How to cite this article:
Karimi, S. E., Janipour, A., & Pourjavaheri, A. (2025). The Tension Between Blockchain Transparency and Privacy in Smart Contracts: A Comparative Study of Iran and the European Union. *Journal of Historical Research, Law and Policy, 3*(1), 1-14. https://doi.org/10.61838/jhrlp.221

Article history:
Original Research

Dates:
Submission Date: 08 November 2024
Revision Date: 04 February 2025
Acceptance Date: 11 February 2025
Publication Date: 01 March 2025

The Tension Between Blockchain Transparency and Privacy in Smart Contracts: A Comparative Study of Iran and the European Union

1. Seyedeh Elnaz. Karimi[1] : Department of Law, Yas.C. Islamic Azad University, Yasuj, Iran
2. Ali. Janipour[2*]: Department of Law, Yas.C. Islamic Azad University, Yasuj, Iran
3. Ali. Pourjavaheri[3]: Department of Law, Yas.C. Islamic Azad University, Yasuj, Iran

*corresponding author's email: Ali.janipour.2025@iau.ac.ir

ABSTRACT

This study examines the conflict between the inherent transparency of blockchain technology and privacy requirements in the context of smart contracts, and seeks, through a comparative approach, to analyze the legal status of this conflict within the Iranian legal system in comparison with that of the European Union. The primary objective of the study is to elucidate the challenges arising from the immutability of recorded data, transaction traceability, and the self-executing nature of smart contracts in relation to the fundamental principles of personal data protection, including the right to data control, data minimization, and the right to be forgotten. Employing a comparative–analytical research method, and through an examination of legislative documents, European Union regulations—particularly the General Data Protection Regulation (GDPR)—instruments related to electronic identification and trust services, as well as existing laws and practices in Iranian law, this research analyzes the legal dimensions of this conflict. The findings indicate that in the European Union, although blockchain transparency is recognized as a technical advantage, efforts have been made to strike a balance between technological innovation and privacy protection by adopting solutions such as off-chain data segregation, anonymization techniques, and flexible interpretations of certain GDPR principles. In contrast, the Iranian legal system, due to the absence of a comprehensive and explicit framework for personal data protection and the lack of specific regulation of smart contracts, faces significant legal ambiguities and practical challenges. The results suggest that, in order to ensure the secure and lawful utilization of blockchain-based smart contracts, Iranian law requires the development of clear regulations inspired by European Union experiences while remaining compatible with domestic considerations and the structure of the country's private law system.

Keywords: *smart contracts; blockchain; privacy; transparency; Iranian law; European Union*

Introduction

The rapid expansion of emerging digital technologies—particularly blockchain technology and smart contracts—has brought about fundamental transformations in the landscape of private law and commercial law. Blockchain, as a distributed ledger, with features such as transparency, data immutability, and decentralization, promises increased trust, reduced transaction costs, and the elimination of intermediaries in contractual relations. In this context, smart contracts, as mechanisms for the self-execution of contractual obligations, have acquired a prominent position in digital transactions, financial services, supply chains, and even cross-border contracts. These

developments have led many legal systems, including that of the European Union, to reconsider traditional rules of contract law and protective legal institutions (1).

Despite the technical and economic advantages of blockchain, one of its fundamental challenges lies in the tension between its structural transparency and legal requirements for privacy protection. By design, blockchain ensures that data, once recorded, remain permanent and traceable, which may conflict with core principles of personal data protection, such as data control, data minimization, and the right to erasure. This tension becomes particularly significant in the context of smart contracts, as these contracts not only process the parties' identity and financial data but also produce potentially irreversible legal effects through automatic execution (2).

Within the legal system of the European Union, the protection of personal data is recognized as a cornerstone of fundamental rights, and a comprehensive regulatory framework has been developed to govern data processing in the digital environment. Emphasizing principles such as lawfulness, proportionality, transparency, and accountability, this framework seeks to strike a balance between technological innovation and the protection of individual rights (3). Nevertheless, the implementation of these principles in the context of blockchain and smart contracts faces significant theoretical and practical difficulties due to data immutability and the decentralized nature of blockchain networks. For example, the application of the "right to be forgotten" in an environment where data are permanently recorded raises serious questions regarding both technical feasibility and legal interpretation (4).

By contrast, although the Iranian legal system has taken initial steps toward regulating digital commercial relations through the Electronic Commerce Act of 2003, it still lacks a comprehensive and coherent framework for personal data protection and for the specific regulation of blockchain-based smart contracts. This legislative gap has resulted in privacy-related principles being addressed in a fragmented and unsystematic manner across different statutes, without providing clear responses to emerging technological challenges (5). Consequently, the widespread use of smart contracts on blockchain platforms may lead to legal uncertainty, reduced legal security, and diminished user trust.

The importance of examining the conflict between blockchain transparency and privacy can be considered from two perspectives. First, from the standpoint of legal and economic efficiency, as the lack of precise clarification of privacy boundaries and obligations can constitute a major barrier to the adoption and development of smart contracts in emerging legal systems. Second, from the perspective of protecting fundamental rights, since extensive processing of identity and financial data without adequate safeguards may result in privacy violations and data misuse (6). In many practical blockchain applications, such as decentralized financial services, user data are published in a transparent and analyzable manner, thereby increasing the risk of re-identification.

In leading legal systems, efforts have been made to mitigate this tension through the adoption of technical and legal solutions. These include off-chain data storage, anonymization or pseudonymization techniques, and flexible interpretations of certain data protection principles (7). Such approaches demonstrate that blockchain transparency does not necessarily entail full disclosure of personal data and that, through appropriate legal–technical design, a balance can be achieved between functional transparency and data confidentiality.

In Iranian law, the absence of such integrated approaches has resulted in smart contracts remaining largely at a theoretical level or developing without a clear legal foundation. This situation not only increases legal risks but also hinders the harmonization of Iranian law with international standards and limits effective participation in cross-border digital commerce (8). Accordingly, a comparative examination of the European Union's experience and an analysis of the possibility of its contextualized adaptation constitute an undeniable necessity for the Iranian legal system.

This study adopts a comparative–analytical approach with three primary objectives: first, to clarify the theoretical foundations of blockchain transparency and privacy requirements; second, to examine how European Union regulations and related legal instruments address this conflict; and third, to analyze the Iranian legal framework and propose solutions compatible with the structure of Iranian private law to mitigate this tension. The main research questions are as follows: What legal foundations underlie the conflict between blockchain transparency and privacy in smart contracts? What mechanisms has the European Union adopted to manage this conflict? And how can these experiences be utilized to develop a localized framework within Iranian law?

The central hypothesis of this research is that by adopting a flexible and hybrid approach—based on differentiating levels of transparency and employing legal–technical solutions—it is possible to safeguard privacy requirements without negating the advantages of blockchain technology. Achieving this objective requires revising domestic legislation, enacting comprehensive personal data protection regulations, and specifically regulating smart contracts. The findings of this study may help identify existing legislative gaps and provide a basis for future legal reforms aimed at enhancing legal security in blockchain-based transactions.

Fundamental Concepts and Principles

Definition of Data and Relevant Parties in Smart Contracts

In the context of blockchain-based smart contracts, “relevant parties” refers to a broad range of actors who, although they may not be direct contractual parties, are considered stakeholders due to their involvement in personal data processing, their technical role, or their exposure to the effects of automated contract execution. These actors may include network users, blockchain service providers, smart contract developers, validators, and even individuals whose data are indirectly recorded or processed on the chain. Unlike the traditional doctrine of the relativity of contractual effects, smart contracts extend their impact beyond the immediate parties, thereby underscoring the necessity of identifying the legal status of relevant parties (1).

In advanced legal systems, particularly within the European Union, the concepts of “data subjects” and “data controllers and processors” are recognized as the basis for defining the rights and obligations of non-contractual actors. Relying on these concepts, the European regulatory framework enables the exercise of privacy rights even with respect to data processing activities that occur outside the traditional contractual framework (3). This approach demonstrates that, in the blockchain environment, the absence of a direct contractual relationship does not preclude the recognition of rights for individuals affected by data processing.

By contrast, Iranian law has yet to provide a clear definition of relevant parties in the context of smart contracts and blockchain technology, with existing legislation primarily focusing on direct contractual relationships. This conceptual gap has left the legal status of individuals whose data are processed on blockchain platforms uncertain and has posed challenges to the effective protection of their privacy rights (5).

Principles of Transparency and Privacy in Smart Contracts

Transparency is a fundamental principle of blockchain technology, ensuring trust among network participants through the public and immutable recording of data. In smart contracts, this transparency enhances traceability in the performance of obligations and reduces disputes arising from non-performance (2). However, this same feature

may conflict with the principle of privacy, as data recorded on blockchain platforms—despite not directly revealing identities—can often be re-identified.

The principle of privacy, particularly in European Union law, is recognized as a fundamental right and encompasses rights such as control over personal data, limitations on processing, and the right to data erasure. Applying these principles in an environment where data are permanently and distributively stored involves significant technical and legal challenges (4). For instance, enforcing the “right to be forgotten” conflicts with the immutable nature of blockchain data, and differing interpretations of this right can have varying implications for the development of smart contracts.

In the Iranian legal system, although respect for privacy is emphasized in various legal instruments, no clear balance has been established between technological transparency and data confidentiality in the context of smart contracts and blockchain. As a result, blockchain transparency is often implemented without sufficient guarantees for personal data protection, thereby increasing the risk of privacy violations (8).

Concepts Related to Data Recording, Processing Control, and Actor Responsibility

Data recording on blockchain: Data recording on blockchain refers to the storage of information in interconnected and immutable blocks. While this process enhances transparency and security, it also raises legal questions regarding the nature of personal data, the scope of their dissemination, and the possibility of modification or deletion. European approaches have sought to mitigate this tension by distinguishing between on-chain and off-chain data storage (7).

Control and processing of personal data: In smart contracts, determining which entity qualifies as the “data controller” is of fundamental importance. In public blockchains, the decentralized structure distributes this role collectively among participants, complicating the attribution of legal responsibility (6). In the European Union, broad interpretations of the concept of data controller have enabled responsibility to be attributed to developers or principal network operators.

Responsibility of non-contractual actors: One of the core challenges in smart contracts concerns the liability of actors who are not contractual parties but are involved in design, execution, or maintenance. Code developers, platform providers, and validators may all be subject to claims in cases of privacy violations or damages arising from data processing. In Iranian law, the absence of specific rules in this area has led to uncertainty in liability attribution and a reduction in legal security (9).

Overall, an examination of these fundamental concepts and principles demonstrates that blockchain-based smart contracts, by expanding the range of relevant parties and creating tensions between transparency and privacy, pose novel challenges for legal systems. While the European Union has taken steps toward managing this conflict through comprehensive regulation and flexible interpretation, Iranian law still requires precise conceptual clarification and the development of clear legal frameworks to simultaneously support technological innovation and protect fundamental rights.

International Legal Frameworks

The Role of European Union Regulations in Managing the Transparency–Privacy Conflict

As one of the most advanced legal systems in regulating emerging technologies, the European Union has played a decisive role in developing legal frameworks for the protection of personal data in digital environments, including blockchain and smart contracts. With the aim of balancing technological innovation and the safeguarding of individuals' fundamental rights, the EU has articulated a set of binding principles governing the processing of personal data (3). Although these rules were not drafted specifically for blockchain, they are frequently treated as a reference framework for analyzing the tension between transparency and privacy in blockchain-based systems (4).

A key element in the EU approach is the identification of the roles of "data controller" and "data processor," which enables the attribution of legal responsibility to different actors within the blockchain ecosystem. While accurately assigning these roles in decentralized networks is inherently difficult, European legal and regulatory interpretations have adopted an expansive reading of these concepts in order to mitigate accountability gaps in smart-contract settings (7). This indicates that the European Union is not attempting to negate blockchain transparency, but rather to regulate its legal effects within a privacy-oriented normative structure.

From an operational perspective, EU rules allow the exercise of certain data-subject rights—such as the right of access, the right to restriction of processing, and, in specific circumstances, the right to erasure. Although these rights appear to conflict with blockchain immutability, they have been considered partially achievable through interpretive and technical strategies, including off-chain data storage (4). In this way, EU data-protection regulation plays a central role in managing the conflict between blockchain's structural transparency and privacy requirements.

The Status of Digital Trust Instruments and the Regulation of Smart Contracts

In addition to EU data-protection rules, the European regulatory framework governing electronic identification and trust services provides an important basis for structuring digital interactions and technology-enabled contracting. By emphasizing the legal validity of electronic signatures, digital identification, and trust services, this framework complements privacy and accountability standards by reinforcing the legal security of smart-contract transactions—particularly where authenticity, attribution, and evidentiary reliability are at stake (8). Even when such rules do not explicitly reference blockchain, their principles on attribution and legal enforceability are highly instructive in assessing the legal effects of smart contracts.

One of the core challenges of smart contracts is identifying the parties and attributing automated actions to natural or legal persons. By recognizing tiers of electronic signatures and trust services, the EU model facilitates alignment between blockchain's technical processes and legal requirements. This becomes especially significant where blockchain transparency may lead to disclosure of identity-related data and where robust identification mechanisms and access controls are needed to reduce privacy risk (6).

Alongside these instruments, the European Union adopted the "Artificial Intelligence Act" in 2024, reflecting a more holistic approach to automated technologies. Although the Act primarily addresses artificial intelligence, its emphasis on algorithmic transparency, accountability, and risk management can also inform regulatory thinking about smart contracts. This regulatory overlap suggests that the EU is seeking an integrated governance architecture for emerging technologies, designed to minimize conflicts between technical transparency and individuals' fundamental rights.

A Comparative Review of International Tools for Managing the Transparency–Privacy Conflict

Comparing the European Union's approach with that of other systems indicates that the EU strategy for managing the conflict between blockchain transparency and privacy is grounded in flexible, multi-layered regulation. The principal tools used in this framework include the following:

1. **Differentiation of transparency levels:** In the EU approach, transparency is not treated as an absolute requirement. Rather, different levels of disclosure and access are contemplated depending on the nature of the data and the degree of sensitivity. This allows the preservation of blockchain's functional transparency without necessarily disclosing personal data (2).
2. **Complementary legal–technical measures:** Off-chain storage, pseudonymization, and advanced cryptographic techniques are employed alongside legal rules to reduce tensions between blockchain immutability and privacy rights (7).
3. **Accountability and attribution of responsibility:** By defining the concepts of data controller and data processor, European rules attempt to make privacy violations attributable even in decentralized networks, thereby strengthening user trust and enhancing legal certainty for smart contracts (4).
4. **Dynamic interpretation of fundamental rights:** When confronting issues such as the right to erasure (often framed as the "right to be forgotten"), European institutions have tended toward a dynamic rather than rigid interpretation, enabling practical compatibility between the right and blockchain's technical characteristics (1).

Overall, international legal frameworks—particularly in the European Union—demonstrate that the transparency–privacy tension in blockchain systems is not inherently insoluble. With appropriate legal and technical design, a workable equilibrium can be achieved. By contrast, comparison with Iran highlights that the absence of comprehensive data-protection rules and the lack of specific regulation for smart contracts remain the principal barriers to the secure and lawful use of blockchain. Selective borrowing and contextual adaptation of international tools could therefore be an effective step toward strengthening Iran's legal system and reducing transparency–privacy challenges in smart contracts.

The Iranian Legal System

Examining Iran's Legal Frameworks for Data Protection and Digital Contracts

Digital transformation and the expanding use of blockchain and smart contracts have placed the Iranian legal system before new questions—questions that centrally concern the relationship between "technical transparency" and "privacy." In Iran, while certain rules exist in the field of electronic commerce and the legal recognition of data messages, there is still no comprehensive, integrated framework comparable to the EU model for protecting personal data and allocating responsibility for data processing in novel technological environments. As a result, analyzing the tension between blockchain transparency and privacy in smart contracts within Iran necessarily depends on fragmented provisions and general legal principles, such as the binding force of obligations, the prohibition of harm, respect for others' rights, and privacy protections.

The Electronic Commerce Act of 2003, by recognizing "data messages" and "electronic signatures," represents an initial step toward acknowledging the legal effects of digital interactions. However, it primarily addresses the validity of electronic documents and transactions rather than systematically regulating data-processing operations

or defining responsibility-bearing roles within technology chains. Meanwhile, smart contracts deployed on blockchain networks may permanently record and redistribute transactional, identity-related, or behavioral data, yet Iranian law lacks explicit rules on the “lawfulness limits of permanent storage,” the “right of access/correction,” or the “responsibility of actors involved in data processing” in such contexts.

From a comparative standpoint, the EU model treats concepts such as data controller and data processor as the foundation for allocating legal responsibility in personal data processing (4). In Iran, even if one attempts to derive liability for developers or operators of smart-contract systems from general civil-liability doctrines, the absence of parallel statutory concepts and the lack of operational standards create substantial uncertainty in practice (5).

Legal Challenges Related to the Transparency–Privacy Conflict in Iran

Iran’s challenges in addressing the conflict between transparency and privacy can be assessed across three levels: legislative, supervisory, and enforcement.

1. **Absence of a comprehensive personal data protection law**: The most significant gap in Iran is the lack of an overarching statute governing the processing of personal data in digital environments. This gap prevents essential requirements—such as informed consent, purpose limitation, data minimization, and storage limitation—from becoming enforceable and systematically reviewable within the legal system. In such circumstances, blockchain transparency—premised on permanent recording and transaction traceability—may lead to disclosure of personal data or to the re-identification of users without clearly defined remedies or safeguards (1).
2. **Ambiguity in allocating responsibility among blockchain and smart-contract actors**: In blockchain networks, roles are distributed among developers, platform operators, network nodes/validators, and users. Iranian law does not provide a clear mechanism for determining “who is responsible for data processing.” This ambiguity complicates attribution of civil liability and the pursuit of damages in cases of privacy infringement (7). At the same time, it may cause smart contracts to be perceived in practice as “low-accountability” tools, despite their capacity to directly affect individuals’ fundamental rights (4).
3. **Conflict between blockchain immutability and requirements for data erasure/correction**: A focal point of the tension is blockchain’s immutability. While technically advantageous, it can conflict with privacy-related rights associated with correcting or deleting data. In the EU context, this conflict is managed through interpretive and technical solutions such as off-chain data handling and pseudonymization (4). In Iran, not only is the legal basis for such rights not clearly specified, but even where such rights might be inferred, the supervisory and enforcement instruments needed to compel compliance are largely absent (9).

Iran’s Practical Practice and Status in Dealing with Smart Contracts and Related Data

In Iran, practical engagement with smart contracts and their privacy implications has been shaped less by a settled body of judicial practice and more by “caution,” “case-by-case interpretation,” and, at times, “implementation ambiguity.” Part of this stems from the novelty of the subject, and part from the absence of explicit rules and a specialized data-protection supervisory authority. Accordingly, legal assessment of smart contracts before courts or quasi-judicial bodies tends to focus on evidentiary admissibility, proof value of digital data, and the binding nature of obligations, rather than on the legality boundaries of data processing or the rights of data subjects (10).

1. **Evidentiary admissibility and the risk of data disclosure**: Some domestic studies emphasize the feasibility of invoking smart contracts before Iranian courts, while simultaneously warning that transparent and permanent on-chain recording may lead to unintended disclosure or re-identification, generating notable legal and social risk in the absence of protective standards (10). This risk becomes more acute in financial and banking disputes, where transactional data can reveal individuals' behavioral and economic patterns (11).
2. **Lack of a clear practice on liability for privacy violations in smart-contract settings**: In the absence of explicit legislation, where privacy is violated through the execution of a smart contract, legal claims are typically routed through general civil-liability rules and broad legal principles. However, these frameworks were not designed for decentralized technologies and often fail to provide a clear answer to the question of "the primary responsible party" (5). As a result, even where harm occurs, proving causation, fault, and attribution to an identifiable party may be difficult.
3. **Implementation challenges for legal–technical safeguards**: In certain fields, measures such as digital identity management and access control have been proposed to reduce privacy risk. While these tools can restrict data visibility, they require binding legal rules and supervisory standards to avoid remaining purely technical recommendations (12). Otherwise, the transparency–privacy tension is not "regulated," but instead becomes a mechanism for shifting risk to users.

Overall, the Iranian legal system faces three structural problems in addressing the transparency–privacy conflict in blockchain-based smart contracts: the absence of a comprehensive data-protection statute, ambiguity in allocating responsibility among network actors, and the lack of enforcement and supervisory mechanisms capable of managing data immutability. In contrast, the European Union has attempted—through its data-protection framework and complementary instruments—to strike a balance between innovation and fundamental rights. Moving toward a localized data-protection framework and defining roles and responsibilities within the blockchain ecosystem can therefore be an effective step in reducing this conflict and enhancing legal certainty for smart contracts in Iran.

Aligning Iran's Legal System with International Rules

Differences and Similarities Between Iran's Approach and International Standards in the Blockchain Transparency–Privacy Conflict

In responding to emerging digital technologies—particularly blockchain and smart contracts—Iran's legal system has generally adopted a gradual and cautious approach. The enactment of the Electronic Commerce Act of 2003 and the recognition of the legal validity of data messages and electronic signatures reflect the Iranian legislature's willingness to achieve a degree of alignment with technological developments, which may be considered partially consistent with international approaches. However, with respect to the conflict between blockchain's inherent transparency and privacy requirements, fundamental differences can be observed between Iran's legal system and international standards, particularly those associated with the European Union.

1. **Conceptual approach to privacy**: Under international standards—especially the EU model—privacy (and, more precisely, personal data protection) is treated as an independent, fundamental right, and the processing of personal data is conditioned on principles such as informed consent, purpose limitation, proportionality, and data minimization (4). By contrast, within Iran's legal system, privacy protection tends

to be scattered and implicit, operating through general doctrines such as civil liability, the prohibition of harm, and certain constitutional principles, without a coherent legislative framework tailored to decentralized technologies. This divergence has contributed to a tendency in Iran to view blockchain transparency primarily as a technical advantage, rather than as a phenomenon that can potentially endanger individuals' fundamental rights.

2. **Technical transparency versus legal transparency**: In the European Union, transparency in data processing is understood in legal terms as the possibility of legal oversight, accountability, and the enforceability of data-subject rights. In Iran, however, blockchain transparency is often analyzed mainly at the technical and evidentiary level, with less attention to its legal dimensions—such as rights of access, rectification, or erasure. This difference increases the risk that technical transparency in smart contracts, absent controlling legal mechanisms, becomes a tool for user re-identification and traceability.
3. **The role of consent and data control**: In international standards, consent is central to the lawfulness of data processing, and mechanisms exist for withdrawal or restriction. In Iran, although consent may be conceptualized through contractual clauses or acceptance of platform terms, the lack of specific regulation means that such consent is often formalistic and not meaningfully revisable—particularly in smart contracts that, once executed, provide little practical opportunity for suspension or correction (1).

Analyzing Legal Weaknesses and Gaps in Iran's Approach to Blockchain and Smart Contracts

Despite certain legal capacities, Iran's legal system faces substantial weaknesses and gaps in regulating the conflict between blockchain transparency and privacy, which can be analyzed along several core dimensions.

1. **Absence of explicit and comprehensive data protection regulation**: The most significant legislative gap in Iran is the lack of a comprehensive personal data protection law. This omission means that core standards for data processing—such as the lawfulness of permanent on-chain storage, limits on secondary uses of transactional data, and rules on responsibility for privacy violations—are not clearly defined. As a result, smart contracts may record and redistribute data with long-term privacy implications without effective legal constraints.
2. **Ambiguity in allocating legal responsibility among blockchain actors**: In international standards, the concepts of "data controller" and "data processor" provide the basis for responsibility attribution. In Iran, the absence of comparable legal categories makes it unclear whether liability for a privacy breach rests with the smart-contract developer, the platform operator, users, or the distributed network itself. This ambiguity significantly weakens the ability to claim damages and to apply meaningful sanctions (7).
3. **Blockchain immutability versus individual rights**: Blockchain immutability is managed in international systems through flexible interpretations and legal–technical measures. In Iran, the lack of legal recognition for concepts analogous to a "right to be forgotten" or a "right to rectification" means that this conflict remains largely unresolved and, in practice, tends to be settled in favor of technical transparency at the expense of individuals' privacy.
4. **Absence of settled judicial practice**: Within Iran's judiciary, disputes involving blockchain and smart contracts are still addressed sporadically and on a case-by-case basis, and no consistent jurisprudential approach has emerged regarding the transparency–privacy conflict. This increases legal uncertainty and raises the risk of using smart contracts in sensitive transactions.

Opportunities for Harmonizing Iran's Legal System with International Standards

Notwithstanding these challenges, Iran's legal system has certain pathways for gradual convergence with international standards in the area of blockchain and privacy.

1. **Enacting a comprehensive data protection law with a localized approach**: A calibrated borrowing from international data-protection models—adapted to Iran's domestic legal, cultural, and security considerations—could provide a coherent framework for governing personal data in smart contracts. Such a statute could clearly draw the boundary between technical transparency and legal transparency.
2. **Defining roles and responsibilities within the blockchain ecosystem**: Clarifying the legal position of developers, operators, and users of smart contracts could reduce responsibility ambiguity and enable meaningful accountability.
3. **Providing exceptions and legal solutions for immutability**: Recognizing measures such as off-chain storage for personal data and access-restriction mechanisms could substantially mitigate tensions between blockchain architecture and privacy rights (7).
4. **Strengthening judicial training and specialized adjudication**: Judicial training and the development of specialized guidance for decentralized technologies could contribute to more consistent jurisprudence and enhance the predictability of judicial outcomes.

Overall, aligning Iran's legal system with international standards on the blockchain transparency–privacy conflict requires a shift from fragmented, reactive regulation toward active and anticipatory governance. Drawing on the European Union's experience—without mechanical imitation—can support the development of a sustainable balance between technological innovation and the protection of fundamental rights, a balance that is essential to the trustworthiness and effectiveness of smart contracts within Iran's legal environment.

Research Findings

Challenges and Limitations in Iranian Law

The findings of this research indicate that Iran's legal system, despite generally recognizing the validity of electronic instruments, faces serious challenges and constraints in managing the tension between blockchain's structural transparency and the protection of users' privacy. These challenges can be explained along several fundamental axes.

1. **Conflict between blockchain's technical transparency and legal protection of privacy**: A defining feature of blockchain is the transparency and traceability of transactions, which is regarded at the technical level as an advantage for trust and security. However, the findings show that in Iran this technical transparency is not accompanied by adequate legal constraints and may therefore lead to disclosure of personal data or indirect re-identification of users. The absence of explicit rules defining permissible transparency boundaries means that blockchain transparency can prevail over privacy without due regard to proportionality and necessity, thereby undermining data-centered fairness.
2. **Lack of a comprehensive framework for personal data protection**: The research further shows that one of Iran's most serious legal gaps is the absence of an independent and comprehensive personal data protection statute. As a result, concepts such as informed consent, purpose limitation, data minimization, and the right to control personal information lack binding legal support in the context of smart contracts.

Consequently, permanent data recording in distributed ledgers, without legal safeguards, may produce ongoing privacy violations and conflict with fundamental-rights principles (4).

3. **Ambiguity in allocating legal responsibility in the blockchain ecosystem**: Another key finding is the severe uncertainty surrounding responsibility attribution among blockchain actors. Iranian law does not clearly indicate which party bears legal responsibility for privacy violations arising from smart-contract execution—whether the developer, the platform operator, the user, or the decentralized network as a whole. This ambiguity impedes effective compensation claims and enforcement mechanisms and weakens practical protection of individual rights (7).
4. **Absence of coherent and specialized judicial practice**: An assessment of available judicial practice indicates that Iranian courts have not yet developed a systematic legal approach to blockchain and smart contracts. Technical–legal expertise remains limited, and interpretive guidance is lacking, resulting in scattered and occasionally inconsistent decisions. This intensifies legal uncertainty and reduces economic actors' confidence in deploying smart contracts in practice (10).

Advantages of Applying International Principles and Standards to Iran's Legal System

The comparative findings of this research indicate that a targeted application of international principles and standards—particularly the European Union's approach to personal data protection—can play a meaningful role in mitigating existing challenges within Iran's legal system. The most significant advantages of such alignment include the following.

1. **Establishing a balance between technological innovation and fundamental rights**: International standards demonstrate that it is possible to preserve the technical advantages of blockchain while, through intelligent regulation, achieving a sustainable balance between transparency and privacy. This balance is realized through principles such as proportionality, necessity, and purpose limitation (4).
2. **Enhancing legal predictability and legal security**: The adoption of clear data-protection frameworks increases legal predictability for users, investors, and smart-contract developers. This reduces legal risks and facilitates the use of blockchain technology in economic activities (7).
3. **Strengthening accountability and responsibility**: By precisely defining roles and responsibilities in data processing, international standards enable effective accountability in cases of privacy violations. This approach can likewise serve as a foundation for legislative reform within Iran's legal system (5).
4. **Improving Iran's position in cross-border digital interactions**: Relative harmonization with international standards—especially in the field of data protection—can enhance Iran's participation in cross-border blockchain projects and attract foreign investment, developments that are difficult to achieve in the absence of legal trust (3).

The Impact of Adaptive Mechanisms on Ensuring Data-Centered Justice

The results of the research indicate that employing international adaptive mechanisms has a direct impact on achieving data-centered justice in smart contracts. These impacts can be summarized along several core dimensions.

1. **Lawful control of blockchain transparency**: Regulating blockchain transparency within a clearly defined legal framework prevents technical transparency from becoming a tool for privacy infringement and ensures proportionate data use (1).
2. **Guaranteeing users' informational rights**: The legal recognition of rights such as the right to information, the right of access, the right to restriction of processing, and even moderated forms of the right to erasure can strengthen users' positions vis-à-vis decentralized structures (4).
3. **Reducing conflict between immutability and individual rights**: Legal–technical measures such as off-chain storage of personal data and advanced cryptographic techniques can mitigate tensions between blockchain immutability and privacy requirements (7).
4. **Standardizing judicial and legislative practices**: Alignment with international principles can provide a basis for developing judicial guidelines and fostering consistency in adjudicating blockchain-related disputes, which plays a key role in ensuring justice and public trust (10).

Overall, the findings indicate that the conflict between blockchain transparency and privacy in smart contracts within Iran's legal system stems less from the inherent nature of the technology and more from legislative gaps and the absence of data-centered regulation. A measured adoption of international standards—without mechanical imitation—can facilitate a balanced approach that reconciles digital innovation with the protection of fundamental rights and supports the secure and lawful development of smart contracts in Iran.

Conclusion

The present study, focusing on the tension between the inherent transparency of blockchain technology and the legal requirements of privacy in the context of smart contracts, has undertaken a comparative analysis of the Iranian legal system and the standards of the European Union. The findings demonstrate that although blockchain, as an innovative infrastructure, offers significant potential for enhancing security, trust, and transparency in digital transactions, the absence of coherent legal frameworks in Iran has, in some instances, transformed this technical transparency into a threat to individuals' privacy.

The results indicate that within the Iranian legal system, privacy protection in the realm of smart contracts is largely fragmented, unsystematic, and grounded in general legal principles rather than in a comprehensive, data-centered regime. This situation has led to the practical lack of effective enforcement for fundamental concepts such as informed consent, proportionality in data processing, purpose limitation, and the right to control personal information. By contrast, the European Union, through the adoption of instruments such as the General Data Protection Regulation, has succeeded in establishing a coherent framework for regulating the relationship between technological transparency and individuals' fundamental rights—a framework that embraces technological innovation while treating privacy as a non-derogable fundamental right.

The comparative analysis reveals that the principal difference between the two systems lies not in the acceptance of blockchain technology itself, but in the manner of its legal regulation. While the European Union's approach is characterized by proactive, responsibility-oriented, and data-centered regulation, Iran's legal system continues to rely on a reactive and minimalist approach and has yet to provide clear legal responses to the emerging challenges of blockchain. This legislative and practical gap has not only weakened the protection of users' privacy but has also reduced legal certainty, increased contractual risks, and limited the practical usability of smart contracts in sensitive transactions.

The study further shows that continuation of this situation may have wide-ranging negative effects on public trust in decentralized technologies, the development of the digital economy, and Iran's cross-border interactions. Conversely, a gradual and intelligent alignment with international standards—without mechanical imitation and with due regard to domestic considerations—can create the conditions for a sustainable balance between blockchain transparency and privacy protection, thereby strengthening Iran's legal position in the field of emerging technologies.

Based on the research findings, the following recommendations are proposed to improve Iran's legal framework in addressing the conflict between blockchain transparency and privacy in smart contracts.

1. **Enactment of a comprehensive personal data protection law with a localized approach**: It is recommended that the Iranian legislature adopt a selective and contextualized approach to international models and enact an independent and comprehensive personal data protection law that specifically addresses data processing in decentralized technologies and smart contracts.
2. **Clear definition of legal responsibilities within the blockchain ecosystem**: It is essential to precisely define the roles and legal responsibilities of various blockchain actors, including smart-contract developers, platform operators, and users, in order to enable accountability and compensation in cases of privacy violations.
3. **Regulating blockchain transparency based on proportionality and necessity**: Blockchain transparency should be legally constrained and guided so that it is applied only to the extent necessary to achieve legitimate contractual objectives and does not result in unnecessary or permanent disclosure of personal data.
4. **Recognition of legal–technical solutions to mitigate data immutability conflicts**: The legislature may formally recognize measures such as off-chain storage of personal data, advanced encryption, and the separation of identity data from transactional data as complementary legal tools for reducing conflicts arising from data immutability.
5. **Strengthening specialized training for judges and legal professionals in blockchain matters**: Providing specialized training programs for judges, lawyers, and policymakers in blockchain technology and its legal implications can contribute to the development of consistent jurisprudence and improve the quality of judicial decision-making.
6. **Gradual convergence with international standards in cross-border interactions**: It is recommended that Iran, in cross-border smart contracts, progressively consider internationally accepted principles and standards in data protection and privacy in order to strengthen legal trust among foreign counterparties.

Ultimately, this study demonstrates that resolving the conflict between blockchain transparency and privacy in smart contracts requires not the restriction of technology, but rather intelligent, data-centered, and balanced legal regulation. Advancing toward such an approach can preserve the innovative advantages of blockchain while safeguarding individuals' fundamental rights and fostering the sustainable development of the digital economy within Iran's legal system.

Acknowledgments

We would like to express our appreciation and gratitude to all those who helped us carrying out this study.

Authors' Contributions

All authors equally contributed to this study.

Declaration of Interest

The authors of this article declared no conflict of interest.

Ethical Considerations

All ethical principles were adhered in conducting and writing this article.

Transparency of Data

In accordance with the principles of transparency and open research, we declare that all data and materials used in this study are available upon request.

Funding

This research was carried out independently with personal funding and without the financial support of any governmental or private institution or organization.

References

1. Sklaroff J. Smart contracts and the cost of inflexibility. University of Pennsylvania Law Review. 2017;166:263-303.
2. Mougayar W. The business blockchain: Promise, practice, and application of the next internet technology: Wiley; 2016.
3. Martinet L. Exercising digital sovereignty over blockchains: A case study from France. Stanford Journal of Blockchain Law & Policy. 2020;4(1):1-25.
4. Kasatkina M. The interpretation of smart contracts in the EU and the USA. International Comparative Jurisprudence. 2021;7(2):202-17.
5. Naser M, Sadeghi H. Validation and legal challenges of employing smart contracts with a comparative study of the Iranian and American legal systems. Private Law Research. 2019;7(27):225-88.
6. Allen T, Widdison R. Can computers make contracts? Harvard Journal of Law & Technology. 1999;12(1):25-52.
7. Finocchiaro G, Bomprezzi C. A legal analysis of the use of blockchain technology for the formation of smart legal contracts. Media Laws. 2020(2):111-35.
8. Karimi S, Sinambari P. A comparative study of digital signatures in smart contracts in the laws of Iran and the United States. Legal Research. 2024(10):2-14.
9. Hooshmand S, Pirouzi P, Monavari H, Mazloum-Rahni A. Challenges of implementing smart contracts in the legal systems of Iran and India. Legal Studies in the Digital Age. 2024;3(3):143-58. doi: 10.61838/kman.lsda.3.3.13.
10. Razavi SM, Khandani SP. Feasibility of citing smart contracts in Iranian courts. Media Jurisprudence and Law Studies. 2024;6(2):181-206.
11. Eynollahi N, Ahmadi F, Mohammadipour R, Arayesh M. Presenting a blockchain technology model in smart contracts for the banking industry. Investment Knowledge. 2023;14(53):179-200.
12. Abizadeh A, Fathi Z, Minoui M. Access control in financial smart contracts using digital identity management and machine learning to facilitate IoT exchanges. Financial Knowledge of Securities Analysis (Financial Studies). 2022(53):111-22.