

Legal Challenges of Restitution of Counter-Performances in Blockchain-Based Smart Contracts: From Code Rigidity to the Enforcement of Judicial Decisions

1. Abdul Ghafoor Kor¹: Department of Law, Go.C., Islamic Azad University, Gorgan, Iran

2. Hosein Miri^{2*}: Department of Law, GKM.C., Islamic Azad University, Gonbad kavooos, Iran

3. Akram Tajik³: Department of Law, Az.C., Islamic Azad University, Azadshahr, Iran

*Correspondence: Hosein.Miri@iau.ac.ir

Abstract

The emergence of distributed ledger technology and smart contracts has brought about a profound transformation in the fundamental concepts of contract law and the remedies governing contractual relationships, confronting legal systems with unprecedented challenges at the level of enforcement. This study aims to examine and explain the legal challenges associated with the restitution of counter-performances in blockchain-based smart contracts, with particular emphasis on the tension between the technical rigidity of computer code and the legal imperative of restoring the parties to their pre-contractual position. The central research question concerns how the immutability inherent in smart contracts can be reconciled with mandatory legal rules, including the legal consequences of contractual nullity, rescission, and automatic termination, particularly in an environment where the power to enforce judicial decisions has become detached from sovereign authority and is instead tied to control over private cryptographic keys. Employing a descriptive-analytical and comparative approach, the study demonstrates that, in decentralized systems, the absence of an accountable intermediary creates significant technical obstacles to the restitution in kind of digital assets. The findings indicate that overcoming these impasses requires two complementary strategies. First, at the technical level, there is a need to move toward legally compliant smart contracts and to incorporate legal gateways into the architecture of their code. Second, at the legal level, it is necessary to recognize the theory of compulsory valuation of digital assets and to prioritize restitution by equivalent or monetary value within the physical legal order. Ultimately, this study argues that justice in the digital age requires a new synthesis between the logic of law and the architecture of code so that technological complexity does not impede the application of mandatory legal rules or the protection of proprietary rights.

Keywords: smart contract, blockchain, restitution of counter-performances, enforcement of judicial decisions, technical rigidity, immutability, rule of law.

Received: 23 June 2026

Revised: 28 September 2026

Accepted: 02 October 2026

Initial Publication: 08 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: Kor, A. G., Miri, H., & Tajik, A. (2027). Legal Challenges of Restitution of Counter-Performances in Blockchain-Based Smart Contracts: From Code Rigidity to the Enforcement of Judicial Decisions. *Legal Studies in Digital Age*, 6(6), 1-17.

1. Introduction

Fundamental developments in the field of information technology and the emergence of the digital economy paradigm have not only transformed the methods of exchanging goods and services but have also confronted the classical foundations of contract law with novel and unprecedented challenges. Among these developments, blockchain technology and, consequently, “smart contracts,” as one of the most significant achievements of the digital age, have promised the precise performance of obligations without the need for centralized or human intermediaries (De Filippi & Wright, 2018). These contracts, which are executed in the form of computer code on decentralized infrastructures, possess characteristics such as self-execution, transparency, and immutability, distinguishing them from traditional contracts and even conventional electronic contracts (Savelyev, 2017).

Nevertheless, this very fundamental characteristic of “immutability,” which is regarded as blockchain’s principal technical advantage and a guarantee of transactional security and finality, becomes a serious challenge and structural impasse when mandatory legal rules are to be enforced and traditional institutions such as nullity, rescission, and automatic termination are implicated. When a smart contract is rendered void or rescinded for reasons such as absence of intention, unlawful purpose, usury, or *gharar*, the traditional legal system is required to give retroactive effect to such invalidity and restore the “counter-performances” to their pre-contractual status. However, once a transaction has been conclusively recorded on a blockchain, no central institution or superior authority exists that can, by judicial order, invalidate that transaction or return the transferred asset to its original owner (Durovic & Janssen, 2022).

This fundamental conflict raises several essential questions within the fields of digital contract law and the procedural law governing enforcement of judgments. On the one hand, mandatory legal rules, including those relating to nullity and rescission, constitute fundamental pillars of public order and commutative justice and cannot simply be suspended or disregarded. On the other hand, the decentralized and cryptographic nature of blockchain resists external intervention and judicial commands. The principal question is how the “rule of law,” grounded in sovereign authority and the coercive power of the state, can be reconciled with the “rule of code,” grounded in mathematical logic and immutability. In other words, how can the immutability of code be harmonized with the necessity of *restitutio in integrum* where a contract is void or rescinded?

The significance and necessity of this research can be examined from several perspectives. First, the rapidly expanding use of smart contracts in various commercial fields, particularly digital marketing, has transformed this question into an immediate and practical concern. Economic actors and users operating within this environment face the reality that, in the event of a dispute or contractual invalidity, they may have no effective means of recovering their assets (Werbach, 2018). Second, the existing legislative gap in the Iranian legal system and many other jurisdictions reinforces the need for comparative analysis and legislative solutions. Existing legislation, including Iran’s Electronic Commerce Act of 2003, was largely enacted before the emergence of blockchain technology and provides no clear response to the complex circumstances generated by automated code execution (Mafi & Kaviyar, 2013).

Third, the technical and legal complexities of this subject require an interdisciplinary approach capable of understanding both the technical dimensions of blockchain and smart code and analyzing them within the legal and jurisprudential foundations of different legal systems. By focusing on the legal challenges associated with restitution of counter-performances, this study seeks to provide a comprehensive analytical framework for understanding and resolving this complex problem.

Structurally, this study is organized into seven sections. Following this introduction, Section 2 reviews the literature and explains the theoretical foundations. Section 3 examines the technical rigidity of code and its conflict with mandatory rules of contract law. Section 4 constitutes the core of the study and provides a detailed examination of the challenges associated with restitution of counter-performances in smart contracts. Section 5 addresses civil liability arising from algorithmic and oracle-related errors. Section 6 examines jurisdiction, applicable law, and dispute resolution, while Section 7 concludes the study and presents practical solutions.

2. Literature Review and Theoretical Foundations

2.1. Literature Review

A review of the literature demonstrates that smart contracts and their associated legal challenges have attracted considerable attention from domestic and international scholars in recent years. Nevertheless, “restitution of counter-performances” as a fundamental enforcement challenge has received relatively limited systematic examination.

Among Iranian studies, Golresan (2025), in *Contractual Obligations in Artificial Intelligence and Smart Contracts*, examined the legal dimensions of contractual obligations in the field of artificial intelligence and analyzed challenges concerning civil liability, cross-border dispute resolution, and conflict of laws. He concluded that self-execution and decentralized technologies enhance the speed and certainty of contractual performance but can never eliminate the need for legal reinterpretation and adaptation (Golresan, 2025). Nevertheless, his study did not specifically address the challenge of restitution of counter-performances where a contract is void or rescinded.

Nasri (2024), in the study *Use of Artificial Intelligence in the Formation and Performance of Contracts*, analyzed the role of artificial intelligence in contract formation and performance and examined challenges concerning legal liability where errors arise during automated execution. The study emphasized that, despite the existence of the Electronic Commerce Act, the Iranian legal system continues to face serious legislative gaps concerning the determination of legal responsibility in smart contracts (Nasri, 2024).

Jomehzadeh Bahabadi (2020), in a doctoral dissertation entitled *Legal Challenges of Using Smart Contracts in Joint Ventures*, examined the concept, legal nature, and functions of smart contracts and concluded that effective utilization of this technology requires an accurate characterization of its legal nature and the development of appropriate legal frameworks (Hacker, 2021). Nevertheless, that study focused primarily on legal characterization and conditions of formation rather than on enforcement challenges and restitution of counter-performances.

Golmohammadi Naneh Karan and Nasabpour Molaei (2024), in their article “Digital Smart Contracts and the Law Governing Them in Light of Private International Law,” examined the challenges of determining the law applicable to smart contracts and concluded that, where the parties have not expressly selected a governing law, recourse to general conflict-of-laws rules is unavoidable (Golmohammadi Naneh Karan & Nasabpour Molaei, 2024). Although this study is valuable in the field of conflict of laws, it does not specifically address restitution of counter-performances.

In international scholarship, De Filippi and Wright (2018), in their work on blockchain and law, provided a comprehensive analysis of the legal and technical dimensions of smart contracts and critically examined the theory of “code as law.” They argue that resolving the conflict between blockchain immutability and the requirements of justice necessitates an intermediary layer between code and law (De Filippi & Wright, 2018). This work constitutes one of the principal theoretical sources of the present study.

Savelyev (2017), in his analysis of smart contracts and contract law, examined their technical and legal foundations and concluded that, within automated systems, enforcement power becomes detached from sovereign authority and instead becomes linked to control over private keys. He emphasized the need to recognize remedial doctrines capable of resolving enforcement impasses (Savelyev, 2017).

Durovic and Janssen (2022), in their article on the formation of blockchain-based smart contracts under EU and US law, provided a comparative analysis of legal approaches to smart contracts and emphasized the need to recognize “reversibility” as a principle in smart-contract design (Durovic & Janssen, 2022). Their study constitutes one of the key sources for technical and legal solutions to the problem of immutability examined in the present article.

Werbach (2018), in his analysis of blockchain and trust, examined the role of governance within decentralized environments and argued that, even within automated systems, the coercive power of the state may still operate at blockchain “boundaries,” namely entry and exit points (Werbach, 2018). This idea provides a theoretical foundation for the enforcement mechanisms examined in Section 6 of the present study.

Despite the existence of numerous studies, no comprehensive study appears to have focused specifically on the “legal challenges of restitution of counter-performances in blockchain-based smart contracts” with particular emphasis on the conflict

between code rigidity and the necessity of restoring the parties to their previous position. The present article seeks to fill this gap.

2.2. Theoretical Foundations

2.2.1. The Concept of a Smart Contract

From a technical perspective, a smart contract is a computerized transactional protocol operating on a distributed ledger and designed to automate events and actions associated with the terms of an agreement (Savelyev, 2017). These contracts are expressed through programming code and, once deployed on a blockchain network, acquire decentralized and immutable characteristics. They are designed to perform contractual obligations automatically when predetermined logical conditions are satisfied (De Filippi et al., 2020).

From a legal perspective, a smart contract, as an emerging phenomenon in contract law, may be defined as an agreement in which all or part of the resulting obligations are automatically managed and performed by computer code (Werbach, 2018). Contemporary legal approaches nevertheless maintain that where such code incorporates the elements of offer and acceptance and reflects the parties' intention to create legal effects, self-executing code may itself qualify as an electronic contract, with its legal validity recognized under principles such as functional equivalence (Fox & Johnston, 2020).

2.2.2. The Concept of Restitution of Counter-Performances

Restitution of counter-performances (*restitutio in integrum*) in contract law refers to restoring the parties to the position they occupied before conclusion of the contract. This legal institution constitutes one of the principal consequences of nullity, rescission, and automatic termination and seeks to restore the economic equilibrium of the transaction and prevent unjust enrichment (Katouzian, 2016). Under Iranian law, Articles 288 and 391 of the Civil Code address, respectively, the effects of rescission and invalidity in relation to restitution of counter-performances.

Within the digital environment, particularly in smart contracts, restitution of counter-performances encounters new challenges. On the one hand, the counter-performances may consist of digital assets, such as cryptocurrencies and tokens, which have no physical existence and are recorded on a distributed ledger. On the other hand, blockchain immutability means that once a transaction has been recorded, it cannot technically and directly be reversed. This situation raises fundamental questions concerning the feasibility of applying traditional restitution rules in the digital environment (Durovic & Janssen, 2022).

2.2.3. Technical Rigidity and Immutability

Technical rigidity refers to a characteristic of blockchain-based systems whereby, once code has been deployed and a transaction recorded, alteration, amendment, or deletion becomes impossible (De Filippi & Wright, 2018). This characteristic, resulting from cryptographic algorithms and distributed consensus mechanisms, guarantees security, transparency, and transactional finality, while simultaneously obstructing the application of mandatory legal rules concerning nullity, rescission, and automatic termination.

Blockchain immutability effectively substitutes a form of "mathematical finality" for the "legal relativity" characteristic of traditional contracts. Under conventional law, even after contractual performance, a judge may rely on mandatory rules or principles of equity to invalidate or adjust the contract. In the blockchain environment, however, the code continues to operate, and no inherent mechanism exists for stopping it (Mik, 2017).

2.2.4. The "Code Is Law" Theory and Its Critique

The "Code Is Law" theory, first advanced by Lawrence Lessig, is based on the proposition that software code in cyberspace performs a role analogous to law by regulating users' conduct (Lessig, 2006). Within the smart-contract paradigm, this theory

has been interpreted to mean that code is not merely an instrument for contractual performance but itself constitutes the law governing the parties' relationship.

Critics of this theory, including De Filippi and Wright (2018) and Hacker (2019), argue that reducing law to code eliminates the "safety valves of justice" (De Filippi & Wright, 2018; Hacker, 2019). Code lacks the capacity to comprehend qualitative concepts such as good faith, equity, hardship, and fundamental change of circumstances, all of which function as principal mechanisms for contractual adjustment in traditional law. Accordingly, the "Code Is Law" theory cannot legitimately serve as a basis for disregarding mandatory rules and fundamental legal principles (Savelyev, 2017).

3. Code Rigidity and Its Conflict with Mandatory Rules of Contract Law

3.1. Analysis of the "Code Is Law" Theory

The "Code Is Law" theory originates in Lawrence Lessig's work in the late 1990s. Lessig argued that software code in cyberspace performs the same function that law performs in the physical world: it determines which actions are permitted and which are prohibited (Lessig, 2006). Within the smart-contract paradigm, this theory has been interpreted to mean that code is not merely an instrument of contractual performance but itself constitutes the law governing the relationship between the parties, such that any deviation from it is treated as a violation of that governing order (De Filippi & Wright, 2018).

In explaining this theory, De Filippi and Wright (2018) maintain that, because of their self-executing and immutable nature, smart contracts create a form of "autonomous legal order" in which traditional concepts such as intention, consent, capacity, and contractual interpretation are displaced by the formal logic of mathematics (De Filippi & Wright, 2018). From this perspective, "code" functions as a form of "governing law" that determines not only performance of obligations but also the legal consequences resulting from the contract.

Nevertheless, this theory has been subjected to fundamental criticism. Hacker (2019) argues that reducing law to code eliminates the "safety valves of justice" (Hacker, 2019). Code is incapable of understanding qualitative concepts such as good faith, equity, hardship, and fundamental change of circumstances, which constitute principal tools of contractual adjustment in traditional law. Savelyev (2017), similarly emphasizing that "code cannot completely replace law," underscores the necessity of preserving the supremacy of mandatory legal rules within the digital environment (Savelyev, 2017).

3.2. Conflict with Mandatory Rules

Mandatory rules are provisions from which contracting parties may not derogate by agreement and where any inconsistent agreement is void and without legal effect (Katouzian, 2016). Under Iranian law, Articles 10 and 975 of the Civil Code constitute principal foundations for the operation of mandatory rules and public order. Within smart contracts, these mandatory rules may conflict with the technical rigidity of code in several circumstances, the most important of which are discussed below.

(a) **Conflict with the prohibition of usury (*riba*):** One of the clearest manifestations of such conflict appears in decentralized finance (DeFi), where interest rates are determined algorithmically according to supply and demand (Durovic & Janssen, 2022). Although these economic models may be fully lawful within liberal legal systems, they encounter serious difficulty under Iranian law because of the prohibition of *riba*. Accordingly, if a smart contract is structured around compound interest and assets are transferred through blockchain infrastructure, an Iranian judge may invoke Article 975 of the Civil Code and the prohibition of *riba* to declare the agreement void and order restitution of the principal counter-performances, excluding usurious profit. The central challenge, however, is that no central institution exists within a decentralized environment capable of enforcing such an order (Savelyev, 2017).

(b) **Conflict with the prohibition of *gharar*:** The rule prohibiting *gharar* constitutes another mandatory principle reflected in Article 216 of the Iranian Civil Code. Certain financial protocols used in smart contracts may constitute excessive *gharar* because of their dependence on external data and significant market volatility (Mik, 2017). In particular, contracts in which payment is determined by variable and unpredictable indicators may be regarded as *gharar*-based and therefore void under Iranian law. In such circumstances, even where the code has functioned correctly, a judge may invoke mandatory rules to

declare the contract void and order restitution of the counter-performances; yet the resulting order may still encounter enforcement difficulties within a decentralized environment (Golmohammadi Naneh Karan & Nasabpour Molaei, 2024).

(c) **Conflict with the prohibition of unlawful purpose:** Article 217 of the Iranian Civil Code requires the purpose underlying a transaction, where expressed, to be lawful. Smart-contract code may be used for purposes such as money laundering, gambling, or financing prohibited activities (De Filippi et al., 2020). In such circumstances, although the code may continue executing automatically, the underlying contract may be legally void and therefore subject to restitution. Yet no mechanism exists within blockchain architecture to halt automated execution and recover the assets unless supervisory mechanisms have been incorporated into the code from the outset (Werbach, 2018).

3.3. *The Crisis of Interpretation and the Erosion of Judicial Discretion*

One of the most profound challenges arising from code rigidity is the erosion of “judicial discretion” in contractual interpretation and application. Under traditional law, the judge, as an arbiter of justice, has the authority to consider the particular circumstances of each case, interpret qualitative concepts such as “good faith,” “reasonable efforts,” or “hardship,” and, where necessary, modify or invalidate the contract (Katouzian, 2016).

In smart contracts, however, such discretion is effectively eliminated. Code has no “margin of discretion” and functions solely through conditional “if-then” instructions (Mik, 2017). For example, the notion of a “reasonable period,” which is common in traditional marketing contracts, cannot readily be encoded in a smart contract unless it is translated into precise numerical variables, such as seconds or a specified number of transactions. This results in a “rigid” contractual system that differs fundamentally from the flexibility of conventionally drafted contracts (Zheng, 2022).

In analyzing this phenomenon, Savelyev (2017) argues that within the smart-contract system, the judge’s authority to intervene in contractual terms and modify them in the interests of justice is substantially diminished in the face of rigid and automated algorithmic execution (Savelyev, 2017). He characterizes this condition as the decline of “law as an art of achieving justice” and warns that its replacement by “law as a technique for executing instructions” may weaken public confidence in emerging transactional systems.

3.4. *Conflict with the Right of Rescission and Contractual Options (Khiyarat)*

Under Iranian law, institutions such as *khiyar* (contractual or statutory options permitting rescission) and *iqala* (mutual cancellation) operate as balancing mechanisms that allow parties, under specified circumstances, to withdraw from continued contractual performance (Katouzian, 2016). Articles 396 to 401 of the Civil Code enumerate various options, including the option of the contractual session, the option based on defect, the option based on gross disparity, and the option based on fraud.

In smart contracts, however, blockchain immutability renders restoration of the prior state technically almost impossible once the code has executed, unless a termination function has been incorporated into the code in advance. In traditional contracts, by contrast, a judge may order invalidation and restitution of the price and subject matter even after performance. Smart contracts therefore increase the risk of “irreversible error,” a risk traditionally controlled through legal remedies (Luo, 2024).

Savelyev (2017) argues that under such circumstances, a form of “machine governance” emerges in which human intention becomes “frozen” at the moment the code is deployed and thereafter leaves no effective avenue for exercising legally recognized rights of rescission (Savelyev, 2017). He therefore emphasizes the need to embed “emergency exit mechanisms” within contractual code so that rights of termination may be exercised in exceptional circumstances.

3.5. *Summary of the Conflicts*

The foregoing analysis demonstrates that the technical rigidity of blockchain code may conflict with numerous mandatory rules of contract law, including the prohibitions of *riba*, *gharar*, and unlawful purpose, rights of rescission and contractual options, and judicial discretion in contractual interpretation. These conflicts originate in the fundamental difference between the “logic of law,” based on flexibility, interpretation, and justice, and the “logic of code,” based on certainty, inflexibility, and

mechanical execution. Resolving these conflicts requires the incorporation of “legal gateways” and “stopping mechanisms” into smart-contract design so that mandatory legal rules and judicial decisions can effectively be implemented (De Filippi & Wright, 2018; Werbach, 2018).

4. Challenges of Restitution of Counter-Performances in Smart Contracts

4.1. *The Conflict Between the Retroactive Effect of Nullity and Blockchain Immutability*

An examination of the fundamental conflict between the “retroactive effect of nullity” and “blockchain immutability” reveals one of the most complex legal dilemmas arising at the intersection of law and code. In the Iranian legal system and other civil-law jurisdictions, the principle of restoration to the previous position, or restitution of counter-performances, is not merely a contractual rule but also a manifestation of distributive justice intended to erase the legal effects of a defective transaction (Katouzian, 2016). When a court declares a contract void, a form of “legal time machine” is effectively activated, intended to neutralize all transfers of ownership occurring from the moment of conclusion and restore the assets to their original positions. In blockchain, however, a reality emerges that is fundamentally alien to the flexible logic of law: “time” proceeds not cyclically but linearly and irreversibly, with every block constituting a firm barrier against rewriting the past (De Filippi & Wright, 2018).

This conflict between the “legislator’s will” to restore the previous state and the “technical protocol” designed to preserve transactional finality creates a paradoxical situation. While a judge may declare that ownership was never validly transferred and that the property must be restored, decentralized blockchain architecture contains no “undo key” through which a transaction recorded in the underlying layers of the network can be cancelled (Durovic & Janssen, 2022). Savelyev’s analysis describes the underlying phenomenon as a form of temporal rigidity, reflecting the law’s inability to penetrate the hardened and immutable layers of transaction history (Savelyev, 2017). In smart contracts, therefore, the past is not merely impossible to erase; it remains permanently and immutably visible to all participants, creating a structural impasse for conventional restitution orders.

4.2. *Analysis of Restitution under Iranian Law and Technical Impossibility*

In comparing the traditional rules of Iranian civil law with the emerging realities of digital assets, restitution of counter-performances following dissolution of a smart contract constitutes a particularly challenging point of intersection. Under the logic reflected in Articles 288 and 391 of the Civil Code, the primary rule following rescission or invalidation is restoration in kind of the asset that constituted the subject matter of the transaction (Katouzian, 2016). In classical private law, recourse to a substitute, whether equivalent property or monetary value, generally arises only where the original asset has been destroyed. Blockchain, however, gives rise to what may be termed “technical detention of the asset”: a situation in which the token or digital asset physically and logically continues to exist within the obligor’s wallet and has not been destroyed, yet remains beyond the reach of judicial coercive power because of cryptographic architecture and exclusive access through the private key (Mik, 2017).

At this point, the gap between the judge’s legal authority and technical incapacity becomes apparent. In the physical world, an enforcement officer may use coercive state authority to remove tangible property from a possessor. In smart-contract environments, however, no coercive measure can transfer an asset without access to the relevant private key. Pisa and McCurdy (2023) provide a useful analysis of this legal impasse, suggesting that inaccessibility of the private key and the obligor’s refusal to comply with a judicial order should be treated as equivalent to “constructive loss” of the property (Pisa & McCurdy, 2023). In Iranian law, constructive loss refers to circumstances in which an asset continues to exist physically but access to it becomes permanently or for a prolonged period impossible, analogous to a ring falling to the bottom of the sea.

Accordingly, to preserve the adaptability of Iranian civil law in the face of emerging technologies, judicial practice should recognize a doctrine of “technical loss” or “digital constructive loss.” Such reinterpretation would allow the judge, upon determining that restitution in kind is technically impossible because of wallet locking or code immutability, to abandon insistence on return of the specific token and instead immediately order restitution of a substitute, whether its monetary

equivalent or a comparable digital asset. This theoretical shift would prevent a breaching obligor from escaping the legal consequences of invalidity by sheltering behind blockchain's cryptographic architecture (De Filippi et al., 2020).

4.3. Remedial Mechanisms: Reverse Transactions and Replacement Contracts

In seeking operational solutions to the impasse between “blockchain immutability” and the “necessity of restitution,” it is necessary to move from the impossible idea of erasing transaction history toward the feasible concept of “neutralizing its effects.” Because blockchain preserves the past as though engraved in stone, rigid and untouched, the only legally viable means of giving effect to nullity or rescission is through a “reverse transaction.” Under this approach, rather than attempting to eliminate the previous block, a new block is created whose economic and proprietary consequences restore the parties to the original position. At this point, the connection between technical architecture and legal intent becomes visible through the design of “flexible” smart contracts (Durovic & Janssen, 2022).

Scholten and Janssen (2021) explain that, if blockchain is not to become an anarchic sphere operating beyond the reach of law, smart contracts should from the outset be designed around the principle of “reversibility” (Scholten & Janssen, 2021). This requires incorporating specific functions into the code that operate as “supervisory gateways.” Under this model, the contract code contains a conditional function whose activation depends upon a valid digital signature issued by a trusted authority, such as a judicial oracle or online arbitrator. This mechanism effectively injects the “rule of law” into computer code, allowing assets, following a judgment of invalidity, to return automatically to their original source without requiring voluntary cooperation from the breaching obligor (De Filippi et al., 2020).

Within Iranian law, this technical solution can be analyzed and justified through traditional institutions such as a “condition to perform an act” or a “condition as to result.” Where parties agree, upon conclusion of a smart contract, to include a function that returns property upon rescission, this may effectively operate as a “condition as to result,” under which the reverse transfer of ownership occurs automatically within the code as soon as rescission takes effect and is verified by the arbitrator. Alternatively, it may be conceptualized as a “condition to perform an act entrusted to the code,” thereby eliminating friction resulting from a person's refusal to make restitution (Katouzian, 2016). Luo (2024) likewise maintains that these intermediary layers reconcile technological finality with legal equity and contribute to the legal recognition of smart contracts (Luo, 2024).

4.4. Examination of Benefits and Tokens Attached to the Counter-Performances During the Period Preceding Rescission

Determining the legal treatment of benefits and derivative tokens attached to the counter-performances during the period between conclusion and rescission constitutes one of the most subtle issues at the intersection of property law and blockchain technology. The problem concerns the management of benefits generated under an initially valid contract that must subsequently be allocated following dissolution of that contract. Article 287 of the Iranian Civil Code draws a clear distinction between attached and detached benefits, but transferring this logic into the binary environment of digital assets is substantially more difficult than applying classical legal doctrine (Katouzian, 2016).

In the digital-asset environment, benefits may assume highly diverse and complex forms, ranging from staking rewards and liquidity-provision returns to airdropped tokens and assets generated through network forks. The central problem is that smart contracts, in their present design, frequently operate holistically: they do not distinguish between the principal asset and derivative benefits when restitution occurs. Where code is designed to return property, it typically returns either the entire wallet balance or only the original amount, while the legal subtleties reflected in Article 287 of the Civil Code are disregarded (Mik, 2017).

As Hacker (2021) observes, computer code lacks “contextual understanding” capable of determining the legal nature of such benefits (Hacker, 2021). For a smart contract, there is no inherent distinction between an increase in value resulting intrinsically from the asset itself, which may constitute an attached benefit that should accompany restitution of the principal asset, and gains resulting from the holder's voluntary activity on other platforms, which may constitute detached benefits legally belonging to the interim owner. This absence of analytical capacity within code may result in the “unjust enrichment” of one

party, a condition inconsistent both with the spirit of Iranian civil law and with general legal principles recognized internationally (Luo, 2024).

In this context, the role of “technological expertise” and “human adjudication” becomes particularly important as a complement to the impermeability of code. Because restitution of benefits at this level of complexity exceeds the current capabilities of oracles and smart contracts, judicial authorities must rely upon expert opinions to calculate the monetary value or digital equivalent of such benefits and order either their restitution or retention. Accordingly, complete restitution in blockchain environments lies not merely in automated execution but in “equitable settlement,” which necessarily requires judicial supervision (Pisa & McCurdy, 2023).

4.5. Comparative Approaches and International Standards for Digital Restitution

Comparative approaches and emerging international standards reflect a transition from “technical idealism” toward “legal realism.” Whereas the early years of blockchain development were characterized by the assumption that decentralized environments could exist entirely beyond the reach of national law, contemporary instruments of international commerce and advanced judicial practices increasingly seek points of connection between decentralized systems and sovereign enforcement mechanisms (Durovic & Janssen, 2022). One notable development is the emergence of “on-chain arbitration,” in which dispute resolution and restitution are managed not by conventional courts but through intermediary code and digitally identified arbitrators (Werth & Cairns, 2024).

Under emerging approaches reflected in contemporary European and international commercial frameworks, where a contract is invalidated because of mistake or fraud, parties may be understood as bearing a “duty of technical cooperation.” This means that they must undertake the measures reasonably necessary to neutralize the effects of the code and restore the pre-contractual position (Durovic & Janssen, 2022). Luo (2024) adopts a pragmatic position, arguing that an obligor’s refusal to cooperate should not permit a technical blockchain impasse to become an impasse of justice (Luo, 2024). At this point, “points of centralization” within decentralized ecosystems, particularly centralized exchanges and fiat conversion gateways, may function as enforcement arms of the legal system.

This approach reflects a strategic transformation in international legal practice: reliance upon “bridges between the digital and physical worlds” for enforcement of restitution orders. Although a blockchain transaction itself may not be reversible, the asset generated through that transaction will often need to reach a centralized exchange or banking account in order to realize conventional economic value. National courts may therefore restore financial equilibrium between the parties by issuing attachment orders and directing exchanges to freeze or retransfer relevant assets. This mechanism provides a practical response to the assumption that blockchain decentralization permits parties to evade the legal consequences of contractual nullity or rescission (Werth & Cairns, 2024).

Finally, the connection between these international approaches and Iranian law may be reconstructed through the institution of compulsory performance and the mechanisms of international judicial assistance. Restitution of counter-performances in the contemporary era is therefore a hybrid process: one part occurs within the cryptographic layer through reverse transactions, while another takes place through physical intermediaries and relies upon the coercive authority of states. This comprehensive approach reflects an emerging paradigm of “transnational digital law,” in which technology operates not in opposition to law but alongside it in pursuit of commutative justice (De Filippi & Wright, 2018).

5. Civil Liability Arising from Algorithmic and Oracle Errors

5.1. The Nature of Programmer Fault: From General Fault to Professional Negligence

Analyzing the civil liability of smart-contract programmers requires moving beyond conventional concepts of fault into the specialized domain of information-technology law. Within Iranian civil law, particularly Articles 951 to 953 of the Civil Code, fault is structured around the concepts of *ta’addi* and *tafrit*, with *tafrit*, or negligent omission, being particularly relevant to defects in code. *Tafrit* refers to failure to perform an act necessary for preservation of property or proper performance of an obligation. Accordingly, where a developer neglects necessary safeguards within the architecture of a smart contract, such

conduct may constitute a form of negligent omission resulting in loss of users' assets (Katouzian, 2016). This failure to discharge technical duties provides the foundation for liability for resulting losses and the obligation to restore lost funds.

Nevertheless, a programmer's conduct should not be assessed against the standard of an ordinary person; rather, the concept of "professional negligence" should apply. In legal analysis, where a specialist is involved, the standard of care becomes that of a "reasonable, competent, and trustworthy programmer" operating under comparable technical circumstances. Where established international and cybersecurity standards, such as safeguards against re-entrancy attacks or integer overflow, are disregarded during code development, such conduct may constitute professional negligence. Under these circumstances, departure from contemporary professional standards may be sufficient to establish fault without proof of malicious intent, because technical expertise carries with it a corresponding duty of care concerning technical detail (Savelyev, 2017).

A fundamental question nevertheless concerns the legal nature of the programmer's obligation, specifically whether it constitutes an "obligation of means" or an "obligation of result." If the obligation is characterized as one of result, even a minor bug or security defect causing loss may trigger liability. Yet the realities of software development and the inherent complexity of coding have led the dominant legal tendency toward characterization as an "obligation of means." Under this approach, the programmer must demonstrate that appropriate efforts were undertaken and that up-to-date technical knowledge and reliable testing tools were used to ensure code security. This approach strikes a rational balance between promoting innovation and protecting users' rights (Forder, 2020).

Ultimately, determination of programmer fault facilitates judicial recovery of counter-performances. Where a technical defect resulting from professional negligence is established, a court may rely on principles of causation to require the programmer or development entity to compensate the loss and restore the injured party's financial position to that existing before the relevant transaction. This legal analysis demonstrates that expertise is not a basis for excluding liability; rather, because it generates user reliance, it may impose an enhanced responsibility upon blockchain professionals to exercise heightened care in protecting digital assets circulating through their code (Fox & Johnston, 2020).

5.2. Basis of Liability: Causation or Non-Contractual Liability?

Analysis of liability within decentralized environments, particularly where no direct contractual relationship exists between developers and users, necessarily points toward extra-contractual liability. In decentralized finance protocols, users frequently interact with code rather than with an identifiable legal person. Traditional contractual-liability rules may therefore be insufficient to attribute resulting losses to the developer. This is where the Iranian doctrine of causation becomes relevant. Under Article 331 of the Civil Code, any person who causes the destruction or impairment of another's property is liable for the loss. A smart-contract developer may thus be regarded as a "creator of risk" who, by releasing vulnerable code, establishes the conditions through which digital property may be lost (Katouzian, 2016).

This approach is also compatible with broader international legal analysis. Savelyev's analysis suggests that responsibility should rest with the actor occupying the "best position" to prevent the harmful event (Savelyev, 2017). In smart contracts, an ordinary user generally lacks both the technical expertise required to audit code and the power to modify its architecture. Attributing the entire loss to such a user on the basis of voluntary assumption of risk would therefore conflict with commutative justice and economic public order. Iranian courts could accordingly establish liability by identifying an ordinary causal relationship between the code defect and the resulting damage, thereby ordering the programmer or platform to compensate the loss and restore the relevant counter-performances. This approach both protects users' proprietary rights and requires digital-service providers to observe high standards of care and precaution (Low & Teo, 2017).

5.3. Allocation of Liability Among the Marketing Platform, Programmer, and User

Where a smart contract causes loss, a chain of actors is typically involved: the programmer who wrote the code, the platform, such as an exchange or NFT marketplace, through which it was offered, and the user who authorized the transaction. Equitable allocation of responsibility among these actors constitutes one of the central challenges in restitution disputes (Werbach, 2018).

First, the programmer's responsibility is grounded in "professional negligence." Where the loss results from a serious coding defect that could have been avoided through observance of ordinary professional standards and contemporary technical

knowledge, primary and direct responsibility may rest with the developer. From a legal perspective, releasing code containing fundamental security vulnerabilities constitutes a breach of the duty to provide a reasonably safe product or system (Savelyev, 2017).

At the second level, the responsibility of marketing platforms and intermediaries must be analyzed in light of their operational role within the value chain. Where an exchange or marketplace has “recommended” a particular smart contract to its users or received a “fee” for facilitating transactions involving it, it can no longer rely solely on its status as an “intermediary” to exclude liability. Under the Iranian Consumer Protection Act of 2009, suppliers of goods and services bear responsibility regarding the safety and functionality of products they make available to the public. By listing a smart contract, a platform may provide a form of “implicit endorsement” and, under reliance-based theories, may acquire joint or shared responsibility for losses resulting from its insecurity (Fox & Johnston, 2020).

The third level concerns user responsibility and application of the doctrine of voluntary assumption of risk. Under this principle, where a person knowingly undertakes an action despite awareness of existing dangers, the right of recourse against others may be lost or the recoverable amount of damages may be reduced. In digital-asset markets, where a user enters a high-risk project without reviewing the “white paper,” ignores the results of a “code audit,” and acts purely for speculative purposes, the user may be regarded as having contributed to the risk. Nevertheless, Low and Teo (2017) emphasize that voluntary assumption of risk should completely exclude the responsibility of the causal actor only where the user possessed “full technical knowledge” of the hidden defect (Low & Teo, 2017). Otherwise, because of severe informational asymmetry between users and developers, user fault should operate merely as a factor reducing liability, while the underlying responsibility of the programmer and platform to provide restitution in relation to a defective product remains intact.

5.4. Liability Arising from Oracle Errors

Oracles operate as bridges between the external world, or off-chain environment, and the blockchain, or on-chain environment. Because smart contracts cannot independently access external information, such as real-time exchange rates, the results of sporting events, or weather conditions, they necessarily rely upon oracles. Where such data are inaccurate, the smart contract may execute an incorrect decision with uncompromising precision, thereby causing an unjust transfer of assets (De Filippi et al., 2020).

Two different approaches may be adopted when determining the basis of oracle liability. Under the first, where the oracle is treated merely as an “agent” or “trustee” transmitting information, general rules governing entrusted property and fiduciary conduct may apply. Under Article 614 of the Civil Code, a trustee is not liable for loss or impairment of entrusted property unless *ta’addi* or *tafrit* is established. Under this paradigm, where the oracle has transmitted data in accordance with relevant professional standards but the original source itself supplied incorrect information, liability should not attach to the oracle because no fault occurred in its own conduct (Katouzian, 2016).

A second approach conceptualizes the oracle’s role in terms of an “obligation of result.” Under this view, however, the oracle’s essential responsibility may still be understood as using “reasonable efforts” to transmit faithfully the message generated at the source rather than guaranteeing the truth of content produced by third parties (Katouzian, 2016). Nevertheless, where an oracle is marketed as dedicated infrastructure guaranteeing absolute accuracy, its responsibility becomes substantially heavier and may approach strict liability. Savelyev’s analysis of blockchain risk suggests that because data directly determine automated outcomes, oracle providers that receive fees for directing the data flows of smart contracts may need to internalize risks associated with erroneous sources as part of their professional costs in order to preserve confidence in the digital ecosystem (Savelyev, 2017).

This distinction demonstrates that, in restitution disputes, a court must first examine the legal nature of the relationship between the platform and the oracle. Where the oracle has been presented as dedicated infrastructure guaranteeing absolute accuracy, its liability should be more extensive and may approximate strict liability. By contrast, decentralized oracle models and data-aggregation mechanisms reduce single-source error and consequently reduce the likelihood of legal liability arising from transmission of incorrect data (Werth & Cairns, 2024).

5.5. The European Union Approach: From Traditional Liability to the AI Act and MiCA

In recent years, the European Union, recognizing that traditional rules of civil liability are not fully equipped to address the complex and cross-border challenges associated with blockchain, has increasingly moved toward a paradigm of “risk management” and “targeted responsibility.” This legal transition is reflected principally in the areas of “product liability” and “intermediary obligations” (Zetzsche et al., 2023).

At the first level, reforms to product-liability rules have expanded the legal understanding of software as a “product.” This conceptual development may move programmer responsibility beyond exclusively fault-based liability and toward forms of strict product liability. Under this approach, a user or injured party need not necessarily prove negligence, carelessness, or wrongful conduct by the programmer; establishing that the distributed code was “defective” and that the defect caused loss may suffice to establish responsibility and an obligation to compensate or restore the relevant value (Savelyev, 2017).

At the second level, through the Markets in Crypto-Assets Regulation (MiCA), the European Union has established an expanded regulatory role for platforms and crypto-asset service providers. Platforms marketing or facilitating transactions involving digital assets cannot simply rely upon a claim of technological neutrality to avoid the consequences of defective systems. These intermediaries are subject to due-diligence, governance, disclosure, and operational requirements that increasingly emphasize ex ante risk assessment and transparency. Within the broader literature on consumer protection in smart-contract environments, failure to adequately assess security or disclose material risks may constitute a breach of the relevant duty of care (Lacker & Noone, 2021).

From this perspective, “technical silence” or failure to incorporate appropriate remedial mechanisms into sensitive financial systems may contribute to a finding that product-safety expectations have not been met. Consequently, broad and ambiguous disclaimers placed at the outset of such projects cannot necessarily neutralize liability arising from a defective product or negligent distribution. By moving away from exclusively individualized conceptions of fault and toward “structural product safety,” this model seeks to allocate the costs of technical errors to those actors that possess the greatest capacity to control, modify, or insure the relevant systems rather than to ordinary users (Fox & Johnston, 2020).

This comparative analysis demonstrates that Iranian law could similarly reinterpret civil-liability rules and utilize the capacities already present within the Electronic Commerce Act and consumer-protection legislation to develop a framework protecting users against algorithmic errors.

6. Jurisdiction, Applicable Law, and Dispute Resolution

6.1. Challenges in Determining the Applicable Law in Cross-Border Smart Contracts

In the digital age, smart contracts are inherently cross-border in character; they operate on nodes distributed throughout the world and may have no identifiable physical connection to any particular jurisdiction. This characteristic presents fundamental challenges to traditional private international law. Classical conflict-of-laws rules determine the law applicable to contracts through connecting factors such as the place of contract formation, place of performance, parties’ domicile, or situs of property (Katouzian, 2016). In blockchain environments, however, such physical connecting factors become difficult to apply because the place of formation, place of performance, and even the physical identity of the parties may not be readily ascertainable (Durovic & Janssen, 2022).

(a) **Decline of traditional connecting factors:** Article 968 of the Iranian Civil Code provides that contractual obligations are governed by the law of the place where the contract is concluded unless the contracting parties are foreign nationals and have expressly or impliedly subjected the contract to another law. This provision, which presupposes a relatively straightforward and physical understanding of the “place of contract formation,” encounters substantial difficulty when applied to smart contracts. If a contract is concluded on the Ethereum network, where precisely is the “place of formation”? Is it the place where a user opens the wallet, the locations of the nodes validating the transaction, or the location of servers operated by the hosting platform? None of these answers is independently satisfactory (Golmohammadi Naneh Karan & Nasabpour Molaei, 2024).

(b) **The theory of “law as code” and party autonomy:** In response to this difficulty, some scholars have relied upon the “law as code” theory and argued that, in decentralized environments, the code itself should function as the law governing the parties’ relationship (Lessig, 2006). Under this approach, disputes would be resolved according to the internal logic of code rather than national laws. Nevertheless, this approach is subject to substantial criticism from the perspective of Iranian law and international legal principles because it conflicts with state sovereignty and may effectively eliminate the operation of mandatory rules and public policy (Savelyev, 2017).

(c) **Party autonomy and express clauses:** Party autonomy constitutes one of the most important foundations for determining applicable law in private international law. In smart contracts, this challenge may be mitigated through inclusion of an “express governing-law clause” in the contractual text or project “white paper.” Where the parties expressly designate the governing law, conflicts concerning applicable law can be substantially reduced (Werth & Cairns, 2024). The central difficulty arises where the parties remain silent or where their chosen law conflicts with mandatory rules of the jurisdiction in which enforcement is sought.

(d) **The crisis of anonymity and collapse of personal connecting factors:** Another major challenge is blockchain anonymity. In traditional contracts, the parties’ domicile constitutes an important factor for determining applicable law. In decentralized systems, users transact through cryptographic addresses that disclose no direct information concerning physical identity. Consequently, even where domicile is theoretically selected as the relevant connecting factor, an informational impasse may arise (Hacker, 2019). This anonymity crisis reinforces the need to move toward “functional connecting factors” rather than exclusively “territorial connecting factors.”

6.2. *The Status of Digital Arbitration under International Instruments and Iranian Law*

One of the most effective mechanisms for resolving disputes arising from smart contracts is “digital arbitration,” meaning dispute resolution conducted through online platforms or even directly on-chain rather than exclusively through conventional courts. Because of its speed, flexibility, and technical specialization, this form of arbitration may constitute an effective alternative to traditional litigation in disputes concerning restitution of counter-performances (Werth & Cairns, 2024).

(a) **Typology of arbitration in the digital ecosystem:** Digital arbitration can be divided into two principal categories. The first is “electronic arbitration” or online dispute resolution (ODR), in which the arbitral process is conducted through electronic tools, including email, videoconferencing, and online platforms, while remaining grounded in conventional arbitration rules and human supervision. The second is “blockchain arbitration” or “decentralized arbitration,” in which the arbitration process itself operates on a blockchain network and arbitrators are selected and make decisions through consensus mechanisms and game-theoretic structures (De Filippi & Wright, 2018).

(b) **Electronic arbitration: transition from paper to data messages:** In electronic arbitration, proceedings are based on digital documents and evidence. Under Iranian law, Article 454 of the Code of Civil Procedure recognizes the parties’ ability to refer disputes to arbitration. Article 2 of the Electronic Commerce Act defines a “data message” as a representation of facts, information, or concepts generated and stored by electronic means and accords it legal recognition. Accordingly, where the parties incorporate an arbitration clause into the code of a smart contract, such a clause may constitute a binding arbitration agreement under Article 454 of the Code of Civil Procedure (Mafi & Kaviyar, 2013). Within this structure, the arbitrator can examine transaction history and analyze blockchain data in order to determine the nature of the dispute and whether restitution is required.

(c) **Blockchain arbitration: algorithmic governance and crowd consensus:** Blockchain arbitration represents a substantial departure from conventional concepts of adjudication. On platforms such as Kleros, adjudication is transformed from a formal legal office into an “incentive-based process” structured around game theory. Arbitrators are selected randomly through token staking rather than solely on the basis of formal legal expertise. The governing logic seeks a “Schelling point”: arbitrators are incentivized to choose the outcome they expect the majority of other arbitrators to select in order to avoid economic penalties (De Filippi & Wright, 2018). The fundamental difference is that blockchain arbitral decisions may be self-executing: once a decision becomes final within the arbitration protocol, the smart contract automatically transfers

escrowed assets without requiring a judicial enforcement officer. Although this substantially increases technical efficiency, it may simultaneously remove conventional judicial supervision from the restitution process (Savelyev, 2017).

(d) **Challenges of identity and eligibility in the selection of arbitrators:** A principal obstacle to recognizing blockchain arbitration arises from the anonymity of arbitrators. Article 466 of the Iranian Code of Civil Procedure imposes legal restrictions and qualifications concerning persons who may serve as arbitrators. The concept of a legally eligible “person” within the Iranian system presupposes an identifiable natural or legal person. In decentralized arbitration, by contrast, arbitrators may be represented only through wallet addresses and selected algorithmically. Such anonymity conflicts with mandatory rules concerning challenges to arbitrators. Where arbitrator identity is unknown, parties cannot determine disqualifying circumstances, family relationships, conflicts of interest, or financial interests. Hacker’s analysis highlights the risk that game-theoretic platforms may reduce justice to statistical consensus, thereby weakening rights of defense and meaningful challenge to adjudicators (Hacker, 2019). From the standpoint of Iranian public policy, recognition of an award rendered by an anonymous and effectively unchallengeable adjudicator therefore raises substantial difficulties because transparency concerning the identity of the decision-maker constitutes an important guarantee of procedural fairness (Werth & Cairns, 2024).

(e) **Conflict between automatic enforcement and formal enforcement procedures:** In blockchain arbitration, the distinction between adjudication and enforcement largely disappears. When a smart contract automatically restores counter-performances following a digital arbitral decision, the process constitutes a form of private and automated enforcement. Under Articles 488 et seq. of the Iranian Code of Civil Procedure, however, enforcement of arbitral awards requires an application by the interested party, notification of the award, and issuance of an enforcement order by the court. Savelyev’s analysis emphasizes that smart contracts, by eliminating meaningful judicial intervention at the enforcement stage, may disrupt conventional institutional balances (Savelyev, 2017). Where an award is immediately executed by code, rights to challenge the award or seek its annulment under Articles 489 and 490 may become practically ineffective because the digital asset may already have been retransferred before judicial review can occur. Accordingly, for such procedures to acquire full legal effect within the Iranian legal system, a mechanism of judicial confirmation before irreversible execution may be required to ensure consistency with public policy.

6.3. Recognition and Enforcement of Foreign Judgments in the Digital Environment

Recognition and enforcement of foreign judgments involving digital assets combine classical challenges of conflict of laws and jurisdiction with the geopolitical complexities of cyberspace. Under Iranian law, the relevant Civil Code provisions concerning foreign-law effects and public policy operate alongside procedural rules governing recognition and enforcement of foreign judgments. Blockchain’s cross-border nature nevertheless creates uncertainty regarding the “place of enforcement,” a concept central to private international law. Savelyev’s analysis correctly highlights that, while judicial decisions are ordinarily tied to geographical boundaries, blockchain operates in an “a-territorial” environment in which effective control over an asset may depend primarily upon possession of the relevant private key (Savelyev, 2017).

In restitution disputes, where the asset concerned is controlled through a hardware wallet located within Iranian territory, a foreign judgment will ordinarily require recognition by Iranian courts before domestic coercive power can be used to compel the holder to transfer the property. A more fundamental difficulty arises where the asset is located within a liquidity pool or global smart contract belonging to no particular jurisdiction. In such circumstances, De Filippi and Wright’s analysis points to a phenomenon that may be described as the “distributed nature of the enforcement object”: the asset is neither conventionally situated in Iran nor in the state issuing the judgment but instead exists within a distributed computational layer (De Filippi & Wright, 2018). Traditional judicial-assistance mechanisms therefore encounter difficulty because no local enforcement authority exists to which the order can readily be directed.

To address this difficulty, comparative analysis increasingly considers forms of “transnational automated enforcement.” Under this paradigm, instead of relying exclusively upon lengthy recognition procedures across multiple jurisdictions, blockchain protocols could be designed to accept decisions from predetermined arbitral institutions or courts as authenticated inputs through international judicial oracles. Werbach’s analysis suggests that if blockchain protocols are designed to recognize

agreed judicial or arbitral decisions automatically as “valid inputs,” restitution may occur independently of the parties’ physical locations (Werbach, 2018). From the perspective of Iranian law, adapting to such developments may require interpreting public-policy constraints, including those reflected in Article 975 of the Civil Code, in a manner that does not automatically characterize technical recognition of agreed foreign decisions within self-executing code as a violation of sovereignty, particularly where such recognition protects digital commerce and proprietary rights.

6.4. Summary of Jurisdictional and Applicable-Law Challenges

The foregoing analysis demonstrates that smart contracts create serious difficulties for traditional private international law. The declining utility of territorial connecting factors, anonymity, conflict between automated execution and formal procedural mechanisms, and complexities concerning recognition and enforcement of foreign judgments all point toward the need for new legal paradigms. Several practical mechanisms may therefore be considered.

First, express governing-law and arbitration clauses should be incorporated into smart contracts as preventive mechanisms. Second, Iranian law should formally recognize “electronic arbitration” and potentially certain forms of “blockchain arbitration,” provided that fundamental guarantees of procedural fairness are preserved. Third, international cooperation should be strengthened for recognition and enforcement of decisions concerning digital environments on the basis of reciprocity and public policy. Fourth, legal systems should encourage the development of “legally compliant smart contracts” incorporating legal gateways through which judicial intervention and enforcement can occur (De Filippi & Wright, 2018; Werth & Cairns, 2024).

7. Conclusion

The present study examined the legal challenges associated with restitution of counter-performances in blockchain-based smart contracts, focusing specifically on the conflict between the technical rigidity of computer code and the legal necessity of restoring the parties to their pre-contractual position. The findings demonstrate that this conflict constitutes one of the most profound legal challenges of the digital age and raises fundamental questions for traditional legal systems.

First, blockchain immutability, regarded as one of the technology’s principal technical advantages, becomes a substantial obstacle when mandatory legal rules must be implemented. Mandatory rules concerning the prohibition of *riba*, prohibition of *gharar*, unlawful purpose, rights of rescission and contractual options, and judicial discretion in contractual interpretation may all conflict with rigid code execution. This conflict originates in the fundamental difference between the “logic of law,” which depends upon flexibility, interpretation, and justice, and the “logic of code,” which depends upon certainty, inflexibility, and mechanical execution (De Filippi & Wright, 2018; Savelyev, 2017).

Second, where a smart contract is void or rescinded, restitution may encounter a technical impasse. In decentralized systems, because no accountable intermediary exists, no central authority can directly impose a judicial order upon the distributed ledger. This situation, described in the present study in terms of “temporal rigidity” or “technical detention of the asset,” may result in digital assets remaining within the breaching obligor’s wallet even after the contract has been legally invalidated, without a technically direct method of returning them to the original owner (Durovic & Janssen, 2022; Mik, 2017).

Third, analysis of civil liability arising from algorithmic errors demonstrates that allocation of responsibility among the programmer, platform, and user should be based on “control and knowledge.” The programmer may be liable under the concept of “professional negligence”; the platform may incur shared responsibility under theories of reliance and implicit endorsement; and user conduct should fully exclude recovery only where the user possessed complete technical knowledge of the hidden defect. With respect to oracles, the distinction between an “entrusted intermediary” and an actor assuming an “obligation of result” may provide a basis for allocating responsibility (Fox & Johnston, 2020; Katouzian, 2016; Savelyev, 2017).

Fourth, in the fields of jurisdiction and applicable law, the findings demonstrate that traditional connecting factors lose much of their effectiveness in decentralized environments. The decline of territorial criteria, anonymity, and conflict between automated execution and formal judicial procedures indicate the need to move toward new legal paradigms. Formal recognition of “electronic arbitration” and carefully regulated forms of “blockchain arbitration,” subject to fundamental guarantees of procedural fairness, may constitute practical solutions (Hacker, 2019; Werth & Cairns, 2024).

The principal hypothesis of the study—that “the immutability of smart contracts, when confronted with the necessity of restitution following contractual invalidity or rescission, creates an enforcement impasse”—is supported by the analysis. The findings demonstrate that, within decentralized systems, the absence of an accountable intermediary and the cryptographic nature of digital assets mean that a judicial order requiring restitution in kind may lack a directly available technical enforcement mechanism.

The subsidiary hypothesis—that “remedial doctrines such as reverse transactions, compulsory valuation of digital assets, and the design of legally compliant smart contracts can overcome these enforcement impasses”—is likewise supported. The analysis demonstrates that a transition from “physical or direct restitution” toward “compensation of digital value,” combined with incorporation of “legal gateways” into code architecture, can provide practical mechanisms for addressing these difficulties.

On the basis of the findings, the following practical solutions are proposed at the legislative, judicial, and technical levels.

(a) Legislative Solutions

1. Enactment of comprehensive smart-contract legislation: Given that Iran’s Electronic Commerce Act of 2003 was enacted before the emergence of blockchain, the legislature should adopt comprehensive legislation defining the concept and legal status of smart contracts, the relationship between legal text and computer code, the effects of coding errors or defects, and mechanisms governing restitution of counter-performances.

2. Updating rules governing restitution of counter-performances: In light of Articles 288 and 391 of the Civil Code, it is proposed that the doctrine of “digital constructive loss” be formally recognized as a new legal concept. Accordingly, where restitution in kind of a digital asset is impossible because of “technical detention” or “technical impossibility,” the court should be authorized to order restitution through an equivalent asset or monetary value.

3. Formal recognition of digital arbitration: Amendments to the Code of Civil Procedure should provide for recognition and enforcement of awards issued through electronic and blockchain-based arbitration platforms, provided that fundamental guarantees of due process, including transparency of arbitrator identity, the right to be heard, and the possibility of challenging the arbitrator, are observed.

4. Mandatory transparency in smart contracts: Legislators should require smart-contract platforms and developers to provide transparent “white papers” and credible “code audits” so that users enter transactions with adequate knowledge of relevant technical risks.

(b) Judicial Solutions

1. Judicial specialization: Given the technical complexity of smart contracts, specialized courts or dedicated judicial branches should be established to adjudicate disputes involving digital assets.

2. Use of technology experts: In restitution disputes, judges should rely upon expert opinions from blockchain and programming specialists in order to trace the precise movement of assets and issue appropriate decisions.

3. Issuance of precedent-setting decisions: The Supreme Court should develop clear and consistent standards concerning “digital constructive loss,” allocation of responsibility among programmers, platforms, and users, and the application of mandatory rules to smart contracts.

(c) Technical Solutions

1. Design of “legally compliant” smart contracts: Developers should incorporate “legal gateways” or “emergency stop keys” into code architecture so that lawful judicial intervention remains possible when a court order is issued.

2. Development of decentralized oracles: To reduce the risk of erroneous input data, developers should employ “decentralized oracle” models or data-aggregation mechanisms, such as reliance on multiple independent sources.

3. Establishment of a “judicial oracle”: Through cooperation between the judiciary and technology institutions, a “national judicial oracle” could be developed to function as an interface between final court judgments and legally compliant smart contracts. Such a system could automatically transmit the status of judgments, including nullity or rescission, to smart contracts and facilitate reverse transfers of digital assets.

The present study primarily focused on theoretical and comparative analysis of the challenges associated with restitution of counter-performances in smart contracts. Future researchers may employ empirical methods, including interviews with judges, lawyers, and blockchain specialists, to examine practical challenges and potential solutions. More detailed comparative studies

involving Islamic legal systems, such as Malaysia and the United Arab Emirates, which have advanced significantly in the field of Islamic financial technologies, may also provide valuable insights.

Justice in the digital age requires a new synthesis between the logic of law and the architecture of code. Although smart contracts constitute powerful instruments for increasing efficiency and transparency in commercial relationships, these advantages cannot justify disregard for mandatory rules, fundamental principles of due process, or proprietary rights. By drawing upon the capacities already present in the Civil Code, the Electronic Commerce Act, and Islamic jurisprudential principles, the Iranian legal system can develop a balanced framework for addressing restitution challenges in blockchain environments through recognition of emerging doctrines such as digital constructive loss, compulsory valuation of digital assets, and legally compliant smart contracts. Such an approach can both protect citizens' rights and facilitate the secure and sustainable development of the digital economy.

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

- De Filippi, P., Mannan, M., & Reijers, W. (2020). Blockchain as a Confidence Machine: The Problem of Trust & Challenges of Governance. *Technology in Society*, 62, 101284.
- De Filippi, P., & Wright, A. (2018). *Blockchain and the Law: The Rule of Code*. Harvard University Press.
- Durovic, M., & Janssen, A. (2022). The Formation of Blockchain-Based Smart Contracts in the Light of EU and US Law. *European Review of Private Law*, 30(2), 243-268.
- Forder, J. (2020). *Blockchain and the Law: The Rule of Code*. Oxford University Press.
- Fox, G., & Johnston, A. (2020). *Smart Contracts and the Law: A Comparative Analysis*. Routledge.
- Golmohammadi Naneh Karan, M., & Nasabpour Molaei, A. (2024). Digital Smart Contracts and the Law Governing Them in Light of Private International Law. *Encyclopedia of Comparative Jurisprudence and Law*, 3(2), 179-199.
- Golresan, M. (2025). *Contractual Obligations in Artificial Intelligence and Smart Contracts*. Hoorin Publications.
- Hacker, P. (2019). AI and the Rule of Law: The Jurisdiction of Algorithms. *European Journal of Legal Studies*, 12(Special Issue), 145-162.
- Hacker, P. (2021). Smart Contracts and the Law: A New Way of Thinking? *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 11(1), 3-15.
- Katouzian, N. (2016). *General Rules of Contracts* (Vol. 2). Enteshar Joint Stock Company.
- Lacker, M., & Noone, S. (2021). Smart Contracts and Consumer Protection. In *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms*. Cambridge University Press.
- Lessig, L. (2006). *Code: Version 2.0*. Basic Books.
- Low, K. F. K., & Teo, E. (2017). *Bitcoin and the Law*. Cambridge University Press.
- Luo, Y. (2024). *Smart Contracts and the Law: A Comparative and International Perspective*. Routledge.
- Mafi, H., & Kaviyar, H. (2013). A Comparative Study of the Law Governing Electronic Contracts Concluded on the Internet from the Perspective of the Legal Systems of the United States, the European Union, and Iran. *University of Tehran Journal of Private Law Studies*, 4(1), 105-125.
- Mik, E. (2017). Smart Contracts: Terminology, Technical Limitations and Real-World Complexity. *Law, Innovation and Technology*, 9(2), 269-300.
- Nasri, F. (2024). *Use of Artificial Intelligence in the Formation and Performance of Contracts* [Master's thesis, Shomal University].
- Pisa, M., & McCurdy, S. (2023). *Blockchain and the Law: A Practitioner's Guide*. Edward Elgar Publishing.
- 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.
- Scholten, M., & Janssen, A. (2021). *Smart Contracts and the Law: A European Perspective*. Oxford University Press.
- Werbach, K. (2018). *The Blockchain and the New Architecture of Trust*. MIT Press.

- Werth, C., & Cairns, S. (2024). *Digital Arbitration and Smart Contracts*. Kluwer Law International.
- Zetsche, D. A., Buckley, R. P., & Arner, D. W. (2023). *FinTech: Law and Regulation*. Oxford University Press.
- Zheng, G. (2022). Choice of Law for Smart Contracts: The Decentralized Approach. *Journal of Private International Law*, 18(2), 231-255.