SMART CONTRACTS AND ENFORCEABILITY UNDER TRADITIONAL CONTRACT LAW

Naina Verma, BA LLB (H), Amity University Lucknow

ABSTRACT

Despite the growing use of smart contracts in commercial laws, their enforceability under traditional contract law still remains uncertain. Smart contracts are "E-contracts", a self -executing contract to be precise but traditional law are those who enforces intentions and agreements between parties, this creates uncertainty among parties regarding legality of binding contracts, parties may avoid using smart contracts due to legal risk. Examining there two concepts of contracts widely apart from each other, this paper will explore cases, types, features, limitations, validity and enforceability of Smart Contracts and will evaluate to the solution of the problem by providing a refined insight of how the smart contracts are enforceable and limited under the contract law through the development of a conceptual framework. In addition, this paper will provide a proper understanding of the nature of smart contracts as well as the difficulty in establishing intentions to create legal relations. In the end, the paper concludes by proposing a hybrid legal technical framework to enhance legal certainty.

Keywords: smart contracts, traditional contract law, enforceability, self-executing contract, limitations

Introduction

With the rapid digitalization of commercial transactions, traditional contract law is increasingly intersecting with emerging technologies. One such innovation is the smart contract, a self-executing agreement powered by blockchain technology. While smart contracts promise efficiency, transparency, and automation, their integration into existing legal frameworks raises critical questions particularly regarding their enforceability under traditional contract law**.** This topic explores whether smart contracts satisfy classical legal requirements such as offer, acceptance, consideration, and intention to create legal relations.

Smart contracts are digital agreements that execute themselves automatically once certain conditions are met. Instead of relying on written clauses and third-party enforcement, they are built using computer code and usually operate on blockchain technology. This means that when the agreed terms are fulfilled, the contract carries out its obligations without the need for intermediaries such as courts or lawyers. By offering speed, transparency, and reduced costs, smart contracts present a modern alternative to traditional contracts, though their reliance on technology also raises important legal and practical considerations. The validity of contracts formed through electronic means (smart contracts) can be derived from Section 10 of the Information Technology Act, 2000.

This research aims to explain how smart contracts can be enforced under Indian law. It looks at existing laws, court principles, and gaps in regulation to better understand how technology and law interact. Since smart contracts have the potential to change how agreements are made and enforced, it is important to understand their role in India's legal system. This study can help lawmakers, judges, and businesses make better decisions about using and regulating smart contracts. Smart contracts can be legally enforceable, but this depends on whether they follow the basic rules of traditional contract law, not just on being created on a blockchain. Understanding how courts look at these agreements helps businesses use blockchain technology in a way that is practical, reliable, and more likely to be legally accepted.

When predetermined conditions are met, the contract executes automatically without requiring human intervention. For example, the smart contract is programmed so that once the payment is received, digital access to the house is automatically given to the tenant.

If the payment is not made on time, access is not granted or is automatically revoked. This

happens without the need for a landlord or third party to manually enforce the agreement. This example shows how smart contracts automatically carry out agreed terms, while still reflecting a traditional contractual relationship.

Review of Literature

In the preparation of this research paper, I have meticulously consulted a range of authoritative legal and scholarly platforms, including **DailyJus**, **iPleaders by LawSikho**, and **Naya Legal**. These erudite sources have been instrumental in facilitating a profound and nuanced comprehension of the intricate doctrines underpinning smart contracts and digitally executed agreements. They afforded a rigorous exposition of both the theoretical constructs and the pragmatic applications, encompassing contemporary regulatory frameworks, jurisprudential interpretations, and evolving legal paradigms. By synthesizing and critically engaging with the insights gleaned from these platforms, I was able to cultivate a holistic and multidimensional understanding that seamlessly integrates the technical, legal, and practical facets of blockchain-mediated contractual mechanisms.

Statement of problems

The advent of blockchain technology has revolutionized the way agreements are created and executed, giving rise to smart contracts**,** self-executing digital agreements that automatically enforce obligations when predefined conditions are met. While smart contracts offer unparalleled efficiency, transparency, and automation, their legal recognition and enforceability under traditional contract law remain uncertain**.** Traditional contract principles such as offer, acceptance, consideration, intention to create legal relations, and capacity were designed for agreements executed through conventional means, often involving written documents and signatures.

The decentralized and automated nature of smart contracts challenges these foundational principles, raising critical questions: Can consent manifested through digital interaction or automated execution satisfy the legal requirements of a contract? How do courts interpret liability, breach, and remedies when a contract executes itself without human intervention? Moreover, the immutability and code-driven nature of smart contracts complicate modification, dispute resolution, and compliance with jurisdictional laws. This research seeks to examine the intersection of blockchain-based smart contracts and traditional legal doctrines, identifying the

gaps, challenges, and potential frameworks for their enforceability within the established legal system.

Hypothesis

While smart contracts are fast, automatic, and secure, they may face challenges being fully recognized or enforced under traditional contract law because of differences in how consent, execution, and legal interpretation work.

Research objectives

- To analyse the concept, functioning, and legal nature of smart contracts in comparison to traditional contracts.
- To examine the enforceability of smart contracts under traditional contract law, identifying key challenges and ambiguities.
- To evaluate relevant case laws, judicial interpretations, and digital agreement precedents to understand legal recognition.
- To assess the potential integration of smart contracts within existing legal frameworks, considering their advantages, limitations, and regulatory implications.

Research methodology

The research adopts a **doctrinal methodology**, which is primarily library based and focused on analysing existing legal principles, statutes, case laws, and scholarly writings. This approach involves a detailed examination of the theoretical and conceptual foundations of smart contracts, as well as their enforceability under traditional contract law. Through the systematic study of primary sources such as legislations, judicial decisions, and recognized contract law doctrines, alongside secondary sources like articles, commentaries, and legal databases, the research seeks to interpret, critically analyse, and synthesize the prevailing legal framework. The doctrinal method enables a comprehensive understanding of the legal issues, identification of gaps, and assessment of the practical applicability of smart contracts within the existing

jurisprudence, thereby providing a robust foundation for evaluating their enforceability and potential regulatory adaptations.

"Smart Contracts"

A "smart contract" is a computer program that automatically enforces, executes, and records the terms of an agreement between parties without the need for intermediaries like lawyers, banks, or courts. It operates on a blockchain, making the contract transparent, secure, and tamper-proof. The contract is triggered when specific conditions are met.

"Traditional Contracts"

A "traditional contract" is a legally binding agreement between two or more parties. Traditional contracts are typically written in a natural language, such as English, and are enforced by the legal system. Traditional contracts are used in a wide variety of legal and financial transactions, such as sales agreements, employment contracts, and real estate transactions.

Difference between smart contracts and traditional contracts

There are number of factors which lays down the distinction between the two on the basis of legality, execution, validity, modification, record keeping, cost, security, transparency, traceability and accuracy.

Types of smart contracts

Smart contracts can be classified based on their purpose, level of automation, and interaction with external systems. There are five kinds of smart contracts:

- **Shrink wrap agreements:** In blockchain systems, shrink-wrap agreements can be implemented using smart contracts, where acceptance of terms is recorded digitally and enforced automatically. In this approach, the contract rules are written directly into computer code. A user shows their agreement by taking an action on the blockchain, such as clicking an "accept" button, approving the contract through a digital wallet, or starting a transaction. Once this action is taken, the smart contract automatically carries out and enforces the terms of the agreement.

- **Click wrap agreements:** A click-wrap agreement is a digital contract that requires users to actively agree to the rules and conditions before using a service or product. This usually happens when a user clicks an "I Agree" or similar button on a website or app. By clicking the button, the user is clearly saying that they understand and accept the terms. Only after giving this consent, they are allowed to access the service or continue using the product.

- **Browse wrap agreements:** In blockchain and smart contracts, a browse-wrap agreement works in a similar way. The contract terms are made available for users to see like on a webpage or through a link in the app and simply using the service can count as agreeing to those terms. The difference is that, on the blockchain, this acceptance can be automatically recorded and enforced without needing a middleman. Once this implied consent occurs, the smart contract automatically enforces the rules, such as granting access or transferring tokens, without requiring any manual intervention.

- **E-mails:** The concept of email as a smart contract combines traditional email communication with blockchain technology to automate and enforce actions. In this system, an email can include instructions or conditions that act like a smart contract. When the recipient interacts with the email, such as replying or clicking a link, the smart contract automatically executes the agreed action, like transferring payment or granting access. All interactions and outcomes are recorded on the blockchain, making the process transparent, secure, and tamper-proof.

- **Digitally executed agreements:** Digitally executed agreements are contracts that are created, signed, and enforced electronically. When implemented through smart contracts, the terms are encoded in code, and parties accept them through digital actions such as signing with a cryptographic wallet or interacting with the blockchain. Once the conditions are met, the smart contract automatically executes the obligations, like transferring funds or granting access, while recording all actions on the blockchain for transparency, security, and immutability. This reduces reliance on intermediaries, speeds up execution, and ensures a tamper-proof record, though legal recognition and coding errors remain potential challenges.

Feature/Nature of Smart Contracts

- **Transparent:** Transparency is one of the fundamental characteristics of smart contracts, ensuring that all parties involved have clear visibility into the contract terms, conditions, and execution processes. Unlike traditional contracts, where enforcement and compliance often rely on intermediaries or private monitoring, smart contracts operate on a blockchain, a decentralized and publicly accessible ledger. This means that once a contract is deployed, its code, rules, and transactions can be verified by all authorized participants, reducing information asymmetry and building trust between parties.

- **Automation:** Smart contracts execute terms automatically when predefined conditions are met, reducing the need for intermediaries. Unlike traditional contracts, which often require intermediaries such as lawyers, banks, or notaries to monitor performance and enforce compliance, smart contracts are **s**elf-executing, reducing human error and delays.

- **Decentralization:** Decentralization is a core characteristic of smart contracts, referring to the distribution of control and validation across a blockchain network rather than relying on a single centralized authority. In traditional contractual systems, a central entity such as a bank, government agency, or legal authority typically oversees enforcement, record-keeping, and dispute resolution.

- **Legal Recognition:** Legal recognition is a critical factor that determines whether smart contracts are enforceable under traditional contract law. While smart contracts are technologically sophisticated and self-executing, their acceptance in legal systems depends on whether they satisfy the fundamental principles of contract law, such as offer, acceptance, consideration, capacity, and intention to create legal relations. Unlike traditional contracts, which involve human signatures and tangible documentation, smart contracts rely on digital interactions and code-based execution, raising questions about whether parties' consent is adequately manifested and legally valid. Courts and regulatory authorities are still adapting to these innovations, and the enforceability of smart contracts may vary across jurisdictions depending on statutory provisions and judicial interpretation.

- **Security:** Security is a fundamental factor in the effective functioning and reliability of smart contracts. Since smart contracts operate on blockchain networks, they benefit from the inherent security features of blockchain technology, including cryptographic encryption, decentralized validation, and immutability, which make it extremely difficult for unauthorized parties to tamper with the contract or manipulate its execution.

Limitations of Smart Contracts

- **Coding Errors and Vulnerabilities** – Mistakes in the code can lead to unintended execution, financial loss, or exploitation.

- **Lack of Flexibility** – Once deployed on a blockchain, smart contracts are immutable and difficult to modify.

- **Interoperability Challenges** – Reliance on external data sources (oracles) or systems can create points of failure.

- **User Awareness and Consent** – Parties may not fully understand the terms or implications of execution.

- **Regulatory and Jurisdictional Issues** – Different laws across countries complicate cross-border enforceability.

Validity and Enforceability of Smart Contracts

Section 10, of the **Indian Contract Act, 1872** defines the essential elements of a valid contract, stating that all agreements are enforceable if they are made with the free consent of the parties, for a lawful consideration, and with a lawful object.

This provides the foundation for contract enforceability in India. The **Information Technology Act, 2000** further recognizes digital contracts as legally valid and enforceable, provided they carry a digital or electronic signature issued by a government-authorized certifying authority, ensuring authenticity and accountability. Smart contracts, however, challenge this traditional framework because they are decentralized, automated, and self-executing, operating without any human intermediary or government-controlled authentication. Their execution is driven

entirely by code on a blockchain, which ensures immutability and automation but bypasses the conventional requirement of certification under the IT Act. As a result, while smart contracts satisfy the principles of mutual consent, lawful consideration, and lawful object in a practical sense, their lack of formalized signatures and government oversight raises questions about legal enforceability under existing Indian law. This tension highlights the need for legal reforms or interpretative frameworks that can bridge the gap between traditional contract principles and emerging digital contractual technologies.

Conclusion

By combining the principles of contract law with blockchain technology, smart contracts automate obligations, reduce the need for intermediaries, and provide transparency, immutability, and efficiency. Their decentralized and self-executing nature ensures that transactions occur exactly as programmed, minimizing the risk of human error, fraud, or delays. Features such as automation, transparency, decentralization, security, and coding precision make smart contracts an innovative tool for facilitating digital transactions in a wide range of industries, including finance, supply chain, and intellectual property management. However, despite their technological sophistication, smart contracts face significant challenges in aligning with traditional contract law, particularly regarding legal recognition and enforceability.

In India, while the Contract Act, 1872, and the Information Technology Act, 2000, provide a framework for valid and enforceable digital agreements, smart contracts often operate without government-authorized digital signatures or centralized oversight. This raises legal ambiguities concerning consent, authentication, modification, dispute resolution, and compliance with statutory requirements.

The limitations of smart contracts, including coding errors, interoperability challenges, lack of flexibility, and jurisdictional complexities, underscore the need for careful design, rigorous auditing, and supportive regulatory frameworks. Legal systems must adapt to provide clarity on enforceability while maintaining the benefits of decentralization and automation. There is a pressing need for legal reforms or interpretative guidelines that bridge the gap between traditional contract law and emerging digital technologies, ensuring that parties can rely on smart contracts with confidence.

In conclusion, smart contracts are valid and effective technological instruments that have the potential to transform contract execution and enforcement. While they satisfy the practical principles of consent, consideration, and lawful object, their full legal enforceability depends on evolving statutory recognition and judicial acceptance.

By addressing legal ambiguities and implementing clear regulatory standards, smart contracts can complement traditional contract law, offering a secure, efficient, and reliable mechanism for the future of digital agreements. As the world increasingly moves toward digital transactions, integrating smart contracts within the legal framework will be critical to balancing innovation with legal certainty.

References

- https://www.nayalegal.com/contract-law-and-smart-contracts
- https://blog.ipleaders.in/smart-contracts-and-their-enforceability-in-india/
- https://dailyjus.com/legal-tech/2025/08/smart-contracts-global-perspectives-and-legal-realities-part-2
- https://www.rapidinnovation.io/post/the-legal-implications-of-smart-contracts-regulations-and-compliance
- https://www.lawjournals.org/assets/archives/2025/vol11issue7/11154.pdf