# Challenges and Solutions for Establishing the Parties' Intent in Blockchain-Based Contracts under Iranian and European Law

**1. Peyman Moradi: Department of Law, Ya.C., Islamic Azad University, Yazd, Iran**
**2. Ghazaleh Kabirabadi*: Assistant Professor, Department of Law, Y.C., Islamic Azad University, Yazd, Iran**
**3. Majid Dehghan Chenari: Department of Law, Bafg.C., Islamic Azad University, Bafgh, Iran**
**3. Mohammad Amini: Department of Computer, Ya.C., Islamic Azad University, Yazd, Iran**

*Correspondence: Ghazaleh.kabirabadi@iau.ac.ir

**Abstract**

Blockchain-based contracts, as a new generation of digital obligations, provide a self-executing and decentralized method for structuring contractual relationships, in which the role of human will is fundamentally transformed when confronted with automated mechanisms. In this context, establishing the parties' intent—one of the identity-defining elements of any legal agreement—faces challenges such as user anonymity, disintermediation, reliance on pre-determined code, and difficulties in identifying the moment and content of consent. The main issue addressed by this research is how a valid and legally attributable intent of the parties can be established in blockchain contracts under Iranian and European law, and what conflicts arise between traditional doctrines of intention and consent and technological mechanisms. This study adopts a descriptive–analytical method with a comparative approach. Data were collected through the examination of statutory instruments, specialized technology regulations, judicial decisions, and up-to-date scholarly literature. The analytical tools include a limited empirical review of sample smart contracts, legal analysis of code, and a comparative interpretation between classical contract law principles and European Union regulations. The findings indicate that although blockchain technology offers transparency, immutable record-keeping, and automation of obligations, shortcomings such as the lack of reliable identity verification, the possibility of programming errors, difficulties in applying traditional theories of intent, and conflicts between code and the parties' actual will create serious ambiguities in establishing consent. The study proposes the adoption of supplementary regulations on digital identity verification, mandatory inclusion of declaratory layers, the possibility of judicial review of code, and the development of integrated frameworks bridging technology and law, in order to strike a balance between automation and human intent.

**Keywords:** Blockchain, parties' intent, smart contract, digital identity verification, Iranian law, European law.

Received: 06 January 2026
Revised: 30 April 2026
Accepted: 05 May 2026
Initial Publication 08 May 2026
Final Publication 01 January 2027



**Citation**: Moradi, P., Kabirabadi, G., Dehghan Chenari, M., & Amini, M. (2027). Challenges and Solutions for Establishing the Parties' Intent in Blockchain-Based Contracts under Iranian and European Law. *Legal Studies in Digital Age*, 6(1), 1-13.

## 1. Introduction

In recent years, digital transformation—particularly in the field of distributed ledger technologies—has confronted the traditional structure of contracts with new questions. Blockchain, with features such as decentralization, immutable data recording, and the capacity for self-executing obligations, has created a new platform for contract formation known as smart contracts or "code as contract." This technology has not only transformed the methods of creating, interpreting, and performing contracts, but has also subjected the fundamental concept of the parties' intention and consent to a serious redefinition. In the traditional model, the parties' intent could be established through words, conduct, or external indications, allowing judges to infer the true intention of the contracting parties by reference to surrounding circumstances. By contrast, in blockchain-based contracts, this process takes place within an encrypted, decentralized, and code-driven environment, thereby generating new legal challenges in establishing and relying upon the parties' intent (Smith, 2021).

Core elements such as the anonymity or pseudonymity of users, the automated execution of obligations, the limited or sometimes eliminated role of human intermediaries, and the difficulty of judicial intervention after automatic code execution have led to situations in which it is unclear how the parties' true intent was formed, what its scope is, and which element should prevail in the event of a conflict between actual intent and the content of the code (Werbach & Cornell, 2017). These questions are of particular importance in Iranian law, where contractual foundations rest on declaratory intent and the genuine agreement of the parties. In European law, although recent instruments such as the MiCA Regulation and amendments to the eIDAS2 framework seek to align legal regimes with emerging technologies, significant gaps remain with respect to the establishment of intent, liability arising from coding errors, and the validity of self-executing contracts (European, 2023).

The importance of this issue becomes more evident given the rapid growth in the use of blockchain-based contracts across sectors such as decentralized financial markets, crypto-assets, supply chains, insurance, and digital services. In many of these areas, agreements are concluded not through classical negotiation, but through clicking, digital signatures, or direct interaction with smart interfaces, and parties may not be fully aware of the legal consequences of their commitments. Moreover, blockchain environments are designed so that transactions and agreements, once recorded, are effectively irreversible or immutable, shifting the importance of accurately establishing intent to the pre-execution stage. From a contract law perspective, this necessitates a reassessment of tools for discovering intent, criteria for contractual validity, and the scope of liability arising from discrepancies between code and actual intent (Raskin, 2019).

From a theoretical standpoint, several overarching challenges can be identified. The first is the overlap or conflict between "actual intent" and "expressed intent" in smart contracts. In Iranian legal tradition, actual intent is of fundamental importance, and defects such as mistake, duress, or fraud may render a contract ineffective. However, in code-based contracts, the prevailing assumption is often that "code is law," meaning that what is executed is the definitive outcome of programming instructions rather than the parties' subjective intent. This increases the risk that the practical result of the contract may diverge from the parties' intentions (Zargari, 2021). The second challenge is the issue of identity verification and authentication of the parties. In blockchain systems, which are inherently based on relative anonymity, this constitutes one of the most significant obstacles to aligning contractual institutions with the traditional requirements of Iranian law. In European Union law, efforts have been made to provide reliable identity verification through mechanisms such as advanced electronic signatures; however, in practice, many blockchain-based contracts are concluded outside formal identity verification frameworks, casting doubt on their legal validity (Kuner, 2020).

The third challenge concerns the difficulty of applying traditional principles of contractual interpretation. In the Iranian legal system, judges typically rely on principles such as interpretation in favor of the weaker party, discovery of the parties' common intent, and consideration of custom and usage to resolve disputes. In self-executing contracts, however, the contract text consists not of words but of machine-readable code, and judges are generally not experts in programming languages. Consequently, the scope for human interpretation is limited, and the execution of code is often treated as producing a definitive outcome without judicial intervention. This issue is also debated in Europe, where some courts have accepted intervention to mitigate unfair consequences of code execution, while others prioritize the technical execution of transactions.

Alongside these theoretical challenges, significant research gaps exist in the literature. First, a substantial portion of Iranian scholarship remains limited to general discussions of blockchain and smart contracts, with little in-depth analysis of the

relationship between the parties' intent and technical mechanisms. Second, comparative studies between Iran and Europe are fragmented and often focus on issues such as data protection or digital asset ownership rather than fundamental contract law concepts. Third, no coherent model has yet been proposed to reconcile traditional contractual principles with technology-based mechanisms, a gap that may lead to complex and multifaceted disputes in the future (Behzadi, 2022).

Methodologically, the present study adopts a descriptive–analytical approach with a comparative perspective between Iranian and European law. Data are drawn from library-based sources, including statutes, regulations, international instruments, judicial decisions, and scholarly studies. To better understand the relationship between intent and code, the research also incorporates technical analysis of sample smart contracts and technical documentation of blockchain platforms. This approach enables examination of the theoretical foundations of intent and consent in Iranian and European law while simultaneously analyzing the practical operation of contractual code in real-world settings. The research tools include legal analysis, comparative study, review of technical documentation, and examination of executed contracts in digital markets. From an applied perspective, key markets analyzed include crypto-asset markets, decentralized finance platforms, NFT marketplaces, blockchain-based supply chain platforms, and smart insurance contracts. Owing to their complexity and extensive use of blockchain-based contracts, these markets provide a natural laboratory for analyzing challenges related to the establishment of intent.

Ultimately, the complexity of blockchain technology and its growing role in economic and legal domains underscore the need to reconsider traditional contractual concepts and to build a bridge between human intent and automated mechanisms. Existing research gaps—such as the absence of a coherent framework for establishing intent, the lack of clear comparative rules between Iran and Europe, the limitations of traditional interpretive tools when confronting code, and challenges of identity verification—further amplify the importance of this study. Accordingly, the central research question is: How can the valid intent and consent of the parties be established and validated in blockchain-based contracts under Iranian and European law, and in the event of a conflict between code and actual intent, which should prevail?

Technological advancements and the expanding use of blockchain-based smart contracts have fundamentally challenged the traditional concept of intent and consent in contract formation. In contract law, the parties' actual intent constitutes the foundation of contractual validity and enforceability, and without its establishment, no obligation attains legal legitimacy. Blockchain-based contracts, however, are generally designed through self-executing code and not only lack conventional verbal or written structures, but often involve parties who do not know one another, with human interaction reduced to a minimum. The core question therefore arises: in the absence of traditional tools for establishing intent, what mechanisms do legal systems offer to identify the parties' will, and can software code serve as a valid substitute for classical legal concepts?

In Iranian law, which is grounded in voluntarism and the requirement of intent and consent under Article 190 of the Civil Code, "intent" is a personal and psychological concept that must be inferred from verbal or practical indications. In blockchain contracts, however, such indications are either absent or fundamentally transformed. For example, the confirmation of a transaction on the network, the submission of a digital signature, or the invocation of a smart function may all constitute expressions of intent; yet the jurisprudential and legal basis for recognizing these acts remains in need of analysis. Moreover, the immutability of blockchain renders legal remediation difficult in cases of mistake or lack of genuine intent, creating gaps in the application of rules on liability, nullity, and rescission.

In European Union law, although instruments such as Regulation (EU) 2022/858 and guidance issued by ESMA and EBA have strengthened recognition of distributed ledger technologies, the establishment of intent and the validity of smart contracts remain contested. The EU has tended toward an "objective intent" approach based on digital conduct and user interaction with the network. Nevertheless, the absence of a uniform definition of smart contracts, legislative divergence among Member States, and misalignment between traditional contract rules and the self-executing, irreversible nature of blockchain continue to generate significant uncertainty. From this perspective, a comparative analysis of Iran and Europe provides an opportunity to identify strengths and weaknesses in two distinct legal approaches.

Practical challenges further complicate the issue. Many users and developers lack sufficient legal knowledge and rely solely on code rather than drafting clear legal agreements. Where code contains errors, ambiguities, or unexpected behavior, discerning the parties' actual intent becomes difficult. Additionally, the use of technical intermediaries such as wallets, trading platforms, and oracles introduces third-party elements into the agreement process, complicating the determination of whose intent and authority are being expressed. This situation increases legal risk and undermines transactional security.

Accordingly, the fundamental problem addressed by this research is how intent and consent are formed in blockchain-based contracts, by what criteria they can be established, and what mechanisms Iranian and European legal systems provide to resolve ambiguities arising from the self-executing nature of smart contracts. The existing research gap stems from the absence of systematic comparative analysis, limited clarity in Iranian law, and a lack of harmonized interpretations in European law. This study seeks, through examination of theoretical foundations, regulatory frameworks, and practice, to answer how legal systems can establish the parties' intent in blockchain-based self-executing contracts and prevent legal conflicts.

## 2. Literature Review

One of the earliest theoretical discussions of smart contracts was introduced by Nick Szabo in the 1990s through the concept of "code as contract." Szabo argued that smart contracts could serve as precise substitutes for human will, with automated code execution eliminating human error (Szabo, 1997). Critics such as Lawrence Lessig, however, regarded this view as overly simplistic, arguing that code cannot fully replace legal intent because contracts possess social and intentional dimensions that programming cannot entirely capture (Lessig, 2006).

Subsequently, Werbach and Cornell advanced the theory of Contracts ex Machina, contending that code is merely an execution tool and cannot represent the parties' actual intent, as it focuses on future behavior rather than past will (Werbach & Cornell, 2017). This position was challenged by Raskin, who argued that user interaction with the network and acceptance of code mechanisms constitute implicit intent, and that judges should seek intent in digital behavior rather than in subjective mental states (Raskin, 2019). This debate reflects two overarching approaches: actual intent versus objective digital intent. In European law, extensive research has emerged in the past decade. Kuner argues that the lack of reliable identification mechanisms undermines the legal validity of smart contracts (Kuner, 2020). Conversely, scholars such as Greenberg, citing eIDAS2 reforms, contend that advanced electronic signatures and EU digital identity systems can address much of this gap (Greenberg, 2022). These divergent views demonstrate the absence of a unified mechanism for establishing intent at the European level. Regarding the interpretation of smart contracts, Surden adopts a cautious approach, maintaining that judicial interpretation must remain part of contract execution because code often fails to express true intent (Surden, 2022). By contrast, some scholars argue that judicial intervention in self-executing contracts undermines the essence of blockchain and challenges the principle of immutability. This dichotomy between "legal flexibility" and "technical certainty" represents a central debate in the literature.

In Iranian scholarship, early research largely focused on introducing blockchain technology. For instance, Zargari offered one of the first serious jurisprudential analyses of self-executing contracts, arguing that smart contracts are valid only if genuine declaratory intent exists prior to code execution (Zargari, 2021). This view was criticized by Behzadi, who emphasized that many blockchain interactions lack preliminary negotiations and that intent should instead be inferred from digital interactions and user behavior (Behzadi, 2022). Some Iranian authors, such as Nazemi, argue that the immutability of transactions enhances transparency and security, thereby providing a new criterion for establishing intent (Nazemi, 2022). Opponents such as Moradi, however, reject this argument, asserting that immutability does not equate to validity, since the absence of genuine intent cannot be cured by immutable recording (Moradi, 2023).

On liability for coding errors, foreign scholars such as Ferguson and Wright view programming errors as analogous to mistakes in intent, allowing for contract invalidation or correction (Ferguson & Wright, 2018). Others, such as Peltz, argue that developers are not contracting parties and that liability should fall on users who execute the code (Peltz, 2019). This divergence complicates the theoretical understanding of the tripartite relationship among user, developer, and network.

Iranian studies on developer liability remain limited, though works such as Mousavi have compared the developer's role with jurisprudential doctrines of causation and liability (Mousavi, 2022). Some scholars argue that the developer functions as a "cause" rather than a "direct actor," placing primary liability on the user who executes the transaction. Critics counter that users often lack the capacity to detect technical errors, and if intent is formed on the basis of incomplete information, valid consent does not exist.

Comparative studies between Iran and Europe are scarce. Research such as Paknejad attempts to compare traditional intent principles with European regimes but often lacks technical blockchain analysis (Paknejad, 2023). Conversely, European studies frequently adopt a technical perspective while neglecting the theoretical foundations of intent. This asymmetry has hindered comprehensive comparative analysis and underscores the need for interdisciplinary research.

Overall, the literature on establishing intent in blockchain-based contracts is fragmented, conflicting, and often one-dimensional. Some scholars locate intent in digital behavior, others emphasize subjective will, some regard code as sufficient, and others insist on the primacy of human interpretation. In Iran, the voluntarist nature of the legal system further intensifies these ambiguities. Consequently, there remains a clear need for comprehensive research that examines theoretical foundations while analyzing technical mechanisms and European regulatory frameworks—an imperative that justifies the present study.

## 3. Theoretical Foundations of the Research

The theoretical foundations for establishing intent in blockchain-based contracts emerge from the intersection of two distinct epistemic domains. The first is the traditional theory of intent and consent in contract law, which has long regarded will as the central pillar in the formation of obligations. The second is blockchain technology and smart contracts, which, through algorithmic logic and automated execution, introduce a novel conception of agreement. In Iranian law and many European legal systems, intent and consent constitute fundamental conditions for the formation of a contract, and their absence renders the contract void or ineffective. In the classical view, intent is based on the declaration of will through words, gestures, or writing, and judges may infer it from contextual indications and surrounding circumstances. With the advent of decentralized blockchain technology, however, declarations of intent take new forms, such as digital signatures, private keys, encrypted messages, and smart contract code. This development confronts traditional contract theories with new questions, including whether algorithmic code can be regarded as an instrument for expressing intent, or whether algorithms merely serve as tools for executing agreed terms, with intent needing to be established at a human layer external to the code.

In traditional contract theory, the principle of correspondence between offer and acceptance forms the core of intent analysis. In blockchain environments, however, many interactions are automated and time-stamped, blurring the boundaries between offer, acceptance, and even contract performance. According to some European scholars, smart contracts are less "contracts" than "tools for enforcing agreements," and the parties' intent must therefore be established outside the code (Werbach, 2018). By contrast, theorists such as Wright and De Filippi argue that code and individuals' digital behavior on the chain may themselves constitute declarations of intent, because by submitting a transaction, activating a contract, or applying a digital signature, users perform acts equivalent to intentional conduct in the physical world (Wright & De Filippi, 2019). In Iranian law, the prevailing view is that intent must be inferred from "conduct customarily indicative of will" and is not limited to verbal or written expressions. Accordingly, it may be argued that user behavior on the blockchain can amount to a declaration of intent, provided that sufficient indications of attribution and awareness are present (Kazemi, 2022).

A fundamental issue within the theoretical framework concerns the distinction between "consent" and "intent." In Iranian law, consent signifies that the will is free from defects such as mistake, duress, or fraud (Heydari, 2021). This raises the question of how claims of duress or mistake can be substantiated in blockchain environments, where transactions are irreversible. Some legal technology scholars argue that blockchain's transparency and immutable record-keeping make proof of mistake more difficult, as courts must reconcile on-chain records with the claimant's alleged reality (Allen, 2020). In Iran as well, although the principle of autonomy of will is recognized, proving mistake or duress in digital contexts requires technical tools such as network traffic analysis, digital signature logs, and wallet data. Consequently, the theoretical foundations for establishing consent must necessarily bridge traditional legal rules and technical instruments.

In the realm of contract interpretation theories, a critical question arises: are smart contracts interpretable? In Iranian law, principles such as the parties' common intent, custom, and supplementary statutory rules serve as interpretive tools. Smart contracts, however, are typically written in code and are often described functionally as "non-interpretable," because code executes exactly what is written—no more and no less (Karimi, 2023). As Szabo, the pioneer of smart contracts, famously argued, code can structure and secure contractual relationships through automated mechanisms (Szabo, 1997). Many legal scholars have criticized this view, arguing that the legal nature of smart contracts must refer back to the parties' antecedent

intent rather than the literal meaning of code, since code is merely a technical instrument and the parties' intent may be broader or narrower than what the code executes. Accordingly, contract interpretation theories require redefinition when applied to self-executing contracts.

From the perspective of liability theories, one theoretical foundation related to intent concerns the role of technological intermediaries. Blockchain is based on decentralization and lacks a single contractual intermediary, yet code developers, wallet operators, and platforms interacting with smart contracts may influence the formation or weakening of the parties' intent. In European literature, this issue is discussed under the theory of "programmer liability." If code is defective or produces undesirable behavior, can such defects undermine the establishment of the parties' genuine intent? Theorists such as Raskin argue that in such circumstances, traditional doctrines of mistake and fraud should apply, as coding errors constitute a form of mistake regarding the subject matter (Raskin, 2019). Others contend that smart contracts are the result of joint action by parties and programmers, necessitating new mechanisms to distinguish human intent from the network's technical behavior. In Iranian law, programmer liability has not been expressly regulated, creating a significant theoretical gap.

Within electronic signature theory, the attribution of intent is of particular importance. Iranian e-commerce laws and the EU's eIDAS Regulation recognize digital signatures as valid and equivalent to handwritten signatures, provided that attribution and authenticity can be established (Yazdan-Panah, 2019). In blockchain systems, each transaction is signed with a private key that technically functions as a signature. The challenge, however, is that possession of a private key does not definitively establish the identity of a specific natural or legal person, due to the possibility of shared use, key theft, or unauthorized access. Digital identity theories in blockchain lack unified standards, compelling courts in both Iran and Europe to rely on external indications, interaction histories, and supplementary technical evidence to establish intent. Thus, the theoretical foundations of digital signatures in blockchain require the development of supplementary rules for attributing intent.

The concept of the "irreversibility of transactions" constitutes another core theoretical element of blockchain. In contract law, rescission or invalidation of contracts is permitted under certain conditions, whereas blockchain lacks such flexibility unless reversal mechanisms or control modules are designed at the application layer (Shafi'i, 2020). The theoretical question arises as to whether irreversibility is compatible with traditional principles for remedying defects in consent. Many scholars argue that this rigidity may lead to legal vulnerability and necessitates the design of corrective models. This debate contributes to the evolution of intent theory, because if annulment or rescission becomes impossible after automated execution, the element of consent effectively loses its function.

A major challenge also exists in the theoretical foundations of "common intent." In many smart contracts, users enter interactions with a single click, often without carefully reading the code or possessing sufficient technical knowledge. Consequently, scholars such as Hacker argue that common intent in blockchain contexts is often "constructive" rather than "actual" (Hacker, 2021). In Iranian law, awareness of contractual terms is a condition for valid consent, and this requirement becomes ambiguous in code-based interactions. Thus, the theoretical basis of common intent in algorithmic environments requires substantial reconsideration.

Trust occupies an important place in contract theory as well. Blockchain is designed around the notion of being "trustless," yet from a legal perspective, trust cannot be entirely eliminated, because concepts such as awareness, choice, mistake, and transactional motives are grounded in trust. Scholars in law and technology argue for distinguishing between "institutional trust" and "technical trust." Blockchain reduces institutional trust but remains dependent on technical trust in code and networks. Therefore, the theoretical foundations for establishing intent must differentiate between these forms of trust and clarify how user behavior on the network can indicate rational intent.

Ultimately, the theoretical foundations of this research demonstrate that establishing intent in blockchain environments is neither purely a legal nor purely a technical issue, but rather lies at the intersection of these two epistemic systems. The manifestation of will in digital behavior, its attribution to users, the interpretability of smart contracts, the role of programmers, liability for coding errors, the absence of transaction reversibility, and challenges related to users' awareness of code terms all indicate that the traditional theory of intent requires rearticulation in the context of blockchain technology.

### *3.1. The Theory of Autonomy of Will and Its Transformation in the Context of Digital and Smart Contracts*

The theory of autonomy of will constitutes one of the most fundamental foundations of contract law in classical legal systems, including both Iranian and European law. This theory rests on the assumption that the free and informed will of individuals is the primary source of contractual obligations, while the legislature plays merely a regulatory and supplementary role in private relations. In other words, a contract is viewed as the manifestation of the common will of two or more persons, and as long as this will is properly formed, the law is obliged to protect it. In Iranian law, this foundation is reflected in Articles 10, 183, and 190 of the Civil Code, and many Iranian jurists have described will as the "spirit" of the contract (Jafari Langroudi, 2019). In European law, contractual freedom has likewise been regarded as a hallmark of classical legal liberalism, forming the basis of traditional contract rules in French, German, and English legal systems (European, 2019).

With the emergence of digital contracts—particularly blockchain-based smart contracts—this theory has encountered conceptual and functional challenges. In traditional contracts, will is expressed through words, writings, or legal acts, and the offer-and-acceptance process unfolds in a manner intelligible to humans. In smart contracts, however, a significant portion of the expression of will is manifested not in natural language, but in programming languages and algorithmic logic. This has led some jurists to speak of a transition from human will to machine logic. Within this framework, the parties' will must be reflected not only at the mental and legal levels, but also at the technical and coding levels, introducing new complexities into the theory of autonomy of will.

Two principal approaches can be identified in the legal literature regarding this transformation. The first emphasizes the continued validity of the autonomy of will theory, viewing smart contracts as merely new instruments for expressing traditional will. From this perspective, software code replaces traditional modes of expressing intent without altering the legal essence of the contract. For example, comparative research between Iranian and French law has argued that smart contracts should be regarded as a logical continuation of contractual freedom rather than a departure from it (Dehghani-Tafti et al., 2022). In European law as well, it is emphasized that classical contract principles can still govern smart contracts, provided that mechanisms for establishing intent are properly designed.

The second approach contends that smart contracts have subjected the classical theory of autonomy of will to a form of structural transformation. From this viewpoint, when contract execution becomes automated and immune to human intervention, the role of the parties' subsequent will is significantly diminished, and what prevails is the governance of code. Scholars describe this situation by noting that in blockchain-based contracts, code gradually replaces legal norms and creates a form of autonomous technical order (Werbach & Cornell, 2017). This perspective critiques the traditional approach and underscores the need to redefine the theory of autonomy of will in the digital age.

This debate has increasingly emerged in Iranian law as well. Some Iranian scholars argue that the self-executing nature of smart contracts may conflict with the principle of continuous consent, because once code is deployed on the blockchain, human will is effectively removed from the execution cycle (Soleimani & Eskandari, 2025). Others, however, have sought to articulate a theory of "enhanced autonomy of will," suggesting that if the design and approval processes are properly conducted, human will can remain valid even in digital environments (Amiri-Moqaddam, 2025).

Overall, these developments indicate that the theory of autonomy of will, when confronted with digital and smart contracts, has neither completely collapsed nor entirely preserved its traditional form. Rather, it is evolving toward a more flexible configuration in which human will must extend from the realm of mental intent and linguistic expression into the realm of technical and algorithmic design. In the blockchain era, will thus acquires two layers: a legal–mental layer and a technical–code layer. Recognizing and regulating these layers in Iranian and European law requires the development of evidentiary rules, transparency mechanisms, standardization of coding languages, and clear linkages between legal text and executable code.

In conclusion, the theory of autonomy of will in the context of digital and smart contracts is undergoing a transformation from a purely human-centered theory to a hybrid model in which human will and machine logic jointly constitute the basis for contractual obligations. This transformation presents both Iranian and European legal systems with an opportunity to reconsider traditional contractual foundations and to establish a sustainable balance between technological efficiency and the fundamental principles of contractual justice.

## 4. Discussion and Analysis

The introduction of blockchain technology and smart contracts into the realm of contractual relations has fundamentally transformed the classical foundations for establishing the parties' intent and will. In traditional legal systems—particularly in Iranian law, which is influenced by Imami jurisprudence and the theory of autonomy of will—intent to create legal effects and the parties' consent are regarded as essential pillars of contractual validity. However, in blockchain-based contracts, the direct and classical relationship between the parties' mental states and their legal conduct is disrupted by technical structures and algorithmic intermediaries. In such contracts, human decisions are recorded in the form of digital data and coded instructions, and instead of contract performance depending on the parties' continuing will, it is entrusted to the predetermined logic of machines. This raises a fundamental question: can such a mechanism genuinely represent valid legal intent, or are we merely witnessing the substitution of human will with machine will, the legal legitimacy of which is questionable?

In Iranian law, intent and consent are not merely formal or outward phenomena; rather, they are grounded in awareness, freedom, and the seriousness of will. Article 190 of the Iranian Civil Code recognizes intent and consent—alongside capacity, a definite subject matter, and lawful purpose—as the essential elements of a valid contract. In smart contracts, users typically enter into an automated process by clicking an option or applying a digital signature, the consequences of which are executed automatically. The key issue here is whether such a click or electronic confirmation can be considered equivalent to profound legal intent, or whether it merely reflects a superficial and technical form of consent. Research has shown that in many of these contracts, the gap between the appearance of consent and the reality of intent widens, creating the risk of purely formal contracts devoid of genuine volitional substance (Dehghani-Tafti et al., 2022). From this perspective, blockchain-based contracts face serious challenges in proving the internal element of intent, as technical systems are incapable of capturing and analyzing the qualitative mental dimensions of will and can only record its external manifestations.

In European law as well, although the theoretical foundations differ in some respects from Iranian law, the necessity of establishing an intention to create legal relations remains central. Particularly in English law and continental European legal systems, the parties' intention to assume legal obligations is a prerequisite for contractual validity. In these systems, smart contracts have similarly raised the question of whether agreements formed largely at the level of code and without human negotiation can truly reflect genuine legal intent. Although European judicial practice has not yet extensively addressed this issue, certain discussions involving digital and self-executing contracts have emphasized the requirement of informed and real consent (European, 2019). This demonstrates that the challenge of establishing intent is common across legal systems and has become a transnational concern.

One of the most important focal points of discussion is the issue of the parties' knowledge and awareness of the contract's actual terms. In traditional contracts, terms are usually drafted in natural language, allowing for negotiation, questioning, and modification. In smart contracts, however, a substantial portion of the terms appears in the form of programmed code, which is extremely difficult for non-specialists to understand. This creates a form of informational asymmetry between technical designers and ordinary users, potentially undermining informed intent, as one party may accept the contract without fully understanding its legal and economic consequences. In Iranian law, this situation can be analyzed through principles such as excessive uncertainty and ignorance, since ambiguity regarding essential elements or insufficient awareness of consequences casts doubt on contractual validity. European law similarly emphasizes consumer protection and contractual transparency, allowing complex contracts lacking adequate disclosure to be invalidated. Analytically, a distinction must be drawn between technical intent and legal intent. Technical intent refers to the process by which a user enters an automated system through digital tools, such as private keys, cryptographic signatures, clicks, or machine confirmations. Legal intent, by contrast, is a deeper concept involving understanding, evaluation of benefits and risks, and a conscious decision to enter into a legal obligation. The core problem in blockchain contracts is that technical intent often automatically replaces legal intent without any mechanism to assess the quality of that decision. In European systems, particularly in consumer protection and standard-form contracts, efforts have been made to reduce this gap through mandatory disclosure of key information and the design of more transparent user interfaces (European, 2023). In Iranian law as well, it has been proposed that explanatory pre-contracts and transparency clauses be recognized as prerequisites for the validity of smart contracts.

Another issue concerns good faith and the parties' true motivations. In traditional contracts, courts can examine pre- and post-contractual behavior, correspondence, negotiations, and external indications to ascertain real intent in case of dispute. In

blockchain-based contracts, however, most interactions occur in decentralized, anonymous, or semi-anonymous environments, reducing the availability of such external indicators. Consequently, some European scholars speak of a "crisis of intent proof" in self-executing contracts. In Iranian law, this challenge is compounded by an evidentiary system that relies heavily on traditional forms of proof such as documents, testimony, and customary presumptions, all of which face limitations in digital environments (Soleimani & Eskandari, 2025).

In response to these challenges, various reform-oriented approaches have been proposed. One of the most significant is the design of hybrid contracts. In this model, the legal text of the contract is drafted in human language, explicitly specifying the parties' intent, legal effects, termination clauses, and dispute resolution mechanisms, while computer code serves merely as an execution tool. This model seeks to reduce the conflict between human will and machine logic and to prioritize legal intent. In Iranian law, it has been suggested that legislators formally recognize such structures and allow reliance on the legal text independent of code (Amiri-Moqaddam, 2025). In Europe, the concept of Ricardian contracts has similarly emphasized the linkage between human-readable legal text and machine-executable code.

Comparative analysis shows that the primary difference between Iran and Europe in this field lies not in theoretical foundations, but in institutional and practical implementation. In Europe, legislative and research bodies are actively developing guidelines and techno-legal standards for smart contracts, leading to the gradual emergence of quasi-judicial practices. In Iran, however, legal gaps and lack of practical experience have left the validity of such contracts uncertain, potentially increasing future disputes due to the parties' unclear understanding of their legal obligations at the time of contract formation.

### *4.1. The Conflict Between Human Will and Machine Logic in Blockchain-Based Contracts*

The conflict between human will and machine logic in blockchain-based contracts represents one of the most fundamental theoretical and practical challenges in digital contract law. In traditional legal systems, human will is recognized as the central element of contract formation, with intent, consent, awareness, and freedom constituting the core requirements for contractual validity. Blockchain-based contracts, by contrast, operate according to automated execution logic based on pre-written code, without any human evaluation at the moment of performance. This inherent difference creates fertile ground for conflict between human will and machine logic (Werbach & Cornell, 2017).

Legally, human will has always been regarded as dynamic, interpretable, and sometimes influenced by external circumstances. Classical contract theory in Iranian law emphasizes intent and consent, a principle likewise accepted in European comparative law (Paknejad, 2023). In blockchain contracts, however, the governing logic is the rigid and non-interpretable logic of code, which executes predetermined terms regardless of the parties' actual circumstances, good faith, mistake, duress, or changes in conditions. This has led some scholars to speak of the emergence of technical will in opposition to human will (Lessig, 2006; Werbach & Cornell, 2017).

One of the most evident manifestations of this conflict appears in the issue of post-contractual change of will. In traditional contracts, freedom of contract and institutions such as rescission, mutual termination, and contract adjustment allow parties to reconsider their initial intent when circumstances change. In blockchain contracts, however, immutability and irreversibility of transactions leave little room for flexibility. Studies show that this feature transforms smart contracts from legal instruments into binding technical mechanisms that marginalize human will at the execution stage. In Iranian law, this conflict may clash with jurisprudential and legal foundations emphasizing real intent and consensualism. Since what ultimately executes is code—which may not perfectly reflect the parties' true intent—there is a serious risk of divergence between actual intent and coded intent, potentially rendering the contract void or voidable (Dehghani-Tafti et al., 2022).

European law has likewise acknowledged this conflict. Some European scholars argue that smart contracts create a form of technical normativity that replaces human will, whose legitimacy remains questionable from a legal-philosophical perspective (Lessig, 2006; Werbach, 2018). Courts, when confronted with self-executing contracts, have sought to distinguish between code as a tool and the contract as a legal agreement in order to preserve the primacy of human intent. A particularly complex aspect of this conflict concerns the translation of intent into code. Programmers often convert legal text into programming language, a process prone to error, misinterpretation, or oversimplification of legal concepts. As a result, the executing code

may diverge from what the parties actually intended, a phenomenon known in legal literature as the translation gap (Surden, 2022).

In traditional legal systems, such discrepancies are resolved through contract interpretation rules. In smart contracts, however, code is typically immune to judicial interpretation and executes rigidly. Consequently, some legal thinkers advocate a middle-ground solution: smart contracts should not replace legal contracts entirely, but rather serve as execution tools for legal agreements (Werbach & Cornell, 2017). In this model, the classical legal text remains the primary reference for determining intent, while code merely enforces obligations. This approach has gained attention in the European Union, where strategic documents emphasize preserving the centrality of human will (European, 2023).

Comparatively, European law has taken steps toward human-centered blockchain governance, while in Iranian law, these discussions remain largely theoretical. The absence of specific regulations regarding the relationship between code and human will in Iran may lead to serious disputes in the future. Iranian scholars have therefore proposed that legislators explicitly declare the precedence of actual human intent over machine logic in cases of conflict, a proposal consistent with Islamic jurisprudential foundations and Iranian civil law principles (Amiri-Moqaddam, 2025).

Ultimately, this research demonstrates that the conflict between human will and machine logic is not merely a technical issue, but a deep-rooted question in the philosophy of contract law. Ignoring human will as the basis of contractual legitimacy risks reducing contracts to engineered processes that undermine contractual justice, fairness, and protection of genuine intent. The sustainable solution lies not in replacing human will with machine logic, but in designing mechanisms that integrate the two, ensuring that machine logic serves the realization of human intent rather than opposing it. Accordingly, blockchain-based contracts must be structured so that machine logic functions solely as a means of ensuring precise execution of human intent, thereby achieving a stable balance between technological efficiency and legal legitimacy.

### *4.2. Challenges of Proving Intent Amid Technical Transparency and Code Complexity*

In blockchain-based contracts, intent and will—cornerstones of classical contract formation—face serious evidentiary challenges in a novel and complex environment. Blockchain's technical transparency is often presented as a fundamental advantage, since all transactions are immutably recorded and publicly visible; yet due to the specialized nature of recorded information, this transparency becomes an obstacle to proving genuine intent (Werbach, 2018). Blockchain data mainly consist of hashes, cryptographic addresses, digital signatures, and machine instructions, rarely reflecting legal concepts such as consent, intent, free will, or informed awareness.

A core challenge lies in the cognitive gap between what is recorded on the blockchain and what courts require to establish intent. Judges in Iranian and European systems seek evidence of real agreement, prior negotiations, conduct, and contextual factors. In smart contracts, however, the primary available evidence is often the code itself, which shows what was executed, not the level of awareness or volition behind it. Thus, technical transparency does not equate to legal transparency. Code complexity further exacerbates this evidentiary crisis. Many smart contracts are written in specialized programming languages inaccessible to non-experts. Even where a simplified legal text accompanies the contract, discrepancies between human-readable text and code execution can obscure intent (Raskin, 2019). This raises the critical question of which should prevail in case of conflict: the legal text or the executing code. Iranian law, with its emphasis on actual internal intent, may prioritize the legal text, whereas some European systems may afford greater practical weight to automated execution.

Another challenge concerns the parties' real identities. While blockchain renders transactions traceable, user identities often remain represented by cryptographic keys and addresses. This pseudo-anonymity complicates proof of who entered the contract and with what intent. Even if a digital address is shown to have signed a contract, proving that the natural or legal person behind it acted freely and knowingly remains uncertain. In Iranian law, this issue intersects with evidentiary rules traditionally based on documents, testimony, and presumptions—tools that are limited or transformed in digital contexts (Jafari Langroudi, 2019). European law, despite broader acceptance of electronic evidence, still grapples with whether blockchain data alone can demonstrate genuine intent.

In conclusion, challenges of proving intent amid technical transparency and code complexity stem from the deep divide between the language of law and the language of technology. Blockchain transparency is technical rather than legal, and code

conveys instructions rather than meaning. Until a bridge is established between these languages—through hybrid contracts, standardized legal representations of code, and recognition of specialized digital evidentiary rules—proof of intent will remain fraught with uncertainty. The sustainable solution lies not in increasing technical transparency alone, but in systematically translating technical data into legally intelligible concepts for courts.

## 5. Conclusion

The present study demonstrates that blockchain-based contracts, owing to their salient characteristics, such as self-execution, transparent and immutable data recording, and the potential elimination of traditional intermediaries, offer significant capacity to enhance contract enforceability, reduce intermediary costs, accelerate processes, and increase trust. However, these capacities are accompanied by fundamental legal challenges that must be seriously addressed in both the Iranian and European legal systems. The most important of these challenges include establishing the parties' intent in the traditional sense, namely free and informed will and mutual consent; ensuring transparency and accessibility of contractual terms; securing the parties' accurate understanding of contractual conditions; enabling the reversal or modification of contracts where necessary; and adapting existing contract law doctrines to the requirements of emerging technologies. Ultimately, without appropriate legal and technical mechanisms, many blockchain-based contracts may face uncertainty regarding their validity and binding force.

The comparative analysis between Iran and Europe reveals that Europe has developed a relatively more advanced legal framework for the acceptance of blockchain-based contracts. By contrast, Iranian law has not yet formulated specific rules or a distinct and systematic judicial approach for such contracts, and most existing studies remain theoretical and analytical. Consequently, a more pronounced legal–institutional gap is evident in Iran, one that, if left unaddressed, may expose blockchain-based contracts to serious legal risks.

One of the key findings of this research is that the parties' intent—one of the fundamental pillars of contract law—must be analyzed in smart contracts along two dimensions: first, the parties' legal intent in the traditional sense, namely the free and informed expression of agreement; and second, technical intent or machine will, namely the code that is executed. In traditional contract law, intent materializes through offer and acceptance in a context of freedom and awareness. In smart contracts, however, agreement may be formed and executed through code and machines without the parties having a full traditional understanding of the terms or having expressed a clear legal will. This structural divergence creates difficulties for both Iranian and European legal systems, although Europe, benefiting from greater practical experience and certain operational recommendations, has been able to take preliminary steps. Accordingly, solutions must be coordinated at the legal, institutional, and technical levels to ensure that the parties' intent can be reliably established.

From a remedial perspective, a balance must first be established between the contractual text, expressed in legal language, and machine code. Hybrid contracts—where the legal component is drafted in ordinary human language and the execution component is implemented through code—can provide a viable framework for establishing intent. This approach has gained some traction in Europe, where it has been recommended that legal terms be clearly disclosed to the parties prior to code execution and that adequate information be provided. In Iranian law, it has likewise been proposed that legislators enact specific regulations for blockchain-based contracts, mandating disclosure, transparency of terms, and support for mechanisms allowing contract reversal or modification when necessary.

In conclusion, while blockchain-based contracts possess significant potential to improve contractual systems, realizing this potential requires that the parties' will and intent be legally valid and verifiable. If intent is not formed openly, knowingly, and freely, or if contractual terms are structured in a way that prevents one party from attaining sufficient understanding, the contract may be vulnerable in terms of validity or enforceability. In Iran, the absence of clear regulations, established judicial practice, and sufficient practical experience exacerbates these challenges. In Europe, although a more supportive framework exists, issues such as the interaction between code and law, conflicts between human and machine will, and the delineation of liability horizons, for example under the notion of "code as law," remain unresolved.

In particular, this research conveys several clear messages for legislators, judicial bodies, and the legal community. First, Iranian legislators should urgently develop specific regulations for blockchain-based contracts that explicitly incorporate requirements of intent, information, transparency, and reversibility, and that establish mechanisms for code oversight and legal enforcement. Second, judicial and legal institutions should enhance their knowledge and capacity to understand blockchain

technology, smart contracts, and related technical issues in order to deliver well-reasoned decisions in disputes involving such contracts. Third, economic and legal actors are advised to adopt hybrid contract models that integrate legal and technical components and to clearly document the parties' intent prior to execution. Fourth, at the international and transnational levels, the development of shared frameworks, standardization of smart contract terms, and constructive cooperation between the Iranian and European legal systems can help reduce legal and technological gaps.

Furthermore, the findings indicate the need for further research in several areas, including the extent of the parties' understanding of smart contract terms, methods for proving intent in digital environments, the interaction between smart contracts and protective regulations such as consumer protection and personal data law, and the management of cross-border disputes between Iran and Europe. Future studies employing empirical methods, such as examining real-world smart contract applications in industry and analyzing related legal disputes, could add greater depth to the subject.

Finally, the answer to the study's main question may be summarized as follows: to ensure the clear and valid establishment of the parties' intent in blockchain-based contracts under Iranian and European law, it is necessary to ensure that the parties' will is manifested in the traditional legal sense, draft contractual terms in clear and comprehensible language, align the executable component or code with the legal text, provide mechanisms for reversal, modification, or dispute resolution, and develop and update laws, regulations, and judicial practices in accordance with blockchain technology. Only by fulfilling these requirements can blockchain-based contracts attain a solid legal standing and fully realize their technological potential. Ultimately, the future of contracts in the digital age lies at the intersection of blockchain technology and contract law. If the Iranian and European legal systems advance together with both technical and legal insight, not only will current challenges in establishing intent in smart contracts be overcome, but a new level of contractual security, transparency, and efficiency will emerge, benefiting the parties, the legal system, and the digital economy alike.

## 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, J. (2020). Blockchain and the future of contract law: Challenges in consent and error. *Oxford Journal of Legal Studies*, *40*(3), 455-478.

Amiri-Moqaddam, M. (2025). A legal study of smart contracts in Iranian private law. *Social Sciences Studies*, *11*(Special Issue 1), 95-100.

Behzadi, H. (2022). The law of smart contracts in Iran: A feasibility analysis and executive challenges. *Journal of Modern Law*, *12*(3), 80-102.

Dehghani-Tafti, M., Afzali-Mehr, M., & Eskini, R. (2022). A comparative study of the legal requirements for designing digital smart contracts in Iranian and French law. *Comparative Law Research Quarterly*, *6*(2), 29-51.

European, C. (2023). *Regulation of crypto-assets under MiCA and the revised eIDAS framework*.

European, U. (2019). *European blockchain strategy: Legal challenges and regulatory framework*.

Ferguson, T., & Wright, J. (2018). Coding errors and contractual intent in automated systems. *Journal of Law & Digital Technology*, *11*(2), 145-170.

Greenberg, D. (2022). Digital identity and the eIDAS2 transformation in the EU. *European law review*, *47*(3), 201-225.

Hacker, P. (2021). The semantics of smart contracts: Reconsidering intention in algorithmic contracting. *European Review of Private Law*, *29*(2), 175-210.

Heydari, M. (2021). An examination of the legal nature of blockchain transactions in the Iranian legal system. *Law and Technology Quarterly*, *5*(1), 33-62.

Jafari Langroudi, M. J. (2019). *Legal terminology*. Ganj-e Danesh.
Karimi, S. (2023). Challenges in the interpretation of smart contracts and the role of parties' intention. *Comparative Law Research Quarterly*, *10*(4), 55-88.
Kazemi, M. R. (2022). Digital signature and its legal validity in Iranian law. *Journal of Modern Law*, *14*(2), 77-102.
Kuner, C. (2020). Blockchain, identity, and the future of digital trust. *Journal of Internet Law*, *24*(4), 123-145.
Lessig, L. (2006). *Code and other laws of cyberspace*. Basic Books.
Moradi, R. (2023). A critique of the foundations of the validity of blockchain-based contracts in the Iranian legal system. *International Journal of Contemporary Law*, *9*(4), 60-84.
Mousavi, A. (2022). Civil liability of smart contract developers based on Islamic jurisprudence and Iranian law. *Studies in Jurisprudence and Law of Technology*, *5*(2), 110-134.
Nazemi, H. (2022). Validation of parties' intention in digital environments: A novel blockchain-based approach. *Journal of Communications and Technology Law*, *6*(1), 33-59.
Paknejad, F. (2023). A comparative study of the rules of intention and consent in electronic contracts in Iran and the European Union. *Private Law Research Quarterly*, *18*(1), 55-78.
Peltz, M. (2019). Liability and intent in smart contract ecosystems. *Harvard Journal of Law & Technology*, *33*(1), 78-102.
Raskin, M. (2019). The law and legality of smart contracts. *Georgetown Law Technology Review*, *3*(2), 300-334.
Shafi'i, A. (2020). A legal analysis of smart contracts and the issue of ascertaining intention. *Journal of Private Law Research*, *8*(3), 121-150.
Smith, J. (2021). Smart contracts and contractual intent: Reconsidering autonomy in blockchain transactions. *International Journal of Law and Technology*, *15*(1), 70-95.
Soleimani, E., & Eskandari, M. (2025). A critical and comparative analysis of the nature of smart contracts in the legal systems of Iran and the United States of America. *Legal Civilization*, *8*(23), 215-240.
Surden, H. (2022). Computable contracts, automation, and the limits of legal interpretation. *Stanford Technology Law Review*, *25*(1), 180-215.
Szabo, N. (1997). Formalizing and securing relationships on public networks. *First Monday*, *2*(9).
Werbach, K. (2018). *The blockchain and the new architecture of trust*. MIT Press.
Werbach, K., & Cornell, N. (2017). Contracts ex machina. *Duke Law Journal*, *67*(2), 313-371.
Wright, A., & De Filippi, P. (2019). *Blockchain and the law: The rule of code*. Harvard University Press.
Yazdan-Panah, H. (2019). Liability of programmers and developers in blockchain-based contracts. *Journal of Information Technology and Law*, *4*(2), 89-114.
Zargari, M. (2021). Legal challenges of self-executing contracts. *Legal Research Quarterly*, *23*(2), 45-72.