# Smart Contracts and Their Status in the Validity of Contracts from the Perspective of Iranian Law

**1. Amir Mirzavand *: Master of Private Law, Borujerd Branch, University of Science and Research, Borujerd, Iran**

*Correspondence: Mirzavandamir@gmail.com

**Abstract**

The rapid expansion of blockchain-based transactions and automated digital systems has created new questions for contract law, particularly regarding the validity of agreements formed, recorded, or executed through computer code. This article examines the legal status of smart contracts from the perspective of Iranian law, with specific attention to the general requirements of contractual validity. The study adopts a doctrinal and analytical approach and argues that smart contracts should not be considered legally valid merely because they are technically executable, nor should they be rejected simply because they are coded or automated. Rather, their validity must be assessed according to the established principles of Iranian contract law, including intention and consent, legal capacity, definiteness of subject matter, and lawfulness of purpose. The article explains that code may function as a means of expressing contractual intention, recording agreement, or performing obligations, but it cannot replace the substantive legal foundations of a valid contract. Particular attention is given to problems of offer and acceptance, attribution of automated acts, cryptographic authorization, defects of consent, coding errors, oracle failure, pseudonymity, consumer protection, and the conflict between coded terms and natural-language agreements. The article further argues that the most appropriate model for Iranian law is a hybrid model in which a legally understandable written agreement defines the parties' rights and obligations, while the smart contract automates selected aspects of performance. This approach allows Iranian law to recognize the practical advantages of smart contracts, including efficiency, certainty, and evidentiary reliability, while preserving judicial authority to examine validity, interpret intention, correct defective transactions, and provide remedies. The article concludes that smart contracts can have a valid place in Iranian contract law when they satisfy ordinary contractual requirements and when their electronic operation can be reliably attributed to legally responsible parties.

**Keywords:** Smart contracts; contract validity; Iranian law; electronic contracts; blockchain; contractual intention; automated performance

Received: 18 January 2024
Revised: 01 March 2024
Accepted: 04 March 2024
Published: 10 March 2024



**Citation**: Mirzavand, A. (2024). Smart Contracts and Their Status in the Validity of Contracts from the Perspective of Iranian Law. *Legal Studies in Digital Age,* 3(1), 148-160.

## 1. Introduction

The expansion of digital transactions has transformed the traditional image of contract formation, performance, and enforcement. In classical contract law, a contract is usually imagined as an agreement expressed through words, writings, signatures, or conduct, and later performed through human action or institutional enforcement. Smart contracts challenge this

familiar image because they combine agreement, code, and automated execution in a single technological arrangement. The term "smart contract" was originally introduced to describe computerized transaction protocols capable of executing the terms of an agreement, and this early understanding already connected contractual relations with technical architecture rather than with written language alone (Szabo, 1996). In later discussions, smart contracts became closely associated with blockchain technology, distributed ledgers, crypto-assets, and decentralized systems, but their conceptual importance is broader than blockchain itself. They raise a fundamental legal question: can contractual intention, consent, obligation, and performance be validly expressed through code? This question is especially important in Iranian law because the validity of contracts is traditionally assessed through general principles of civil law, while electronic communication has also been recognized through statutory rules concerning data messages and digital transactions. Therefore, the legal status of smart contracts cannot be answered merely by technological description; it requires a doctrinal analysis of whether coded and automated agreements satisfy the substantive conditions of contractual validity.

The problem becomes more complex because smart contracts are not always "contracts" in the legal sense. Some smart contracts are only technical tools that automate a payment, transfer a token, verify a condition, or execute a digital instruction. Others are linked to a broader legal agreement written in ordinary language, while some are intended to represent the entire agreement between the parties in coded form. This difference has been emphasized in legal scholarship because the phrase "smart contract" often obscures the distinction between technical code and legal obligation (Mik, 2017). A computer program may execute a transaction, but execution does not necessarily prove that a legally valid contract exists. Conversely, a legally valid contract may exist even when the smart contract is merely a mechanism of performance. The legal inquiry must therefore begin by separating code as a technological instrument from contract as a juridical act. In Iranian law, this distinction is important because contract validity depends on substantive legal requirements such as intention, consent, capacity, definiteness of subject matter, and lawful purpose. These requirements cannot be replaced by automation. A transaction may be technically irreversible while still legally defective. Similarly, a smart contract may operate flawlessly from a computational point of view while failing to satisfy a legal condition of validity.

The rise of blockchain-based smart contracts has also affected the relationship between private autonomy and legal regulation. Blockchain systems are often described as creating a technological environment in which rules are executed automatically by code, reducing dependence on courts, intermediaries, banks, registries, or centralized authorities. Wright and De Filippi describe this development through the concept of "Lex Cryptographia," meaning a set of rules administered through cryptographic systems and decentralized protocols rather than through traditional legal institutions (Wright & De Filippi, 2015). De Filippi and Wright later argue that blockchain technology gives code a regulatory function because programmed rules can shape behavior directly and automatically (De Filippi & Wright, 2018). However, from the perspective of contract law, the replacement of institutional enforcement with automatic execution does not eliminate the need for legal analysis. It only changes the stage at which law intervenes. Traditional law often intervenes after breach, whereas smart contracts may execute before a legal dispute is examined. This feature makes validity analysis more important, not less important, because an invalid or defective smart contract may already have produced consequences before a court reviews the transaction.

The central issue of this article is the status of smart contracts in the validity of contracts under Iranian law. Iranian contract law, like many civil-law systems, emphasizes the essential conditions of contractual validity. The Civil Code recognizes the binding force of contracts when legal requirements are satisfied, and it treats intention, consent, capacity, definite subject matter, and lawful cause as essential elements of a valid transaction. The question is whether these elements can be satisfied when the agreement is formed, expressed, recorded, or performed through code. Nejatzadegan and Soltani specifically analyze smart-contract validity from Iranian and American legal perspectives and show that the general conditions of contract validity remain central even when the transaction is technologically mediated (Nejatzadegan & Soltani, 2023). This means that Iranian law should not treat smart contracts as legally valid merely because they are executable, nor should it reject them merely because they are coded. Instead, the correct approach is functional: if the coded arrangement performs the same legal functions as offer, acceptance, consent, expression of intention, and performance, it may be recognized within the existing framework of contract law, provided that no mandatory rule is violated.

The relevance of this inquiry is increased by the ambiguity of smart contracts. Although smart contracts are often promoted as precise, objective, and self-executing, legal scholars have challenged this claim. Grimmelmann argues that all smart contracts

are ambiguous because ambiguity may arise not only from natural language but also from the relationship between code, external facts, user expectations, legal consequences, and institutional interpretation (Grimmelmann, 2019). This insight is crucial for Iranian law because the validity of a contract is not determined only by the mechanical operation of its terms. Courts may need to determine what the parties intended, whether the coded performance corresponded to their agreement, whether a mistake occurred, whether a condition was manipulated, and whether the transaction had a lawful basis. In ordinary contracts, ambiguity is addressed through interpretation. In smart contracts, ambiguity may be hidden behind technical precision. Code may be syntactically exact but legally incomplete. It may define an automatic transfer without explaining the legal basis of the transfer. It may execute payment without resolving questions of capacity, fraud, duress, or illegality. Therefore, smart contracts do not abolish interpretation; they relocate interpretive problems into the relationship between code and law.

The article also proceeds from the assumption that smart contracts must be analyzed within the broader evolution of electronic contracting. Before blockchain, legal systems had already confronted the question of whether computers could form contracts. Allen and Widdison examined whether computers can make contracts and showed that automated contracting challenges traditional assumptions about human communication, agency, and intention (Allen & Widdison, 1996). Their analysis remains relevant because smart contracts are not the first form of automated legal transaction. Online purchases, automated trading systems, electronic agents, and platform-based transactions already created situations in which a person's legal will is expressed through a machine. Smart contracts intensify these problems because they may not only form or record contractual relations but also execute performance without further human decision. The legal system must therefore distinguish between the human intention behind the automated system and the automatic operation of the system itself. This distinction is particularly important in cases where the smart contract performs unexpectedly because of coding error, oracle failure, hacking, or interface manipulation.

The objective of this article is to analyze whether smart contracts can satisfy the conditions of contractual validity under Iranian law and to explain how their legal status should be understood in relation to intention, consent, capacity, subject matter, lawful purpose, evidence, attribution, and enforcement. The article argues that smart contracts may be valid under Iranian law when they represent or implement a legally recognizable agreement, but their validity cannot be inferred solely from technical execution. The article further argues that the most reliable legal model for Iranian law is a hybrid model in which coded performance is connected to legally intelligible contractual terms. This model preserves the efficiency of smart contracts while reducing uncertainty regarding interpretation, defects of consent, liability, dispute resolution, and judicial review.

## 2. Conceptual and Technical Foundations of Smart Contracts

The concept of the smart contract must be clarified before its legal validity can be assessed. In its original formulation, a smart contract was not necessarily a blockchain application but a computerized protocol designed to facilitate, verify, or enforce contractual performance (Szabo, 1996). Szabo's later work emphasized the formalization and securing of relationships on public networks, suggesting that digital systems could reduce reliance on trust by embedding transaction rules into technical architecture (Szabo, 1997). This early definition reveals two elements that remain central to contemporary smart contracts. First, smart contracts involve formalization: contractual relations are translated into precise operational instructions. Second, they involve execution: once the programmed conditions are satisfied, the system performs the agreed consequence. However, these technological features do not themselves determine legal validity. The law must still ask whether the formalized instructions correspond to a valid juridical act. A vending machine may automatically exchange money for goods, but the legal analysis still depends on offer, acceptance, capacity, ownership, and lawful transaction. Smart contracts operate at a more complex digital level, but the underlying legal question is similar.

Modern smart contracts are most commonly discussed in connection with blockchain. A blockchain is a distributed ledger maintained by a network of participants rather than by a single central authority. Smart contracts deployed on blockchain platforms can automatically transfer digital assets, create tokens, record transactions, or execute conditional obligations when predetermined inputs are received. De Filippi and Wright explain that blockchain systems create a form of governance in which code can become a regulatory mechanism, shaping conduct through technological constraints rather than through traditional legal commands (De Filippi & Wright, 2018). This has encouraged the idea that "code is law" or that blockchain can create self-enforcing private ordering. Yet this idea should not be overstated in contract law. Code can determine what happens

technologically, but law determines whether what happened is valid, binding, voidable, enforceable, reversible, compensable, or unlawful. A blockchain transfer may be technically final, but legal finality depends on the legal system. The distinction between technological finality and legal validity is essential for understanding the position of smart contracts in Iranian law.

A useful conceptual distinction is the difference between smart contract code and smart legal contract. Clack, Bakshi, and Braine discuss smart contract templates as mechanisms that may combine legal prose, parameters, and executable code (Clack et al., 2016). This approach is important because it avoids the false assumption that all contractual meaning must be written directly in code. In many real transactions, the code performs certain functions while the legal contract remains in natural language. For example, a sale contract may be written in ordinary legal language, while a smart contract automatically releases payment after confirmation of delivery. In that situation, the smart contract is not the entire contract; it is a performance layer attached to a legal agreement. By contrast, in a fully coded transaction, the parties may rely on the code itself as the primary expression of their obligations. This creates greater legal difficulty because code is not always understandable to non-programmers, and legal concepts such as good faith, reasonableness, mistake, and lawful purpose are difficult to translate into deterministic instructions.

The most important characteristics of smart contracts are automation, conditionality, self-execution, digital recordability, and resistance to unilateral alteration. Automation means that performance occurs without a fresh human decision at the moment of execution. Conditionality means that performance depends on predetermined triggers, such as payment, delivery confirmation, passage of time, price movement, or external data. Self-execution means that once the condition is met, the system automatically performs the consequence. Digital recordability means that the transaction can be stored, traced, and verified through electronic records. Resistance to unilateral alteration means that, particularly in blockchain environments, one party cannot easily modify the code after deployment. These features explain why smart contracts are attractive for commercial transactions, but they also explain their legal risks. Raskin describes smart contracts as arrangements that may reduce enforcement costs by making performance automatic, yet he also notes that the legal consequences of such automation require careful examination (Raskin, 2017). The law must determine whether automatic performance is a valid expression of private autonomy or an uncontrolled technical consequence that may conflict with legal rules.

Smart contracts differ from ordinary electronic contracts. An electronic contract may be formed by email, website terms, online acceptance, electronic signature, or digital communication. It remains primarily a contract expressed in language and supported by electronic evidence. A smart contract, by contrast, may embed performance in code. This means that the difference is not merely the medium of communication but the relationship between agreement and execution. Giancaspro argues that smart contracts raise legal problems because their technical operation may not correspond neatly to legal concepts such as contractual intention, mistake, and remedies (Giancaspro, 2017). This is particularly significant for Iranian law because electronic contracting has already been accommodated through rules on data messages and electronic signatures, but smart contracts introduce the additional issue of automatic performance. A click on a website may show acceptance, but a blockchain transaction may simultaneously show acceptance, payment, transfer, and performance. This compression of formation and execution creates doctrinal difficulty because contract law traditionally separates the existence of a contract from its performance.

Another conceptual problem concerns the identity of the parties. In many blockchain-based smart contracts, parties interact through wallet addresses rather than through names, national identification numbers, or corporate registration data. This creates difficulty for capacity, attribution, liability, and enforcement. Fairfield's discussion of Bitcoin bots and consumer protection shows that automated and pseudonymous systems can expose consumers to risks that traditional contract law did not fully anticipate (Fairfield, 2014). From the Iranian-law perspective, the problem is not merely practical but doctrinal. A contract requires legally capable parties. If a party cannot be identified, it becomes difficult to determine capacity, authority, representation, and liability. A pseudonymous blockchain address may be technically sufficient to transfer digital assets, but it may not be legally sufficient to establish that a valid contract exists between identifiable legal persons. Therefore, smart contracts are strongest legally when they are connected to reliable identification, authentication, and attribution mechanisms.

Smart contracts are also often described as trustless, but this description is misleading. They may reduce the need to trust a counterparty's future performance, but they create new forms of trust in code, platform architecture, developers, private-key security, oracles, user interfaces, and network governance. Mik emphasizes that smart contracts involve technical limitations

and real-world complexity that are often underestimated in simplified legal and commercial narratives (Mik, 2017). For example, a smart contract may depend on an external oracle to determine whether goods were delivered, whether a price reached a threshold, or whether a date or event occurred. If the oracle provides incorrect data, the code may execute correctly according to its instructions while producing a legally incorrect result. Similarly, if a user interface misrepresents the terms of the code, the party may consent to one transaction while the smart contract performs another. These problems show that smart contracts do not eliminate factual uncertainty. They may even intensify it because the law must examine both the human agreement and the technical system through which the agreement was implemented.

The legal classification of smart contracts should therefore be functional rather than formal. A smart contract may be classified as a method of communication, a method of evidence, a method of performance, a technical escrow mechanism, a digital agent, or a legal agreement in coded form. O'Shields describes smart contracts as legal agreements for the blockchain, but this formulation must be handled carefully because not every blockchain script contains a legal agreement (O'Shields, 2017). The correct legal question is whether the smart contract performs a contractual function. If it expresses offer and acceptance, it may be relevant to formation. If it records terms, it may be relevant to evidence. If it executes payment, it may be relevant to performance. If it controls assets, it may be relevant to remedies and restitution. This functional approach is suitable for Iranian law because it allows existing doctrines to be applied without requiring premature creation of a separate legal category for all smart contracts.

The conceptual foundation of this article is therefore that smart contracts should not be understood as replacing contract law. They are technological instruments that may support, express, or execute contractual relations. Savelyev argues that smart contracts may represent a movement toward "Contract Law 2.0," but his analysis also shows that they challenge rather than simply abolish classical contract law (Savelyev, 2017). The Iranian legal system can recognize smart contracts without abandoning the Civil Code's validity requirements. The decisive issue is whether coded relations can be interpreted through existing legal categories. If intention and consent are present, if the parties are capable, if the subject matter is definite, and if the purpose is lawful, a smart contract may have legal effect. If these conditions are absent, automation cannot cure the defect. Thus, the technological nature of smart contracts affects the evidence, interpretation, performance, and enforcement of contractual obligations, but it does not remove the need for legal validity.

## 3. General Conditions of Contractual Validity under Iranian Law

The validity of smart contracts under Iranian law must be examined through the general principles governing contracts. The central point is that a smart contract is not valid simply because it is technologically operative. It must satisfy the same substantive requirements that make any contract legally valid. Nejatzadegan and Soltani emphasize that the general conditions of validity remain applicable to smart contracts in Iranian law, especially because smart contracts do not exist outside the legal system even when they operate on decentralized networks (Nejatzadegan & Soltani, 2023). This means that the legal analysis should not begin with blockchain architecture but with the elements of contract validity. The Civil Code's requirements concerning intention, consent, capacity, definite subject matter, and lawful purpose remain the main doctrinal framework. The smart contract may alter the form in which these elements appear, but it does not eliminate them. Therefore, the essential inquiry is whether code can express intention, whether interaction with a digital protocol can demonstrate consent, whether the party behind the digital act has capacity, whether the coded transaction has a definite subject matter, and whether the purpose of the transaction is lawful.

The first and most important requirement is intention and consent. In ordinary contracts, intention may be expressed through words, writing, signature, conduct, or other legally meaningful acts. In smart contracts, intention may be expressed through deployment of code, interaction with a smart contract address, use of a private key, digital confirmation, or performance of a programmed transaction. Allen and Widdison's early analysis of computer-made contracts is useful because it shows that automated contracting should be linked to the human intention behind the system rather than to the machine as an independent legal person (Allen & Widdison, 1996). In Iranian law, the same logic can be applied. The computer or blockchain protocol does not possess legal will; the relevant will belongs to the person who programmed, deployed, authorized, or used the system. Therefore, a smart contract can show intention when the conduct of the party reasonably indicates willingness to enter into

legal relations. However, this conclusion must be limited by awareness and understanding. If a person interacts with a smart contract without understanding its legal effect, or if the interface conceals the real terms of the code, consent may be defective. This is why legal recognition of smart contracts must be connected to transparency, accessibility, and proof of assent.

Offer and acceptance also require special attention. A deployed smart contract may be interpreted in different ways depending on context. It may constitute an offer to anyone who performs a specified act, an invitation to negotiate, a mechanism for accepting a prior written agreement, or a technical tool that has no independent contractual meaning. Raskin notes that smart contracts can automate execution but their legal status depends on whether they correspond to recognizable contractual relations (Raskin, 2017). Under Iranian law, the same deployment of code may have different legal implications. For example, if a seller publishes a smart contract that automatically transfers a token to any person who pays a specified amount, the code may function as an offer to the public, provided the subject matter, price, and conditions are sufficiently definite. If, however, the smart contract is only a technical escrow mechanism created after the parties have already concluded a written agreement, the code does not itself constitute the offer; it merely performs an obligation. Courts should therefore determine the legal meaning of deployment and interaction by examining the parties' conduct, commercial context, and the relationship between code and any accompanying legal text.

Capacity is another essential condition. In smart contracts, the problem of capacity is intensified by pseudonymity, automation, and digital access. A blockchain address does not reveal whether the user is a minor, a legally incapacitated person, an authorized representative, a company officer, or an unauthorized actor. Fairfield's work on automated Bitcoin transactions and consumer protection illustrates how digital systems may weaken traditional safeguards that protect weaker or incapable parties (Fairfield, 2014). In Iranian law, technical ability to use a digital wallet cannot be equated with legal capacity. A minor may be able to send a blockchain transaction, but the legal validity of that transaction remains subject to capacity rules. Similarly, an employee may have technical access to a company wallet without legal authority to bind the company. Therefore, smart-contract validity requires a distinction between technical control and legal authority. A private key may prove control over a digital address, but it does not always prove legal capacity or representative authority.

The subject matter of a smart contract must also be definite. Smart contracts may concern payment, digital assets, tokens, software access, decentralized services, automated licensing, or tokenized representations of external assets. In principle, code can define subject matter with great precision because it can specify amount, time, asset identifier, wallet address, and execution conditions. Clack, Bakshi, and Braine's discussion of smart contract templates shows that structured parameters can make contractual performance more precise than ordinary prose in certain contexts (Clack et al., 2016). However, precision in code is not always the same as legal definiteness. A token may be technically identifiable while its legal nature remains uncertain. A coded transfer may specify a digital asset but fail to clarify whether the asset represents ownership, a claim, a license, a right to use a service, or merely a speculative unit within a platform. Therefore, Iranian law should require that the subject matter be legally identifiable, not merely technically identifiable. If the code is connected to a written agreement that explains the legal nature of the digital asset or obligation, the requirement of definiteness is more easily satisfied.

Lawful purpose is equally important. Smart contracts can be used for legitimate commercial automation, but they can also be used for unlawful transactions, illegal gambling, fraud, unauthorized asset transfers, circumvention of mandatory rules, or concealment of illicit financial flows. Wright and De Filippi's concept of decentralized blockchain governance shows that blockchain systems can create autonomous rule structures outside centralized oversight (Wright & De Filippi, 2015). This autonomy may increase efficiency, but it may also make unlawful activity harder to detect and regulate. Under Iranian law, the technological form of a transaction cannot legalize an unlawful purpose. A smart contract designed to perform an unlawful exchange, conceal illegal payment, or enforce an obligation contrary to mandatory law cannot be recognized as valid merely because the code executes automatically. The legal system must distinguish between technological enforceability and juridical enforceability. A transaction may be executed by the network, yet remain void or unenforceable in law.

Defects of consent are among the most difficult issues in smart-contract validity. Mistake, fraud, and duress can occur in coded transactions, although they may appear differently than in traditional contracts. A party may make a mistake about the code, the asset, the price, the identity of the counterparty, the legal effect of a transaction, or the operation of an external oracle. Giancaspro argues that smart contracts may create serious legal difficulties where the code does not correspond to the parties' actual understanding or where automatic execution prevents ordinary corrective mechanisms (Giancaspro, 2017). In Iranian

law, a coding error may be analyzed differently depending on whether it affects the expression of intention, the subject matter, or performance. If both parties agreed to one legal result but the code performs another result because of a programming mistake, the code should not automatically override the legal agreement. If, however, the parties expressly agreed that the code would define their obligations, then the party alleging mistake must show that the code failed to represent the intended agreement or that consent was otherwise defective. The court may need expert evidence to determine whether the error was in code, interpretation, interface, or external data.

Fraud in smart contracts may occur through deceptive interfaces, hidden code functions, manipulated information, false descriptions of tokens, or intentional exploitation of technical ignorance. Mik's critique of the terminology and real-world complexity of smart contracts is relevant because it shows that users may not fully understand what coded systems actually do (Mik, 2017). A person may be told that a smart contract performs one function, while the code contains another mechanism. A platform may advertise a token as representing a legal right, while the code only transfers a digital unit with no enforceable claim. In such cases, the problem is not merely technical vulnerability but fraudulent inducement. Iranian law can address this through established doctrines of defective consent and civil liability. The fact that the transaction was executed on a blockchain does not prevent a court from examining whether consent was obtained through deception.

Duress and exploitation may also arise in digital environments. A person may be compelled to transfer digital assets through a smart contract, threatened into revealing a private key, or forced to interact with a coded system. The existence of a cryptographic signature does not by itself prove free consent. Sklaroff's analysis of smart contracts and the cost of inflexibility is relevant here because automated execution can make it difficult to stop or reverse performance once the process begins (Sklaroff, 2017). This inflexibility may increase the harm caused by defective consent. In traditional contracts, a party may refuse performance after discovering duress or fraud; in a smart contract, the performance may already have occurred. Iranian law must therefore separate the factual occurrence of performance from its legal legitimacy. If the underlying consent was defective, the court may still recognize remedies such as restitution, damages, or invalidity, even if the blockchain record itself cannot be technically changed.

A further problem is the relationship between code and natural language. Grimmelmann's argument that smart contracts are ambiguous is especially important for validity analysis because a legal dispute often arises where code, written terms, and party expectations diverge (Grimmelmann, 2019). If a written contract says payment will be released upon satisfactory delivery, but the smart contract releases payment automatically upon receipt of a tracking number, the question becomes whether the coded condition replaced or merely implemented the legal condition. In Iranian law, courts should determine the parties' true intention by examining the entire contractual arrangement. Code should be treated as one expression of intention, not necessarily the exclusive expression. Where the parties clearly agree that code has priority, that agreement may be respected unless it violates mandatory law. Where the relationship between code and text is unclear, legal interpretation should prevent unjust results caused by purely mechanical execution.

The general conditions of contractual validity therefore show that smart contracts can be compatible with Iranian law, but only under a careful doctrinal approach. Savelyev suggests that smart contracts challenge classical contract law because they reduce reliance on legal enforcement and replace some legal functions with technical execution (Savelyev, 2017). Yet Iranian law can respond by maintaining the distinction between execution and validity. If the parties are capable, if their consent is genuine, if the subject matter is definite, and if the purpose is lawful, the smart contract may be valid. If any of these conditions is absent, the smart contract may be void, voidable, or unenforceable according to general legal principles. The code may accelerate performance, but it cannot create legal validity out of a defective transaction. This conclusion preserves both technological innovation and legal coherence.

## 4. Smart Contracts under Iranian Electronic Commerce Law

Smart contracts must also be examined in relation to electronic commerce law because they operate through digital communication, electronic records, and automated systems. Iranian electronic commerce law provides a framework for recognizing data messages, electronic signatures, attribution, and evidential value. Although it was not enacted specifically for blockchain or smart contracts, its concepts are useful for analyzing the legal effects of coded transactions. Allen and Widdison's analysis of computer-made contracts anticipated many of these issues by showing that electronic systems can participate in

contract formation without eliminating the human legal responsibility behind them (Allen & Widdison, 1996). This idea is important for Iranian law because smart contracts should not be treated as autonomous legal persons. They are electronic mechanisms through which natural or legal persons communicate, assent, and perform. Therefore, the rules of electronic commerce can support smart-contract recognition when they allow digital messages and automated systems to be attributed to legally responsible parties.

The concept of the data message is particularly relevant. A smart contract may generate or contain several forms of electronic information: source code, deployed bytecode, transaction hashes, wallet addresses, timestamps, digital signatures, event logs, and performance records. These elements may serve as evidence of offer, acceptance, payment, transfer, or performance. O'Shields describes smart contracts as blockchain-based legal agreements, but the legal evidentiary value of such agreements depends on whether the digital record can be connected to the parties and to their legal intention (O'Shields, 2017). In Iranian law, a blockchain record should not be dismissed merely because it is electronic. If it is reliable, retrievable, and attributable, it may help prove the existence and content of a transaction. However, the record does not interpret itself. A transaction hash may prove that a digital instruction occurred, but it does not necessarily prove why the instruction occurred, whether the party had capacity, or whether the transaction had a lawful basis.

Electronic signatures and authentication mechanisms create another important connection between smart contracts and Iranian electronic commerce law. In blockchain systems, transactions are usually authorized through private keys and verified through cryptographic signatures. These mechanisms can identify control over a digital address and indicate approval of a transaction. Raskin explains that cryptographic tools can make smart contracts highly reliable from a technical perspective because they enable automatic execution and verification without traditional intermediaries (Raskin, 2017). Yet legal authentication is broader than technical verification. A private key proves that the transaction was signed by whoever controlled the key at that moment, but it does not always prove that the legal owner consented freely and knowingly. If a private key is stolen, if a wallet is hacked, if a person is coerced, or if malware triggers a transaction, the cryptographic signature may be technically valid while legal consent is absent. Iranian courts should therefore treat cryptographic signatures as strong but rebuttable evidence, not as conclusive proof of validity in all circumstances.

Attribution is one of the most important legal issues. When an automated system sends a message, executes a transaction, or transfers an asset, the law must decide whether that act is attributable to a party. Werbach and Cornell describe smart contracts as "contracts ex machina," emphasizing that machines may perform contractual functions while the legal system must decide how to attribute the resulting acts (Werbach & Cornell, 2017). In Iranian law, attribution should depend on authorization, control, and reasonable connection between the party and the automated system. If a person deploys a smart contract and invites others to interact with it, the actions of the code may be attributable to that person within the intended scope of deployment. If a company authorizes an automated payment smart contract, the system's performance may be attributable to the company. However, if the system is altered by an attacker, triggered by unauthorized access, or manipulated through false data, attribution becomes more difficult. The legal inquiry must determine whether the act was within the risk accepted by the party or outside the scope of authorization.

The use of external data sources, commonly called oracles, creates a special attribution and evidence problem. Smart contracts cannot independently know many real-world facts. They may need external inputs concerning market prices, delivery status, identity verification, weather events, exchange rates, or administrative approvals. De Filippi and Wright explain that blockchain systems operate through technical rules, but their connection to social and legal reality often depends on interfaces between code and the outside world (De Filippi & Wright, 2018). When an oracle provides incorrect information, the smart contract may execute exactly as coded but contrary to the parties' real agreement. For example, if payment is released based on a false delivery confirmation, the code has not malfunctioned, but the legal performance may be defective. Iranian law should therefore distinguish between code failure, oracle failure, and contractual risk allocation. Parties may agree that oracle data is final, but such an agreement should not protect fraud, manipulation, or illegality.

Smart contracts also raise evidentiary questions regarding interpretation. A court may need to understand what the code did, what the parties believed it would do, and whether the coded operation corresponded to the legal agreement. Grimmelmann's argument about smart-contract ambiguity is directly relevant because it shows that code may be clear to a machine but ambiguous in legal context (Grimmelmann, 2019). A judge may not be able to interpret a smart contract without technical

expertise. Expert evidence may be necessary to explain the code, the blockchain platform, the transaction history, and the relationship between the code and any written agreement. This does not mean that code should be treated as foreign to law. Rather, it means that code is a form of evidence requiring interpretation. Just as courts may interpret accounting records, engineering reports, or digital communications, they may interpret smart contract records with the assistance of experts.

Enforcement is another central issue. Smart contracts are often described as self-enforcing because they perform automatically. However, this description is only partially accurate. Sklaroff warns that the inflexibility of smart contracts may create costs because automatic performance can occur even when changed circumstances, mistake, or unfair results would justify human intervention (Sklaroff, 2017). In Iranian law, self-execution should not be confused with legal enforcement. A smart contract may transfer a digital asset automatically, but a court may still need to decide whether the transfer was valid, whether restitution is required, whether damages must be paid, or whether another party is liable. Automatic execution may reduce certain enforcement costs, but it does not eliminate disputes. In fact, smart contracts may create new disputes after performance has occurred, especially where technical irreversibility conflicts with legal remedies.

The problem of remedies is especially serious where blockchain transactions are practically irreversible. If a smart contract transfers digital assets to another address, reversal may be technically impossible unless the receiving party cooperates or unless the platform contains a reversal mechanism. Giancaspro notes that the legal system must confront the difficulty of applying traditional remedies to automatic transactions that may not be easily undone (Giancaspro, 2017). Iranian law can respond by distinguishing between technical reversal and legal restitution. Even if the blockchain record cannot be altered, the court may order the recipient to return equivalent value, compensate damages, or restore the parties as far as legally possible. Therefore, the impossibility of technical reversal should not be treated as the impossibility of legal remedy. However, practical enforcement may be difficult if the recipient is anonymous, outside jurisdiction, or unable to be identified.

Consumer protection and unequal bargaining power also deserve attention. Smart contracts may be presented to users through simplified interfaces while the actual code remains unreadable to them. Fairfield's analysis shows that automated digital transactions can create consumer-protection concerns because users may not understand the risks embedded in code, digital assets, or automated systems (Fairfield, 2014). In Iranian law, this concern is relevant wherever one party is technically sophisticated and the other is not. If a business uses smart contracts with consumers, the business should not be allowed to avoid legal responsibility by claiming that the code was publicly available. Legal transparency requires more than technical availability. It requires that the legally relevant terms be understandable. A consumer cannot reasonably be expected to audit code before entering into a routine digital transaction.

The relationship between smart contracts and electronic commerce law therefore supports recognition, but not unconditional recognition. Electronic records, digital signatures, and automated messages may help prove agreement and performance. However, they must be interpreted through ordinary legal principles concerning consent, capacity, attribution, and legality. Mik's critique of exaggerated smart-contract claims is important because it reminds legal systems that technology does not remove real-world complexity (Mik, 2017). Iranian law should adopt a balanced approach. It should accept that smart contracts can produce legally relevant electronic acts, but it should also require sufficient proof that those acts were authorized, meaningful, and connected to valid legal intention. This approach allows innovation without surrendering legal control to code.

## 5. Legal Challenges, Interpretation, and the Appropriate Model for Iranian Law

The most suitable model for Iranian law is not the complete replacement of legal contracts by code, but the integration of smart contracts into existing contract doctrine. Smart contracts can improve efficiency by automating performance, reducing transaction costs, creating reliable records, and limiting opportunistic breach. Werbach and Cornell argue that smart contracts can change the economics of contracting by making certain obligations self-executing, but they also show that legal institutions remain necessary because not all contractual relations can be reduced to code (Werbach & Cornell, 2017). This is especially true in Iranian law, where contract validity depends not only on external expression but also on substantive legal conditions. A smart contract may be very useful for obligations that are objective, measurable, and binary, such as payment upon a date or transfer after receipt of a defined digital asset. It is less suitable for obligations requiring judgment, fairness, good faith, reasonableness, quality assessment, or equitable adjustment.

A hybrid model is therefore the most appropriate. In this model, the parties conclude a legal agreement in ordinary language and use a smart contract to execute specific obligations. The written agreement explains the legal relationship, identifies the parties, defines the subject matter, allocates risks, determines governing law, specifies dispute-resolution mechanisms, and clarifies the priority between legal prose and code. The smart contract then performs technical functions such as payment, escrow, delivery confirmation, or access control. Clack, Bakshi, and Braine's work on smart contract templates is particularly useful for this model because it shows how legal prose and executable code may be connected through structured design (Clack et al., 2016). For Iranian law, the hybrid model reduces uncertainty because the judge can interpret the legal contract while using the code as evidence of performance or implementation. This model also allows parties to benefit from automation without forcing all legal meaning into programming language.

The fully coded model is more problematic. In a fully coded smart contract, the parties may claim that the code is the entire agreement. This model creates difficulty because code is not naturally designed to express many legal concepts. Grimmelmann's argument that all smart contracts are ambiguous is important because the claim that code is perfectly precise ignores the gap between computational execution and legal meaning (Grimmelmann, 2019). A program can specify that if X occurs, Y will happen, but it may not explain whether X was lawfully obtained, whether Y is a valid legal consequence, whether one party acted fraudulently, or whether changed circumstances justify relief. Legal contracts often contain standards rather than rules because human relations cannot always be anticipated in advance. Smart contracts are strongest when the obligation is narrow and objective; they are weakest when the obligation requires flexible evaluation.

Interpretation becomes especially difficult when the written agreement and the code conflict. Suppose the written agreement states that payment is due only after successful delivery, while the smart contract releases payment when an external tracking system records dispatch. If the goods are dispatched but never received, the code may release payment even though the legal condition has not been satisfied. In such cases, Iranian law should not automatically treat code as superior. The court should examine whether the parties intended code to define the condition or merely to implement it. Sklaroff's discussion of inflexibility supports the view that smart contracts can create unfair or inefficient results where automatic performance cannot adapt to factual complexity (Sklaroff, 2017). The legal agreement should therefore include a priority clause explaining whether the code prevails over prose, whether prose prevails over code, or whether the code is only a performance mechanism.

Liability for coding errors is another major challenge. A coding error may be introduced by one party, a jointly appointed developer, a third-party platform, or an open-source software component. The legal consequences depend on who assumed responsibility for the code and whether the error affected formation, performance, or risk allocation. Giancaspro's analysis highlights that smart contracts may be vulnerable to legal problems when technical design does not correspond to contractual intention (Giancaspro, 2017). Iranian law should approach coding errors through general principles of contractual interpretation, mistake, negligence, and liability. If one party provides defective code and the other party relies on it, liability may arise. If both parties agree to use a particular code "as is," the allocation of risk may be different, although mandatory rules and defects of consent may still intervene. If a developer negligently writes code for the parties, professional liability may be relevant.

The question of hacking and unauthorized access also affects validity and enforcement. If an attacker exploits a vulnerability in a smart contract, the code may execute according to its internal logic but contrary to the parties' intended legal relationship. De Filippi and Wright explain that blockchain systems often rely on the rule of code, but legal systems must still respond when code-based outcomes conflict with social and legal expectations (De Filippi & Wright, 2018). In Iranian law, exploitation of a vulnerability should not automatically be treated as a valid exercise of contractual rights. If the attacker was not a party acting in good faith but an unauthorized exploiter, the resulting transfer may be legally defective. The difficult question is whether the vulnerability was part of the agreed rules or an unintended defect. Courts must examine the parties' expectations, the documentation, the code, and the nature of the exploit. This requires technical expertise and legal interpretation together.

Another challenge concerns anonymous or cross-border transactions. Smart contracts may connect parties from different jurisdictions without clear identification or choice of law. Wright and De Filippi's discussion of decentralized blockchain systems shows that such systems operate across territorial boundaries and can challenge traditional jurisdictional assumptions (Wright & De Filippi, 2015). For Iranian law, this raises questions of applicable law, jurisdiction, enforcement of judgments, and compliance with mandatory domestic rules. If a smart contract is used by Iranian parties or has effects in Iran, Iranian law

may be relevant even if the blockchain network is global. However, practical enforcement may be difficult if assets, parties, or developers are located abroad. The hybrid model can reduce this problem by including governing-law and dispute-resolution clauses, but fully anonymous smart contracts remain legally fragile.

Smart contracts also raise questions concerning contractual justice and public order. Savelyev suggests that smart contracts may represent a challenge to classical contract law by shifting enforcement from law to technology (Savelyev, 2017). This shift may be efficient where parties are equal and terms are clear, but it may be problematic where one party imposes coded terms that the other cannot understand or negotiate. Iranian law should not permit the technical form of a transaction to weaken mandatory protections. If a smart contract includes unfair, illegal, or abusive terms, the court should be able to examine them. If a party uses code to avoid obligations imposed by law, the transaction should not be shielded by technological execution. The principle is that private autonomy operates within legal limits. Smart contracts can serve autonomy, but they cannot transform autonomy into a private technical regime immune from law.

The appropriate interpretive approach for Iranian courts should be contextual, functional, and evidence-based. Courts should ask what legal function the smart contract performed. Did it express consent, record a prior agreement, automate performance, hold assets in escrow, or merely provide technical infrastructure? O'Shields' description of blockchain smart contracts as legal agreements should be supplemented by this functional distinction because not every coded operation is a contract (O'Shields, 2017). Once the function is identified, the court can apply the relevant legal doctrine. If the code expresses offer and acceptance, formation rules apply. If it performs an existing obligation, performance and breach rules apply. If it records evidence, evidentiary rules apply. If it transfers assets without valid basis, restitution and liability rules apply. This method prevents both over-recognition and under-recognition of smart contracts.

From a legislative perspective, Iranian law would benefit from clearer standards on smart contracts, but recognition does not require waiting for a comprehensive smart-contract statute. Existing principles of contract law and electronic commerce can already support many smart-contract transactions. Nejatzadegan and Soltani's analysis of general validity conditions confirms that smart contracts can be examined within the ordinary structure of Iranian private law (Nejatzadegan & Soltani, 2023). However, future clarification would be useful regarding cryptographic signatures, attribution of automated acts, legal effect of code-prose conflicts, liability for coding errors, oracle failure, digital-asset restitution, and expert interpretation of code. Such clarification would not create a separate universe of blockchain law; it would adapt existing doctrines to new technological forms.

The best doctrinal conclusion is that smart contracts should be treated neither as automatically valid nor as inherently invalid. They should be treated as legally relevant digital arrangements whose validity depends on the same substantive requirements that govern contracts generally. Szabo's original vision of smart contracts emphasized the possibility of embedding contractual performance into digital systems (Szabo, 1996). That vision has become technically more realistic through blockchain and distributed ledgers, but legal validity still depends on law. In Iranian law, smart contracts can have contractual value when they are connected to genuine intention, valid consent, legal capacity, definite subject matter, and lawful purpose. Their greatest promise lies in performance, evidence, and transaction efficiency; their greatest risks lie in ambiguity, inflexibility, anonymity, coding error, and unlawful use. A balanced legal model should recognize their usefulness while preserving judicial authority to examine validity and provide remedies.

## 6. Conclusion

Smart contracts represent one of the most important developments in the digital transformation of contract law. They do not merely change the medium through which contracts are written or communicated; they change the relationship between agreement and performance by embedding execution into code. This feature gives smart contracts practical power, but it also creates legal uncertainty. A transaction may be executed automatically before a court has examined whether the parties had valid consent, whether they possessed legal capacity, whether the subject matter was definite, or whether the purpose of the transaction was lawful. For this reason, the legal analysis of smart contracts must begin with contractual validity rather than technological performance.

From the perspective of Iranian law, smart contracts should be assessed within the existing framework of contract law. The general conditions of contractual validity remain applicable. Intention and consent may be expressed through digital conduct, interaction with code, deployment of a smart contract, or cryptographic authorization, but these acts must genuinely indicate legal will. Capacity remains necessary, and technical control over a wallet or private key should not be confused with legal competence or representative authority. The subject matter must be legally definite, not merely technically identifiable. The purpose of the transaction must also be lawful, because code cannot legitimize a transaction that violates mandatory rules or public order.

The analysis shows that smart contracts may be valid under Iranian law, but their validity cannot be presumed solely from automatic execution. Code can be a means of expressing contractual terms, a method of performance, a form of electronic evidence, or a technical mechanism attached to a broader agreement. However, code is not a substitute for the legal foundations of contract. If the parties' intention is defective, if consent is obtained through fraud or duress, if the party lacks capacity, if the subject matter is uncertain, or if the transaction has an unlawful purpose, the smart contract should not be treated as valid merely because it has operated successfully on a digital network.

The most appropriate model for Iranian law is the hybrid model. In this model, a legally understandable contract defines the parties, obligations, governing law, dispute-resolution mechanism, liability rules, and priority between written terms and code, while the smart contract automates selected aspects of performance. This model preserves the efficiency of automation while maintaining the interpretive and corrective functions of law. It is especially suitable for transactions involving payment, escrow, digital access, licensing, and other objective obligations that can be translated into clear coded conditions. It is less suitable for complex obligations requiring judgment, fairness, discretion, or continuous human evaluation.

Smart contracts also require careful treatment under electronic commerce principles. Their records, signatures, timestamps, and transaction logs may provide strong evidence of digital conduct, but such evidence must remain legally interpretable. A cryptographic signature may show technical authorization, but it should not be treated as conclusive proof of valid consent in cases of theft, hacking, coercion, mistake, or unauthorized use. Attribution must be based on authorization, control, and legal responsibility. Courts may need expert assistance to interpret code, determine the meaning of technical records, and assess whether the coded operation corresponded to the parties' actual agreement.

The main legal challenges are ambiguity, inflexibility, coding error, oracle failure, pseudonymity, consumer protection, cross-border enforcement, and the possible conflict between code and written agreement. These challenges do not justify rejecting smart contracts. They show that smart contracts must be integrated into legal doctrine with caution. The legal system should recognize their usefulness in reducing transaction costs and improving performance certainty, while preserving judicial power to examine validity, interpret intention, correct unjust outcomes, and provide remedies.

In conclusion, smart contracts can have a valid place in Iranian contract law when they satisfy the ordinary requirements of contractual validity and when their electronic operation can be reliably attributed to legally responsible parties. Their technological form should be treated as a new method of contracting and performance, not as an autonomous legal order outside the Civil Code and electronic commerce principles. The future development of Iranian law should therefore move toward recognition accompanied by regulation: recognition of coded agreements and automated performance where legal requirements are met, and regulation of attribution, evidence, liability, interpretation, and remedies where technological execution creates legal risk.

## Ethical Considerations

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

## Acknowledgments

Authors thank all who helped us through 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**

Allen, T., & Widdison, R. (1996). Can Computers Make Contracts? *Harvard Journal of Law & Technology*, *9*(1), 25-52.

Clack, C. D., Bakshi, V. A., & Braine, L. (2016). Smart Contract Templates: Foundations, Design Landscape and Research Directions. https://arxiv.org/abs/1608.00771

De Filippi, P., & Wright, A. (2018). *Blockchain and the Law: The Rule of Code*. Harvard University Press. https://www.hup.harvard.edu/books/9780674976429

Fairfield, J. A. T. (2014). Smart Contracts, Bitcoin Bots, and Consumer Protection. *Washington and Lee Law Review Online*, *71*(2), 35-50. https://scholarlycommons.law.wlu.edu/wlulr-online/vol71/iss2/3/

Giancaspro, M. (2017). Is a 'Smart Contract' Really a Smart Idea? Insights from a Legal Perspective. *Computer Law & Security Review*, *33*(6), 825-835. https://doi.org/10.1016/j.clsr.2017.05.007

Grimmelmann, J. (2019). All Smart Contracts Are Ambiguous. *Journal of Law & Innovation*, *2*(1), 1-22. https://repository.law.upenn.edu/jli/vol2/iss1/1/

Mik, E. (2017). Smart Contracts: Terminology, Technical Limitations and Real World Complexity. *Law, Innovation and Technology*, *9*(2), 269-300. https://doi.org/10.1080/17579961.2017.1378468

Nejatzadegan, S., & Soltani, M. (2023). Analysis of General Conditions of Smart Contracts Validity from Iranian and American Legal Perspective. *Legal Research Quarterly*, *25*(Special Issue of Law & Technology), 303-335. https://doi.org/10.52547/jlr.2023.226492.2144

O'Shields, R. (2017). Smart Contracts: Legal Agreements for the Blockchain. *North Carolina Banking Institute*, *21*, 177-194. https://scholarship.law.unc.edu/ncbi/vol21/iss1/11/

Raskin, M. (2017). The Law and Legality of Smart Contracts. *Georgetown Law Technology Review*, *1*(2), 305-341. https://georgetownlawtechreview.org/wp-content/uploads/2017/05/Raskin-1-GEO.-L.-TECH.-REV.-305-.pdf

Savelyev, A. (2017). Contract Law 2.0: 'Smart' Contracts as the Beginning of the End of Classic Contract Law. *Information & Communications Technology Law*, *26*(2), 116-134. https://doi.org/10.1080/13600834.2017.1301036

Sklaroff, J. M. (2017). Smart Contracts and the Cost of Inflexibility. *University of Pennsylvania Law Review*, *166*(1), 263-303. https://scholarship.law.upenn.edu/prize_papers/9/

Szabo, N. (1996). Smart Contracts: Building Blocks for Digital Markets. *Extropy: The Journal of Transhumanist Thought*(16). https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

Szabo, N. (1997). Formalizing and Securing Relationships on Public Networks. *First Monday*, *2*(9). https://doi.org/10.5210/fm.v2i9.548

Werbach, K., & Cornell, N. (2017). Contracts Ex Machina. *Duke Law Journal*, *67*(2), 313-382. https://scholarship.law.duke.edu/dlj/vol67/iss2/2/

Wright, A., & De Filippi, P. (2015). Decentralized Blockchain Technology and the Rise of Lex Cryptographia. https://doi.org/10.2139/ssrn.2580664