A Comprehensive Technical–Legal Elucidation of the Nature of Cryptocurrency Mining and Exchange within the Framework of Positive Law Requirements

1. Ahmad Jalili: Department of Computer Engineering, Gonbad Kavoos University, Golestan, Iran
2. Omid Dehghani *: Department of Law, NT.C., Islamic Azad University, Tehran, Iran

*Correspondence: omiddehghani@yahoo.com

Abstract

By adopting an interdisciplinary approach, the present study examines the nature of cryptocurrency mining and exchange within the framework of legal requirements. From a technical perspective, it is argued that the mining process is not merely a form of data processing; rather, it is a function of "consensus mechanisms," such as proof-of-work, which ensure the security and immutability of the network through hashing functions and the expenditure of computational power. The findings of the study at this level indicate that network rewards are the outcome of an automated and algorithmic technical process that derives its intrinsic value from mathematical scarcity and market demand. From a legal perspective, by aligning the technical characteristics of cryptocurrencies with the general principles of contract law, the principal question concerning the origin of ownership of mining rewards is addressed. The study demonstrates that cryptocurrency mining is not fully compatible with the theory of "appropriation of ownerless property" due to the absence of prior physical tangibility. Instead, the most appropriate legal framework for explaining this process is the "general Ju'alah contract." Under this model, the blockchain protocol functions as the "offeror," while the miner acts as the "agent," thereby establishing a legal relationship in which the "code" serves as a systemic offer and the "expenditure of computational power" constitutes practical acceptance. In the discussion of exchange, the study emphasizes the "constructive proprietary value" of cryptocurrencies and argues that despite their intangible nature, cryptocurrencies may function as the "price" in a contract of sale or as "consideration" in barter transactions due to their exchange value and recognition by commercial custom (assuming the absence of an explicit legal prohibition). Furthermore, challenges associated with civil liability arising from coding errors, 51% attacks, and anonymity in transactions are examined. It is proposed that legislators, by recognizing the concept of "algorithmic governance," should formulate new legal requirements aimed at consumer protection and the stability of the digital capital market. Ultimately, the article emphasizes the necessity of transitioning from traditional legal frameworks toward "technology-oriented regulation" in order to reduce transactional risks in the era of the digital economy.

Keywords: Blockchain, Cryptocurrency Mining, Private Law Requirements, Ju'alah Contract, Constructive Proprietary Value, Consensus Mechanism.

Received: 01 February 2026
Revised: 01 June 2026
Accepted: 08 June 2026
Initial Publication 08 August 2026
Final Publication 01 November 2026

Citation: Jalili, A., & Dehghani, O. (2026). A Comprehensive Technical–Legal Elucidation of the Nature of Cryptocurrency Mining and Exchange within the Framework of Positive Law Requirements. *Legal Studies in Digital Age,* 5(6), 1-10.

1. Introduction

The rapid advancement of knowledge and technology within cyberspace has placed human societies in a global village and has profoundly transformed people's lifestyles. These new developments have not only created new economic opportunities but have also posed complex threats and challenges to legal and technical systems (Murphy, 2015). In this context, ignoring technological realities and failing to provide timely scientific responses may lead to losses and harms arising from ambiguities in economic and social structures. One of the most important innovations arising from the development of the internet is the emergence of new financial systems in which control over the circulation of money has been removed from governments and placed in the hands of people. These new assets indicate the emergence of a system that, due to its distinctive function, has involved different sectors of society, including law, economics, and politics, in both micro- and macro-level ambiguities (Arzanian, 2020). Therefore, sound decision-making regarding this type of invented currency requires a deep understanding of its technical nature and its conformity with legal rules.

Digital currency technology is based on blockchain, which uses complex cryptography to ensure the security and validity of transactions at the global level. From a technical perspective, this system is a distributed ledger that enables peer-to-peer exchanges and financial transactions without the need for centralized intermediaries (Rafiei, 2018). In fact, by combining mathematics and networking, this structure has created a new form of digital credibility that, despite being intangible, possesses economic value. In legal studies, explaining the legal nature of this phenomenon has faced serious challenges because its technical structure differs from traditional definitions of property and assets. Jurists seek to determine whether these data-based numerical units, which are not dependent on another property, can possess constructive proprietary value and be capable of private ownership (Shahidi, 2007). According to modern criteria, anything that is accepted by custom and has rational utility may fall within the domain of legal obligations.

The process of cryptocurrency mining is one of the most complex technical layers in this field, relying on consensus mechanisms and the solution of computational mathematical problems. In this process, miners expend hardware capacity and energy costs to help validate transactions and maintain network stability, receiving a specified reward in return (Nakamoto, 2009). This technical activity has an automatic and algorithmic nature that regulates the production rate of new assets through programming and without human intervention. From the perspective of contractual obligations, aligning the technical activity of mining with legal rules such as the reward undertaking contract is one of the main solutions for explaining the relationship between the network and the miner. In this legal model, cryptographic protocols, as a public offer, promise payment of a reward in exchange for performing the technical act of validating blocks, which is accepted by the miner (Mousavi Khomeini, 2013). This intersection between legal intent and technical process constitutes the main basis for acquiring ownership of assets obtained through mining in positive legal systems. In the field of exchange and sale of these assets, challenges such as determinacy in terms of type and attributes, as well as relative stability of value in transactions, have always been raised. Given severe price fluctuations, some researchers consider such exchanges to involve the suspicion of excessive uncertainty, whereas technical analyses indicate the existence of customary material value and proprietary value in these instruments (Naderi & Motalebi, 2021). Private law is required to understand technological infrastructures and formulate clear rules for the validity of these contracts and the lawful transfer of ownership.

The necessity and importance of this study lie in comprehensively explaining the connection between the technical layers of mining and legal obligations in order to address existing legislative gaps in this field. The main objective of this research is to accurately identify the nature of digital currencies and examine their position in the capital market in order to provide practical solutions for regulating this emerging industry (Rezvani Najafabadi, 2018). Through an interdisciplinary perspective, this study seeks to provide a path for supportive legislation and the reduction of transactional risks in the national economy.

2. Research Methodology

In terms of nature, the present study is qualitative research, and in terms of purpose, it falls within the category of applied research; it explains the subject through a descriptive–analytical method. Given the interdisciplinary nature of this study, an

integrative approach has been used to examine the technical infrastructures of information technology together with the fundamental rules of private law. The theoretical framework of this research is based on content analysis of legal and technical texts in order to establish a logical connection between algorithmic processes and legal obligations. In the data collection phase, the library method and documentary review were used. The sources examined include positive laws, juristic opinions, articles indexed in reputable scientific databases, and technical documents related to blockchain protocols and digital currencies. In addition to domestic sources, international documents and reports issued by information technology regulatory bodies were also reviewed and analyzed to enrich the technical and legal dimensions of the study. The data analysis process in this article was carried out step by step using a systematic matching method. At the first layer, the technical characteristics of cryptocurrency mining and exchange were explained from the perspective of software engineering; at the second layer, these characteristics were applied to traditional institutions of private law. This analytical method makes it possible to redefine emerging technological concepts within recognized legal frameworks, such as nominate contracts and contractual obligations, and to scientifically identify existing legislative gaps (Khademan et al., 2020). Despite limitations such as the novelty of the subject and the lack of comprehensive reference books at the intersection of law and technology, this research seeks to provide legal solutions to the security and legal challenges of this field by relying on logical arguments. Due to the dynamic and evolving nature of decentralized technologies, the validity of the findings of this research is based on the maximum possible alignment between the mathematical logic governing protocols and the foundations of public order in legal studies (Nabavi, 2019).

3. Theoretical Foundations and the Technological Infrastructure of Digital Assets

Blockchain technology, as the main infrastructure of digital currencies, is a decentralized and distributed information-recording system based on cryptographic principles. From a technical perspective, this network consists of a set of blocks, each containing a list of validated transactions, and each block is connected to its preceding block, thereby producing immutability and a high level of data security (Nakamoto, 2009). In fact, this technical structure enables the elimination of centralized intermediaries such as banks and places control over the circulation of assets directly in the hands of mathematical protocols. Mining, which is regarded as the beating heart of this technology, is based on consensus mechanisms, especially the proof-of-work method. In this mechanism, network nodes or miners must solve complex mathematical problems through hashing functions in order to obtain permission to add a new block to the chain (Nakamoto, 2009). This activity, which requires high processing power and significant operational costs, constitutes the basis for producing new currencies and validating transactions in the blockchain network.

From the perspective of legal analysis, one of the fundamental concepts in this field is the explanation of "proprietary value" in the digital environment. In private law, property refers to anything that has economic value, rational utility, and the capacity to be allocated to a person (Katouzian, 2007). Although digital currencies lack physical tangibility, they have acquired constructive proprietary value because of mathematical scarcity, security arising from cryptography, and general acceptance in exchanges; they are therefore recognized as financial rights within the sphere of legal obligations. The substantive difference between traditional money and digital currencies lies in the source of their credibility. While official money or fiat currency derives its credibility from state command and central bank support, digital currencies have a private and decentralized nature, and their credibility derives from protocol coding and users' trust in mathematical algorithms (Toutounchian, 1996). This independence from political sovereignties has transformed cryptocurrencies into cross-border assets that challenge traditional monetary and banking rules. Therefore, explaining the legal nature of these assets requires understanding the technical reality that cryptocurrencies are not merely numbers in a database, but the result of a "systemic contract" among network members. Because these assets possess independent existence and are not dependent on another property, they fall within the category of movable and constructive property (Mandjee, 2019). Understanding this intersection between the technical obligations of the protocol and the legal rules of property forms the main foundation for analyzing mining and exchange contracts in the following sections of this study.

4. A Technological–Legal Explanation of the Nature of Digital Assets

As a first step in explaining the nature of digital assets, it must be understood that these phenomena are not merely financial instruments; rather, they are technical entities created through the combination of sequential data strings and cryptographic algorithms. From the perspective of information technology, a digital asset is the result of the execution of a protocol in a distributed network that defines ownership status through public and private key pairs. This dual nature requires traditional private law to revise its definitions of objects and distinguish between "raw data" and "constructive value" in order to formulate precise legal obligations for them. From the perspective of software engineering, the infrastructure of digital assets is based on asymmetric cryptography, in which each unit of an asset is mathematically connected to a specific address. This technical connection means that, unlike physical property, possession in the digital environment is exercised not through material delivery and receipt, but through possession of the "private key." Therefore, in private law, the concept of possession or proprietary control over property here means exclusive access to the digital signature that enables transfer of the asset within the network (Rafiei, 2018). In analyzing the legal foundations, the fundamental question is whether these intangible assets possess the attribute of "property." In positive law, property refers to something that has the three main elements of "economic value," "rational utility," and "capacity to be allocated to a person" (Katouzian, 2007). Digital assets clearly have economic value because of mathematical scarcity arising from restrictive coding and the existence of demand in the capital market. In addition, the ability of these assets to facilitate cross-border exchanges and preserve value has established their rational utility for custom and merchants.

One of the prominent technical features that affects the legal nature of these assets is the "immutability" of records in the blockchain. From a legal perspective, this feature makes digital assets, unlike paper documents or centralized electronic money, resistant to forgery. This technical security strengthens the basis of "constructive proprietary value" and allows digital assets to be recognized as "constructive objects" in transactions. In fact, legal trust here is created not through governmental institutions but through the mathematical robustness of the protocol (Toutounchian, 1996).

The issue of technical scarcity in digital assets has a direct relationship with their legal value. In computer science, algorithms such as proof-of-work or proof-of-stake are designed to limit the production rate of new assets and prevent excessive inflation. In private law, this technical limitation is recognized as the basis of "customary need," because the more limited access to a resource is and the more exclusive its control becomes, the stronger the customary inclination to allocate ownership rights to it will be (Khademan et al., 2020).

The distinction between traditional "electronic money" and "digital currency" is highly important from both technical and legal perspectives. Electronic money usually represents the debt of a bank or centralized institution to its holder, and its value depends on underlying physical assets. Cryptocurrencies, however, are technically "asset-based"; that is, their value lies in the code itself and does not depend on the obligation of any third party (Mandjee, 2019). This technical independence means that in private law they should be classified not as "debt," but as an "independent financial right." In examining legal obligations, cryptocurrencies are technically considered fungible entities. This means that each unit of a specific cryptocurrency is completely identical and replaceable with another unit of the same type in terms of coding and technical value. However, at the legal layer and in the performance of contractual obligations, severe price fluctuations may challenge their fungible nature at the time of compensation. Nevertheless, the prevailing legal view is that, due to the equality of technical and customary attributes, these assets fall within the category of fungible property (Izadifard et al., 2012).

The concept of "decentralization" in blockchain technology has created new challenges for the concept of "civil liability" in private law. In traditional systems, hacking or system error is attributed to the central institution; however, in digital assets, due to the absence of a central supervisor, responsibility for protecting the asset rests directly with the holder of the private key. This technical structure requires the definition of new legal obligations for explaining "fault" in the digital environment, so that if a user is negligent in protecting their private key, they will be legally regarded as responsible for the loss of their own property (Nakamoto, 2009).

Technical divisibility is another feature that makes the legal nature of these assets flexible. Cryptocurrencies can be divided into very small units, even up to eight decimal places, without changing their technical nature or relative value. In private law, this feature enables the conclusion of micro-contracts and precise payments, which are not easily possible with physical

property. This technical potential has led custom to accept cryptocurrencies as an efficient "price" in modern commercial contracts (Shahidi, 2007).

Therefore, explaining the nature of these assets shows that we are dealing with a "new financial right" rooted in the technical obligations of algorithmic governance. Since international and domestic transactional custom has widely accepted these assets as instruments for transferring value, private law cannot remain indifferent to their ownership and exchange. Accordingly, a digital asset should be regarded as an entity that, although it has no material body, bears all legal effects attached to "property" because of the security arising from cryptography and the credibility arising from customary demand (Khorsandi Kouchesfahani, 2019).

5. Analysis of the Mining Process within the Framework of Contractual Obligations with an Emphasis on the Reward Undertaking Contract

From the perspective of information technology, the mining process in the blockchain network consists of a set of processing activities aimed at solving complex mathematical functions and validating transactions. However, from the perspective of private-law obligations, this activity is not merely data processing; rather, it is a "legal act" that leads to the creation of ownership rights over the network reward. The main challenge here is to explain the source of this acquisition of ownership; that is, it must be determined under which contractual framework the miner obtains the right to recognize the generated cryptocurrency as their own asset (Nakamoto, 2009). Some legal analysts have compared mining with the institution of "appropriation of ownerless property," arguing that cryptocurrencies are ownerless assets and that whoever gains access to them first becomes their owner. However, this analysis is problematic from both technical and legal perspectives, because in appropriation, the property must have external existence before possession, such as hunted fish, whereas in mining, the cryptocurrency does not exist before the computational process; in fact, the "act of mining" is the generating and constitutive cause of its existence (Mousavi Khomeini, 2013). Therefore, a framework must be sought that establishes a legal relationship between "performing work" and "the emergence of property."

Under the rules of Iranian private law, the "reward undertaking contract," defined in Article 561 of the Civil Code, provides the best framework for explaining this process. A reward undertaking is "a person's commitment to pay a specified remuneration in exchange for an act, whether the other party is determined or undetermined." In the blockchain network, the software protocol operates as a "public offer," promising each network user that if they solve mathematical problems and validate a block, they will receive a specified amount of cryptocurrency as a reward (Mousavi Khomeini, 2013).

From the perspective of software engineering, the blockchain protocol has a "self-executing" nature. In private law, this technical feature is understood as the existence of an "intent embedded in code." In fact, the initial designers of the protocol issued a systemic and perpetual offer through coding. Here, the "promisor" is the legal or protocol-based entity issuing the offer, and the "intended act" is the technical activity of mining, namely the expenditure of computational power to preserve the security and stability of the network (Shahid Thani, 1978). One of the main elements of the reward undertaking contract is a "public offer" addressed to the public. Blockchain follows exactly this pattern: the network imposes no limitation on the identity of the miner, and anyone anywhere in the world who has suitable hardware can be addressed by this offer. This intersection between technical anonymity in computer science and the concept of an "undetermined party" in the reward undertaking contract demonstrates the full conformity of the technical obligations of mining with the standards of private law (Bayat & Bayat, 2019). At the layer of "acceptance," unlike other onerous contracts, the reward undertaking contract does not require verbal declaration of intent; rather, "performance of the act" is regarded as contractual acceptance. In the mining process, when the miner turns on their device and begins solving equations, they have in fact practically accepted the systemic offer of the network. This "practical acceptance" begins from the moment processing starts and is completed with the "production of a valid block," thereby giving rise to entitlement to receive the reward (Mousavi Khomeini, 2013).

The technical part of the study emphasizes that the mining reward is a reward for validating transactions. From a legal perspective, this reward possesses "proprietary value," and the miner has created economic value by performing a technical service. Therefore, the relationship between the network and the miner is a service-oriented relationship in which "code" guarantees the obligation to pay. This technical guarantee at the code layer is recognized in positive law as a "legal obligation

arising from contract" borne by the systemic structure (Khademan et al., 2020). Another challenge raised in the reward undertaking analysis of mining concerns the "determinacy of remuneration." In blockchain, the amount of cryptocurrency paid as a reward is fully specified, for example 6.25 units, but its value in national currency or United States dollars constantly changes. Traditional private law may regard this issue as an instance of "excessive uncertainty" or ambiguity. However, since approximate knowledge of remuneration is sufficient in the reward undertaking contract and the "number of units" itself is fixed and determined, this price fluctuation does not impair the validity of the contract and is compatible with the principle of transactional stability (Naderi & Motalebi, 2021).

From the perspective of information technology, mining is a computational competition in which only the first person to reach the answer receives the reward. This technical feature can be analyzed in private law under the title of "a reward undertaking for the first performer." If several persons work on one block simultaneously, under legal rules, only the person who completes the act, that is, publishes the first valid block, will be entitled to the reward. This technical mechanism is precisely consistent with contractual justice in reward-based contracts (Shahid Thani, 1978). Accordingly, explaining mining within the framework of the reward undertaking contract proves that income derived from this activity is fully lawful income arising from a "modern technical–legal contract." This analysis not only removes ambiguities surrounding the legitimacy of acquiring ownership over cryptocurrency, but also allows the legislator to recognize mining as a "service industry in the field of information technology." Under this approach, private-law obligations do not hinder technological growth; rather, they provide a protective framework for algorithmic mining activities (Rezvani Najafabadi, 2018).

6. Analysis of the Legal Obligations Governing the Exchange and Sale of Digital Assets

Transfer of ownership in the digital environment is a process carried out through electronic signature and validation in the distributed ledger. This exchange, which at the technical layers means changing the asset address from one private key to another private key, is recognized in private law as an onerous legal act. To properly understand this process, it must be assessed whether cryptocurrency performs the role of a "commodity" in a contract or can be accepted as "price" or a payment instrument in a contract of sale (Naderi & Motalebi, 2021). The legal nature of cryptocurrency exchange is tied more than anything else to contracts of sale and barter. Under Article 338 of the Civil Code, sale is the transfer of ownership of a specific object in exchange for known consideration. If cryptocurrency is regarded as possessing the attribute of a "constructive object," its exchange for national money or other common currencies will constitute a clear instance of a contract of sale. Where two cryptocurrencies are exchanged with one another, this legal act can be analyzed as "barter," in which both parties exchange their digital assets without one having priority over the other (Shahidi, 2007). One of the main elements of validity in transactions is the existence of proprietary value in the subject matter of the contract. Digital assets possess exchange value recognized by custom because of algorithmic scarcity and security arising from the blockchain structure. Since the legislator has not expressly prohibited the transfer of ownership and exchange of these assets in positive laws, the presumption is the validity and enforceability of these contracts. This customary acceptance forms the foundation of the "constructive proprietary value" of cryptocurrencies and turns them into legitimate subjects of contractual obligations (Khorsandi Kouchesfahani, 2019). At the layer of determinacy of the subject matter, the technical structure of cryptocurrencies minimizes ambiguities related to quantity and type. Each digital unit has a unique identification code determined through hashing, which eliminates confusion regarding the identity of the property. In private law, the requirement that the sold item be known, as reflected in Article 216 of the Civil Code, is fulfilled here through the transparency present in the distributed ledger. In other words, the technical features of coding perform the same function that description of attributes and quantity performs for physical property (Shahidi, 2007).

Value stability is one of the serious issues in the exchange of these assets. Severe cryptocurrency price fluctuations may create the impression that transactions involving them contain "excessive uncertainty" or abnormal risk. However, under a precise analysis of legal obligations, excessive uncertainty invalidates a transaction only when there is ignorance regarding the subject matter itself or the ability to deliver it. In cryptocurrencies, although market value changes, the technical nature and number of units exchanged are completely clear; therefore, these fluctuations do not impair the validity of the contract and may only, under certain conditions, give rise to the option of rescission for gross disparity (Naderi & Motalebi, 2021). The process

of "delivery and receipt," which in private law is a condition for completion or, in some cases, a condition for validity of a transaction, acquires a new meaning in the digital environment. In cryptocurrency exchanges, delivery of the property is realized through transfer of the "private key" or by sending the asset to the buyer's wallet address. From the moment the transaction is validated in the blockchain network and recorded in a block, the seller's proprietary control is terminated and the buyer acquires the right of disposal. This systemic validation is regarded at the legal layer as delivery of the sold item and performance of the seller's obligation (Nakamoto, 2009). In examining the role of cryptocurrency as a payment instrument, there is a subtle distinction between "money" and "currency." In the monetary and banking system, money is an instrument with legal power to discharge obligations. Although cryptocurrencies have not yet been recognized as legal tender in many countries, in private law the parties to a contract may, based on the principle of freedom of will under Article 10 of the Civil Code, accept cryptocurrency as "known consideration" in their contracts. In this case, although cryptocurrency is not official money, it performs the payment obligation as a valid "contractual price" (Toutounchian, 1996).

The security of digital transactions and prevention of offenses such as "double spending" are guaranteed through consensus algorithms. This technical feature prevents a single asset from being sold simultaneously to two persons. In private law, this ensures the stability of ownership and prevents disputes related to unauthorized transactions or the sold item belonging to another. In fact, the technical obligations governing the network protect the validity of the transfer of ownership before judicial authorities intervene (Nakamoto, 2009). Civil liability arising from transfer errors or exchange hacks forms another layer of legal obligations in exchange. If, due to a technical defect in the trading platform, the asset does not reach its destination, the intermediary institution will be liable to compensate damages under the general rules of liability. However, because of the decentralized nature of this technology, in cases where the transfer is made directly and without an intermediary, the risk arising from an error in entering the address rests with the user, which requires users to have sufficient awareness of technical infrastructures (Meredith & Tu, 2015). Accordingly, explaining the legal obligations governing cryptocurrency exchange shows that the private-law system must flexibly accept new models of rights transfer. Digital assets are not only a new subject matter for contracts; they are also instruments that can increase the speed and security of economic exchanges. By legally recognizing these exchanges and formulating tax and protective rules, the potential of this technology can be used to develop the capital market and reduce the costs of financial transfers (Economic Security, 2017).

7. Security Challenges and Regulatory Solutions in the Field of Digital Assets

The development of digital assets within decentralized networks, despite its numerous advantages, has created unique security risks that are unprecedented in traditional private law. From the perspective of information technology, the security of this network is based on computational power and cryptographic algorithms; however, any technical defect at this layer immediately becomes a legal challenge concerning ownership and civil liability. To regulate this field, it is essential to accurately understand threats such as cyberattacks, loss of technical access, and algorithmic fraud (Nabavi, 2019). One of the most serious technical threats affecting the validity of transactions in legal studies is the "51% attack." In this scenario, the attacker, by obtaining the majority of the network's processing power, can rewrite the transaction history and cause double spending. From a legal perspective, the occurrence of such an attack means disruption of the "obligation to transfer ownership" and the creation of invalidity in concluded contracts. Here, the intersection of hardware power and legal validity becomes clearly visible, because the stability of ownership in blockchain is directly connected to the technical security of network nodes (Nakamoto, 2009). Another key challenge is the nature of private keys and the consequences of their loss or theft. In blockchain, "code" is the sole criterion for identifying the owner, and if a user loses their key, their access to the asset is effectively cut off, without any institution existing to restore it. This issue conflicts with classical private-law rules concerning proof of ownership. Whereas in traditional systems documents and witnesses can replace lost property, in the digital world, the loss of the technical means of possession means the permanent loss of proprietary control (Nabavi, 2019).

The civil liability of intermediary institutions such as cryptocurrency exchanges constitutes another layer of legal complexity. In many cases, hacking of exchanges' central servers leads to the loss of users' assets. According to comparative studies, determining liability for such losses requires explicit standards in the field of cybersecurity. If the exchange has committed a technical fault, it will be obliged to compensate damages under the general rules of civil liability. However, the

absence of an explicit legal definition of cryptocurrency in many countries has made the path of judicial pursuit difficult for consumers (Hoye, 2017).

Protection of consumer rights in decentralized transactions faces difficulty because of the absence of a chargeback period. In traditional sale and classical e-commerce, the buyer has the right to withdraw under certain conditions; however, in blockchain, transactions become "irreversible" once validated in a block. This technical immutability requires new legal obligations so that, through escrow-based smart contracts, it becomes possible for the asset to be automatically returned if the seller fails to perform the obligation. This is a clear example of "governance through code" instead of direct judicial intervention (Mandjee, 2019).

The issue of anonymity in transactions has created serious challenges in the field of customer identification and anti-money laundering. Cryptographic technology enables asset transfer without disclosure of identity, and this technical feature can provide a path for criminal activities. However, modern analyses show that the inherent transparency of the distributed ledger can itself serve as a tool for supervision. In explaining this paradox, it is argued that despite the anonymity of addresses, the immutable recording of all transactions in the blockchain network provides substantial potential for tracking the flow of funds; if connected to legal obligations, it can play a key role in preventing money laundering in the capital market (Jalili, 2023). Therefore, aligning private-law obligations with these supervisory rules is a vital necessity for accepting cryptocurrencies in the official capital market (Rafiei, 2018).

Jurisdiction and conflict of laws in the cross-border environment of blockchain are among other legal challenges. Since the cryptocurrency network is distributed across thousands of servers in different countries, determining the competent court for resolving contractual disputes is highly complex. In modern private law, it is suggested that parties accept the "virtual location of the transaction" or the laws of a specific country as the basis for dispute resolution in their contracts. This issue shows that national positive laws must move beyond geographical boundaries and recognize the concepts of "digital jurisdiction" (Meredith & Tu, 2015).

The creation of regulatory sandboxes is one of the successful international solutions for managing the risks of this field. Countries such as Germany and Japan, by allowing innovative companies to operate within a controlled framework, have been able to establish a balance between technological development and protection of consumer rights. In these environments, strict technical requirements are combined with legal flexibility so that the various dimensions of digital assets can be carefully assessed before they enter the macroeconomy (Hoye, 2017).

To regulate this industry, recognizing "mining" as a productive and industrial activity is a major step toward clarifying the business environment. By issuing legal licenses for mining farms, not only are state tax revenues realized, but miners also come under the protective umbrella of private law. This means transforming an underground technical activity into an "official asset" capable of being used as collateral in the banking system and recorded in commercial books (Economic Security, 2017).

Ultimately, explaining regulatory solutions shows that the future of private law in the digital age depends not on rejecting technology, but on the "convergence of law and code." The legislator must accept the technical realities of blockchain and formulate rules that protect public order without obstructing technological innovation. Only through a comprehensive technical–legal approach can the capacities of digital assets be used for economic growth while minimizing their security risks (Khorsandi Kouchesfahani, 2019).

8. Conclusion

The present study showed that the emergence of cryptocurrencies is not merely an economic transformation, but a fundamental shift at the intersection of blockchain technology and the rules of private law. The technical findings confirm that consensus mechanisms and asymmetric cryptographic structures have created a level of security and stability that international transactional custom has accepted as a basis of value. From a legal perspective, despite lacking a material body, these assets fall within the scope of legal and contractual obligations because they possess constructive proprietary value and rational utility. In fact, the convergence between "computational code" and "legal intent" has led to the emergence of a new institution of ownership that requires revision of traditional rules of delivery and receipt. In analyzing the mining process, this study concluded that the technical activity of miners can best be explained within the framework of a "public reward undertaking

contract." Unlike the theory of appropriation of ownerless property, which requires the existence of property before possession, in mining the network reward is the direct result of the performer's act in response to the systemic offer of the protocol. This finding shows that the relationship between the blockchain network and the miner is a modern contractual obligation in which "code" performs the role of guaranteeing performance. Recognizing this legal framework can fully remove ambiguities surrounding the legitimacy of acquiring ownership of assets obtained through mining in positive legal systems.

In the field of exchange, the research findings indicate that cryptocurrencies possess all the necessary characteristics to be treated as "known consideration" in transactions. Although price volatility is a technical reality in the digital capital market, under the rules of private law, such volatility does not result in excessive uncertainty or invalidity of the contract, because the technical identity and number of units exchanged are completely known and determined through the distributed ledger. Therefore, cryptocurrency transactions should be regarded as valid sales or barter transactions in which network validation functions as legal delivery and transfer of proprietary control. One of the key findings of the research in the field of civil liability is the necessity of distinguishing between user error and technical defect in the protocol. Although anonymity is a prominent technical feature of blockchain, legal obligations require the strengthening of customer identification mechanisms at intermediary gateways in order to prevent violation of individuals' rights. The security of digital transactions depends not only on the strength of hashing algorithms, but also on the formulation of legal requirements for protecting private keys and determining the liability of exchanges in the event of cyberattacks. This technical and legal synergy will form the foundation of trust in the digital economy.

Based on the findings of this research, it is proposed that the legislator move away from silence or declaratory prohibition and toward the use of permissive rules and the theory of the "zone of discretionary legislation." Given economic necessities and the need to benefit from technology under sanctions, the formulation of a comprehensive regulation recognizing cryptocurrencies as "constructive movable property" is unavoidable. This can be achieved through revision of the Electronic Commerce Law and the inclusion of a separate chapter on decentralized assets in order to provide judicial security for participants in this field. In the field of mining, the strategic proposal of this research is the official recognition of the "mining industry" as a service sector in information technology. The state should direct underground activities toward the transparent economy by issuing legal licenses and allocating specified energy tariffs. This approach will not only generate sustainable tax revenues for the state, but also make it possible to use mining devices as banking collateral and registered assets in commercial books, thereby contributing to capital market dynamism.

To reduce transactional risks for consumers, it is proposed that the use of "escrow-based smart contracts" be made mandatory on domestic platforms. From a technical perspective, these contracts can keep the transaction price suspended until the buyer's final confirmation that the obligation has been performed. This technological–legal solution fills the gap arising from the impossibility of chargebacks in blockchain and guarantees the integrity of transactions in the private-law system. In fact, coding here functions as a tool serving the enforcement of contractual justice. It is also proposed that the central bank, in cooperation with information technology authorities, establish regulatory sandboxes for national and private cryptocurrency projects. These environments allow the intersection of technical and legal obligations to be tested on a controlled scale and enable potential harms to be identified before they enter the broader social level. The successful experience of countries such as Germany has shown that this model of interactive regulation is the best path for managing disruptive innovations in the monetary and financial system. At the level of education and awareness-building, academic institutions in law and computer science should develop interdisciplinary courses under the title "Law of Decentralized Technologies." Training specialists who are familiar with both the coding layers of blockchain and private-law obligations is essential for the future of the judiciary and arbitration institutions. Without proper technical understanding among judges and attorneys, adjudicating complex disputes related to wallet hacking or disagreements arising from the execution of smart contracts will face serious challenges. Accordingly, the comprehensive technical–legal explanation offered in this research leads to the conclusion that digital assets are not a threat to the rules of private law, but an opportunity to redefine the efficiency of contractual obligations in the digital age. The future of the national economy depends on accepting algorithmic governance and integrating it into positive legal frameworks. Only through an active approach and the formulation of supportive laws based on the realities of blockchain can the potential of this technology be used to bypass international financial restrictions and strengthen the Islamic capital market.

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

Arzanian, N. (2020). Analytical Study of Transactions Based on Digital Currency from the Perspective of Imamiyyah Jurisprudence and the Role of Blockchain in Various Industries. *Quarterly Journal of Economic Jurisprudence Studies*, *2*(4).

Bayat, F., & Bayat, S. (2019). *Comprehensive Commentary on the Civil Code*. Arshad Publications.

Economic Security, J. (2017). Emergence and Expansion of Digital Money: Opportunities and Threats. *Economy Magazine*(45).

Hoye, J. (2017). The Role of Virtual Currency-Specific Legislation in Keeping Pace with Technology. *Wayne Law Review*, *63*(83).

Izadifard, A. A., Abhari, H., & Bahrami, H. (2012). The Concept and Nature of Money and Liability Related to Depreciation in Repayment of Banknote Loans. *Islamic Jurisprudence and Law Research*(27).

Jalili, A. (2023). Examining the Jurisprudential Nature of Digital Currency and Its Role in Preventing Money Laundering. *Quarterly Journal of Comparative Criminal Jurisprudence*, *3*(1), 17-29.

Katouzian, N. (2007). *Property and Ownership* (Seventeenth edition ed.). Mizan Legal Foundation.

Khademan, M., Kousha, A., & Nouri, F. (2020). Identifying the Legal Nature of Cryptocurrencies through Structural Analysis in the Iranian Legal System. *Judicial Law Journal*, *85*(115).

Khorsandi Kouchesfahani, Z. (2019). *The Nature of Digital Currencies and Their Consequences in Imamiyyah Jurisprudence* University of Quran and Hadith, Tehran Campus]. Tehran.

Mandjee, T. (2019). Bitcoin: Its Legal Classification as Property According to Statutory Private Law Frameworks. *Computer Law & Security Review*.

Meredith, M. W., & Tu, K. V. (2015). Rethinking Virtual Currency Regulation in the Bitcoin Age. *Washington Law Review*.

Mousavi Khomeini, R. (2013). *Tahrir al-Wasilah* (Vol. 1). Institute for Compilation and Publication of Imam Khomeini's Works.

Murphy, E. V. (2015). *Cryptocurrency: The Techno-Economic and Legal Framework*.

Nabavi, M. (2019). *Control of Criminal Activities Related to Virtual Currencies in Iran* Tarbiat Modares University]. Tehran.

Naderi, S., & Motalebi, M. (2021). Legal Solutions for Mining and Trading Digital and Cryptographic Currencies: Legal Gaps and Proposed Solutions. *Fars Law Research Journal*, *4*.

Nakamoto, S. (2009). *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://www.bitcoin.org

Rafiei, A. (2018). Requirements of Digital Currency in Iran's Criminal Legal System. Conference on Management and E-Business with an Approach to Resistance Economy,

Rezvani Najafabadi, H. (2018). Legal Analysis of Bitcoin. *Law Research Journal*.

Shahid Thani, Z. a.-D. i. A. (1978). *Masalik al-Afham ila Tanqih Sharayi' al-Islam* (Vol. 4). Al-Ma'arif al-Islamiyah Institute.

Shahidi, M. (2007). *Effects of Contracts and Obligations* (Third edition ed.). Majd Publications.

Toutounchian, I. (1996). *Monetary Economics and Banking*. Monetary and Banking Research Institute.