KMANPUB | AI and Tech in Behavioral and Social Sciences Vol. 4 No. 4 (2026): 1-9

Article history:
Received 21 February 2026
Revised 21 June 2026
Accepted 28 June 2026
Initial Publication 08 July 2026
Final Publication 01 October 2026

Challenges in Harmonizing AI-Enabled Smart Contracts with the General Principles of Contract Law in the Iranian Legal System: A Digital Governance Perspective

Hamid. Kaboudjai[1*]

[1] Master of Science in Computer Engineering - Software, Iran University of Science and Technology, Tehran, Iran

*** Corresponding author email address**: Hamid.ka19@gmail.com

A r t i c l e I n f o

Article type:
Review Article

How to cite this article:
Kaboudjai, H. (2026). Challenges in Harmonizing AI-Enabled Smart Contracts with the General Principles of Contract Law in the Iranian Legal System: A Digital Governance Perspective. *AI and Tech in Behavioral and Social Sciences*, *4*(4), 1-9.
https://doi.org/10.61838/kman.aitech.5727

A B S T R A C T

This study examines the challenges of harmonizing AI-enabled smart contracts with the general principles of contract law in the Iranian legal system from a digital governance perspective. Unlike purely blockchain-based smart contract code, AI-enabled smart contracts may involve algorithmic tools in contract drafting, party verification, oracle-based factual assessment, performance monitoring, risk scoring, or dispute-resolution support. This distinction is central because ordinary smart contract code is typically deterministic, whereas AI systems may generate probabilistic or adaptive outputs that complicate the attribution of consent, responsibility, and legal effect. The study adopts a doctrinal and descriptive-analytical method, relying on Iranian statutory materials, contract-law doctrine, selected comparative scholarship, and leading literature on smart contracts, blockchain governance, and algorithmic accountability. The analysis shows that smart contracts may fall within the scope of Iranian contract law when they operate as electronic instruments for expressing and executing human intention. However, serious challenges remain regarding the verification of legal identity and capacity in pseudonymous blockchain environments, the formation of informed consent through code, the uncertain legal status of cryptocurrencies and tokenized assets, the tension between automated execution and mandatory legal rules, and civil liability for technical or algorithmic failures. The study argues that effective recognition of AI-enabled smart contracts in Iran requires a layered governance model: reliable digital identity mechanisms, human-readable contractual terms accompanying executable code, clear rules on digital assets, auditable and legally responsive code architecture, professional standards for developers, and judicial or arbitral mechanisms capable of reviewing technical execution without undermining innovation. These reforms can help integrate smart contracts into Iran's legal system while preserving contractual justice, public policy, and legal certainty.

Keywords: *artificial intelligence, smart contracts, blockchain, Iranian contract law, digital governance, electronic contracts, cryptocurrency*

1. Introduction

The acceleration of digital transformation and the expanding use of blockchain-based technologies have introduced a new phenomenon known as the smart contract, which has substantially reshaped commercial and legal transactions. Initially conceptualized as a set of protocols designed to execute contractual terms automatically, smart contracts acquired broader legal and technical significance with the emergence of distributed ledger technologies. By combining computer code with network consensus mechanisms, smart contracts enable the automatic performance or recording of obligations without reliance on traditional intermediaries such as banks, notaries, or centralized enforcement institutions (Raskin, 2017; Sadiku et al., 2018; Werbach & Cornell, 2017). These features offer important advantages, including lower transaction costs, faster execution, and greater transparency. At the same time, they raise fundamental questions about the place of such instruments within traditional legal systems, particularly the Iranian legal system.

For conceptual accuracy, this study distinguishes among three related but different categories: smart contract code, smart legal contracts, and AI-enabled smart contracts. Smart contract code refers to software that automatically executes or records pre-defined operations. A smart legal contract refers to a legally binding agreement in which some contractual terms are expressed or performed through code. AI-enabled smart contracts go further: they may incorporate algorithmic tools in contract drafting, party verification, performance monitoring, risk assessment, oracle-based factual evaluation, or dispute-resolution support. This distinction is important because blockchain code is usually deterministic, while AI systems may operate through probabilistic or adaptive outputs. Therefore, the legal questions raised by AI-enabled contracting concern not only automation and immutability but also algorithmic accountability, explainability, and governance (Scherer, 2016; Yeung, 2018).

Iranian contract law, which is rooted in Imami jurisprudence and civil-law principles centered on intention and consent, establishes specific requirements for contractual validity. Article 190 of the Iranian Civil Code identifies four essential conditions for any valid transaction: intention and consent, legal capacity, a definite subject matter, and the lawfulness of the contractual purpose. The compatibility of technically mediated contracting with these requirements requires careful analysis (Bahrkazemi & Mahmoudi, 2024). In conventional contracts, contractual intention is ordinarily expressed through natural language. In smart contracts, however, parties may express intention through cryptographic private keys, digital signatures, interaction with decentralized applications, or deployment of executable code (Antonopoulos & Wood, 2018; Naser, 2018). The central question is whether such technical acts can produce the same legal effects as traditional offer and acceptance.

One of the most complex issues is the identification and legal capacity of contracting parties in decentralized environments. In public blockchain systems, users often operate through pseudonymous or semi-anonymous identities, and no formal mechanism necessarily verifies age, legal maturity, mental competence, or representative authority. This creates the risk that transactions may be concluded by persons lacking legal capacity or by persons who are not legally authorized to bind an organization (Naser, 2018; Rashvand Boukani & Naser, 2019). A related challenge concerns informed consent. Where parties cannot understand the practical and legal consequences of executable code, the assumption of genuine contractual consent becomes weaker.

Digital assets, particularly cryptocurrencies and tokenized assets, create a further layer of uncertainty. The current Iranian regulatory framework has imposed restrictions on the use of cryptocurrencies as means of payment, while some legal and jurisprudential discussions recognize their economic value as digital assets (Khordmand, 2019). This distinction between a tradable asset and a payment instrument is central to assessing contractual validity. Moreover, the immutability and self-execution of blockchain-based smart contracts may conflict with mandatory legal rules and public policy, particularly where illegality, coercion, fraud, mistake, or judicial intervention is involved (Nejatzadegan & Soltani, 2022).

Beyond formation and validity, civil liability arising from technical defects, cybersecurity vulnerabilities, or AI-based decision errors also requires clarification. Since software lacks independent legal personality under Iranian law, liability must generally be attributed to developers, deployers, users, platform operators, or other identifiable actors. However, proving causation between a coding defect, an algorithmic output, and the resulting harm may be difficult in decentralized environments. This problem supports the need for professional standards, audit

AITBSS AI and Tech in Behavioral and Social Sciences E-ISSN: 3041-9433

obligations, insurance mechanisms, and a broader digital governance framework.

This article therefore examines the principal legal challenges involved in harmonizing AI-enabled smart contracts with the general principles of contract law in Iran. It focuses on contractual nature, software agency, legal capacity and identity, intention and consent, lawful subject matter, cryptocurrencies, public policy, judicial intervention, and civil liability. By adopting a digital governance perspective, it identifies where existing Iranian legal doctrines are sufficient and where legislative, regulatory, or technical reform is required.

2. Methodology

This study uses a doctrinal and descriptive-analytical legal method. It examines relevant provisions of Iranian private law, particularly the Iranian Civil Code and the Electronic Commerce Act, and analyzes them in light of domestic legal doctrine on electronic contracts, smart contracts, legal capacity, consent, and civil liability. The study also relies on selected comparative and international scholarship on smart contracts, blockchain, automated contracting, algorithmic liability, and digital governance.

The sources were selected on the basis of their direct relevance to four questions: whether smart contracts may constitute legally binding contracts under Iranian law; how intention, consent, capacity, and subject matter can be verified in automated environments; how mandatory rules and public policy interact with self-executing code; and how liability should be allocated where technical or AI-related errors cause loss. Sources that merely described blockchain technology without legal analysis, or that did not directly relate to contract formation, validity, governance, or liability, were excluded. This method does not claim to offer empirical measurement; rather, it provides a structured normative and doctrinal analysis.

3. The Legal Nature of Smart Contracts Under Iranian Law

The concept of the smart contract was first introduced by Nick Szabo as a mechanism for automating contractual performance through computer protocols (Szabo, 1997). With the emergence of distributed ledger technology, particularly blockchain, the functionality and legal significance of smart contracts expanded. From a technical perspective, a smart contract may be understood as software that automates performance, records legally relevant events, or transfers digital assets according to pre-defined conditions, sometimes using external inputs supplied by oracles or connected systems (Clack et al., 2016; Raskin, 2017).

This technical definition, however, should not obscure the legal distinction between code and contract. Not every smart contract code is a legal contract. Some code merely performs a technical operation, such as transferring tokens or recording data. A legally relevant smart contract exists only where the code implements or evidences a juridical agreement between parties. This distinction is necessary to avoid the overly broad claim that all executable code is contract law. Under Iranian law, smart contracts are best classified as advanced electronic instruments capable of expressing, recording, or executing contractual intention, provided that the substantive requirements of contract formation are satisfied (Naser & Sadeghi, 2019; Rezaei, 2008).

The principle of “code is law” therefore cannot replace legal analysis. Although code may determine technical execution, legal systems determine validity, enforceability, liability, and remedies (Savelyev, 2017; Werbach & Cornell, 2017). Iranian legal doctrine recognizes electronic data messages as legally meaningful means of communication. Consequently, smart contracts should not be treated as autonomous legal orders detached from law but as technological instruments embedded within existing legal frameworks. Their validity depends on whether the parties’ intention, legal capacity, lawful subject matter, and lawful purpose can be established under Iranian contract law.

Accordingly, the legal nature of smart contracts under Iranian law is hybrid. They are not merely ordinary contracts, because execution may be automated and recorded on a distributed ledger. They are also not purely technical artifacts, because they can express and implement legal obligations. The appropriate classification is therefore conditional: smart contracts are legally relevant electronic contracting mechanisms when they are connected to identifiable parties, lawful subject matter, informed consent, and enforceable obligations.

4. The Legal Status of Intelligent Software in the Formation of Contractual Intent

The prevailing view among Iranian legal scholars is that intelligent software functions as a medium for expressing contractual intention rather than as an independent legal actor. Under this approach, actions performed

AITBSS AI and Tech in Behavioral and Social Sciences E-ISSN: 3041-9433

automatically by software are legally attributable to the individual or legal entity controlling the software. Consequently, the contract is concluded between legally competent natural or juridical persons, while the software merely facilitates communication, execution, or documentation (Ahangaran & Ahmadi, 2019; Rahbari & Rezaei, 2011).

This interpretation is consistent with Article 191 of the Iranian Civil Code, under which contracts may be formed through any legally recognizable expression of intention. It is also consistent with Article 10 of the Civil Code, which recognizes party autonomy subject to mandatory rules and public policy (Afzali Mehr, 2019). In this framework, software does not possess intention; rather, it executes or communicates the intention previously attributed to the user, deployer, or principal.

A competing theory analogizes intelligent software to an agent or representative. This analogy may be useful descriptively, especially where AI systems negotiate, recommend, or select terms. However, it encounters doctrinal limits under Iranian law. Agency requires legal capacity and a legally meaningful relationship between principal and agent. Software lacks consciousness, independent volition, patrimony, and legal personality. Therefore, calling it an agent does not solve the problem of liability; it merely shifts the analysis back to the human or legal person who configured, authorized, or deployed the system (Shiravi & Mohammadi, 2009).

The theory of independent legal personality is even more problematic. The Iranian Electronic Commerce Act recognizes electronic systems and data messages for transactional purposes, but such recognition should not be interpreted as granting software independent legal personality. Legal personality requires a statutory basis and entails attributes such as patrimony, legal capacity, rights, duties, and litigation capacity. Intelligent software lacks these attributes. Therefore, in the absence of explicit legislative reform, the dominant position should remain attribution to the user, developer, platform operator, or deployer, depending on the factual context.

This conclusion is particularly important for AI-enabled smart contracts. Where AI participates in drafting, recommending, scoring, or triggering performance, the relevant question is not whether AI itself has legal personality but whether the human or institutional actor behind the system exercised appropriate control, disclosure, supervision, and professional care. This shifts the debate from fictional personhood to governance, accountability, and allocation of risk.

5. Digital Governance Framework for AI-Enabled Smart Contracts

The digital governance perspective requires more than applying traditional contract-law categories to new technology. It asks how legal, technical, institutional, and compliance mechanisms can be designed together so that automated contracting remains compatible with legal certainty, public policy, and accountability. For AI-enabled smart contracts, this requires attention to identity governance, code audit, explainability, human-readable disclosure, cybersecurity standards, data protection, and mechanisms for dispute resolution.

A layered governance model is more appropriate than either full technological autonomy or strict prohibition. At the identity layer, parties should be linked to reliable digital identity mechanisms or qualified electronic signatures when high-value transactions are involved. At the contractual layer, executable code should be accompanied by natural-language terms that define legal obligations, risk allocation, governing law, dispute resolution, and the relationship between code and text. At the technical layer, code should be auditable and, where legally necessary, capable of suspension or controlled intervention. At the institutional layer, courts, arbitral bodies, and regulators should develop technical competence to review code, oracles, and algorithmic decision pathways.

In comparative digital governance, similar concerns appear in debates around algorithmic accountability and AI regulation. The European Union's Artificial Intelligence Act reflects a risk-based regulatory approach to AI systems, while scholarship on algorithmic regulation emphasizes transparency, oversight, and accountability (European & Council, 2024; Scherer, 2016; Yeung, 2018). Although these instruments do not directly determine Iranian law, they provide useful governance concepts: risk classification, human oversight, documentation, auditability, and post-market monitoring. These concepts can be adapted to the Iranian legal context without abandoning domestic contract-law principles.

6. Challenges in Verifying the Identity and Legal Capacity of Contracting Parties

Under Iranian law, legal capacity refers to an individual's competence to acquire and exercise rights and

AITBSS AI and Tech in Behavioral and Social Sciences
E-ISSN: 3041-9433

obligations. Article 211 of the Iranian Civil Code requires maturity, mental competence, and legal capacity (Shahidi, 2011). In smart contracts, the challenge is not the concept of capacity itself but the ability to verify the identity and status of the person using the cryptographic credentials. Determining legal capacity presupposes reliable identification.

Some Iranian scholars argue that qualified electronic signatures reduce this concern because the issuance of a trusted digital certificate requires identity verification by accredited authorities (Rashvand Boukani & Naser, 2019). This argument is stronger for permissioned or regulated systems but weaker for public blockchains. Many smart contracts operate on permissionless networks in which users participate by generating cryptographic key pairs without governmental or institutional identity verification (Naser, 2018). A blockchain address proves control of a private key; it does not prove age, sanity, maturity, legal capacity, representative authority, or lawful possession of the key.

This problem extends beyond natural persons. In commercial settings, a smart contract may be executed by an employee, software agent, or compromised wallet purporting to represent a company. The legal issue is therefore not only whether a natural person is legally competent but also whether the signer had authority to bind a legal entity. Iranian law must address whether cryptographic authorization can be treated as organizational authorization, and under what conditions.

Several mechanisms can mitigate these risks. Permissioned blockchain networks can condition participation on prior identity verification. Off-chain identity verification can connect public keys to verified legal identities through trusted services. Qualified electronic signatures may provide additional safeguards where required by law. However, these solutions also create governance costs: they may reduce decentralization, require trusted intermediaries, and raise data protection concerns. Therefore, the appropriate model should be risk-based. Low-value automated transactions may not require intensive identity verification, while high-value or legally sensitive smart contracts should require stronger digital identity, representative authority verification, and auditable records.

7. Formation of Mutual Intent and Consent

Mutual intention and consent constitute the cornerstone of contractual validity under Iranian law and are expressly recognized under Article 190 of the Civil Code. In smart contracts, intention is typically expressed through digital signatures, deployment of code, transfer of assets to a contract address, or interaction with a decentralized application. Such conduct may constitute an objective manifestation of acceptance where it clearly indicates assent to the relevant terms (O'Shields, 2017; Raskin, 2017). This is broadly consistent with Article 191 of the Civil Code, which does not require a specific form for the expression of intention.

However, code-based consent raises the problem of informed consent. Where the contractual terms are expressed only in programming language, a party may not understand the legal or practical effects of the transaction. Some scholars argue that parties may choose programming language as the medium of contractual expression under the principle of contractual freedom (Durovic & Janssen, 2019). This argument is persuasive only where the parties knowingly understand the code or have access to reliable explanations. If the complexity of the code creates uncertainty about the subject matter, consideration, performance trigger, or allocation of risk, the contract may be vulnerable to challenge under doctrines of mistake, uncertainty, or lack of genuine consent.

For this reason, AI-enabled smart contracts should use dual-layer documentation. The executable code should be accompanied by natural-language terms specifying the legal obligations, the function of the code, the role of any AI system or oracle, the hierarchy between code and text, and the consequences of technical failure. This approach does not deny the validity of code as a medium of expression. Rather, it ensures that code-based execution remains connected to legally meaningful consent.

8. Legality of the Contractual Subject Matter and the Legal Status of Cryptocurrencies

Under Iranian contract law, the legality of the contractual subject matter and the existence of valid consideration are essential requirements for contractual validity under Article 190 of the Civil Code. In many smart contracts, the subject matter or consideration consists of cryptocurrencies or other digital assets. From the perspective of Islamic jurisprudence, views on the permissibility of cryptocurrency transactions remain

AITBSS AI and Tech in Behavioral and Social Sciences E-ISSN: 3041-9433

divided. Some jurists have accepted that Bitcoin may possess proprietary value because it has economic value and is exchanged in markets (Khordmand, 2019). However, the regulatory position in Iran has been more restrictive. Iranian authorities have prohibited the use of Bitcoin and other virtual currencies within monetary and financial institutions and have restricted their use as means of payment in domestic transactions (Council of, 2019; Supreme Council for Combating Money, 2018).

The legal issue should not be oversimplified as a direct equation between regulatory prohibition and civil invalidity. A distinction must be drawn between holding or transferring a digital asset, using it as an investment or object of exchange, and using it as money or a payment instrument. A regulatory restriction on payment use does not automatically resolve whether the asset has proprietary value for civil-law purposes. Therefore, courts may need to assess separately whether a digital asset possesses rational economic benefit, determinacy, transferability, and lawful deliverability under Article 214 of the Civil Code (Dehghani Tafti et al., 2021; Nejatzadegan & Soltani, 2022).

Non-fungible tokens and tokenized assets add further complexity because their legal value may depend on the underlying right they represent. A token may represent a digital artwork, access right, financial entitlement, or merely a technical record. Therefore, the legal analysis should not treat all tokens alike. The legitimacy of the underlying asset, the clarity of ownership, and the ability to deliver or transfer the right are decisive factors.

For smart contracts governed by Iranian law, parties should avoid treating cryptocurrencies as ordinary domestic payment instruments unless the regulatory framework clearly permits such use. Where digital assets are used, the contract should specify their legal function, allocation of volatility risk, governing law, dispute resolution, and consequences of regulatory change. However, private risk allocation cannot override mandatory rules or public policy.

9. Compatibility with Mandatory Rules and Public Policy

One of the fundamental challenges of smart contracts is the tension between self-executing code and mandatory rules of Iranian law. Article 217 of the Civil Code provides that if the purpose or underlying motive of a transaction is unlawful and forms part of the transaction, the transaction may be void. Articles 10 and 975 also limit contractual freedom where private agreements conflict with law, public order, or good morals. In traditional contracts, courts may respond to illegality, coercion, fraud, mistake, or defective consent through remedies such as annulment, rescission, restitution, damages, or suspension of enforcement. By contrast, blockchain-based smart contracts may execute before a court can intervene (Nejatzadegan & Soltani, 2022).

The problem should be stated precisely. Immutability does not make law irrelevant, nor does it completely prevent judicial remedies. A court may still order restitution, damages, injunctions, or penalties against identifiable parties. The deeper problem is the gap between technical execution and legal effect. A transaction may be technically executed on-chain while legally invalid or unenforceable off-chain. This gap can create practical recovery problems, especially where assets are transferred to anonymous addresses or across jurisdictions.

Hardship and changed circumstances also illustrate the limits of purely automated performance. Smart contracts execute what is written in code and do not naturally account for contextual fairness, proportionality, or changed circumstances (Mik, 2017; Werbach & Cornell, 2017). If code imposes automatic penalties without regard to coercion, mistake, or exceptional hardship, the result may conflict with principles of justice and public policy. These concerns are stronger in consumer, employment, financial, or public-interest transactions than in transactions between sophisticated commercial actors.

Emergency stop mechanisms and judicial override functions may help, but they should not be presented as simple solutions. They can conflict with decentralization, create security risks, concentrate power in a trusted authority, and raise questions about jurisdiction. Who holds the override key? Under what procedure may it be activated? What happens if the authority acts wrongly? These questions show that legal intervention functions must be designed with due process, audit trails, limited scope, and multi-signature or institutional safeguards. Accordingly, the appropriate governance model is not unrestricted immutability and not unrestricted state control, but legally responsive code architecture that allows limited, transparent, and reviewable intervention in exceptional cases (O'Shields, 2017; Raskin, 2017).

10. Civil Liability Arising from Technical Errors and Smart Contract Vulnerabilities

Under Iranian law, civil liability is primarily based on fault and legal responsibility for wrongful harm. In smart

AITBSS AI and Tech in Behavioral and Social Sciences E-ISSN: 3041-9433

contracts, technical defects such as software bugs, programming errors, flawed logic, oracle manipulation, and cybersecurity vulnerabilities may result in erroneous transfers of digital assets or other losses. Empirical and technical literature shows that smart contract vulnerabilities can produce substantial risks, particularly on public blockchain platforms (Atzei et al., 2017; Zhou et al., 2022).

Because software lacks independent legal personality, compensation must be sought from natural or legal persons responsible for designing, developing, deploying, auditing, maintaining, or using the system. The relevant actor may differ depending on the facts. A developer may be liable for negligent coding, a deployer for using unaudited code in a commercial product, a platform operator for failing to follow known security practices, and a user for misuse of credentials. Therefore, liability should not be attributed mechanically to a single actor; it should be allocated according to control, foreseeability, professional duty, and causation.

The evidentiary problem is substantial. In decentralized development, multiple programmers, auditors, libraries, and oracle providers may contribute to the final system. Courts may find it difficult to identify the specific vulnerability that caused the harm and to determine whether that vulnerability resulted from negligence or an unavoidable technical risk. For AI-enabled smart contracts, this problem becomes more complex where an AI system generates, modifies, or recommends contractual logic. Liability analysis must then consider whether the AI output was foreseeable, whether human review was required, and whether reasonable testing and documentation were performed.

Reducing these risks requires governance measures. Smart contract code should undergo independent security audits before deployment, especially in high-value transactions. Developers and platform operators should follow professional standards, maintain documentation, disclose known limitations, and use tested libraries where possible. Insurance mechanisms may also help compensate injured parties. Within Iranian law, these measures can be supported by the principle of la darar and general rules of professional negligence. However, a comprehensive statutory framework for algorithmic liability, code audit, and smart contract governance would provide greater certainty.

11. Conclusion

This study examined the challenges of harmonizing AI-enabled smart contracts with the general principles of contract law in Iran. The analysis shows that blockchain technology and AI-enabled contracting do not operate outside the legal system. Rather, they create new modes of expressing, documenting, and executing legal obligations. Their validity remains dependent on traditional requirements such as intention, consent, capacity, lawful subject matter, and lawful purpose.

The first contribution of this study is conceptual. It distinguishes smart contract code from smart legal contracts and AI-enabled smart contracts. This distinction matters because deterministic blockchain code, legally binding contractual terms, and AI-assisted decision-making raise different legal questions. Without this distinction, the article would risk conflating ordinary automation with autonomous or algorithmic decision-making. The Iranian legal system can accommodate smart contracts more coherently if it treats software as a technical instrument rather than an independent legal subject, while assigning legal consequences to identifiable users, developers, deployers, or platform operators.

The second contribution concerns governance. The principal challenge is not simply whether smart contracts are valid under Iranian law, but how they can be governed so that technical execution remains compatible with legal safeguards. A risk-based governance framework is required. High-value or legally sensitive smart contracts should use verified digital identity, human-readable contractual terms, auditable code, clear allocation of risk, professional standards, and legally responsive mechanisms for dispute resolution.

The study also showed that cryptocurrencies and tokenized assets create serious uncertainty. Their use as payment instruments may conflict with Iranian regulatory restrictions, while their treatment as digital assets requires separate analysis of proprietary value, determinacy, lawful benefit, and deliverability. Therefore, the legal consequences of using cryptocurrencies in smart contracts should not be reduced to a single claim of validity or invalidity; they must be assessed according to the function of the asset in the transaction and the applicable mandatory rules.

Finally, the tension between self-executing code and public policy is not merely a technical problem. Courts may still declare a transaction invalid or order restitution and

AITBSS AI and Tech in Behavioral and Social Sciences
E-ISSN: 3041-9433

damages, but technical execution can make legal remedies difficult to implement. The appropriate solution is not to reject smart contracts entirely, nor to allow uncontrolled automation. Iranian law should move toward legally responsive code architecture, specialized arbitration or judicial expertise, audit standards, and limited emergency intervention mechanisms designed with due process safeguards.

Accordingly, the Iranian legislature should consider comprehensive reform, either by amending the Electronic Commerce Act or by adopting dedicated legislation on digital contracting, blockchain, and AI-enabled smart contracts. Such legislation should address digital identity, electronic consent, legal status of tokenized assets, code audit, algorithmic liability, developer obligations, and judicial oversight. These reforms would allow Iranian law to support technological innovation while preserving contractual justice, legal certainty, public policy, and the rule of law.

Authors' Contributions

All authors equally contributed to the study.

Declaration

Artificial intelligence (AI)-assisted tools were used to improve the linguistic quality, readability, and grammatical accuracy of the manuscript. The authors retained full responsibility for the study design, data collection, data analysis, interpretation of the findings, and final content. All AI-assisted outputs were reviewed, verified, and edited by the authors before submission. No AI tool was used as an author of the manuscript.

Transparency Statement

Data are available for research purposes upon reasonable request to the corresponding author.

Acknowledgments

We would like to express our gratitude to all individuals helped us to do the project.

Declaration of Interest

The authors report no conflict of interest.

Funding

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

Ethics Considerations

Not applicable.

References

Afzali Mehr, M. (2019). *Conflict of laws in contractual and non-contractual obligations*. Shahr-e Danesh Legal Studies and Research Institute.

Ahangaran, M. R., & Ahmadi, A. (2019). *Electronic contracts: From formation to termination*. Majd.

Antonopoulos, A. M., & Wood, G. (2018). *Mastering Ethereum: Building smart contracts and DApps*. O'Reilly Media.

Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A survey of attacks on Ethereum smart contracts (SoK). Principles of security and trust,

Bahrkazemi, M., & Mahmoudi, A. R. (2024). Challenges arising from the conclusion of smart contracts in Iran and Iraq. *Comparative Studies on the Law of Islamic Countries*, *2*(3), 29-46.

Clack, C. D., Bakshi, V. A., & Braine, L. (2016). *Smart contract templates: Foundations, design landscape and research directions* (arXiv, Issue. https://arxiv.org/abs/1608.00771

Council of, M. (2019). *Resolution on cryptocurrency mining and the use of cryptocurrencies in domestic transactions*.

Dehghani Tafti, M., Afzali Mehr, M., & Eskini, R. (2021). A comparative study of the law governing digital smart contracts from the perspective of private international law in the Iranian legal system and Rome I Regulation. *Law of New Technologies*, *2*(4), 203-225. https://mtlj.usc.ac.ir/article_148754_en.html

Durovic, M., & Janssen, A. (2019). The formation of smart contracts and beyond: Shaking the fundamentals of contract law. Smart contracts and blockchain technology: Role of contract law,

European, P., & Council. (2024). *Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. https://researchportal.unamur.be/en/publications/regulation-eu-20241689-laying-down-harmonised-rules-on-artificial/

Khordmand, M. (2019). A jurisprudential analysis of cryptocurrency mining and exchange with a focus on the Bitcoin network. *Islamic Economics Knowledge*, *10*(2), 109-124.

Mik, E. (2017). Smart contracts: Terminology, technical limitations and real world complexity. *Law, Innovation and Technology*, *9*(2), 269-300. https://doi.org/10.1080/17579961.2017.1378468

Naser, M. (2018). *Smart contracts: A comparative study of Iranian and American law*. Majd. https://jplr.atu.ac.ir/article_10182_en.html

Naser, M., & Sadeghi, H. (2019). Validation and legal challenges of using smart contracts: A comparative study of the legal systems of Iran and the United States. *Private Law Research*, *7*(27), 225-288. https://jecjl.com/index.php/jecjl/article/view/174?articlesBySimilarityPage=1

Nejatzadegan, S., & Soltani, M. (2022). Evaluation of the general conditions for the validity of smart contracts from the

AITBSS
E-ISSN: 3041-9433

perspective of Iranian and American law. *Journal of Legal Research*, *25*, 303-335.

O'Shields, R. (2017). Smart contracts: Legal agreements for the blockchain. *North Carolina Banking Institute*, *21*, 177-194. https://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=1435&context=ncbi

Rahbari, E., & Rezaei, A. (2011). The role of electronic agents in contract formation. *Private Law Studies*, *41*(4), 159-178.

Rashvand Boukani, M., & Naser, M. (2019). The intention of contracting parties in smart contracts: Conditions of validity and methods of verification. *Islamic Law Research Journal*, *20*(1), 271-300.

Raskin, M. (2017). The law and legality of smart contracts. *Georgetown Law Technology Review*, *1*(2), 305-341. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2959166

Rezaei, A. (2008). *Electronic commerce law*. Mizan. https://csjlp.org/index.php/csjlp/article/view/372?articlesBySimilarityPage=15

Sadiku, M. N. O., Eze, K. G., & Musa, S. M. (2018). Smart contracts: A primer. *Journal of Scientific and Engineering Research*, *5*(5), 538-541.

Savelyev, A. (2017). Contract law 2.0: Smart contracts as the beginning of the end of classic contract law. *Information & Communications Technology Law*, *26*(2), 116-134.

Scherer, M. U. (2016). Regulating artificial intelligence systems: Risks, challenges, competencies, and strategies. *Harvard Journal of Law & Technology*, *29*(2), 353-400. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2609777

Shahidi, M. (2011). *Civil law: Vol. 1. Formation of contracts and obligations*. Majd. https://jecjl.com/index.php/jecjl/article/view/102?articlesBySimilarityPage=7

Shiravi, A. H., & Mohammadi, M. (2009). Contract formation through intelligent system agency. *Comparative Law Review*, *16*, 23-46. https://journals.kmanpub.com/index.php/aitechbesosci/article/view/5727

Supreme Council for Combating Money, L. (2018). *Resolution prohibiting the use of Bitcoin and other virtual currencies in monetary and financial institutions*.

Szabo, N. (1997). Formalizing and securing relationships on public networks. *First Monday*, *2*(9). https://doi.org/10.5210/fm.v2i9.548

Werbach, K., & Cornell, N. (2017). Contracts ex machina. *Duke Law Journal*, *67*(2), 313-382. https://www.jstor.org/stable/26672953

Yeung, K. (2018). Algorithmic regulation: A critical interrogation. *Regulation & Governance*, *12*(4), 505-523. https://doi.org/10.1111/rego.12158

Zhou, H., Fard, A. M., & Makanju, A. (2022). The state of Ethereum smart contracts security: Vulnerabilities, countermeasures, and tool support. *Journal of Cybersecurity and Privacy*, *2*(2), 358-378. https://doi.org/10.3390/jcp2020019

AITBSS
E-ISSN: 3041-9433