Challenges in the Implementation of Smart Contracts in the Legal Systems of Iran and India

1. Sara Houshmand: PhD Student, Department of Law, Shahr-e-Quds Branch, Islamic Azad University, Shahr-e-Quds, Iran
2. Pejman Piroozi*: Assistant Professor, Department of Private Law, , Shahr-e-Quds Branch, Islamic Azad University, Shahr-e-Quds, Iran
3. Hossein Monavari: Assistant Professor, Department of Public Law, Shahr-e-Quds Branch, Islamic Azad University, Shahr-e-Quds, Iran
4. Alireza Mazloum Rahani: Assistant Professor, Department of Private Law, Shahr-e-Quds Branch, Islamic Azad University, Shahr-e-Quds, Iran

*Correspondence: e-mail: Pezhman_pirouzy@yahoo.com

Abstract

The emergence of smart contracts and the increasing integration of artificial intelligence (AI) have introduced new dimensions to traditional contract law. These advancements have fundamentally transformed the nature of contractual relationships, raising questions about their legal validity, enforceability, and alignment with established legal doctrines. This research article aims to examine the profound impact of smart contracts and AI on the principles and foundations of contract law, particularly within the legal systems of Iran and India. Smart contracts, which operate through blockchain technology and automated execution mechanisms, challenge conventional notions of offer, acceptance, and consideration. The study explores the extent to which these contracts conform to existing legal frameworks and whether legislative adaptations are required to accommodate their unique characteristics. Additionally, the research investigates issues of liability, dispute resolution, and contractual interpretation in the context of AI-driven automation. Given the decentralized nature of blockchain and the self-executing nature of smart contracts, concerns regarding jurisdiction, regulatory oversight, and consumer protection have also emerged. This study employs a comparative legal analysis by examining relevant judicial precedents, academic literature, and statutory provisions from both Iran and India. The findings highlight the need for regulatory frameworks that balance innovation with legal certainty, ensuring that smart contracts function effectively while upholding fundamental legal principles. The article also provides insights into the broader implications of AI in contract law, discussing whether AI-generated contracts challenge traditional notions of contractual autonomy and intent. By addressing the advantages, challenges, and legal implications of smart contracts, this research contributes to the ongoing discourse on legal adaptation in the face of rapid technological change. The study emphasizes the importance of legal reform in facilitating the seamless integration of smart contracts within modern legal systems.

Keywords: Smart contracts, legal system of Iran, legal system of India, artificial intelligence, contract law

Received: 03 May 2024
Revised: 01 June 2024
Accepted: 10 June 2024
Published: 23 August 2024

Citation: Houshmand, S., Piroozi, P., Monavari, H., & Mazloum Rahani, A. (2024). Challenges in the Implementation of Smart Contracts in the Legal Systems of Iran and India. *Legal Studies in Digital Age*, 3(3), 143-158.

1. Introduction

Over time, technology has influenced every aspect of life. Despite the fact that financial institutions have been able to maintain profitable business models for decades, they now face significant challenges due to the emergence of innovative technologies that could disrupt their operations. Although the global circulation of cash has increased in recent years, this accounts for only a small portion of economic liquidity issues. For instance, in India, 45% of financial transactions are conducted in cash, whereas in the United States, this figure is merely 27%, and in Sweden, only 3% of total payments involve cash transactions (De Caria, 2019).

Enhancing the security of financial transactions, reducing the likelihood of bank theft, combating the trade of illicit drugs and arms, preventing currency counterfeiting, and addressing money laundering are among the key motivations behind the transition to alternative payment methods and the introduction of new forms of currency. These issues have arisen alongside societal advancements, creating dissatisfaction and necessitating innovative financial solutions. One of the most critical developments in the fintech industry is Bitcoin, along with its foundational concept, blockchain technology (Brooke, 2005).

Blockchain is built upon principles derived from cryptography, game theory, and peer-to-peer networking. It serves as a decentralized ledger of digital transactions shared among multiple parties. Once recorded, information cannot be erased and can only be updated with the consensus of the majority of system participants. Following the financial crisis of 2008, while banks were grappling with multiple challenges and unable to focus on innovation, the fintech industry began to expand. Today, fintech continues to thrive and is regarded as an efficient alternative to traditional financial services. Customers seek a system that preserves their interests while remaining transparent and reliable (Raskin, 2017).

In this context, cryptocurrencies and new applications of blockchain technology have emerged. The concept of "smart contracts," although previously introduced, found an optimal environment for development with the advent of blockchain. Recognizing its potential, numerous public and private industries, both small and large, are exploring legal mechanisms to integrate smart contracts into their operations. However, for this integration to materialize, the legal challenges governing smart contracts must be examined to address specific issues that accompany this new technology. The correct approach must be adopted to mitigate risks while simultaneously fostering innovation and ensuring the successful implementation of smart contracts (Channing Palmer, 2012).

Smart contracts exhibit several distinctions from traditional contracts. The primary difference lies in their self-executing nature, whereby pre-programmed code automatically executes contractual obligations when certain conditions are met or remain unfulfilled. In contrast, the enforcement of traditional contracts requires legal intervention. One of the most significant advantages of smart contracts is their self-executing and self-enforcing nature, based on the coded program. A smart contract built on blockchain is a legally binding agreement between two or more parties, stored and executed digitally using blockchain codes. For blockchain-based smart contracts, transactions can be programmed to require the parties' encrypted keys to proceed. This ensures the creation of a transaction record and verifies the parties' identities. Once users reach a consensus on the validity of a transaction, it is added as a new block to the existing blockchain. Hence, the system is referred to as a "blockchain."

This research aims to address a fundamental question: Can smart contracts be enforced in the same manner as traditional contracts? (Lincoln, 2004). The structure of a contract is a combination of legal principles and economic realities, encoded in a set of predefined rules. Contract law is flexible, allowing parties to include specific terms to define their agreements. Whether a contract is smart or traditional, if it meets the necessary legal elements, courts will uphold its enforceability. However, from the perspective of technology developers, smart contracts should operate outside traditional legal frameworks. Accepting this notion, however, could lead to numerous legal challenges (Levi & Lipton, 2018).

Contract law is one of the most dynamic areas of legal study, constantly evolving in response to technological advancements (Savelyev, 2016). Under Iranian law, a contract is defined as an agreement in which one or more persons commit to an obligation towards one or more other persons, and this obligation is accepted by the latter (Article 183 of the Iranian Civil Code). This definition closely resembles Article 1101 of the French Civil Code, which states that a contract is an agreement in

which one or more persons commit to delivering something, performing an act, or refraining from an act in favor of one or more other persons (Hayati, 2013).

This study explores the concept of smart contracts, their legal validity within the legal frameworks of Iran and India, and the challenges associated with their implementation. The objective is to propose a foundation for incorporating smart contracts as the most advanced form of electronic contracting in Iran's legal system.

The evolution of contract law in India has been marked by extensive and scattered changes. Before the establishment of a colonial empire, contractual principles were integrated into a codified legal framework known as the "Indian Contract Act of 1872." Since its enactment, this law has successfully guided contractual jurisprudence. Over the past century and a half, the Indian Contract Act has played a crucial role in protecting contractual rights. However, it has faced criticisms due to procedural complexities, third-party involvement, and resistance to anonymous amendments. The rapid advancement of technology necessitates legal adaptation to accommodate a new era of contract interpretation (Singh & Shilpa, 2021).

Despite the clarity surrounding the functionality and significance of smart contracts within blockchain technology, their legal status in India remains ambiguous. This uncertainty stems from concerns regarding the legitimacy of digital currencies and the presumed prohibition of unauthorized digital signatures, making blockchain applications a highly sensitive legal issue. The Indian government appears to be taking considerable time in establishing precise legal frameworks defining smart contracts, virtual currencies, and their associated legal aspects. Meanwhile, governmental bodies simultaneously endorse and adopt blockchain technology (Levi & Lipton, 2018).

The primary concern now is determining the legal stance on virtual currencies that may be essential for smart contract execution. This study aims to address these ambiguities as soon as possible. There is no doubt that the acceptance and development of smart contracts represent the next phase of progress, significantly reducing billions of dollars in additional costs and improving overall network efficiency. However, regulatory barriers remain, particularly in India, where legal provisions regarding the technical aspects of smart contracts are scarce. Unless specific legal measures are enacted, the widespread adoption of this technology will require amendments to the Indian Contract Act of 1872 and the Information Technology Act of 2000.

Although legal developments are underway, and the corporate sector is gradually embracing smart contracts, the legal framework remains in a gray area. A determined effort is necessary to establish a comprehensive regulatory network for overseeing smart contract operations in India. However, before expanding the scope of smart contracts, it is essential to consider the various legal challenges and complexities associated with artificial intelligence (AI). The implementation of smart contracts should be confined to specific domains where potential risks can be more easily assessed.

Moreover, using AI algorithms in contract formation raises legal questions concerning contractual intent and liability. In traditional contract law, the parties' intent to enter into an agreement is paramount. When AI generates contractual terms or offers recommendations, uncertainties arise as to whether AI-driven actions genuinely reflect the contractual intent of the parties. Ensuring that AI-generated contracts accurately represent the parties' intentions and comply with legal requirements remains a significant challenge (Kumar Sadual, 2018).

Additionally, the enforceability of smart contracts in Iran and India may require legal clarification. While Indian contract law recognizes electronically concluded contracts, the enforceability of smart contracts executed on blockchain platforms remains uncertain. Legal reforms and judicial interpretations may be necessary to establish their legal standing and ensure their enforceability under Indian law.

Smart contracts and AI-driven technologies have the potential to significantly impact contract formation in Iran and India by streamlining processes, enhancing efficiency, and introducing novel legal considerations. Although these advancements offer benefits in terms of automation and operational efficiency, their integration into contract law necessitates careful consideration to ensure alignment with existing legal principles and address emerging challenges.

The objective of this article is to contribute to the ongoing discourse on the impact of smart contracts and AI on traditional contract law. By examining their advantages, challenges, and legal implications, this study provides a comprehensive analysis that can assist policymakers, legal professionals, and researchers in navigating the evolving landscape of contract law in the digital age.

2. Concepts and Theoretical Foundations

2.1. Blockchain Technology and Smart Contracts

Simply put, blockchain is a type of database (a collection of data or information) that differs from conventional databases in its structuring and sequencing of data. Unlike other types of databases where information is organized in tabular form, in a blockchain, data is arranged in "blocks," each linked to the previous block, forming a "chain." Additionally, a timestamp is assigned to each block as soon as it is added to the existing chain.

Blockchain is recognized as a type of Distributed Ledger Technology (DLT), where a ledger—a digital database—is "distributed," meaning it is shared among a network of computers known as "nodes." These "nodes" are responsible for verifying any additions to the ledger through a "consensus mechanism," which is the process by which nodes agree on modifications to the ledger. This means that all network participants share a common understanding of any proposed change, ensuring no disputes arise among nodes regarding new additions. One of the key features of the consensus protocol is that it treats all members or nodes in a network as a collective group: even if one member fails, the remaining nodes continue to function. The consensus mechanism can be likened to the "meeting of wills" concept in traditional contract law.

It is important to note that no central authority governs blockchain, making it decentralized. In a conventional database environment, a single entity that owns a server with multiple computers containing all the relevant data has complete control over these units, all housed under one roof. However, in a blockchain environment, computers (or, more precisely, nodes) are dispersed across different locations and are controlled by separate individuals or groups of entities. Thus, blockchain is essentially a decentralized, distributed, and peer-to-peer database. This decentralized nature of blockchain enhances transparency. Each node has a copy of the block that is immediately added to the chain, making transaction visibility straightforward and, consequently, increasing transparency. Therefore, transparency is a key characteristic of blockchain technology, contributing to the "smartness" of smart contracts.

Every database primarily stores user information, but blockchain, due to its unique structuring of data, extends beyond merely recording transactions. This brings us to the concept of "smart contracts": a smart contract is created when a piece of code or software facilitates the automated execution of multilateral agreements. A smart contract consists of code that includes a constructor function, which is a segment of code used to create a smart contract, along with a storage file and an account balance. To initiate the code, a transaction is sent to the blockchain network. In this context, a "transaction" refers to the transfer of digital currency or a digital asset by a user (known as the sender) who wishes to create a contract and publish this information on a blockchain. Based on the received transaction, a smart contract can read from or write into its private storage, hold funds in its account balance, or send and receive messages or funds from users or other contracts. Upon transaction submission, the constructor function (a segment of the smart contract code) is executed, creating a smart contract. At this stage, all nodes or computers execute and verify the transaction based on a consensus mechanism.

In a blockchain, validation occurs internally within the network without requiring any external entity, as the verification mechanism is embedded within the smart contract code. Thus, "trust" is established within the blockchain-based smart contract ecosystem. A smart contract also contains state variables, which are stored on the blockchain and hold specific data and the sender's "wallet" address (i.e., the source of funds). To execute the code of a smart contract and subsequently encode it into a blockchain, the Ethereum blockchain utilizes "fuel" (referred to as "gas") available in the sender's wallet. The code does not execute indefinitely, as it must terminate when the wallet runs out of gas. It is the sender's responsibility to ensure that sufficient gas is available for code execution. Upon processing a transaction, a smart contract can return a value to the sender.

One of the fundamental characteristics of a smart contract is its immutability. This means that once a smart contract is deployed on a blockchain, no one can alter its code. The data remains permanently accessible in the blockchain ledger as long as the associated digital currency exists. For instance, every one of the approximately 640 million transactions executed on the Bitcoin blockchain since its launch in 2009 will remain recorded as long as Bitcoin exists (Singh & Shilpa, 2021). This feature contrasts with traditional paper-based contracts and electronic contracts, which can be modified at the discretion of the parties involved.

Another critical feature of blockchain is the requirement to solve a complex mathematical algorithm known as a cryptographic hash function, which makes blockchain-based smart contracts inherently "tamper-proof." A hash function is essentially an algorithm (i.e., a set of instructions for a computer program) that converts ordinary alphanumeric data input into an encrypted output. In hashing, a fixed-length output is generated through mathematical computations that are difficult to decrypt, thereby enhancing security. Each hash function is linked to a block, and each subsequent block header (used to identify the block) in the blockchain contains the hash function and timestamp of the preceding block. Consequently, if any data is tampered with, the resulting hash value will differ from the original, making any modifications immediately detectable. This advanced security feature is not characteristic of traditional contractual environments.

A simplified understanding of the above discussion is that a smart contract is essentially code. Therefore, a preliminary observation is that such contracts can only be used for straightforward tasks, such as ensuring fund transfers or enforcing financial penalties when certain conditions are met or unmet. Consequently, smart contracts are inherently "objective." Technically speaking, they follow an "if/then" logic, meaning the algorithm is designed so that if a specific event occurs, a corresponding action is executed—for example, "if X happens, then execute Y." Since this transaction occurs automatically without the need for an independent arbitrator or a trusted third-party intermediary, smart contracts are time- and cost-efficient.

3. Compatibility of Smart Contracts with the Principles and Laws Governing Contracts in Iran and India

3.1. The Iranian Legal System

3.1.1. Establishing the Contractual Nature of Smart Contracts

Contract law, as one of the most dynamic branches of legal science, is continually influenced by emerging technologies. In the Iranian legal system, a contract is defined as a commitment by one or more persons to one or more other persons to perform an act that has been mutually agreed upon.

As previously discussed, electronic contracts are essentially agreements formed through the mutual consent of two or more parties within a virtual environment. These contracts do not significantly differ in substance from traditional contracts, with the primary distinction being their conclusion through electronic means. Smart contracts, as a subset of electronic contracts, are concluded through the mutual offer and acceptance of parties within a blockchain framework. By fulfilling the general conditions of transactions, these contracts are recognized as valid and enforceable under the legal systems of both Iran and India.

Since parties entering into smart contracts must use digital signatures, individuals engaging in such contracts must meet all necessary legal requirements, including possessing legal capacity and having a sound intention to contract. If any of these requirements are lacking or compromised, the individual's authorization (i.e., the assigned private key) will be rendered invalid. Furthermore, for a contract to be considered legally valid after its conclusion, it must be free from defects such as mistake, fraud, coercion, or conflict with public norms. Since these defects arise from external factors affecting the contract, in smart contracts, as in traditional contracts, a claimant alleging contractual defects may seek recourse from competent legal authorities. Until a judicial ruling confirms the claimant’s assertions, the concluded contract will be presumed valid (Hayati, 2013).

In Iranian law, considering that under Article 183 of the Iranian Civil Code, a contract is defined as an agreement between two or more persons that is mutually accepted, smart contracts align with this definition. Therefore, as long as smart contracts meet the general conditions of transactions, they are regarded as legally binding contracts. To be considered valid and legally enforceable under the Iranian legal system, a contract must satisfy the essential requirements of transactions stipulated in Article 190 of the Iranian Civil Code. Smart contracts are not exempt from this rule, and their applicability within Iran's legal framework depends on their compliance with the fundamental elements of contract formation under Iranian law.

3.1.2. Establishing the Fundamental Elements of Contracts in Smart Contracts

In the Iranian legal system, and pursuant to Article 190 of the Civil Code, the validity of any contract depends on the presence of necessary elements and the absence of legal impediments. Essential elements include the existence of intent, mutual consent, the legal capacity of the parties, and the specification of the contract’s subject matter. Additionally, the absence of an unlawful

purpose is considered a primary condition for validating contracts. The absence of any of these elements or the presence of a specified impediment could present significant challenges for the enforceability of smart contracts within Iran's legal system.

Thus, the compatibility of smart contracts with the fundamental requirements of contract formation, and the demonstration of their conformity with these essential conditions, constitute critical areas of investigation in this study. With this introduction in mind, the following section examines the formalities and structure of smart contracts concerning the fundamental principles of contract formation in Iranian law (Mafi & Kavyar, 2013).

3.1.2.1 Establishing Legal Capacity

In the Iranian legal system, legal capacity is classified into two types: "capacity to enjoy rights" (Ahliyyat-e-Tamattu) and "capacity to exercise rights" (Ahliyyat-e-Istifa). Capacity to enjoy rights refers to the qualification that enables a person to possess private rights. Capacity to exercise rights, on the other hand, refers to an individual's entitlement to exercise civil rights (Katouzian, 2015).

The basis of capacity to enjoy rights is human existence; thus, under Article 956 of the Iranian Civil Code, natural persons acquire this capacity from the moment of birth. This capacity remains throughout life unless revoked due to factors such as a judicial ruling on apostasy, which results in the loss of this capacity and the individual being treated as deceased. In certain cases, legislators may deem individuals as lacking capacity to enjoy rights to protect particular interests (Shahidi, 2014).

The basis of capacity to exercise rights, as stipulated in Article 211 of the Iranian Civil Code, is intelligence, puberty, and maturity. Individuals lacking these attributes are legally considered incapacitated (Safaei, 2013; Safaei & Ghasemzadeh, 2015). One of the essential prerequisites for entering into a smart contract is the issuance of a digital signature for individuals. Digital signatures may be issued to all citizens of a country within the boundaries of its territorial laws. In developed countries, a key requirement for issuing a digital signature is identity verification and confirmation that the individual possesses the legal capacity to enter into contracts under the laws of the issuing country.

Under the Electronic Commerce Law of 2003, electronic signatures are categorized into two types: simple electronic signatures and secure electronic signatures. The latter, which closely resembles digital signatures, provides similar advantages but does not carry a government guarantee for transaction validity. Considering that, under Article 10(b) of the mentioned law, identity verification is a prerequisite for the establishment of a secure electronic signature under Iranian law, obtaining such a signature is also contingent on possessing both capacity to enjoy and capacity to exercise rights.

In developed countries, once an individual loses the capacity to enter into contracts, their authorization to use digital signatures is revoked. To regain authorization, they must undergo a re-evaluation of their eligibility. It can be anticipated that, under Iran's legal system, if an individual's capacity to enjoy or exercise rights is revoked, their authorization to use a digital signature will also be invalidated.

Given that smart contracts are concluded within a blockchain framework, should such an infrastructure be established within Iran's legal system, obtaining authorization to use secure electronic signatures would become a necessity. The use of digital signatures in contracting is subject to the requirement that the individual possesses the necessary legal capacity to enter into the specific contract. It is possible that an individual may have the capacity to enter into one type of contract but not another. In such cases, they would be prohibited from using a digital signature to conclude the latter transaction.

For instance, under Article 961 of the Iranian Civil Code, if a foreign national in Iran intends to enter into a contract using a digital signature, they must first obtain authorization from the competent authorities in Iran. The prohibition against certain transactions for foreign nationals under Article 961 stems from their lack of capacity to enjoy rights in such cases. For example, if a foreign individual in Iran attempts to acquire real estate classified as agricultural land, the finalization of the contract and transfer of ownership would not be legally permissible (Safaei, 2013).

In smart contracts, individuals are only authorized to transact properties and lands that they legally own or those recognized as owned by the state. Foreign nationals cannot transfer ownership of properties that they do not legally possess. A pertinent question arises: if an Iranian citizen intends to enter into a contract with a foreign national involving their privately owned agricultural land, how can the competent authorities identify and prevent the conclusion of such a contract? In conventional circumstances, contracts concluded in violation of these restrictions are deemed null and void.

To finalize smart contracts, compliance with legal requirements must be verified through artificial intelligence (AI). AI must obtain specific information, such as the example provided, by accessing relevant property records. If an individual is declared an apostate by judicial ruling, their transactions become void due to the loss of capacity to enjoy rights. To verify such cases, AI or any of the contracting parties may access relevant information through oracle systems. These systems can provide AI with data during transaction validation, preventing unauthorized transactions and ownership conflicts.

Another method for verifying individuals' legal capacity for entering into smart contracts is through the establishment of legal frameworks governing the ownership and use of digital currencies. With the adoption of the Uniform Law on Digital Currency Transactions in 2017, digital exchanges based on such currencies are governed by this law, provided that individuals meet the eligibility criteria set forth in Article 2.

A noteworthy aspect of this convention is the possibility of obtaining authorization to use digital currencies in a country other than the applicant's country of nationality (Article 3). This provision applies where reciprocal relations exist between the two countries. If at any stage of the authorization process an individual's legal capacity is revoked or becomes doubtful, the authorization will either be denied or invalidated. Although Iran has not yet acceded to this convention, the implementation of such mechanisms within its legal system would be contingent on accepting international legal standards governing smart contracts, including the aforementioned convention.

3.1.2.2 Establishing the Parties' Intent

The conditions and methods for determining a person's intent to enter into a contract under normal circumstances, as well as the validity of their intent in cases such as insanity, have been thoroughly discussed in the section on legal capacity. In other words, the verification of the parties' intent in smart contracts is conducted through a mechanism that has already been examined in the context of assessing their legal capacity. This is because compromised legal capacity itself can be a factor that affects the validity of the parties' intent, potentially leading to the nullity or unenforceability of the contract. In cases where individuals lack intent due to external material pressures, such as coercion, the contract can be annulled through legal action. However, except in cases where coercion is proven, this issue does not necessarily undermine the validity of smart contracts.

Regarding the alignment of the parties' intent, if each party intends to enter into different types of contracts, such a divergence in intent renders the conclusion of a contract impossible. In an electronic environment, negotiations between parties are based on an offer and an acceptance, which each party must explicitly express. In cases of misalignment, no contract will be signed or finalized, and such an incomplete agreement will not be validated by artificial intelligence. However, an important question arises: Do smart contracts encompass what are known as Follow-on Contracts?

Follow-on Contracts refer to contracts in which, after their initial conclusion, circumstances change in such a way that the original agreement compels the parties to enter into a secondary contract. This may occur when an action taken by one party necessitates the other party to enter into another agreement. For example, if a contract for the development of an advanced weapon system is awarded to a defense contractor with the objective of securing military superiority for a country, the contract may stipulate that payments will be made in exchange for each phase of progress. If the contractor unilaterally introduces additional features that enhance the weapon's quality, given the parties' shared goal of achieving military superiority, this would effectively constitute a secondary contract, obligating the government to cover the costs of the enhanced weapon.

A similar scenario can arise in technology transfer agreements. For instance, a country on the verge of war may enter into a technology transfer agreement with another country to acquire nuclear weapons technology for defense. If the contracting party subsequently offers superior technology, such as hydrogen weapons, this would serve as a strategic advantage in warfare. In such a case, the agreement would extend to a secondary contract. Similarly, if a contract is signed for the development of liquid-fuel weapons but the contractor manufactures solid-fuel weapons instead, a comparable legal issue would arise.

The central question here is whether smart contracts can accommodate such contracts. Can the intent established in the primary contract be extended to a secondary contract?

In the Roman-Germanic legal system, these matters must be analyzed within the framework of established legal principles and regulations. If no explicit statutory provisions address such cases, procedural principles, such as the principle of non-existence (i.e., the presumption that legal obligations do not exist unless explicitly recognized), will prevail, rendering such cases legally void.

3.1.2.3 Legitimacy of the Contractual Purpose

The illegitimacy of a contractual purpose is one of the primary obstacles to validating a contract. In the Iranian legal system, a valid and legally binding contract is one in which the parties have a legitimate purpose for entering into the agreement. In some Western legal systems, such as France, the requirement for a legitimate contractual purpose has been abolished. In these jurisdictions, legislators, based on the principle of ownership rights, respect the owner's discretion regarding the use of their property without imposing inquiries into their intent.

However, Article 217 of the Iranian Civil Code explicitly states that if the purpose of a contract is unlawful, the contract is void. In practice, it is rare for a contracting party to explicitly declare an illegal intent within a contract. Consequently, legal scholars argue that mere awareness of one party's unlawful intent by the other party is sufficient grounds for invalidating the contract. Some jurists even suggest that an inference of illegal intent from the surrounding circumstances may be enough to annul an agreement.

Given the challenges associated with proving unlawful intent and the legal difficulties that courts and contracting parties face in this regard, reforming Iranian contract law may be necessary. Determining whether a contractual purpose was known to the parties is inherently difficult. Additionally, considering the electronic nature of transactions, verifying the legitimacy of a contractual purpose in smart contracts appears even more challenging.

To address this issue, Article 217 could be reinterpreted in light of the specific nature of both traditional and electronic contracts, limiting its applicability to traditional contracts only. Alternatively, under the view that a contract remains valid until a judicial decision declares it void, this requirement could still be upheld in Iranian law. However, to prevent uncertainties that could undermine the validity of smart contracts, it would be appropriate to restrict the applicability of Article 217 to only those conditions explicitly stipulated within the smart contract itself.

In the American legal system, the legitimacy of a contractual purpose is interpreted based on the explicit objectives of the parties. The scope of this requirement is limited to express contractual objectives, avoiding an examination of the parties' internal motives or intentions when determining the contract's validity.

3.2. The Indian Legal System

A review of Indian law reveals that there is no separate legislation governing electronic contracts in the country. Fundamentally, electronic contracts are agreements executed through electronic means, such as computers (Raskin, 2017). With the advancement of the internet, businesses across the world have become interconnected, e-commerce has expanded, and companies frequently present contract terms on their websites, allowing customers to enter into agreements with a single click (De Caria, 2019).

In India, the Information Technology Act of 2000 provides legal recognition for transactions conducted via electronic means. However, the enactment of this law has not altered traditional contract law. Instead, it contains provisions that facilitate electronic contracts (Almajid, 2010; Bidgoli, 2002). It is important to emphasize that while technology has posed challenges to contract law, India's existing legal framework has remained fundamentally unchanged. The effectiveness of this approach is a separate issue for analysis, but the traditional legal framework has not been rendered obsolete.

Since Indian contract law has already been exposed to electronic contract technology, it is reasonable to further investigate whether the existing legal framework can accommodate blockchain technology, which underpins smart contracts. Although electronic contracts have been legally recognized, a separate analysis of smart contracts remains necessary.

Section 10-A of the Information Technology Act of 2000 discusses the validity of contracts concluded through electronic means, stating that if the formation of a contract—including the communication of offers, acceptance, withdrawal of offers, or revocations—occurs electronically or through an electronic record, the contract shall not be deemed unenforceable merely because an electronic medium was used (emphasis added).

This provision could be extended to blockchain-based smart contracts. Under Section 2(1)(t) of the Information Technology Act of 2000, an "electronic record" is defined as any data or data record in electronic form. Consequently, a "block" on a blockchain may be legally considered an electronic record under this definition. However, to eliminate future uncertainties, the Indian legal system could benefit from explicit statutory provisions addressing blockchain-based smart contracts.

A similar legal amendment was made in the Arizona Statutes (United States), which explicitly states that no law shall prohibit the enforceability of a smart contract (Mafi & Kavyar, 2013). Given India's focus on blockchain technology and its applications, it would be desirable for future legislative amendments to explicitly recognize smart contracts (Kumar Sadual, 2018).

Thus, necessary legal modifications could be made to existing legislation without the need for an entirely separate statute dedicated to smart contracts.

3.2.1. Conditions for Contract Formation

This is because there is no fundamental difference between the essential functioning of a traditional contract and an electronic contract. The only difference lies in the method of contract formation. Electronic contracts emerge as a mode of contract execution in the traditional sense rather than forming a distinct legal category, such as sales contracts or agency contracts. Therefore, no special legal requirements exist for the conclusion of an electronic contract.

3.2.1.1 Agreement

According to Section 2(h) of the Indian Contract Act, 1872, a contract is an agreement that is enforceable by law. An agreement is formed when one party makes an "offer" or "proposal", and the other party "accepts" the offer (Singh & Shilpa, 2021). However, not every agreement qualifies as a contract because not all agreements require legal enforcement (De Caria, 2019).

Section 10 of the Indian Contract Act, 1872, elaborates on agreements that can form contracts. It states that an agreement constitutes a legally binding contract if it is made with the "free consent" of parties competent to contract and if it is executed for lawful consideration and a lawful object. To determine whether a smart contract qualifies as a contract under this law, it must be analyzed within the scope of Section 10, which outlines the fundamental criteria for contract formation.

When considering smart contracts, agreements contained within them do not follow a formalistic approach. As previously discussed, no comprehensive legal framework currently governs smart contracts, and thus, a preliminary assessment of smart contracts does not immediately present a structured legal image. However, there have been cases involving traditional contracts where the formal validity of agreements has been examined.

For instance, in the case of Shankarlal Narayandas Mundade v. The New Mofussil Co. Ltd. (AIR 1946), it was ruled that unless it can be inferred from the facts that the parties intended to be bound only upon the execution of a formal agreement, the enforceability of the agreement would not be affected by its lack of formality. The importance courts place on the circumstances of each case is relevant to this discussion.

For example, consider a smart contract deployed on an Ethereum-based permissionless DLT (Distributed Ledger Technology) system. On Ethereum, anyone can lend or borrow money without relying on formal financial services, such as a bank (Singh & Shilpa, 2021). In this scenario, the enforceability of a smart contract is determined as a matter of fact under contract law.

3.2.1.2 Offer and Acceptance

As discussed earlier, an offer, when accepted, forms an agreement. To classify blockchain-based smart contracts as agreements, it is necessary to determine what constitutes an "offer" and an "acceptance" in this context.

The first stage in contract formation is the offer. The Indian Contract Act, 1872, uses the term "proposal" for an offer and defines it in Section 2(a) as follows:

"When one person signifies to another his willingness to do or abstain from doing anything, with a view to obtaining the assent of that other person to such act or abstinence, he is said to make a proposal."

Section 2(b) further states that when the person to whom the proposal is made signifies their assent, the proposal is said to be accepted. Once accepted, an offer becomes a promise.

Under Section 2(c), the party making the offer is referred to as the "promisor", while the party accepting the offer is called the "promisee". An offer can be express, meaning it is conveyed through words or written statements, or implied, meaning it is inferred from the conduct of the parties (Almajid, 2010).

The initial stage of an agreement in smart contracts does not significantly differ from traditional contracts because, before any contract takes effect, both parties must agree on a set of contractual terms (Raskin, 2017).

An example of a smart contract illustrating offer and acceptance can be found in crowdfunding smart contracts (Savelyev, 2016). Crowdfunding involves raising capital by pooling funds from multiple small investors for a business venture (Siemer, 2008).

In a crowdfunding smart contract, the "offer" is formed when the beneficiary (business entity), i.e., the promisor, predefines the contract terms within the code. Technically, this is done by the node associated with the business entity. When contributors willing to fund the project transfer their assets, this action constitutes "acceptance". The transfer of assets represents the behavioral act that signifies acceptance (Savelyev, 2016).

Additionally, essential requirements for a valid offer under Indian law, as discussed by the Supreme Court of India in Trimex International Fze Limited, Dubai v. Vedanta Aluminum Ltd [(2010) 3 SCC 1], are applicable to smart contracts as well. These conditions can be explained as follows in the context of smart contracts:

1. Multiplicity of persons – A smart contract involves parties, or at a minimum, computer nodes, where one acts as the offeror and the other as the offeree.
2. Communication of the offer to the offeree – Smart contracts are deployed on the Ethereum network, making them available for offerees to accept.
3. Subject matter of the offer – Smart contracts specify the subject of the agreement and its execution criteria.
4. Definiteness and clarity of the offer's terms – Smart contracts operate strictly according to their coded parameters, ensuring clarity and definiteness.
5. Conditional nature of the offer – The offeree must accept the entire smart contract as encoded without modifying its conditions, provided that the contract terms are specific and unambiguous.

In an Ethereum-based smart contract, the offeror deploys the contract on the Ethereum blockchain, which functions as an offer. If a participant on the blockchain (the offeree) interacts with the contract by submitting a transaction and executing the contract code, this constitutes acceptance (Kumar Sadual, 2018)

However, due to its resemblance to an advertisement, a smart contract could be classified as an invitation to treat rather than a direct offer. For example, when an auctioneer advertises an item for sale, this is not an offer but merely an invitation to treat. However, this distinction does not apply to smart contracts, as the offeror explicitly deploys the smart contract on a blockchain in binary code, defining the terms of the transaction.

The contractual conditions, embedded in the smart contract code, function as the contractual terms. The offeree must accept these terms as they are to execute the smart contract. Upon acceptance, the offeree submits a transaction, which is subsequently verified by all nodes in the blockchain network.

In contrast, in a traditional contract, the contract terms do not appear in an invitation to treat. For example, consider a bookseller who sends a price list to a group of customers. This list does not constitute an offer but merely an invitation to treat, as the books may not necessarily be sold at the listed prices. The contract terms only materialize once a customer makes an offer, and the bookseller accepts it.

Once a smart contract is deployed, the offeree can accept it in two ways:

1. By signing with a cryptographic private key.
2. In specific cases, by initiating or executing the contract itself.

At present, smart contracts predominantly resemble unilateral contracts, meaning they involve a promise that X will be transferred when Y occurs.

Commonly, digital asset transfers, such as cryptocurrency transactions or digital representations of offline assets, serve as examples of performance-based acceptance (Atzei, Bartoletti, & Cimoli, 2017, p. 49). However, this does not pose a challenge in determining the formation of a smart contract.

Thus, the deployment of a smart contract on the Ethereum blockchain and the execution of the contract using a cryptographic private key should satisfy the offer and acceptance criteria under Indian contract law, making the smart contract legally enforceable.

3.2.1.3 Legal Capacity of the Parties

One of the essential requirements for a valid contract under Section 10 of the Indian Contract Act, 1872, is that the parties must be "competent" to contract. According to Section 11 of the Act, a competent person is one who has attained the age of majority, is of sound mind, and is not disqualified from contracting by any law.

In India, minors cannot enter into contracts, although they may be beneficiaries or promisees, as the law "does not prevent a minor from binding the other party to an agreement" (Singh & Shilpa, 2021). Furthermore, in Mohori Bibee v. Dharmodas Ghose [(1903) 30 Cal 539], the Indian courts ruled that any agreement entered into by or with a minor is void ab initio. This means that an agreement entered into by a minor cannot be validated even after the minor attains the age of majority.

When linking competence to smart contracts, it is important to note that the code of a smart contract cannot determine the legal competence of a contracting party (Kumar Sadual, 2018). A minor, an intoxicated person, or an individual legally disqualified from contracting can still create an account on a blockchain. For instance, Ethereum is an open-source and freely accessible platform that can be used by anyone, regardless of their legal status (Bidgoli, 2002). Therefore, any smart contract deployed or accepted by an incompetent party would be deemed void ab initio under Indian law.

However, the absolute void nature of contracts involving minors may not always be ideal (Swaminathan & Surana, 2018, p. 4). The scope of contracts entered into by minors is expanding, as they are increasingly engaging in technologically driven transactions. Minors enter into various contracts, such as when they open an email account, access a social media platform, or use applications for educational purposes. Declaring all contracts involving minors void ab initio may unfairly deprive them of access to lawful goods and services. It is not far-fetched to imagine a scenario where minors may legally engage in smart contracts for specific purposes. The current legal approach in Indian courts may create challenges, as blockchain platforms lack the ability to verify the legal capacity of users.

One possible solution to legally attribute competence to a person accessing a blockchain is by referring to Section 11 of the Information Technology (IT) Act, 2000. This section states that an electronic record can be attributed to an originator (defined under Section 2(1)(za) of the IT Act) when the record is sent by a system programmed for automatic operation by or on behalf of the originator.

In smart contracts, the "minds" are the nodes. According to Section 11 of the IT Act, a transaction can be attributed to the originator, and in a smart contract, the originator can be identified if the blockchain has a "digital identity" that is uniquely linked to an individual (Pandy, 2020). Thus, "minds" can be identified within a smart contract ecosystem.

Typically, when a person without legal competence enters into an agreement, the other party may seek restitution for unjust enrichment or, if possible, reverse the transaction (Siemer, 2008). However, in smart contracts, reversing a transaction on a blockchain is extremely complex and costly, as transactions are recorded permanently in a block, making them part of the immutable blockchain ledger. In practical terms, funds (usually cryptocurrency) may only be retrievable if the sender knows the recipient, allowing for a manual return of assets. This is only possible if the smart contract's purpose is the transfer of funds.

Blockchain users are identified through their addresses, which consist of a sequence of numbers, making it difficult to initiate legal proceedings to cancel a transaction.

3.2.1.4 Consideration in Smart Contracts

Consideration is one of the essential elements of a valid contract under Section 10 of the Indian Contract Act, 1872. Therefore, a smart contract must involve consideration, or it would be void.

According to Section 2(d) of the Act, consideration is defined as:

"When, at the desire of the promisor, the promisee or any other person has done or abstained from doing, or does or abstains from doing, or promises to do or to abstain from doing something, such act or abstinence or promise is called a consideration for the promise."

In most smart contracts, consideration involves the exchange of digital assets, such as virtual currencies or an underlying value for a digital asset.

Some scholars argue that smart contracts lack legal consideration because there is no exchange of promises (Siemer, 2008). However, this argument overlooks the fact that computer nodes simply execute the pre-agreed terms between the parties before the smart contract code is deployed. This exchange of promises may or may not involve digital asset transfers or cryptocurrency as consideration. Consideration does not necessarily need to have monetary value and can be exchanged outside the smart contract code ecosystem.

On the other hand, some scholars affirm that smart contracts are unilateral contracts. For example, a smart contract for an insurance policy that automatically disburses payments when specific conditions are met operates as a unilateral contract (Almajid, 2010). In certain cases, the execution of a smart contract itself serves as sufficient consideration in both conceptual and practical terms.

Smart contracts can also be bilateral. Consider the example of a rental agreement: A smart contract can be programmed to keep a house locked unless the tenant makes the required payment (Kumar Sadual, 2018). In this case, consideration exists.

The legality of consideration is a crucial criterion for the validity of a contract under the Indian Contract Act, 1872. Section 23 states that consideration or an object is unlawful if:

1. It is prohibited by law.
2. It is of such a nature that, if permitted, it would violate legal provisions.
3. It is fraudulent.
4. It involves or implies harm to a person or property.
5. It is deemed immoral or against public policy by the court.

As mentioned earlier, consideration for a smart contract may involve virtual currency. However, this raises the question of the legality of cryptocurrency as consideration.

Since the rise of digital currencies in India, they have faced regulatory scrutiny from the Reserve Bank of India (RBI), which oversees banking services in the country (Wang, 2014). The Financial Action Task Force (FATF), an intergovernmental organization established by the G7 to combat money laundering, issued a report on risk-based approaches for internet-based payment services, though it did not specifically mention virtual currencies. A subsequent 2015 FATF report highlighted the risks associated with virtual currencies, particularly their potential use for terrorist financing and money laundering (Levi & Lipton, 2018).

In 2018, the RBI issued a circular that, while not explicitly banning cryptocurrencies, restricted all RBI-regulated entities from engaging in cryptocurrency-related transactions. This limited crypto-to-fiat conversions and disrupted businesses dealing in cryptocurrencies in India.

However, in Internet and Mobile Association of India v. Reserve Bank of India [(2020) SCC Online SC 275], the Supreme Court of India ruled that the RBI's ban was disproportionate, stating that alternative regulatory measures could have been adopted. Since this ruling, the Indian government has allowed cryptocurrency exchanges but has not recognized cryptocurrency as legal tender.

Thus, smart contracts do not suffer from illegality under Section 24 of the Indian Contract Act, 1872. However, due to concerns regarding money laundering and terrorist financing, the Indian government remains cautious about fully embracing digital currencies, while actively exploring blockchain technology for other applications (Singh & Shilpa, 2021).

3.2.1.5 Self-Executing Capability

Self-execution is one of the key features of a smart contract. This means that contractual obligations are embedded within the code itself. As a result, the contracting parties do not need to "trust" each other, since the contractual promises are encoded. The code executes automatically whenever the parties submit a transaction to the blockchain. Each transaction is stored on the blockchain, which, in turn, triggers the execution of the code. Therefore, once initiated, terminating the transaction is difficult. A notable aspect of this process is that it ensures the parties that their obligations will be fulfilled (Levi & Lipton, 2018). Furthermore, no regulatory mechanism is required to verify whether obligations have been performed.

The logic behind this concept is that smart contracts operate based on an "if/then" rule embedded in the code (Levi & Lipton, 2018). That is, if event X occurs, then Y will follow. The only input required for execution is a trigger, and the execution can occur without any external supervision. Monitoring compliance with obligations is a challenging aspect of traditional contracts.

At the core of contract enforcement lies the concept of obligation. An obligation can be understood as having elements of both rights and duties, or more accurately, the entire relationship between them. It creates a legal bond between two entities, whereby a specific act must be performed in the future (Savelyev, 2016). In the case of smart contracts, determining whether this legal element of obligation exists is complex. Just as parties to a traditional contract have duties toward their contractual obligations, can the same sense of duty be expected from participants in a smart contract? Does the notion of obligation, from a smart contract perspective, completely lack a legal foundation? There is no clear affirmative or negative answer to these questions.

The Indian Contract Act, 1872, refers to contracts that must be performed. Section 37 of the Act, which explains the obligations of the parties, requires contracting parties to either fulfill their respective promises or offer to do so, unless such promises are excused by law or any other provision. In smart contracts, obligations are pre-coded. It is a well-established fact in contract law that even when such contracts are formed through a vending machine, there must still be mutual consent or a "meeting of the minds" (Raskin, 2017). For a contract written purely in programming language, it is difficult to determine the nature of obligation and whether an enforceable performance is expected.

Earlier in this article, the mechanism of consensus was discussed. While it can be used to establish agreement among different nodes, understanding the nature of obligation in this context remains complex.

The element of discretion, which is commonly seen in traditional contracts, does not explicitly exist in smart contracts. For example, the Indian Contract Act, 1872, provides scenarios where contract enforcement may not be required.

According to Section 62 of the Act, if the parties agree to substitute a new contract, cancel, or modify the original contract, enforcement is no longer necessary. This law allows the creation of an entirely new contract by completely nullifying the original agreement.

Such a scenario is unlikely in the domain of smart contracts. The emerging structure of a smart contract, akin to a vending machine, once had some level of discretion—for example, the owner of the vending machine could intervene and stop its operation (Savelyev, 2016). However, in a blockchain-based smart contract, even turning off the computer does not affect the outcome of the contract (Savelyev, 2016).

This is because, once a transaction is submitted to the blockchain, no modifications can be made, and the code will execute autonomously, with verification occurring across all nodes (Werbach & Cornell, 2017, p. 340). Thus, canceling or substituting a smart contract is not a straightforward possibility.

Modifying traditional contracts is a relatively simple process. In smart contracts, however, making modifications is challenging, but can be introduced through oracles (De Caria, 2019).

An oracle is an external entity that sends signals to the smart contract and comes into play when the smart contract needs access to external resources outside its blockchain environment. An oracle can be a digital event, a human-based input, or even an artificial intelligence algorithm (Levi & Lipton, 2018). A human-based oracle can assist in the "subjective evaluation" of real-world events, providing human insight into contract execution (Cardozo Blockchain Project, 2018).

Oracle intervention enables smart contracts to be dynamic and responsive to real-time changes. For example, an oracle can inform a smart contract of any delays that might impact contract performance.

4. Breach and Non-Performance in Smart Contracts

In traditional contract law, non-performance can be attributed to a breach of contract.

Under Indian contract law, breach of contract occurs when the party responsible for performance refuses to execute the contract, finds performance impossible, or when the contract is terminated (Raskin, 2017).

In State of Karnataka v. Shree Rameshwara Rice Mills (AIR 1987 SC 1359), the court ruled that a declaration of breach must be made by an independent entity, not by the aggrieved party itself. However, it remains to be analyzed whether a smart contract can be breached for similar reasons.

Indian contract law also anticipates situations where contract performance may become impossible, thus excusing the promisor from fulfilling the contract. This means that while performance was possible and lawful at the time of contract formation, a subsequent event beyond the parties' control rendered it impossible. Such contracts become void under Section 56 of the Indian Contract Act, 1872, known as the "Doctrine of Frustration."

In Boothalinga Agencies v. V.T.C. Poriaswami Nadar [AIR 1969 SC 110: 1969 (1) S.C.R. 65], the court stated that this provision constitutes a positive rule of law, meaning that courts cannot deviate from its literal interpretation. Frustration automatically discharges a contract and cannot be determined based on the parties' intentions.

For smart contracts, one possible frustrating event could be a technical failure due to hacking (Savelyev, 2017). Technical failures or hacks are not foreseeable by the parties.

Considering Section 56, non-delivery can be classified as a subsequent impossibility caused by external factors, thereby frustrating the smart contract.

In theory, a programmer could incorporate various contingencies that may prevent the execution of a smart contract. This is similar to the "force majeure" clause in traditional contracts, which suspends contract performance in unforeseen future events. However, programming frustration into a smart contract is highly complex, as predicting future impossibilities is inherently difficult.

Determining which party should be excused from performance or held responsible for non-performance is a complex task in smart contracts, especially due to their self-executing nature. Moreover, the identities of the parties may be concealed or only partially determinable (Singh & Shilpa, 2021), further complicating the matter.

However, the previously discussed concepts of "digital identity" and "originator" (as per Section 11 of the Information Technology Act, 2000) may be applicable here. Once the identity is established, liability and damages can be determined.

Coding liquidated damages into smart contracts is feasible, as pre-estimated damages can be established in advance. For smart contracts that may face frustration, a remedial clause can be encoded in accordance with Section 65 of the Indian Contract Act, 1872, which governs the obligations of a party who has received benefits under a void contract.

5. Conclusion

This article has examined the transition in the nature of contracts, from traditional paper-based contracts to electronic contracts, and ultimately to smart contracts on the blockchain. At each stage of this transition, we observed how existing legal frameworks could be adapted to accommodate technological advancements. However, the challenges posed by the nature of smart contracts have made this transition far from seamless. Enforcing a smart contract under traditional contract law has not been an easy task for legislators worldwide (Siemer, 2008), and the burden of legal enforcement of smart contracts should not fall solely on courts.

The analysis of the legal systems of Iran and India in dealing with electronic contracts demonstrates that existing contract law regulations are applicable, provided a new perspective is adopted. In the context of smart contracts, the question arises whether a completely new law is required or whether existing laws should be amended to accommodate emerging technology. The above discussion aimed to demonstrate that smart contracts can form legally valid agreements within the adaptable legal frameworks of Iran and India. However, as a more effective approach, new regulations specific to smart contracts could be incorporated into existing laws. This could help prevent confusion regarding the enforceability of smart contracts. The draft bill on digital currencies could mark the first step toward the legal recognition of smart contracts in India, simplifying the application of regulations under the Indian Contract Act, 1872, and the Information Technology Act, 2000.

The findings of this study reveal that contract formation is a voluntary and cognitive act, but the contract itself is a legal concept that materializes through legislation. More precisely, it is the legislative authority that determines whether a voluntary action with certain characteristics leads to a contractual consequence and whether it is legally recognized. Now, if the same cognitive processes that occur in humans can be artificially replicated in an intelligent system, there is no reason why the legislature should not attribute legal effects to this artificial voluntary action. These systems, with their capabilities, can identify the essence of a contract, its details, and its reciprocal obligations, collect the necessary data to form a contract, and conduct evaluations to eliminate uncertainty and fraud in transactions. Therefore, it can be argued that contract formation is not

exclusively a human function, and artificial intelligence can perform similar functions in contract execution. However, it is important to acknowledge that AI will never achieve complete equivalence with human cognitive abilities.

In addition to possessing the capability of contractual intent, contracting parties must have legal capacity, including both capacity to have rights and capacity to exercise rights. This study has demonstrated the ability of intelligent systems to recognize the fundamental criteria for the exercise of legal rights. The notion of intelligence and maturity in such systems is conceivable given their capabilities, although they lack legal standing to determine the age of majority. However, this requirement is not necessarily relevant. The capacity to exercise rights is closely tied to the capacity to have rights and to legal personality. This study also examined the viability of recognizing legal identity for smart contracts, concluding that while these systems have strong theoretical foundations for legal recognition, their characteristics do not align with conventional legal entities. If current legal structures remain unchanged, granting legal identity to these systems—despite alternative solutions—could result in legal uncertainty.

Smart contracts are not the final stage in the evolution of contracts. In the future, more advanced versions of smart contracts may emerge, driven by continuously evolving technology. Thus, placing excessive emphasis on the self-executing nature of smart contracts may undermine the role of the legal system, leading to undesirable consequences. This is not a desirable outcome, as laws encompass a broader perspective on justice compared to market-driven approaches. If all contractual matters were entrusted solely to technology, this could create a loophole for legally unenforceable agreements, such as contracts that violate public order. Based on this analysis, revising the Indian Contract Act, 1872, to accommodate smart contracts appears to be a logical step for future scenarios. However, explicit amendments to the Information Technology Act, 2000, would be desirable to strengthen the legal standing of smart contracts.

Based on the findings of this research, the following recommendations are proposed:

a. Legal Validity and Formal Requirements:: Smart contracts challenge the traditional legal requirements for contract formation, which typically involve written agreements and signatures. The Indian Contract Act, 1872, recognizes contracts formed through electronic communication. However, greater clarity is needed to determine the legal validity and enforceability of smart contracts that rely solely on code and lack traditional contractual elements.

b. Data Protection and Privacy:: Smart contracts and AI systems used in contract law often involve the processing and storage of sensitive personal information. Compliance with data protection and privacy regulations, such as the Personal Data Protection Bill, 2019, is essential to safeguard individual rights and prevent unauthorized access or misuse of personal data.

c. Liability and Accountability:: The use of AI in contract law raises questions about liability and accountability for decisions or errors generated by AI. When AI determines contractual terms, makes recommendations, or acts autonomously, legal clarity is needed to establish who bears responsibility. Developing guidelines or legal frameworks for allocating liability between AI systems, developers, and users is crucial.

d. Intellectual Property Considerations:: AI algorithms used in contract analysis and drafting may rely on copyrighted materials, including legal databases or case precedents. Striking a balance between intellectual property rights for data providers, developers, and users is critical to ensure fair use and prevent potential infringement issues.

e. Ethical Considerations:: The deployment of AI systems in contract law must adhere to ethical principles, including fairness, transparency, and non-discrimination. Biases in AI algorithms could perpetuate existing inequalities or discriminatory practices in contract formation, negotiation, or enforcement. Ensuring fairness and accountability in AI systems, while addressing ethical considerations, is essential.

f. Jurisdictional Challenges:: The decentralized nature of blockchain technology, which is frequently used in smart contracts, poses jurisdictional challenges in cross-border transactions. Determining applicable law and jurisdiction in case of disputes requires international cooperation and clear legal frameworks for dispute resolution.

g. Regulatory Compliance:: The dynamic nature of smart contracts and AI necessitates adaptive regulatory compliance to keep pace with technological advancements. Regulatory bodies must understand the capabilities and limitations of these technologies to develop appropriate frameworks, guidelines, and standards that promote innovation while safeguarding legal and consumer interests.

Addressing these regulatory and legal challenges requires collaboration among legal experts, technologists, policymakers, and industry stakeholders. A comprehensive review of existing legal frameworks is necessary to determine whether new laws or amendments are required to effectively integrate smart contracts and AI technologies into India's legal landscape.

Ethical Considerations

All procedures performed in this study were under the ethical standards.

Acknowledgments

Authors thank all participants who participate in this study.

Conflict of Interest

The authors report no conflict of interest.

Funding/Financial Support

According to the authors, this article has no financial support.

References

Almajid, W. M. (2010). *The Legal Enforceability of Contracts made by Electronic Agents under Islamic Law: A Critical Analysis of the Effectiveness of Legal Reform in Saudi Arabia* PhD, University of Central Lancashire].

Bidgoli, H. (2002). *Electronic commerce, principles and practice*. Academic Press, California. https://doi.org/https://doi.org/10.1016/B978-012095977-8.50004-5

Brooke, A. (2005). Reconsidering The Proper Law of The Contract. *Melbourne Journal of Californians McGeorge Law Review*, *36*.

Channing Palmer, B. (2012). Disparate Impact of Electronic Signature Legislation on Indigent. *International Law*, *13*.

De Caria, R. (2019). The Legal Meaning of Smart Contracts. *European Review of Private Law*, *6*. https://doi.org/https://doi.org/10.54648/ERPL2018052

Hayati, A. (2013). *General rules of contracts*. Tehran: Mizan Publishing.

Katouzian, N. (2015). *Preliminary course of civil law: Legal acts, contracts, and unilateral acts*. Tehran: Publication Company.

Kumar Sadual, M. (2018). Status of Smart Contract in India: Legal challenges and future trends. *Research Review International Journal of Multidisciplinary*, *3*, 1-6.

Levi, S., & Lipton, A. (2018). An Introduction to Smart Contracts and their Inherent Limitations. *The Harvard Law School Forum on Corporate Governance*.

Lincoln, A. (2004). Electronic Signature Laws and the Need for Uniformity in the Global Market. *The Journal of Small & Emerging Business Law*(67).

Mafi, H., & Kavyar, H. (2013). A comparative study of the governing law on electronic contracts concluded in the internet environment from the perspective of legal systems: USA, European Union, Iran. *Journal of Private Law Studies*, *4*(1).

Pandy, D. (2020). Stationing Smart Contract as a 'Contract': A Case for Interpretative Reform of the Indian Contract Act, 1872. *National University of Juridical Sciences Law Review*, *13*, 2-3.

Raskin, M. (2017). The Law and Legality of Smart Contracts. *Georgetown Law Technology Review*, *1*(305). https://doi.org/https://doi.org/10.2139/ssrn.2842258

Safaei, S. H. (2013). *Preliminary course of civil law: Persons and property*. Tehran: Mizan Publishing.

Safaei, S. H., & Ghasemzadeh, S. M. (2015). *Persons and incapacitated individuals*. Tehran: Samt Publishing.

Savelyev, A. (2016). *Contract Law 2.0: «Smart» Contracts As the Beginning of the End OF Classic Contract Law*. National Research University High School of Economics.

Shahidi, M. (2014). *Civil law: Obligations*. Tehran: Majd Publishing.

Siemer, T. (2008). *Formations of electronic contracts under traditional common law principles*. Grin Verlag, Germany.

Singh, J., & Shilpa. (2021). Smart contracts and blockchain: legal issues and implications for Indian contract law. *International Review of Law, Computers & Technology*, *36*, 313-314. https://doi.org/https://doi.org/10.1080/13600869.2021.1999312

Wang, F. F. (2014). *Law of Electronic Commercial Transactions: Contemporary Issues in the EU, US and China*.