could ultimately lead to humongous fund loss.[27] However, the specific nature of blockchain deployment means that these vulnerabilities cannot be easily corrected through traditional software patching mechanisms. This technical limitation creates a substantial legal risk and reduces confidence in smart contract reliability.

2. Proxy Contract Solutions

The development of **proxy contract patterns** represents an attempt to address technical inflexibility while maintaining blockchain benefits. These systems create an "illusion of changeability" by using routing layers that direct user interactions to different implementation contracts. However, proxy contracts introduce new legal complexities regarding contract interpretation and party obligations.[28]

The distinction between truly immutable and proxy-based "mutable" smart contracts has profound legal implications. Jurisdictions such as Wyoming and Tennessee now require smart contracts to be upgradeable for certain applications, creating a regulatory imperative for technical flexibility that challenges blockchain's immutability principles.[29]

3. Economic Implications of Inflexibility

The cost of inflexibility in smart contracts extends beyond technical considerations to encompass significant economic implications. Research demonstrates that smart contract inflexibility increases transaction costs compared to traditional contracts by

[26] JEREMY M. SKLAROFF, 'Smart Contracts and the Cost of Inflexibility' CLS BLUE SKY BLOG (Jan. 4, 2018) [https://clsbluesky.law.columbia.edu/2018/01/04/smart-contracts-and-the-cost-of-inflexibility/] (accessed 7 September 2025) .
[27] CODERS STOP, 'The Fatal Flaws in 80% of Smart Contracts' CUBED (Apr. 16, 2025) [https://blog.cubed.run/the-fatal-flaws-in-80-of-smart-contracts-and-how-to-avoid-them-a36527df5fbf] (accessed 7 September 2025).
[28] DAVIS & KIM, 'Smart Contracts Ruling Forces a Blockchain Development Rethink' BLOOMBERG LAW (Jan. 30, 2025).
[29] *Id.*

eliminating opportunities for efficient breach and renegotiation.[30] This economic inefficiency undermines the purported benefits of smart contract automation.

The inability to modify smart contracts in response to changed circumstances forces parties into suboptimal performance scenarios, potentially leading to economic waste and market inefficiencies. Traditional contract law's flexibility in allowing contract modification serves important economic functions that smart contracts currently cannot replicate.

B. Innovative Solutions in Smart Contracts

1. Circuit Breaker Mechanisms

Circuit breaker methods are an important legal design innovation that maintains the automated advantages of smart contracts while offering emergency protections. When flaws or unusual circumstances are identified, these systems' implementation of security flags allows trusted parties to stop the execution of contracts.

Circuit breakers operate through modular design patterns that include emergency stop functions directly into smart contract code. When activated, these mechanisms can prevent unauthorized access to contract functions or temporarily suspend operations until issues are resolved.[31] The legal framework surrounding circuit breakers requires careful consideration of who possesses activation authority and under what circumstances intervention is justified.[32]

Advanced circuit breaker implementations employ automated monitoring systems that utilize external data feeds and algorithmic triggers to detect anomalous conditions.[33] Chainlink's automation services, for instance, may keep an eye on price feeds and

[30] SKLAROFF (supra note 25) 263.
[31] YOS RIADY, 'Fault Tolerant Smart Contracts with Circuit Breakers' (July 25, 2020) https://yos.io/2020/07/25/fault-tolerant-smart-contracts/ (last visited Sept. 7, 2025).
[32] SAFEBOXLABS, DeFiCircuitBreaker, GITHUB https://github.com/SafeBoxLabs/DefiCircuitBreaker (last visited Sept. 7, 2025).
[33] CHAINLINK, 'DeFi Circuit Breakers with Chainlink Proof of Reserve and Automation' CHAINLINK BLOG (Jan. 11, 2023) [https://blog.chain.link/defi-circuit-breakers/] (last visited Sept. 7, 2025).

automatically activate circuit breakers when preset thresholds are surpassed, offering real-time defence against technical malfunctions or market manipulation.[34]

2. Hybrid Contracts: Bridging Legal and Technical Domains

Hybrid smart contracts emerge as a solution that combines the benefits of blockchain automation with traditional legal flexibility. These agreements provide a comprehensive framework that overcomes the drawbacks of solely code-based agreements by combining aspects of natural language legal contracts and code-based smart contract components.[35]

The Minimum Hybrid Contract (MHC) model proposed by academic research demonstrates how immutable blockchain transactions can be linked to traditional legal contracts, providing transparency and auditability while maintaining legal enforceability.[36] With this strategy, parties can still utilize conventional legal remedies and dispute resolution procedures while taking advantage of blockchain's transparency and automation.

3. Multi-Signature Escrow Systems

Multi-signature escrow mechanisms provide exclusive governance structures that distribute control among multiple parties, hence addressing concerns about centralized authority in smart contract management.[37] The said systems require multiple authorized signatures to approve transactions or contract modifications, creating built-in checks and balances providing better security.

Multi-signature implementations support various configurations, including 2-of-3, 3-of-5, and n-of-m arrangements, allowing parties to customize security levels based on their specific requirements.[38] These mechanisms find particular application in decentralized

[34] SMARTCONTRACTKIT, quickstarts-circuitbreaker, GITHUB https://github.com/smartcontractkit/quickstarts-circuitbreaker (last visited Sept. 7, 2025).
[35] NILOUFER SELVADURAI, 'Mitigating the Legal Challenges Associated with Blockchain Smart Contracts' (2023) 80(3) WASH. & LEE L. REV. 1163.
[36] JØRGEN S. NOTLAND, JAKOB S. NOTLAND & DONN MORRISON, The Minimum Hybrid Contract (MHC) (arXiv preprint, Feb. 17, 2020).
[37] NADCAB, 'Multisig for Smart Contracts' NADCAB BLOG https://www.nadcab.com/blog/multisig-for-smart-contracts (last visited Sept. 7, 2025).
[38] *Id.*

autonomous organizations (DAOs) and high-value transactions where distributed decision-making enhances security and legitimacy.

The legal foundation for multi-signature escrow necessitates giving fiduciary responsibilities, liability distribution, and signatories' decision-making authority considerable thought. While Vermont upholds basic liability concepts, recent legislation in Wyoming expressly exempts DAO members from customary fiduciary duties.[39]

INDIA'S REGULATORY GAPS AND COMPARATIVE INSIGHTS

A. Lack of Standardized Legal Recognition at Global level

Different jurisdictions approach smart contracts differently. Some (UK, Singapore, US) are proactive, others like India and many civil law countries lag.

Country	**Legal Status of Smart Contracts**	**Mechanism for Override/Amendment**
UK	Recognized (UKJT, 2019)	Legal override possible via court orders
US	Recognized under UETA & ESIGN	Varies by state; Arizona, Tennessee recognize code-as-law
India	Not formally recognized	Traditional contract law applies; no direct override
China	Recognized in sandbox	State override allowed for financial regulation
EU	GDPR challenges exist	"Right to be forgotten" incompatible with immutability

[39] EUROPEAN CORPORATE GOVERNANCE INSTITUTE, The Viability of Blockchain in Corporate Governance (ECGI Working Paper).

B. Legal Status and Regulatory Approaches Worldwide

1. United States: State-by-State Approach

The United States has adopted a fragmented, state-by-state approach to smart contract regulation, with varying degrees of recognition and requirements for upgradeability.[40] Several states have passed legislation recognizing smart contracts as legally valid and enforceable agreements, but with different requirements and standards.[41]

Wyoming has been particularly proactive in addressing smart contract upgradeability challenges. The state's draft legislation requires smart contracts valued above a certain threshold to include resolution plans as a condition of enforceability.[42] The legislation specifically states that smart contracts "be capable of upgrade or amendment" and requires resolution plans that can be either built into the smart contract code or accompany the contract through readily accessible means.[43]

Tennessee has taken a more basic approach, recognizing blockchain technology and smart contracts in electronic transactions while defining smart contracts as "event-driven programs that run on distributed, decentralized, shared, and replicated ledgers". The state's legislation ensures that contracts are not denied legal effect solely because they contain smart contract terms, but does not specifically address modification or upgradeability requirements.

Illinois has implemented the Blockchain Technology Act, making smart contracts and blockchain records admissible as evidence in legal proceedings and prohibiting courts from denying smart contracts legal effect based solely on their technological nature. The act provides legal certainty for parties using smart contracts but does not specifically address modification challenges.

Recent federal court decisions have also impacted smart contract development approaches. The Fifth Circuit's decision in ***Van Loon v. US Treasury*** distinguished between mutable and immutable smart contracts, holding that immutable smart

[40] CODERS STOP (supra note 27).
[41] DAVIS & KIM (supra note 23).
[42] *Id.*
[43] BRONWYN E. HOWELL & PETRUS H. POTGIETER, 'Uncertainty and Dispute Resolution for Blockchain and Smart Contract Institutions' (2021) 17(4) *J. INST. ECON. 545*.

contracts fall outside the legal definition of property and are beyond certain regulatory authorities.[44] This ruling has forced developers to carefully consider the legal consequences of their architectural choices, particularly regarding upgradeability.

2. European Union: Comprehensive Regulatory Framework

The European Union has developed a more comprehensive approach to smart contract regulation through the Data Act,[45] which includes specific provisions on smart contracts for data sharing. The EU's regulatory framework mandates that smart contracts must have the same level of "protection and legal certainty as any other contracts generated through different means".[46]

Significantly, the EU legislation includes provisions requiring the possibility to terminate or interrupt transaction mechanisms, with lawmakers needing to decide which conditions would make such termination permissible. The framework also requires "rigorous access control mechanisms" and protection of trade secrets integrated into smart contract design.[47]

The EU's approach represents a more prescriptive regulatory stance that directly addresses the modification and termination challenges inherent in smart contracts. The legislation requires smart contracts to be subject to "harmonized standards" and mandates that termination mechanisms be built into smart contract systems.

3. India: Evolving Legal Framework

India's approach to smart contracts is primarily governed by existing contract law, particularly the Indian Contract Act of 1872.[48] Section 10 of the Act requires contracts to satisfy basic elements including offer, acceptance, intention, and consideration, and smart contracts can potentially satisfy these requirements.[49]

---

[44] CHAINLINK (supra note 33).
[45] Yos Riady, (supra note 31).
[46] Riady (n 45).
[47] *Id.*
[48] NILOUFER SELVADURAI, 'Mitigating the Legal Challenges Associated with Blockchain Smart Contracts: The Protection of Hybrid On-Chain/ Off-Chain Contracts' (2023) 80(3) WASH. & LEE L. REV. 1163.
[49] INDIAN CONTRACT ACT 1872, § 10, No. 9, Acts of Parliament, 1872 (India).

However, the legal enforceability of smart contracts in India remains uncertain due to several challenges. The Information Technology Act requires digital contracts to have digital signatures,[50] from certified authorities, which conflicts with the decentralized nature of smart contracts. Similarly, the BSA , 2023 requires everyone to have valid digital signatures from certified authorities to prove authenticity of electronic signature, creating additional compliance challenges.[51]

Recent legal analysis indicates that Indian courts may apply traditional contract law principles to smart contract disputes, particularly in cases involving fraud, errors, or unfair outcomes. The Digital Personal Data Protection Act of 2023 imposes additional obligations on data handling that may affect smart contract operations.

Indian judicial precedents have shown a willingness to uphold electronically formed agreements as held in the case of ***Trimex International FZE Limited v. Vedanta Aluminium Limited,***[52] that the contracts entered through electronic communication are completely valid.

4. Singapore: The Pragmatic Approach

With the Monetary Authority of Singapore upholding a crypto-friendly stance and offering a flexible regulatory framework, Singapore has taken a practical approach to smart contract regulation. In Singapore, standard contract law principles which call for offer, acceptance and consideration determine the legal standing of smart contracts.[53] Existing financial regulations apply to the use of smart contracts in dispute resolution and cryptocurrency, but they are not officially regulated in and of themselves.

Singapore's strategy acknowledges that there are numerous unsolved legal concerns related to smart contracts, such as requirements for formality and term certainty. The regulatory framework recognizes that the main avenue for resolving conflicts involving smart contracts seems to be through standard contract law rules.

[50] INFORMATION TECHNOLOGY ACT 2000, § 2(1)(p), No. 21, Acts of Parliament, 2000 (India).
[51] BHARATIYA SAKSHYA ADHINIYAM 2023, § 73, No. 45, Acts of Parliament, 2023 (India)..
[52] *Trimex Int'l FZE Ltd. v. Vedanta Aluminium Ltd*., (2010) 3 SCC 1.
[53] NADCAB (supra note 37).

C. Statistical Analysis of Smart Contract Security and Modification Challenges

1. DeFi Security Breaches and Their Legal Implications

DeFiLlama reports that in 2024 alone, 79 vulnerabilities in the DeFi ecosystem cost more than $1.12 billion.[54] For legal systems trying to handle smart contract malfunctions and changes, this poses a significant obstacle.

The type of legal challenges is revealed by the classification of attacks: Protocol Logic assaults accounted for the majority of events, with 47% of exploits focusing on smart contract flaws. These figures show that there are serious financial and legal repercussions when defective smart contracts cannot be promptly changed or terminated.

According to historical statistics from 2016–2022, the top 50 DeFi hacks resulted in losses of $5.5 billion overall, with unaudited smart contracts being the target of 34% of attacks. This emphasizes how crucial it is to have legal frameworks that mandate sufficient security measures and offer channels for contract revision in the event that vulnerabilities are found.

2. Market Growth and Legal Adaptation of Smart Contracts

The market for smart contracts has grown rapidly, yet research organization's estimates of the market's size differ greatly. Accordingly, the global market was estimated to be worth between USD 2.02 and USD 2.2 billion in 2024, with estimates varying from USD 12.07 billion to USD 815.86 billion by 2032–2035. Significant regulatory gaps have resulted from this quick growth outpacing the development of the legal framework.

According to research, more than 30% of companies are anticipated to use AI-enabled smart contract protocols by 2025, and 70% of attorneys think that decentralized agreements must include incorporated compliance mechanisms. These figures demonstrate how urgently legal frameworks addressing termination and modification

[54] AUDITONE, '2024: A Year of Lessons in DeFi Security' AUDITONE BLOG [https://www.auditone.io/blog-posts/2024-a-year-of-lessons-in-defi-security] (accessed 8 September 2025).

issues are needed.[55]

RECOMMENDATIONS FOR INDIA

A. Modular Contract Architecture for Smart Contracts

One important step in resolving the flexibility issues with smart contracts is the creation of modular contract architectures. Modular design divides the terms of the contract into various parts that can be changed separately without changing the agreement as a whole. This method maintains the general contract structure and current responsibilities while enabling targeted modifications.

Legal frameworks that support modular architectures need to take into account a number of important factors, such as determining which modules are subject to modification, how changes will affect current contractual ties, and how modifications will be implemented. Modular adjustments shall not unintentionally nullify or change unrelated contract clauses, according to the legal design.

Most courts must comprehend how individual modules connect to the entire agreement; the deployment of modular systems necessitates careful consideration of contract interpretation principles.

B. Harmonized International Standards with regards to Smart Contracts

To address the global character of blockchain technology, standardized international standards for smart contract termination and modification must be developed.[56] With due acknowledgement to national sovereignty and legal traditions, these standards should provide uniform approaches to significant topics including, dispute resolution, contract upgradeability and cross-border enforcement.

International standards should cover legal processes for approving changes, technical specifications for contract upgradeability and systems for guaranteeing adherence to

[55] GRADY ANDERSEN & MOLDSTUD RESEARCH TEAM, 'Future Trends in Smart Contracts' MOLDSTUD (May 13, 2025) https://moldstud.com/articles/p-future-trends-in-smart-contracts-what-to-expect-in-the-coming-years (last visited Sept. 8, 2025).

[56] Convergence of Law and AI: Analysing the Legal Framework of Blockchain and Smart Legal Agreements' (2025) INT'L J. INNOVATION IN L.

requirements from several jurisdictions. While still offering sufficient clarity for cross-border transactions, the standards should possess enough to accommodate the diversity of legal systems. Governments, business leaders, and international organizations must work together to establish international standards in order to ensure their widespread adoption and useful application.[57] The formulation of standards that are both technically possible and legally robust requires this cooperative approach.

C. Specialized Legal Frameworks for Smart Contracts

The establishment of specialized legal frameworks specifically designed for smart contracts is essential for addressing their unique features and associated challenges. These frameworks should provide clear provisions for contract formation, termination, modification and dispute resolution while accounting for the technical limitations of blockchain technology.

Specialized frameworks should address critical issues including the legal status of upgradeable contracts, the allocation of authority to authorize modifications, the procedures for implementing changes, and the relationship between technical and legal modification requirements. The frameworks must offer clear guidance to practitioners while maintaining sufficient flexibility to adapt to technological developments.

The formulation of specialized frameworks requires extensive consultation with legal practitioners, technology developers, and industry stakeholders to ensure that the proposed rules are both legally sound and practically implementable. Such a consultative process is essential for developing frameworks that serve the needs of all relevant parties.

D. Enhanced Dispute Resolution Mechanisms for Smart Contracts

The establishment of enhanced dispute resolution mechanisms specifically designed for smart contract disputes is essential for addressing challenges of modification and termination. Such mechanisms should provide resolution of disputes in a cost-effective manner while respecting the technical characteristics of blockchain technology.

[57] *Id.*

To provide comprehensive coverage of potential disputes, these mechanisms should incorporate both traditional legal processes and blockchain-based solutions. The mechanisms must address both technical failures and legal disagreements and providing enforceable remedies for affected parties.

To ensure seamless implementation, enhanced dispute resolution requires coordination between traditional legal institutions and blockchain-based platforms, thereby providing integration and mutual recognition. This coordination is vital for creating systems that are capable of delivering effective relief for smart contract disputes.

CONCLUSION

Smarts contracts can be a game changing development in the area of how agreements can be formed and executed in this digital era. Smart contracts unique features of transparency, immutability and security makes them more preferred than traditional contacts. However, the immutable feature of smart contracts creates many challenges when they are assessed under Indian Legal Frameworks. While they can technically satisfy essentials of a valid contract such as offer, acceptance and consideration but as Cryptocurrencies are not a legal tender in India and using them as consideration in smart contracts creates uncertainty. Also, the lack of certifying authority that can back digital signatures for these smart contracts are creates a hindrance in enforceability and raise concerns of lack of fall-back mechanism in case of disputes.

Under Bharatiya Sakshya Adhiniyam, 2023 though smart contracts can be qualified as electronic records but other procedural requirements are difficult to meet in a decentralized system like India. Also, the absence of statutory clarity on Blockchain Systems, as they contradict the traditional long established laws which allows rescission and modification to prevent unjust outcomes restricts the use of smart contracts.

Other jurisdictions such as the EU, UK and parts of the US have flexible and neutral frameworks which include hybrid design which balances both code and traditional laws and emphasize on judicial oversight. For India the way forward is to amend the legislation or enhance interpretation of existing traditional laws available to include Smart Contracts in its ambit to govern these type of Contracts. The future lies in the sweet balance between technological innovations with foundational legal values not replacing them with each other.