

Evidentiary Challenges in the Attribution of Electronic Evidence in Disputes Arising from Smart Technology Transfer Contracts Based on Public Blockchains

1. Meysam Bashiri[✉]: Department of Private Law, Na.C., Islamic Azad University, Najafabad, Iran

2. Zeinab Pourkhaghan Shahrezaei^{*}: Department of Law, Isf.C., Islamic Azad University, Isfahan, Iran

3. Seyed Mohammad Hadi Mahdavi[✉]: Department of Law, Na.C., Islamic Azad University, Najafabad, Iran

*Correspondence: Pourkhaghan@iau.ac.ir

Abstract

In smart technology transfer contracts concluded on public blockchain platforms (such as Ethereum), establishing the attribution of data, transactions, or algorithmic outputs to a contracting party entails fundamental evidentiary challenges. The concealment of real-world identities behind public keys, the possibility of insider attacks by employees of either contracting party, and cybersecurity vulnerabilities in log-storage infrastructures disrupt the three principal links in the chain of attribution. Using a descriptive-analytical method and drawing on comparative sources, particularly German and United States case law, the authors conclude that recognizing the “public-key appearance rule” as a judicial presumption, requiring the use of X.509 digital certificates, incorporating “non-repudiation” and “segregation of duties” clauses into contracts, and establishing standardized frameworks for the attribution of evidence in decentralized environments are indispensable measures. Furthermore, unless the concept of a “secure electronic signature” is redefined so as to expressly encompass blockchain-based public keys, and unless clear evidentiary rules are developed for decentralized environments, courts will, in practice, be unable to reliably establish the identity of contracting parties in disputes arising from smart contracts.

Keywords: attribution of evidence, public blockchain, smart contract, public-key appearance rule, secure electronic signature.

Received: 21 July 2026

Revised: 01 October 2026

Accepted: 08 October 2026

Initial Publication: 14 October 2026

Final Publication: 01 June 2027



Copyright: © 2027 by the authors. Published under the terms and conditions of Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

Citation: Bashiri, M., Pourkhaghan Shahrezaei, Z., & Mahdavi, S. M. H. (2027). Evidentiary Challenges in the Attribution of Electronic Evidence in Disputes Arising from Smart Technology Transfer Contracts Based on Public Blockchains. *Legal Studies in Digital Age*, 6(6), 1-11.

1. Introduction

With the advancement of information and digital technologies, electronic contracts have emerged as modern and effective instruments in the adjudication of civil and criminal disputes. Items such as digital documents, electronic signatures, text, audio, and video messages, and data stored in cyberspace have acquired a special position in judicial proceedings because of their ease of use, storage capacity, and rapid transmission. Despite the implicit recognition of such evidence in Iranian legislation, including the Electronic Commerce Act, the Regulation on the Admissibility of Electronic Evidence, and the Computer Crimes

Act, no coherent and transparent framework has yet been developed for assessing their authenticity, integrity, and evidentiary admissibility. Today, with technological development and the emergence of decentralized platforms, new tools have appeared in the digital environment whose unique capabilities in electronic commerce have contributed to the expansion of major sectors of this field, including contractual relations. Electronic platforms are generally divided into centralized and decentralized systems. Centralized platforms are environments for the storage and exchange of information in which all exchanges occur under the control of a central authority. Users of such platforms, commonly referred to as nodes, remain capable of carrying out digital transactions only so long as the central controller continues to operate. The most prominent example of this type of platform is the World Wide Web, whose global expansion during the 1990s brought about major transformations in the field of information technology.

Smart contracts based on blockchain technology, as a new generation of electronic contracts, possess self-executing capabilities. However, when such contracts are concluded in the context of smart technology transfer, including learning algorithms, self-adaptive systems, and second- and third-generation blockchain technologies, their decentralized and cryptographically secured nature challenges the traditional law of evidence. Smart contracts raise numerous legal questions, including the existence of a valid and binding legal agreement, the compatibility of immutable blockchain records with contractual defenses, the applicable law, jurisdiction, and consumer rights. In disputes arising from such contracts, evidence predominantly appears in the form of transaction logs, digital signatures, source code, and outputs of decision-making algorithms; these forms of evidence may be fluid, susceptible to alteration without an obvious trace, and dependent on specialized technical expertise for proper interpretation. Previous studies may be divided into two categories. At the domestic level, Delkhoun Asl, Goldouzian, and Kalantari examined the probative value of electronic evidence in criminal proceedings and the importance of the chain of custody ([Delkhoun Asl et al., 2022](#)). Haddadi also demonstrated evidentiary barriers in the arbitration of smart-contract disputes ([Haddadi, 2024](#)). At the international level, Aouidef and Deffains showed that blockchain-based dispute-resolution systems, such as Kleros, remain incapable of reliably proving the connection between a real-world identity and public keys ([Aouidef et al., 2021](#)). Buchwald argues that the self-executing nature of smart contracts makes proving “algorithmic error” or “source-code defects” almost impossible because of their black-box structure ([Buchwald, 2020](#)). Nevertheless, none of the foregoing studies has comprehensively addressed the challenge of evidentiary attribution in decentralized environments; this constitutes the research gap addressed in the present article. The principal research question is as follows: Given the distinctive characteristics of electronic evidence in disputes arising from smart technology transfer contracts based on public blockchains, what challenges arise in proving the identity of the data originator, addressing insider attacks, and overcoming cybersecurity weaknesses, and what technical-legal solutions may be proposed to resolve them? The proposed hypothesis is that reliance solely on traditional rules of evidence cannot adequately respond to these challenges; rather, a new framework for attribution in decentralized environments must be developed through the use of comparative rules and practices, particularly those of Germany and California. This study employs an analytical-comparative method and relies on library sources and international documents. The structure of the article is as follows: following the Introduction, Section 2 explains the general concepts and conceptual framework. Section 3 addresses evidentiary attribution challenges, with particular emphasis on public blockchains. Section 4 presents a comparative study of German and Californian judicial approaches. Section 5 examines the compatibility of the findings with the Iranian legal system. Section 6 proposes technical-legal solutions, and Section 7 provides the conclusion. This article may contribute to the development of judicial practice and the reform of regulations governing the attribution of electronic evidence in disputes arising from public-blockchain-based smart contracts. Its findings may also be used to formulate standard attribution clauses in smart contractual architectures, including non-repudiation clauses, segregation-of-duties provisions, and requirements for the use of X.509 certificates, as well as to design decentralized dispute-resolution systems, such as blockchain courts, capable of reliably authenticating the identities of contracting parties.

2. General Principles and Conceptual Framework

In this section, the key concept of a “smart technology transfer contract” is first defined and distinguished from traditional contracts. The types of electronic evidence specific to such disputes are then introduced, and finally, the comparative framework governing electronic evidence is examined in light of the latest developments.

2.1. Operational Definition of a “Smart Technology Transfer Contract” and Its Distinction from Traditional Technology

A smart technology transfer contract refers to a contract whose subject matter involves the transfer of rights to use systems based on learning algorithms, such as machine learning and deep learning, self-executing contracts, including blockchain-based smart contracts, or Internet of Things platforms capable of autonomous decision-making. This type of contract differs fundamentally from traditional technology-transfer arrangements, such as the transfer of static software, because smart technology possesses characteristics such as dynamism, non-determinism, and black-box operation (Madani, 2023). From a legal perspective, these characteristics complicate traditional concepts such as quality assurance, conformity with technical specifications, and even civil liability. Updating dispute-resolution mechanisms to address disputes arising from blockchain-based contracts and self-executing code is therefore unavoidable. In this context, decentralized dispute-resolution protocols such as Kleros and Aragon Court have attempted to design cryptography-based decentralized adjudicatory systems; however, comparative studies have shown that blockchain registration alone remains insufficient to establish a causal link between human-source data and a public key. More recent analyses demonstrate that aligning the principles of contract law with the technical characteristics of blockchain requires a redefinition of traditional concepts such as “signature” and “unique attribution” in decentralized environments (Vecellio Segate, 2026). In the present study, the term “smart technology transfer contract” refers exclusively to contracts in which self-learning algorithms or cryptographically secured decentralized platforms play a role in at least one stage of formation, performance, or supervision.

2.2. Types of Electronic Evidence Specific to These Disputes

In disputes arising from smart technology transfer contracts, evidence generally appears in four electronic forms, each of which entails a distinct attribution challenge. First, raw data consist of datasets used to train or operate an algorithm, such as images, text, or sensor data. From the perspective of attribution, the principal problem is that raw data often lack a unique signature and can readily be attributed to another person or device or challenged as fabricated. Second, model outputs represent the results of decision-making by an intelligent algorithm, such as facial recognition or price prediction (Assaf et al., 2022). Here, the attribution challenge arises from the black-box nature of the algorithm: even where an output is available, it may not be possible to prove conclusively that the output was generated by the agreed model while under the control of the opposing party. Third, transaction logs, particularly in blockchain-based contracts, record each state change, function call, or asset transfer in a time-stamped and generally immutable manner (Mafike & Mawela, 2026). Despite their immutability, attribution remains problematic because the relevant record usually links the transaction only to a public key rather than to the name or legal identifier of a natural or legal person. Fourth, the source code of the smart contract or algorithm may itself constitute direct evidence of breach, for example by demonstrating the existence of an intentional bug or a security defect (Adu-Amankwa et al., 2023). In this category, attribution is intertwined with the protection of trade secrets: the opposing party may refuse to disclose the source code as evidence, thereby confronting the court with substantial difficulties in attributing the defect to the vendor. Identifying these categories and understanding the attribution-related dimensions of each is therefore essential to designing appropriate evidentiary rules for decentralized environments.

3. Attribution Challenges: Linking Evidence to the Contracting Parties

In disputes involving smart technologies, proving which party is responsible for a particular item of data, such as a log, signature, or algorithmic output, is difficult because public keys conceal real-world identities in decentralized environments, while insider attacks or cybersecurity weaknesses may enable evidence to be fabricated or destroyed (Rabbani Mousavian, 2021). These three challenges—hidden identity, insider threats, and infrastructural vulnerability—have transformed evidentiary attribution into one of the most complex issues in contemporary adjudication.

3.1. Proving the Identity of the Data Originator in Decentralized Environments (Public Blockchain)

In decentralized environments such as public blockchains, each user is identified through a cryptographic key pair consisting of a public key and a private key. Transactions are signed using the private key, while anyone may verify the validity of the signature through the corresponding public key. However, the relationship between the public key and the user's real-world identity is not inherently established within the blockchain architecture. Accordingly, in the event of a dispute, the opposing party may simply deny ownership of the public key or claim that the private key was stolen. Proving the contrary before a court is highly difficult (Buchwald, 2020). In the Iranian legal system, Article 14 of the Electronic Commerce Act treats a "secure electronic signature" as equivalent to a handwritten signature and requires, inter alia, that the signature be uniquely attributable to the signatory and that any subsequent alteration be detectable (Jomezadeh Behabadi, 2020). In a public blockchain environment, proving such "unique attribution" in the event of denial requires collateral evidence, which may be difficult and, in some cases, impossible to obtain. In comparative law, German courts have applied what may be described as the "public-key appearance rule": where a public key has for a prolonged period been associated with a particular individual, an initial presumption arises that the key belongs to that person unless the contrary is proven. In March 2025, the Commercial Court of Marseille held that a timestamp recorded on a public blockchain constituted admissible evidence for establishing copyright ownership in fashion designs (Aouidef et al., 2021). From the perspective of Iranian law, the public-key appearance rule can be aligned with Article 1325 of the Civil Code, which allows judges to treat surrounding facts and circumstances as judicial presumptions. A long history of transactions associated with a particular public key and a particular natural or legal person may therefore establish circumstances sufficient for a court to infer attribution. It is consequently proposed that Iranian judicial practice, without requiring legislative amendment, adopt the public-key appearance rule as a judicial presumption in blockchain disputes through an expansive interpretation of Article 1325. Such an approach would preserve the fundamental principles of evidence while also addressing the difficulty of proving "unique attribution" under Article 14 of the Electronic Commerce Act.

3.2. Insider Attacks and Log Forgery by Employees of Either Contracting Party

The second attribution challenge is the risk of insider attacks, namely, situations in which employees of either contracting party who have direct access to systems, private keys, or logging facilities can forge, delete, or alter logs and subsequently claim that the evidence presented before the court represents the original data. This threat is particularly common in centralized systems. Countermeasures include segregation of duties, recording all access events in a separate encrypted log, and the use of multisignature mechanisms for critical transactions so that no single employee can independently alter the relevant record (Nogaroli, 2025). From a legal perspective, Article 1258 of the Iranian Civil Code enumerates five categories of evidence and recognizes judicial presumptions as one such category. Where an employee has forged logs, the jurisprudential rules of possession and voluntary assumption of risk may provide a basis for shifting the burden of proof and attributing responsibility to the employer (Nejatzadegan & Soltani, 2022). Accordingly, in disputes arising from insider attacks, a court may, without requiring direct proof of the employee's conduct, rely on the rule of assumption of risk—under which a person who causes loss bears responsibility—and on the employer's exclusive access to log-recording systems to place the burden of proving data authenticity on the employer. This approach, known in comparative law as the "dynamic burden of proof," may also be accommodated within Article 1258 of the Iranian Civil Code, because the judicial presumption arising from the employer's control over equipment and private keys provides an evidentiary indication of its responsibility for unauthorized alterations. It is therefore necessary for Iranian judicial practice, drawing on the jurisprudential rule relating to control and possession and through an expansive interpretation of Article 1258, to place responsibility for proving the authenticity of logs on the employer in cases involving insider attacks and to relieve the claimant of the burden of directly proving the employee's conduct.

3.3. The Role of Weak Cybersecurity in the Destruction or Alteration of Evidence

The third attribution challenge is the general weakness of cybersecurity in log-storage infrastructures. An attacker may erase or alter logs through a simple password attack or software vulnerability. Comparative studies indicate that one of the most effective preventive approaches is to use immutable storage environments such as blockchain. Emerging frameworks employ

smart contracts to secure and automate the admissibility of digital evidence in court and use cryptographic mechanisms to establish the authenticity and integrity of the chain of custody (Natanelov et al., 2022). In a blockchain environment, an attacker cannot alter previous transactions unless the attacker controls more than 51% of the network's computational power. Recent systematic studies also show that blockchain creates transformative opportunities for modern judicial proceedings by providing an immutable and decentralized architecture for documenting and auditing the evidentiary chain of traceability, while the use of smart contracts on such platforms can substantially enhance accountability and transparency in the evidentiary process (Kamel et al., 2023). From the perspective of civil liability, weak cybersecurity within either party's infrastructure may itself be treated as a form of presumed fault in relation to the loss of evidence, because maintaining logs and private keys falls within an obligation of due care, the breach of which may be established by failure to comply with accepted security standards such as ISO 27001. On this basis, an Iranian court may invoke the jurisprudential rule of causation, reflected in Article 1 of the Civil Liability Act, together with the no-harm principle, to hold a party whose insecure infrastructure resulted in the destruction or alteration of evidence liable for the loss caused by the opposing party's inability to prove its claim. This approach places the burden of demonstrating adequate security measures on the party exercising physical control and administrative access over the relevant servers and databases.

3.4. *The Public-Key Appearance Rule as a Judicial Presumption*

In comparative law, the "public-key appearance rule" has been accepted as a judicial presumption according to which, where a public key has continuously and for a prolonged period been associated with a particular natural or legal person across multiple transactions, an initial presumption arises that the key belongs to that person unless the contrary is proven (Waqar et al., 2023). The rationale underlying this rule lies in the creation of reasonable customary confidence through repetition and continuity of conduct, as recognized in civil-law systems such as Germany. In March 2025, the Commercial Court of Marseille similarly emphasized that a long history of transactions involving a particular public key and a specific trade name could be sufficient to support an initial appearance of ownership. In Iranian law, Article 1325 of the Civil Code recognizes "facts and circumstances" as a source of judicial presumptions. A recorded and immutable sequence of transactions on a public blockchain is one of the clearest examples of such "facts and circumstances" capable of supporting attribution. This rule is particularly effective in legal systems based on written proceedings and may provide a useful model for other jurisdictions, including Iran (Aydinmehr, 2025). By accepting the public-key appearance rule under Article 1325 of the Iranian Civil Code, courts could resolve the problem of identity proof in public blockchains without requiring legislative amendment. The rule implicitly shifts the burden of proof from the claimant to the defendant because, once a long transactional history has been established, the defendant must prove the contrary, for example by demonstrating that the private key was stolen. Such an approach is also consistent with the jurisprudential rule relating to possession and control and offers a dynamic, technologically responsive interpretation of traditional evidentiary principles.

4. Comparative Study of the Approaches of German and Californian Courts

An examination of two prominent legal systems in the acceptance of algorithmic evidence and blockchain attribution reveals the following:

a) **Germany: Emphasis on Transparency and Judicial Supervision**

In February 2023, the German Federal Constitutional Court held that automated data analysis by the police goes beyond merely technical efficiency and constitutes an independent interference deserving constitutional protection unless sufficient transparency and judicial supervision of the algorithmic process are ensured. In a significant judgment concerning Section 25a HSOG and Section 49 HmbPolDVG, the German Federal Constitutional Court declared that automated police data analysis exceeds "mere technical efficiency" and itself constitutes an "independent interference warranting constitutional protection" unless sufficient transparency and judicial oversight exist with respect to the algorithmic process ("BVerfGE," 2023). Although the judgment concerned law-enforcement activities, its underlying principle is capable of extension to civil litigation: German courts tend to accept algorithmic outputs as evidence only where such outputs are sufficiently transparent and auditable. This

approach demonstrates that the German legal system gives priority to transparency and human supervision over the mere acceptance of algorithmic outputs.

b) California: Gradual Acceptance with Emphasis on Expert Evidence

The legal system of California, which has taken a leading role in technology regulation, adopts a relatively flexible approach. At the same time, legal scholars have warned that artificial-intelligence systems may make errors and that the black-box nature of such systems may prevent experts from adequately defending their findings (Cheng et al., 2023). Accordingly, although the system has gradually expanded the acceptance of algorithmic outputs, courts remain required to examine the logical basis and scientific generalizability of any form of algorithmic evidence. Section 801 of the California Evidence Code continues to emphasize the necessity of expert opinion capable of assisting the trier of fact in understanding the relevant issue (Wu et al., 2022). Both legal systems have confronted the challenge of proving the connection between public keys and the real identities of users in public blockchains. German judicial practice has used the public-key appearance rule as a mechanism for addressing this difficulty. Comparative analyses further demonstrate that legislative initiatives in different countries have taken varying approaches to the phenomenon of smart contracts (Singh et al., 2023). These developments range from legislative initiatives in certain U.S. states, such as Wyoming, Tennessee, and Arizona, which have formally recognized smart contracts, to the more cautious approach of the European Union, which has emphasized transparency and the right to explanation in automated algorithmic systems through its artificial-intelligence regulatory framework and the General Data Protection Regulation. From this perspective, the German model, which prioritizes maximum transparency and judicial supervision and is more consistent with civil-law adjudication, may be regarded as a more appropriate model for developing legal systems such as that of Iran.

5. Comparative Assessment: Compatibility of the Findings with the Iranian Legal System

Although this article primarily adopts a comparative and international approach to the challenges of evidentiary attribution in public blockchains, examining a specific legal system such as Iran demonstrates the depth of the legislative gap in this field. Global markets and international instruments such as the UNIDROIT Principles have taken steps toward adapting to new technologies, including the development of guidance and best practices for transactions involving digital assets, cryptocurrencies, non-fungible tokens, and related systems, while domestic legal regimes are gradually adapting to these standards (Haddadi, 2024). By accepting the general principles of UNIDROIT in international commercial law, national legal systems may draw on this framework to update their attribution rules in response to the challenges of decentralized transactions.

As stated above, artificial intelligence is increasingly used to verify the terms of contracts concluded by individuals. In verifying contractual terms, artificial intelligence reviews the contents of the agreement and, where conformity is established, proceeds to register and deploy them on a blockchain. Artificial intelligence may be understood in this context as a high-capacity computing system whose embedded processor protocols determine how electronic data messages are processed. From the outset, these protocols incorporate rules and criteria used to review the terms of smart contracts. Accordingly, where the rules embedded in the artificial-intelligence processor contain safeguards designed to prevent the inclusion of unfair terms in contracts, the relevant regulatory objectives may be achieved.

The review of contractual provisions and electronic evidence takes place through processes embedded in the relevant processor. Consequently, digital contract terms may be reviewed independently of the broader circumstances surrounding contract formation, which in practice can generate significant challenges. For example, in technology-transfer agreements, the transferring state may seek to prevent rival countries from obtaining the transferred technology by inserting ownership clauses, restricting onward transfer by the recipient state, and providing for specific legal sanctions in order to safeguard its rights. Likewise, under exceptional circumstances such as armed conflict, contracts for the sale of various types of weapons to states involved in war may contain ancillary clauses establishing prices far above ordinary market levels, thereby disrupting the balance between the parties' rights and obligations. A comparative examination of judicial practice in Iran, the European Union, and advanced jurisdictions such as the United Kingdom and the United States demonstrates that the authenticity and probative value of electronic evidence depend on particular technical and legal requirements. It is therefore proposed that the legislature amend existing regulations by introducing clearer criteria governing the validity, probative force, and admissibility of electronic evidence in order to prevent the violation of citizens' rights and potential misuse.

The expansion of electronic evidence and documentation throughout the world has led to a substantial increase in commercial activity. Competition among companies operating in international trade may create tensions that sometimes lead firms to adopt anticompetitive practices in an attempt to eliminate their competitors. Consumers constitute one of the vulnerable groups most likely to suffer harm from such practices. Among these practices is the conclusion of contracts that deviate from legal standards. The close relationship between competition law and contract law means that competition law is consistently influenced by the general principles governing contractual relations. Contracts between producers and consumers constitute an essential component of commercial activity in competitive markets, yet anticompetitive conduct may result in agreements containing invalid terms that create opportunities for producer abuse. To restore balance, states adopt protective rules in favor of consumers. Freedom of contract and fairness in transactions are two established principles of competition law, but anticompetitive practices, including the insertion of unfair terms in consumer contracts, may violate both principles. Such terms may be incorporated for reasons such as the consumer's lack of awareness regarding their legal effect, failure to read the contract carefully, the adhesion nature of the agreement, or other circumstances, sometimes even without meaningful consumer consent, thereby imposing obligations on the consumer.

5.1. Critique of Articles 12–15 of the Iranian Electronic Commerce Act in Relation to Attribution

Articles 12–15 of the Iranian Electronic Commerce Act of 2003 establish the principal framework for assessing the evidentiary value of electronic evidence. Article 14 treats a “secure electronic signature” as equivalent to a handwritten signature and requires conditions such as unique attribution to the signatory and the ability to detect any alteration (Karami Moghaddam, 2025). In a public blockchain environment, each user is identified through a cryptographic key pair consisting of a public key and a private key. However, Article 14 does not specifically refer to blockchain public keys, and the requirement of “unique attribution” raises serious evidentiary difficulties in a decentralized environment because no central institution exists to match a public key with a real-world identity. Article 15, which concerns the authenticity of data messages, likewise fails to address the concept of chain of custody in a decentralized setting (Delkhoun Asl et al., 2022). From a legal analytical perspective, this gap is not merely a technical deficiency but reflects a fundamental disconnect between existing legal rules and the requirements of decentralized systems. Article 14, by focusing on exclusive attribution, effectively presupposes a signature model in which a central authority, such as a certification authority, verifies the identity of the signatory. In a public blockchain, however, no such authority exists, and attribution is established through consensus mechanisms and transaction histories. Article 14 therefore cannot be directly applied to blockchain public keys without expansive interpretation or legislative amendment. This incompatibility may prevent Iranian courts from using blockchain-based evidence for purposes of attribution in disputes arising from smart contracts. Accordingly, amending Article 14 by adding a provision treating a valid blockchain public key as a secure electronic signature constitutes an urgent legislative necessity.

4.2. General Rules of the Iranian Civil Code: Analysis of Articles 1257, 1258, and 1325

Among the general rules of the Iranian Civil Code, Articles 1257, 1258, and 1325 are the provisions most closely connected with evidentiary attribution in public blockchains. Article 1257 establishes the well-known principle that the burden of proof lies on the claimant. In disputes arising from public blockchains, however, where algorithmic outputs are probabilistic and access to evidence is asymmetrical and often concentrated in the hands of one party, identifying the party who should properly bear the burden of proof may be difficult. Jurisprudential rules relating to possession and assumption of risk may provide a basis for shifting the burden from the claimant to the defendant (Aydinmehr, 2025). Article 1258 enumerates five categories of evidence—admission, written documents, testimony, presumptions, and oath—and recognizes judicial presumptions as a legitimate evidentiary category. This provision creates the possibility of admitting emerging forms of evidence, including blockchain logs and the public-key appearance rule, under the category of judicial presumptions. Article 1325 provides that “presumptions are circumstances which, by operation of law or in the opinion of the judge, are recognized as evidence of a matter” (Dehghani Tafti et al., 2021). The automatic and immutable recording of a transaction on a blockchain, together with its validation by thousands of independent nodes, constitutes one of the clearest examples of “circumstances” from which a judge may infer attribution of the transaction to the holder of the relevant public key. In Imami jurisprudence, judicial knowledge refers to reasonable customary certainty rather than philosophical certainty; accordingly, an algorithmic output carrying a 95% confidence level, combined with a long transactional history associated with a particular public key, may

generate sufficient reasonable certainty for a judge. Such an interpretation is not inconsistent with the spirit of Articles 1257 of the Civil Code and 198 of the Iranian Code of Civil Procedure (Saghafian et al., 2021). Reliance on Article 1325 of the Civil Code to recognize the public-key appearance rule offers a practical solution within the existing Iranian legal framework and does not require legislative amendment. A court may treat a long transactional history associated with a public key and a particular person—for example, hundreds of successful transactions on a commercial platform—as a relevant circumstance and infer attribution accordingly. This approach implicitly shifts the burden of proof to the defendant because, once the apparent attribution is established, the defendant must prove the contrary, for example by demonstrating that the private key was stolen. Such an interpretation of Article 1325 is not only consistent with jurisprudential rules relating to control and possession but also reduces, although does not entirely eliminate, the need to amend Article 14 of the Electronic Commerce Act.

5.2. Legislative and Judicial Solutions for the Iranian Legal System

The Iranian legal system has the capacity to adopt the international solutions proposed in this article, particularly the public-key appearance rule, through two mechanisms: first, amendment of Article 14 of the Electronic Commerce Act by adding a provision such as the following: “In decentralized environments such as blockchain, a valid public key that is cryptographically paired with the signatory’s private key and whose authenticity has been confirmed by network nodes shall be deemed a secure electronic signature unless the contrary is proven.” Second, judicial recognition of the public-key appearance rule as a judicial presumption under Article 1325 of the Civil Code. In the absence of such reforms, Iranian courts may in practice be unable to establish the identities of parties in disputes involving smart contracts (Valipour, 2025). The second route, judicial presumption, offers an important practical advantage: there is no need to await legislative reform, and courts may immediately apply the public-key appearance rule through an expansive interpretation of Article 1325. Such progressive judicial practice may itself pave the way for subsequent legislative reform and temporarily bridge the existing statutory gap. Nevertheless, the first route, statutory amendment, offers a more durable solution and reduces uncertainty resulting from divergent judicial interpretations. It is therefore recommended that the legislature amend Article 14 of the Electronic Commerce Act at the earliest opportunity while judicial practice is simultaneously developing.

6. Technical-Legal Solutions for Addressing Attribution Challenges

The three principal attribution challenges—hidden identity, insider attacks, and weak cybersecurity—require combined solutions at both technical and legal levels. Technical mechanisms cannot operate effectively in court without legal recognition, while legal rules cannot be enforced in practice without appropriate technical tools (Hunhevic et al., 2022). Accordingly, this section presents five principal solutions, all of which are capable of adaptation to different legal systems, including Iran. These solutions rest on two fundamental pillars: first, creating predictability at the contract-formation stage through contractual clauses and standardization; and second, ensuring verifiability at the dispute stage through judicial presumptions and cryptographically secured chains of custody. In this way, both contracting parties and courts can manage attribution issues with greater confidence.

1. The Public-Key Appearance Rule as a Judicial Presumption: Drawing on German practice, judges should be permitted to infer attribution of a new transaction to a person where there is a long history of transactions associated with the same public key, unless the inference is rebutted by documented evidence. Recent research indicates that blockchain-based systems can effectively perform evidentiary and attribution-related functions traditionally associated with legal formalities through cryptographic verification and consensus mechanisms, making this rule readily implementable in blockchain environments (Ferreira, 2023). Recent work on blockchain-based proof also emphasizes the advantages of distributed-ledger technology in providing an immutable architecture for documenting and auditing the evidentiary chain of traceability.

2. Reform of Electronic-Signature Legislation: The concept of a “secure electronic signature” in domestic legislation should be redefined so as expressly to encompass valid blockchain public keys (Zamanian & Vatani, 2022). The incompatibility of traditional principles of contract law with the technical nature of blockchain, particularly the concepts of “signature” and “unique attribution” reflected in Article 14 of the Electronic Commerce Act, constitutes one of the principal evidentiary barriers to attribution in decentralized environments. Drawing on studies that provide a deeper understanding of

the decentralized nature of blockchain, it is proposed that the legislature replace the traditional criterion of “unique attribution” with criteria adapted to blockchain architecture.

3. Preventive Contractual Clauses: Smart contracts should incorporate non-repudiation clauses, segregation-of-duties provisions, and requirements mandating the use of X.509 digital certificates issued by trusted third parties (Park et al., 2025). The provision of an algorithmic transparency report and the specification in the contract of an agreed level of reasonable certainty for algorithmic outputs may also facilitate arbitration and judicial decision-making in subsequent disputes.

4. Prevention of Insider Attacks: All employee access should be recorded in separate encrypted logs, access privileges should be segregated across storage and validation systems, multisignature mechanisms should be used for critical transactions, and information-security standards such as ISO 27001 should be mandatory for the protection of private keys (Hassani et al., 2021). From a legal perspective, encrypted access logging and segregation of duties shift the burden of proof in civil disputes in favor of the claimant and compel the defendant to provide documented defenses against allegations of log forgery or alteration. Compliance with standards such as ISO 27001, in addition to enhancing technical security, may be characterized as an obligation of due care in smart contracts, the breach of which may independently constitute contractual liability and civil fault. Moreover, the use of multisignature mechanisms for critical transactions substantially reduces the possibility of unauthorized unilateral conduct and protects the evidentiary chain of custody against repudiation and internal manipulation.

5. Integration of Log-Storage Systems and the Chain of Custody: Recent studies show that blockchain platforms make it possible to record operational logs automatically and immutably, thereby safeguarding the authenticity and integrity of data against denial by the parties or cyberattacks (Mozaffari & Naser, 2021). The use of standardized valid evidence summaries for courts is particularly recommended in disputes involving very large volumes of data, such as disputes arising from Internet of Things systems or digital twins.

Simultaneous implementation of these five solutions would create a multilayered defense system against attribution challenges: contractual clauses would establish primary responsibility, technical standards would prevent the fabrication and alteration of evidence, and the public-key appearance rule, combined with reform of electronic-signature legislation, would facilitate the judicial acceptance of evidence. Among these mechanisms, the public-key appearance rule has greater strategic importance because it can be immediately accommodated within Article 1325 of the Iranian Civil Code. Nevertheless, until Article 14 of the Electronic Commerce Act is amended, legal uncertainty concerning the “unique attribution” of public keys will remain. It is therefore recommended that judicial practice based on judicial presumptions be pursued in the short term and legislative reform in the longer term.

7. Conclusion

Electronic evidence and smart contracts are contractual arrangements concluded on decentralized platforms and, compared with other forms of electronic contracts, are characterized by features such as greater speed and security. The mechanisms governing the formation of such contracts also have the potential to prevent the inclusion of unfair terms. However, the implementation of this mechanism requires legislative policymaking in several areas, including the harmonization of international rules and the determination of the operational scope of oracle information systems. As explained above, one of the challenges arising from the use of artificial intelligence in smart-contract formation is that contractual terms are reviewed on the basis of the rules initially embedded in the processor of the relevant high-capacity computing system. If uniform international rules identifying unfair contractual terms were adopted, many of the challenges associated with artificial-intelligence performance could be mitigated. Furthermore, in obtaining the information necessary to review contractual provisions, artificial intelligence depends on oracles to extract relevant external information. The operational scope of oracles and the extent of their access to available data depend on the degree of informational transparency within the relevant legal system. Legislative policies aimed at increasing informational transparency may therefore constitute another important legal requirement for states, particularly developing countries such as Iran.

The expansion of electronic commerce throughout the world has led to a significant increase in the activities of commercial enterprises. Competition among such enterprises and their rivals in international trade may occasionally create tensions that lead companies to adopt anticompetitive practices in an attempt to eliminate competitors. Consumers constitute one of the vulnerable groups in society and may suffer significant harm from anticompetitive conduct in competitive markets. Such

conduct includes the conclusion of contracts that do not comply with legal standards. The close relationship between competition law and contract law means that competition law is frequently shaped by principles derived from the general law of contracts. Agreements between producers and consumers are a necessary feature of commercial activity in competitive markets, yet anticompetitive practices may lead to agreements containing invalid terms that facilitate producer abuse. To restore balance, governments introduce regulations protecting consumers. Freedom of contract and transactional fairness are two established principles of competition law, but anticompetitive practices such as the insertion of unfair terms into consumer contracts may violate both principles. Such terms may be incorporated because consumers are unaware of their nature, fail to read the agreement carefully, are presented with adhesion contracts, or for other reasons, and may bind consumers even in the absence of meaningful consent.

Smart technology transfer contracts based on public blockchains confront the traditional law of evidence with three fundamental attribution challenges: concealment of real-world identities behind public keys, the possibility of insider attacks and evidence manipulation by employees, and weak cybersecurity within log-storage infrastructures. Comparative analysis of different legal systems, particularly Germany and California, demonstrates that recognition of the public-key appearance rule as a judicial presumption, mandatory use of standardized digital certificates, and modernization of electronic-signature legislation are unavoidable requirements. The comparative assessment undertaken in this article shows that, although Articles 12–15 of the Iranian Electronic Commerce Act are insufficient for addressing smart technologies, an expansive interpretation of Articles 1257 and 1325 of the Civil Code may permit the introduction of the public-key appearance rule into the evidentiary process as a judicial presumption. It is therefore proposed that Article 14 of the Iranian Electronic Commerce Act be amended so that a valid blockchain public key is treated as a secure electronic signature. The proposed solutions, including adoption of the public-key appearance rule, reform of national legislation, and the design of preventive contractual clauses, can facilitate evidentiary attribution in smart-contract disputes and enhance the legal security of such transactions. The principal limitation of the present study lies in its theoretical-analytical nature and the lack of access to actual case files in this field. Future research should therefore focus on empirical studies of decentralized dispute-resolution platforms and on evaluating the feasibility of blockchain implementation within judicial systems.

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

- Adu-Amankwa, N. A. N., Rahimian, F. P., Dawood, N., & Park, C. (2023). Digital twins and blockchain technologies for building lifecycle management. *Automation in Construction*, 155, 105-134.
- Aouidef, Y., Ast, F., & Deffains, B. (2021). Decentralized justice: A comparative analysis of blockchain online dispute resolution projects. *Frontiers in Blockchain Review*, 1-18.
- Assaf, M., Hussein, M., Alsulami, B. T., & Zayed, T. (2022). A mixed review of cash flow modeling: Potential of blockchain for modular construction. *Buildings*, 12, 20-54.
- Aydimmehr, M. (2025). A legal examination of smart contracts in Iranian law with emphasis on evidentiary admissibility, validity and judicial enforcement. *Modern Jurisprudence and Law*(6), 1-19.
- Buchwald, M. (2020). Start contract dispute resolution: The inescapable flaws of blockchain-based arbitration. *University of Pennsylvania Law Review*, 168, 139-163.

- Cheng, J. C. P., Liu, H., Gan, V. J. L., Das, M., Tao, X., & Zhou, S. (2023). Construction cost management using blockchain and encryption. *Automation in Construction*, 152, 104841.
- Dehghani Tafti, M., Afzalimehr, M., & Eskini, R. (2021). A comparative study of the law applicable to digital smart contracts from a private international law perspective in the Iranian legal system and the Rome I Regulation. *Modern Technologies Law*(4), 203-229.
- Delkhoun Asl, R., Goldouzian, I., & Kalantari, K. (2022). A comparative study of the probative value of electronic evidence in criminal proceedings in the Iranian and French legal systems. *Legal Studies of Cyberspace*(1), 16-33.
- Ferreira, A. (2023). Smart contracts and the law. In *Blockchain and the Law* (pp. 125-143).
- Haddadi, S. (2024). Arbitration in smart contracts: Legal challenges of on-chain and off-chain dispute resolution. *Economic and Commercial Law Research*(2), 87-116.
- Hassani, M. A., Bazai, G., & Shahmansouri, A. (2021). Identifying factors affecting a blockchain technology maturity model with emphasis on the blockchain ecosystem. *Business Management*(52), 1-22.
- Hunhevic, J. J., Motie, M., & Hall, D. M. (2022). Digital building twins and blockchain for performance-based (smart) contracts. *Automation in Construction*, 133, 103981.
- Jomezadeh Behabadi, K. (2020). *Legal challenges of using smart contracts in joint ventures* [Doctoral dissertation, Shahid Beheshti University].
- Judgment of 16 February 2023: 1 BvR 1547/19 and 1 BvR 2634/20, 165 363 (2023). https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2023/02/rs20230216_1bvr154719.html
- Kamel, M. A., Bakhoun, E. S., & Marzouk, M. M. (2023). A framework for smart construction contracts using BIM and blockchain. *Scientific reports*, 13(1), 102-137.
- Karami Moghaddam, R. (2025). The role of smart contracts in enhancing transparency and justice in dual-role platforms in Iranian and American administrative law. *New Research in Administrative Law*(7), 452-477.
- Madani, F. (2023). *Conditions and obstacles to electronic smart contracts and practical and legal solutions for overcoming them* [Master's thesis, Kar Higher Education Institute, Qazvin].
- Mafike, S. S., & Mawela, T. (2026). An enterprise framework for blockchain interoperability. *Electronic Markets*, 36, 29-51, Article 14.
- Mozaffari, M., & Naser, M. (2021). The role of smart contracts in securing individuals' property rights. *Legal Research*(95), 253-275.
- Natanelov, V., Cao, S., Foth, M., & Dulleck, U. (2022). Blockchain smart contracts for supply chain finance: Mapping the innovation potential in Australia-China beef supply chains. *Journal of Industrial Information Integration*, 30, 100389.
- Nejatzadegan, S., & Soltani, M. (2022). Assessing the general validity requirements of smart contracts under Iranian and American law. *Legal Research*, 25, 303-339.
- Nogaro, R. (2025). Ethical and legal aspects of artificial intelligence (AI) in medical service contracts. In *Medical Liability and Artificial Intelligence* (pp. 123-206).
- Park, J., Jeong, S., & Yeom, K. (2025). Blockchain transaction refinery: A traceability refinement mechanism to improve the analysis of permissioned blockchain transactions. *Journal of King Saud University Computer and Information Sciences*, 37, 1-36, Article 325.
- Rabbani Mousavian, S. A. (2021). Rules governing smart contracts in Imami jurisprudence and positive law. *Islamic Jurisprudence and Law Research*(17), 178-210.
- Saghafian, A., Sadri, S. M., Jamshidirad, M. S., & Amirpour, H. (2021). The effect of blockchain technology on the jurisprudential and legal status of cryptocurrencies and money issuance. *Iranian Political Sociology*(4), 292-315.
- Singh, A. K., Kumar Varadhaiya, G. R. P., Hu, J., & Irfan, M. (2023). Investigation of barriers and mitigation strategies to blockchain technology implementation in construction industry: An interpretive structural modeling approach. *Environmental Science and Pollution Research*, 30(38), 89-136.
- Valipour, A. (2025). *Challenges of admitting digital evidence in civil and criminal proceedings: A comparative study of Iran and advanced legal systems* Seventh International and Eighth National Conference on Law and Political Science,
- Vecellio Segate, R. (2026). Metaverse: Yet another jeopardy for the constitutional social contract? In *Law and Politics of Virtual Worlds* (pp. 51-95).
- Waqar, A., Qureshi, A. H., Othman, I., Saad, N., & Azab, M. (2023). Exploration of challenges to deployment of blockchain in small construction projects. *Ain Shams Engineering Journal*, 102362.
- Wu, L., Lu, W., & Xu, J. (2022). Blockchain-based smart contract for smart payment in construction: A focus on the payment freezing and disbursement cycle. *Frontiers of Engineering Management*, 9(2), 177-195.
- Zamanian, M., & Vatani, Z. (2022). Enhancing the efficiency of documentary credits through private blockchain technology and smart contracts: A comparative assessment of legal compatibility. *Legal Research*, 25, 445-477.