Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
Special Issue on Global Research Trends in
Multidisciplinary and Interdisciplinary Studies 7(11s)

COMPARATIVE ANALYSIS OF THE LEGAL NATURE OF BLOCKCHAIN AND SMART CONTRACTS: FROM PURE TECHNOLOGY TO LEGAL PERSONALITY

Patryk Chmielarz [1]

[1] University of the National Education Commission, Krakow, Poland

Received 13 March 2026
Accepted 06 May 2026
Published 22 May 2026

Corresponding Author
Patryk Chmielarz,
chmielarzp13@gmail.com

DOI
10.29121/shodhkosh.v7.i11s.2026.8283

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

Today, with the expansion of international trade, the infrastructures associated with this field have also experienced remarkable growth. Among these, two relatively emerging technologies—blockchain and the smart contracts formed on its basis—have emerged with the aim of accelerating, facilitating, and enhancing the security of financial and commercial transactions. Given the increasing pervasiveness of these technologies and their deep, potential impact on various aspects of human life and social relations, it is essential to clarify their legal and regulatory status across different domains. Achieving this goal, above all, requires a precise understanding of the nature of these two technologies. This is because, depending on the nature of each, different legal effects arise, and specific sets of rules come to govern them.On the other hand, it must be said that blockchain technology, for several reasons—including the fact that assets existing on this platform do not belong to the network itself—has not been able to acquire a legal nature and has in practice remained confined to its technical dimension. However, the situation is entirely different when it comes to smart contracts. Unlike blockchain, these contracts possess distinct legal attributes, including "legal personality." The reason for this lies both in their ability to operate independently of the contracting parties and in the existence of explicit legal provisions in this regard. This research attempts to provide a comprehensive analysis of the technical and legal nature of blockchain and smart contracts, while precisely explaining the legal issues surrounding blockchain and the smart contracts based on it.

Keywords: Blockchain Technology, Smart Contract, Ethereum, Technical Nature, Legal Nature, Legislation, Legal Personality

1. INTRODUCTION

Blockchain is a type of information and transaction recording system. What sets it apart from other systems is that the data stored on it is shared among all members of a network. Through the use of encryption and data distribution, the possibility of hacking, deleting, or tampering with recorded information is virtually eliminated. The concept of blockchain first emerged with the advent of Bitcoin, and the king of digital currencies used this mechanism to store user asset data. To better understand blockchain, consider the following example: In a gathering of 100 people, I hold up a sheet containing information, and everyone takes a photo of it with their mobile phones. Now, if I destroy or alter that

information, it is no longer acceptable to the group because they each have a copy of the original version—unless I take everyone's phones and delete it, which is practically impossible on a large scale.

Some regard this revolutionary technology as comparable in importance to the emergence of the internet in the twentieth century. Others, such as Don Tapscott and Alex Tapscott—renowned Canadian authors—go even further, asserting that blockchain is something beyond the arrival of the internet. They claim that with this technology, a world of accelerating breakthroughs in the methods and types of financial and non financial transactions will open up. For this reason, blockchain holds considerable significance and is worthy of research across various fields.

In essence, blockchain is a new technology that enables the permanent recording of information without any possibility of alteration. It is, in fact, a type of database or data platform that does not reside on one or more specific servers but is distributed across all computers connected to the network. Due to the use of encryption and the fact that data is recorded on every computer in the network, the stored records cannot be hacked or deleted. As mentioned, Bitcoin was the first application of this technology; however, this revolutionary system can be used in any context where there is a need to reduce reliance on intermediaries and trusted third parties.

The law of contracts is regarded as one of the most dynamic areas of law, constantly influenced by new forms of technology. In Iran's legal system, a contract is defined as one or more persons undertaking an obligation toward one or more other persons, with that undertaking being accepted by them. This definition closely resembles Article 1101 of the French Civil Code, where a contract is described as a consensual agreement by which one or more persons bind themselves toward one or more others to deliver something, to do something, or to refrain from doing something.

At present, there is a lack of regulatory certainty regarding the status of smart contracts and blockchain. A smart contract is capable of executing itself independently, removing the human element from the contract performance process. From a technical perspective, if no intervention occurs to prevent the operation of a smart contract system, one can be confident in its autonomous performance or execution. However, a system that is under the control and management of one of the contracting parties is not able to resolve issues of interpretation and enforcement in an impartial manner. In short, an independent third party must interpret and enforce the contract in accordance with the intentions and objectives of the parties. This is a problem that public courts typically try to resolve. But that is not the only solution. Another solution to this problem is blockchain technology.

Therefore, it is necessary for legal scholars to promptly understand the technical and complex nature of blockchain technology in order to respond to a society that seeks to use modern technologies: What is the legal nature of blockchain technology? Is it merely a legal representative for executing given commands and instructions? Does it have a contract like nature in the form of a partnership agreement, or does it enjoy an independent legal personality? In this research, after examining blockchain and its applications such as smart contracts and cryptocurrencies, we will analyze the technical dimensions of this important subject, and then, in light of a precise structural understanding, we will proceed to analyze the nature and legal dimensions arising from that understanding.

1.1. RESEARCH QUESTIONS

Main Question

What is the legal status of blockchain technology and the smart contracts concluded on its platform?

Sub questions

What advantages does the use of blockchain technology bring to the conclusion of smart contracts?

Does concluding smart contracts on a blockchain platform mean complete protection of privacy?

1.2. HYPOTHESES

Main Hypothesis

Although blockchain, due to the predominance of its technical aspect over its legal aspect, lacks a purely legal nature and is devoid of a purely legal essence, smart contracts based on it—which, in the form of an electronic system, give rise to the concept of a "person"—nevertheless, by virtue of their self governance, full automation, and absence of intermediary interference, do possess legal personality. Consequently, one can attribute to them rights, obligations, liability, and so forth.

Sub hypotheses

1) Due to features such as decentralization and peer to peer operation, blockchain prevents monopoly, manipulation, and unequal oversight, and effectively eliminates the possibility of fraud or interference from the beginning to the end of a contract. For this reason, it is considered the best platform for smart contracts. The inherent transparency and removal of intermediaries also make processes faster and easier, thereby enhancing commercial efficiency.
2) Even if semi anonymous public addresses are used when storing contracts on a blockchain, the risk of re identification by other users does not disappear entirely. Sophisticated analyses and big data techniques enable private entities to link transactions to specific identities and gain access to individuals' financial, contractual, and confidential details. This problem worsens once data is stored on the blockchain, because there is no way to unilaterally correct or erase the information afterwards.

Figure 1

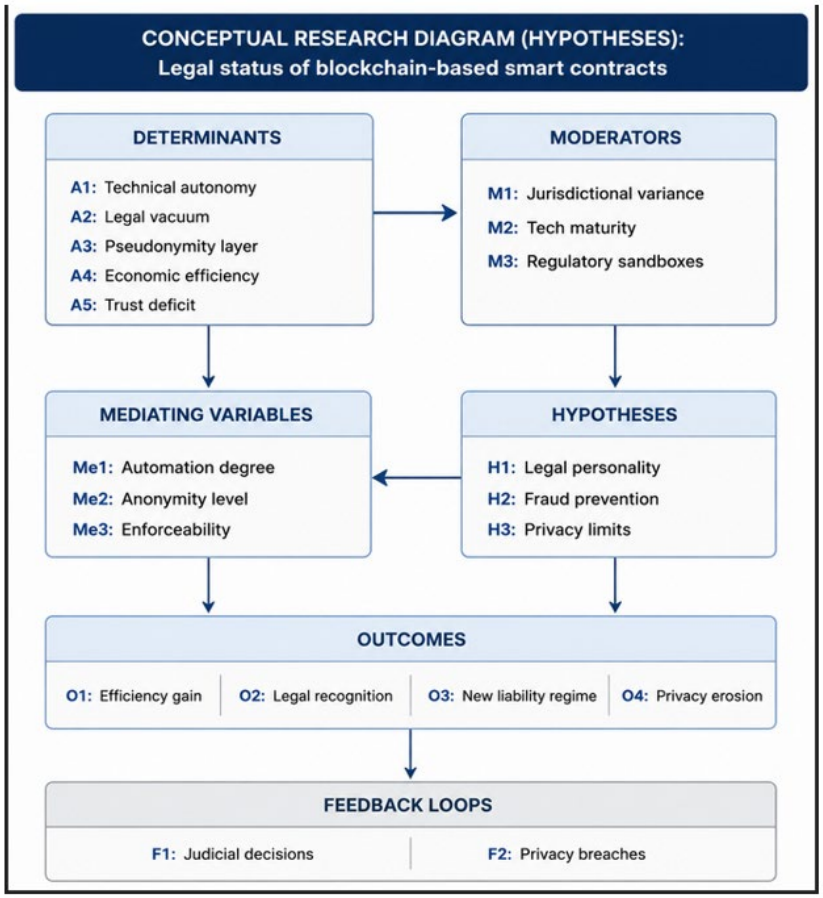

Figure 1 Conceptual Diagram of the Research

Source: Author

The present study is fundamental-applied in terms of its objective. This means that while striving to expand the theoretical foundations concerning the legal nature of blockchain and smart contracts, its findings are also applicable to the process of legislation and regulation. In terms of nature and method, this research falls within the category of qualitative studies and has been conducted using a descriptive analytical and comparative approach.

Data collection was carried out through library and documentary methods. All sources used include books, Persian and English scientific articles, domestic laws, international conventions (including the UNCITRAL Convention on Electronic Commerce), and reputable technical and legal reports (such as reports from the Development Research Center of the Plan and Budget Organization and white papers by Norton Rose Fulbright). To search for sources, keywords such

as "blockchain," "smart contract," "legal personality," "Ethereum," and "technology legislation" were used in scientific databases (Google Scholar, IEEE, SSRN).

The analytical tool in this research is interpretive legal reasoning and comparison of legal systems (particularly France and international instruments). The author first explains the technical aspects of blockchain and smart contracts in detail (using conceptual diagrams and educational analogies), and then analyzes their legal nature based on traditional concepts of contract law (such as elements of a contract, capacity, consent, sanctions) as well as the principles governing electronic commerce.

2. LITERATURE REVIEW AND BACKGROUND

2.1. BLOCKCHAIN

In 1998, Timothy May, one of the founders of the "Cypherpunk" movement, warned of "a monster entering the world, spreading terror and horror in the modern world." This monster is neither political terrorism, nor ethnic conflicts, nor environmental crises. Rather, it is the growth and expansion of a new form of chaos, which May called "cypherpunk chaos." As May explained in his work entitled "The Cyphernomicon," it will not be long before the internet and advances in public private key cryptography enable individuals to interact and communicate with one another anonymously. (Chohn, West, & Parker, 2017)

Cryptographic security protocols render "wiretapping" obsolete—the kind of wiretapping built upon intellectual property and the private, artistic, literary sphere. The free flow of information emerges, and individuals, especially merchants, become acquainted with new capacities for self organization through positive points that accelerate and facilitate the conduct of trade. All aspects of commercial companies and governments change. From May's perspective, what is absolutely inevitable is expansion and progress. As he later explained in his writings: "The genie is out of the bottle," and nothing can stop the ominous wave of technological chaos that leads to legal and regulatory chaos in determining responsibilities and jurisdictions.

The most important blockchain in the world today is Bitcoin's blockchain. This blockchain is responsible for coding data that, as of August 28, 2016, represented an asset value of over 9 billion dollars. What distinguishes and gives superiority to Bitcoin's blockchain is that the verification of information is based on a set of rules, relying on a decentralized network. Each blockchain update is performed by a hash, which gives the network the ability to track and detect any attempt at altering the record. (Clack et al., 2016)

In other words, blockchain is a "chain of blocks," where each block contains a continuously growing list of transactions. These blocks are cryptographically linked to one another in a chain, which is why it is called a "blockchain." Once transactions are confirmed and deemed trustworthy, the blockchain can operate without any central authority, and the possibility of changing the data after it has been uploaded to this platform becomes virtually impossible.

Blockchain is a decentralized, distributed ledger that digitally records the history of all transactions. This technology operates through computers and servers called "nodes," managed in a peer to peer manner without needing approval or authorization from intermediaries or third parties. All data attached to this technology is shared among all members across the entire network. The data is verified and confirmed by anyone possessing the necessary permissions, based on the consensus protocols of the blockchain. The fundamental difference between blockchain as a decentralized, distributed ledger and a wiki lies precisely here: there is no single point of decision making or executive authority in a hierarchy, and the participation of all members is required at every necessary stage.

Figure 2

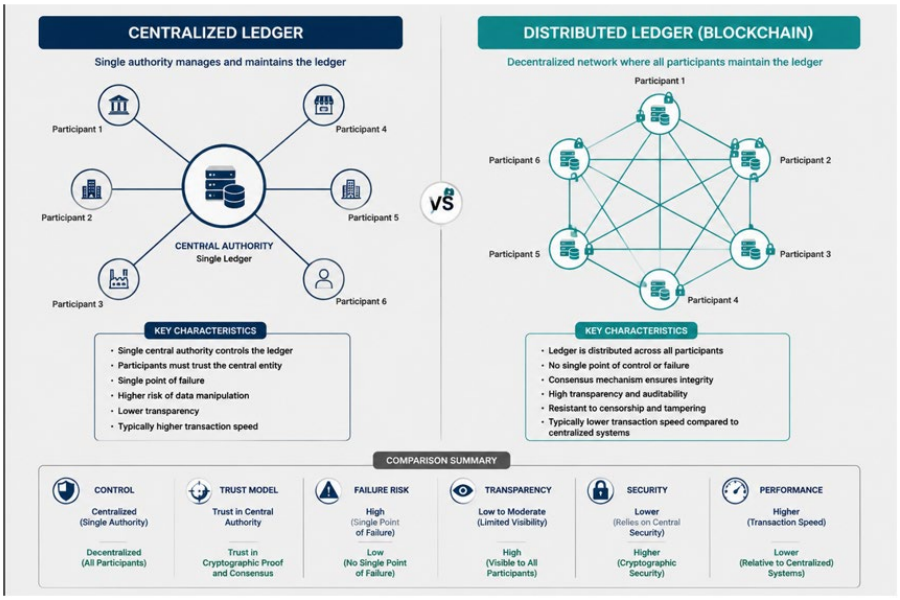

Figure 2 Distributed Ledger Versus Centralized Ledger

Source: Author

After each transaction is verified and confirmed, it is stored in blocks. All blocks are cryptographically linked to one another in chronological order. It is precisely this temporal transparency and encryption that makes any modification or amendment of blockchain records practically impossible. The important point is that this technology has no error correction system. Therefore, if incorrect information (whether intentional or accidental) enters this ledger, it cannot be altered; instead, a corrected version is uploaded afterward.

Figure 3

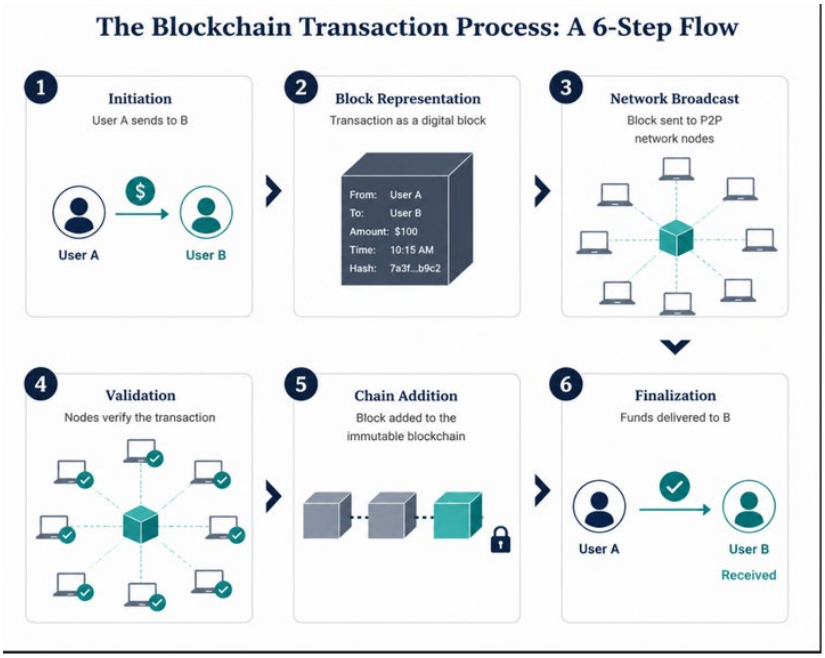

Figure 3 Blockchain in Simple Language

Source: Author

2.1.1. TYPES OF BLOCKCHAIN

One common classification of blockchain is the division into permissionless and permissioned platforms. In permissionless platforms, the level of access is unrestricted and everyone can access them—for example, the Bitcoin platform. In contrast, access in permissioned platforms is limited to those who hold authorisation. Often, we see a combination of these two categories, and it is common for public blockchains to be combined with permissionless ones. In international trade, many blockchain based programmes have been developed within the category of permissioned, consortium oriented blockchains. (Demeyer, 2018)

1) Public Blockchain

In a public platform, not only is there no possibility of management by any specific person or group, and all transactions are public while the anonymity of network participants is largely preserved, but also the possibility of decision making or rule setting by any member is completely absent. A public, permissionless blockchain is essentially the same programme that blockchain technology originally designed for Bitcoin, and this type constitutes the foundation upon which blockchain emerged. Therefore, cryptocurrencies and Bitcoin are the most obvious and earliest examples of public, permissionless blockchains.

2) Private Blockchain

In this type of blockchain, transaction validation is carried out according to that blockchain's rules by a limited number of nodes, resulting in higher speed and efficiency compared to public blockchains. In this type of blockchain—quite contrary to the permissionless nature of public blockchains—rules are laid down for use and benefit. Those rules specify who has the right to enter the blockchain and who may play a role in its development and operation. This type of blockchain is not decentralised and has a hierarchy of control. However, such blockchains are still distributed, and each node operating within them holds a copy on its own device. (Feizi Chekab, 2004)

3) Consortium Blockchain

The term "consortium blockchain" refers to a type of blockchain that has a charter or, in other words, a governing contract. This contract goes beyond stating general principles and encompasses legal dimensions as well, and is fully enforceable. This charter is most often seen in smart contracts. In reality, it is an agreement to clarify the points that are left unspecified in the blockchain. In that charter, the parties to the contract—in a traditional, not smart, manner—set out the legally enforceable principles and items that cannot be included in a smart contract, such as the identities of the parties, the consideration of the transaction, and the governing law. It also directs the parties, in the event of a dispute, to follow a single mechanism such as arbitration or a competent court. (Feizi Chekab, 2004)

2.2. FEATURES OF BLOCKCHAIN AND THE CHALLENGES IT FACES

2.2.1 DECENTRALISATION AND PEER TO PEER OPERATION

As explained earlier, blockchain is a decentralised ledger. What is meant by this feature is the absence of monopoly and managerial independence in dominating or controlling the information recorded on this technology. For example, one might refer to the central bank's separate ledger for recording its own credit and debt accounts with other banks; that ledger is centralised because all transactions are entered into the ledger by an employee or software under the central bank's control and domination. It is therefore monopolistic, and the member banks of the banking system have no choice but to trust the central bank for accurate recording of ledgers; they determine their position solely based on that. In contrast to the central bank's ledger, on the Bitcoin blockchain we see a decentralised ledger where all participating individuals, by connecting their computer systems to the network, can be aware of and participate in the entire process of validating and storing transaction information.

The fundamental and ultimate goal of any blockchain is to implement the protocol agreed upon by the network, through which confidence is achieved that only information that the nodes connected to the network have reached consensus on will be stored on the blockchain. In other words, a group of nodes using common software must reach agreement on whether a change should be made to the information recorded on the blockchain, and if so, what change should be made. By applying this concept to Bitcoin transactions, the Bitcoin ledger records all transfers of Bitcoin from one person to another. Blocks are a simple way to group transactions into larger groups and sequences for processing purposes. (Honarmand, 2011)

2.2.2. MODIFICATION AND CENSORSHIP; TRANSPARENCY

If a computer on the network holds a complete copy of the blockchain, the blockchain will remain in place for use and access. As long as an internet connection is established, the blockchain can be replicated and the network restored—even if internet connectivity in one part of the world faces problems due to government actions or natural disasters. The rest of the network will support the blockchain, and the ability to retrieve new information and access previous data will remain intact. Then, as soon as internet connection is restored, the groups in the former geographical areas can update their personal copy of the blockchain and continue their participation in the network, picking up where others left off. (Kissinger, 2019)

Because blockchain relies on peer to peer networks and digital signatures, the data stored on it is transparent and immutable. The information kept on a blockchain is robust, and metadata and other contextual information about blockchain transactions are exposed to public view. Therefore, anyone who can download a blockchain and assess a specific account in a transaction (just like on Ethereum), and determine whether that account is interacting with a smart contract or not, can perform this process.

2.2.3. CONSENSUS AND AUTONOMY

Another feature of blockchains is their ability to coordinate social activities and help individuals reach consensus about the status of particular matters. The infrastructure of every blockchain network is a consensus mechanism that oversees how information is added to the shared repository. The consensus mechanism makes it possible to record information on the blockchain in an orderly manner, without the need for intermediaries or centralised groups, on distributed peer to peer networks. Since data recorded on the blockchain is visible to everyone and difficult to alter or amend, groups that do not know each other and therefore do not trust one another can rely on this data structure to coordinate their activities, with very little need for trusted institutions.

One of the most important advantages of these autonomous systems is that, if properly designed, they can carry out initial economic transactions at a lower cost and with much higher reliability and speed. Such blockchain systems can reduce or even eliminate the need for human intervention and minimise the ability of groups to act opportunistically in ways that benefit only a few.

2.3. CHALLENGES

2.3.2. SCALABILITY AND SECURITY

For blockchain to achieve widespread acceptance, these emerging technologies must be able to manage an immense number of transactions. The speed and accuracy of these networks must grow at the same rate as public and private institutions, so that this technology can be used to develop new software and innovative business models.

Because blockchain is still novel in nature, governments seek to harness the power to shape this technology by enacting laws and regulations that either restrict or promote its growth and acceptance. Regulations can hinder blockchain development by making the use of cryptocurrencies expensive or difficult, or by imposing requirements on the deployment of autonomous smart contract code on blockchains. (Norton Rose Fulbright, 2016a)

Governments always try to gain the ability and power to shape this technology in the right directions by enacting laws and regulations that either cause restriction or promote technological growth and adoption. Such regulations can hinder blockchain development by making the use of cryptocurrencies expensive or difficult, or by imposing requirements on the deployment of autonomous smart contract code. Conversely, governments can adopt specific regulatory frameworks to protect businesses that regard blockchain as part of their professional and innovative policies.

2.3.3. TURNING THREAT INTO OPPORTUNITY

All challenges concerning the survival of this technology stem from blockchain's dual nature. This technology can be used for harmful purposes, bringing potential evils into actuality and endangering political, registration, and other matters; but it can also be used positively, advancing many legal, financial, and commercial matters at the lowest cost and in the fastest manner. It can also steer the technology—which from some perspectives appears threatening due to

legal chaos and legal ambiguities—onto a desirable path of opportunity creation, and examine its positive benefits. Blockchain systems can support new protocols and applications that are separate and remote from the control of government and corporate institutions. They rely on cryptographic rules for transferring flows of media, communications, and information from centralised groups to large scale autonomous systems. These systems may offer strong guarantees for freedom of expression and ultimately lead to the emergence of a community that can flow freely from one side of the planet to the other.

2.4. LEGAL IMPLICATIONS OF BLOCKCHAIN TECHNOLOGY

The emergence of cryptographic laws and blockchain technology presents a new set of challenges for legislators. Because blockchain facilitates code centric systems that are decentralised, disintermediated, resistant to change, recursive, and potentially autonomous, questions arise as to whether the four forces of legislation that Lessig referred to still operate in the blockchain context. In fact, given the autonomous nature of some of these systems, the "recalcitrant nature" of the subject matter of legislation is gradually being eliminated, and it must merely be replaced by autonomous, code centric systems that operate independently of any natural or legal person. (Norton Rose Fulbright, 2016b)

2.4.1. MARKET REGULATION

By inference, for an autonomous system on a blockchain to function, the relevant smart contracts must receive sufficient digital currency to cover their costs. With the transaction fees claimed on a blockchain, every interaction with the blockchain ultimately becomes an economic transaction, and every participating group operates as an economic agent. Consequently, the cost of blockchain operations affects the behaviour of participants, including miners, software developers who use smart contracts, and end users.

Governments can also influence the execution cost of transactions by manipulating the value of a blockchain's digital currency on secondary markets. While a government does not have the power to enter into monetary policies with a blockchain (for example, by injecting more currency into the system to cause inflation), it can intervene in a free market by buying or selling that blockchain's digital currency with the intention of increasing or decreasing its price.

In addition to regulation, governments can also seek to maintain order within the blockchain environment. This can be done by shaping the social norms that become established in the blockchain community. Since blockchain is ultimately run by people, social norms also have the capacity to turn into powerful legislative tools.

Blockchain relies on distributed understanding for its continued operation. Therefore, miners and other supporting groups of these decentralised data structures can be assured of the application of legal or social rules. On one hand, miners and other transaction processors act as judges and have the power to allocate the laws or values of the blockchain network. Network nodes can take action to stop illegal activities when a sufficient number of them agree on a course of action. Such groups can collectively decide to intervene in the process by making necessary changes to the protocol to remedy a harm, thereby reversing or censoring specific transactions or stopping autonomous code.

Because blockchain relies on code to define its operations, governments can decide to enact laws regarding how blockchain software and smart contracts are created, thereby influencing how these systems are used and developed. For example, new laws could compel software developers to introduce certain features directly into the core protocol of the blockchain—such as giving governments the ability to disable autonomous smart contracts or suspend blockchain based application software that violates the law.

Even if governments want blockchain developers to incorporate specific features into their code, they cannot force users or other private actors to adopt those features outside the governments' jurisdictional boundaries. If government restrictions are harsh, ineffective, or unfair, the miners who support the network may disregard those provisions, refrain from installing software that embeds such laws, or refuse to process transactions or smart contract code that has been forced to comply with those laws. As governments impose restrictions or responsibilities on software developers, the complexity of the legislative approach increases, and governments must be able to identify the creators of blockchain software and smart contracts—a task that may be possible, but is often challenging due to the semi anonymous nature of blockchain.

2.4.2. THE APPROACH OF RELYING ON OTHER LEVERS OF LEGISLATION

Governments can also rely on other levers of legislation, such as social norms or the market, to regulate a specific blockchain network or application software. By influencing the market dynamics of a blockchain network, governments gain the power to transform the natural balance and alter the prevailing practices within the community of actors on that network. Although this may weaken innovation and control technological development, governments can also act as a tool to influence network practices, forcing them to pursue certain political objectives.

Of course, if processing transactions on a blockchain network becomes expensive or inefficient, alternative blockchains may emerge that are not subject to government interference. These new networks will likely rely on different mining algorithms and require different hardware, thus reducing the impact of such regulations. As is often seen in legislation, all regulatory approaches have shortcomings.

2.4.3. BLOCKCHAIN: VIOLATOR OR PROTECTOR OF FINANCIAL AND COMMERCIAL PRIVACY?

When the internet was first introduced, some described it as an unlawful space—a new, borderless world. Yet that perspective proved illusory, if only because of the traceability of IP addresses. As internet acceptance grew, China erected its "Great Firewall," removing content it deemed disruptive to its social system and eliminating material that conflicted with good morals and fundamental norms and that was considered a threat to public order. This firewall, which targeted the IP addresses of websites and other online services, operated under standards set by government censors, thereby limiting the information that Chinese citizens could access. (Norton Rose Fulbright, 2016b)

2.5. SMART CONTRACTS

Smart contracts refer to self executing electronic protocols that are pre written into computer code. The advantage is that the contract becomes machine readable, and in most cases, this enhances the intelligence of the contract in terms of executing the protocol. It was Nick Szabo who first introduced the concept of smart contracts in the mid 1990s. Such contracts have existed for decades, like the transaction processing systems that systematically and accurately perform daily payments and receipts for financial institutions. However, with the advent of Bitcoin and its specific platform—blockchain technology—this concept gained new dimensions in terms of communications and capabilities.

This technology provides a secure and precise platform for these contracts to achieve the utmost possible benefits. A smart contract is designed such that it executes the terms of the contract automatically when the predetermined conditions, specified in defined frameworks, are met. The parties sign it using cryptographic security and deploy it on the distributed ledger—the blockchain. (Norton Rose Fulbright, 2018)

Before smart contracts were invented in their current form, the concept of automation (self operation) has existed since ancient times, and this idea is not new. Automation is not merely a product of human design but also of human action. This means that in the course of economic, social, and daily interactions, the parties—out of a desire to reduce costs—unconsciously move toward automation, independent of academic inventions and recommendations. The earliest reference to an automated vending machine was made by the Greek mathematician Hero in his book Pneumatica in 215 BC.

2.5.1. CONDITIONS OF A SMART CONTRACT

Nick Szabo, a computer scientist, first used the term "smart contract" in a 1995 article entitled "Smart Contracts: Basic Components of Digital Markets." Szabo defined traditional contracts as a set of promised and agreed upon undertakings, a conventional way to formalise a relationship. He considered a smart contract to be a set of digitally expressed promises, including protocols within which the parties perform their obligations contingent upon the other party's performance. (Raskin, 2017)

According to Szabo's definition, the main elements of a smart contract are as follows:

1) **A set of undertakings:** This set of undertakings will vary depending on each smart contract's model. The terms of the contract, or their functional equivalents, are encoded in the software according to the appropriate business logic.

2) **Digital form:** It is a set of code and software that determines the terms and effects of the contract.
3) **Protocols:** Actions such as authorising payments and conditional actions are made possible through a series of rule based operations, all of which are embedded in a specific algorithm consisting of the set of rules and procedures necessary for data processing. The creation of this algorithm is the responsibility of computer protocols.
4) **Conditionality of each party's performance on the other's performance:** Automatic operation, self execution, and full automation are among the most fundamental features of smart contracts—a certainty and necessity that blockchain technology, as a platform, bestows upon such contracts. Usually, there is no possibility of stopping the outcome for which the smart contract was coded, unless the execution process depends on information that has not been fulfilled.

2.5.2. TYPES OF SMART CONTRACTS

Artificial intelligence is one of the fields that emerged after the Second World War. The term was first introduced by John McCarthy in 1965 as "the processing of making intelligent." In his view, artificial intelligence was a specific field of engineering for building intelligent machines. (Savarayi, n.d.) The reason for naming this science "artificial intelligence" refers to its goal, namely to create an intelligent being that has the ability to replicate proven human capabilities such as reasoning and learning. Kurzweil defines artificial intelligence as "the art of creating machines and programmes that can perform tasks that would require high intelligence if done by humans."

It was Nick Szabo who first described the dimensions of smart contracts, citing the automatic vending machine and the device installed on a sold car (to repossess the vehicle title in case of the debtor's non payment) as two early examples of smart contracts.

With regard to the subject of this research, contracts concluded by intelligent computer systems can be divided into two types. The first type consists of contracts where only the formation stage relies on an intelligent computer system on one side or on the interaction of intelligent systems on both sides. The second type consists of contracts where, in addition to the formation stage, the execution stage also relies on an intelligent system on one or both sides. As noted earlier, smart contracts are contracts that execute their terms automatically. Therefore, the first type cannot be classified under the concept of smart contracts, but the second type—due to its self executing capability and the consistent application of that capability—is always regarded as a form of smart contract.

Figure 4

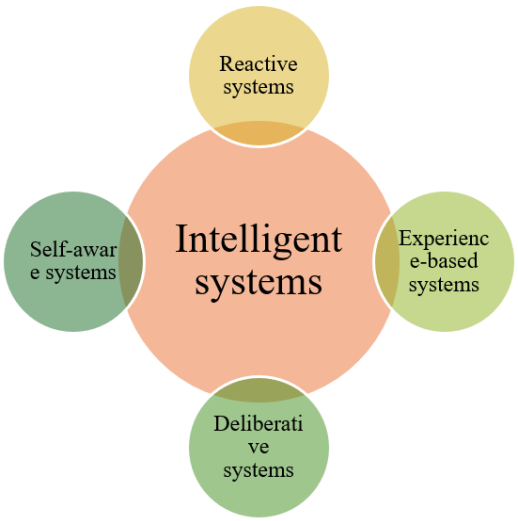

Figure 4 Intelligent Computer Systems (Szabo, 2024)

2.6. THE EXECUTION PROCESS AND DECENTRALISED OPERATION OF A SMART CONTRACT

The operation of a smart contract on a blockchain platform is as follows:

1) Identification of agreement

This stage consists of identifying the context for cooperation and its desired outcomes. The subject of negotiation and ultimately the parties' agreement can cover any of the processes for transferring tangible or intangible assets, as well as all relevant business activities.

2) Setting the conditions

From a technical perspective, if a condition can be defined quantitatively and qualitatively, it can be programmed into a computer system. (Azizi, 2018) The execution of all or part of the stipulated conditions can be made contingent upon the will of the contracting parties, the occurrence of specific circumstances, particular geographical situations, and so on. When someone wishes to participate in a smart contract on a public blockchain, they must:

- Download the software from public sources.
- A public key (a string of letters and numbers uniquely allocated to the person by the software) is assigned by the software as the participant's address across the network.
- Simultaneously with the public key, a corresponding private key is also generated for the participant's address.

3) Programming the business logic

The fundamental logic of smart contract coding is "if this happens, then that action is taken." A computer program can be written so that, when the conditional parameters are met, it executes automatically. To achieve this automatic execution, offer and acceptance can be coded within the business logic framework, so that when the conditions are satisfied, the transaction becomes unavoidable for the computer.

4) Encryption and blockchain

It is the blockchain that, at this stage, controls and directs the execution of the coded agreement. For the blockchain to exercise this control and direction, the contractual terms of the parties must be recorded on the blockchain. First, depending on the nature and subject matter of the agreement, it must be determined which type of blockchain (public or private) is compatible with the contract's execution process. After selecting the appropriate blockchain, the objectives and functionality of the blockchain are defined through a specific protocol. A protocol is a set of procedures that guide the nodes in performing the terms and obligations. (Vasali, 2016)

5) Execution and processing

After the smart contract is uploaded to the blockchain network, the time comes to execute its code. To do this, one of the participants must send an offer to a specific person or group of persons on the network. If that offer is accompanied by acceptance from one of the network participants, the nodes, following the protocol, verify the validity of the contracting parties and the agreement between them is recorded in a new block by the existing nodes. Once the transaction is confirmed, the blockchain issues the execution order to the "smart executor."

2.6.1. ADVANTAGES

1) **Increased speed:** One of the most fundamental principles in commerce is speed, because the higher the speed of transactions, the greater the profit for the merchant—there is a direct relationship between the two. Smart contracts, on the one hand, eliminate the need for physical presence at a location (in smart contracts, the parties need not be physically present) and, on the other hand, enable instant communication, resulting in a dramatic increase in communication speed. (Clack et al., 2016)
2) **Facilitating contract formation:** Facilitating communications in general, and contract formation in particular, is one of the fruits of the digital environment. On the one hand, the parties are not required to be physically present for transactions, and on the other hand, the process of drafting the contract is accelerated, thereby making contract formation easier.
3) **Decentralisation and transparency of information:** Smart contracts, while providing universal access to the technology, have significantly reduced many of the limitations on information exchange.

Regulation

Since 2017, following extreme fluctuations in the price of Bitcoin on global markets, the United Nations Commission on International Trade Law (UNCITRAL) moved to adopt a convention on the harmonisation of transactions based on virtual currencies in July of that year. According to Article 2 of this convention, the allocation of encrypted currencies to

individuals is conditional upon the identification of their identity, assets, and legal and factual status. Applicants must submit documents to the competent authorities demonstrating their legal status, insolvency, and all their legal and criminal records. (Wang, 2019)

2.7. CONCEPTUAL ANALYSIS

2.7.1. PRIMARY NATURE

The question is whether the burden of smart technology on something like a contract overshadows its original and primary nature, transforming it from a mere contract into something beyond its inherent character. A contract is a set of enforceable legal statements. For a contract to be considered legally enforceable, it must possess a number of conditions imposed by the legal system. These conditions are: the parties to the contract, (Honarmand, 2011) the capacity of the parties, mutual consent, and enforceability. Additionally, the absence of obstacles such as mistake, fraud, duress, coercion, and conflict with public order are also regarded as fundamental conditions for contract execution. A contract may be written or oral; important contracts must be concluded in writing. Most business related contracts, whether in the form of a traditional written document or in electronic form such as electronic terms, are concluded in writing.

Courts generally consider proof of "actual knowledge" of the contractual terms to be necessary. Without actual knowledge of the terms (i.e., acceptance by the user, a written notice regarding conditions that, if breached, the user acknowledges having been informed of before proceeding on the website), the user must be placed in a position to search for and become aware of those terms. This normally requires that the terms be made conspicuous and that serious attention be given to the fact that continued use of the website binds the user to those terms. Recently, the US Court of Appeals for the District of Columbia Circuit stated that mere appearance of terms is not sufficient to establish mutual assent. (Wrede, 2018)

The aim is for the Uniform Electronic Transactions Act (UETA) to govern all electronic records and signatures that are not subject to the provisions of Articles 2 and 2(a) of the Uniform Commercial Code – Sales. It also applies when all parties to a transaction agree to proceed electronically.

Given the application of legal principles relating to electronic transactions, it seems quite clear that smart contracts do not require a special set of laws or new regulations. Instead, existing legal principles will be adapted and possibly amended through legislation or judicial rulings to respond precisely and deeply to the legal needs of such contracts. Of course, there will certainly be a significant delay between the adoption of the technology and the amendment of the law.

2.7.2. SECONDARY NATURE

According to this theory, a blockchain based smart contract is merely an instrument for execution. It plays only the role of a telephone or a messenger in transmitting intent and directing matters based on the primary intent to contract. In fact, every action, conduct, and reaction emanating from this intelligent agent originates from a human managerial background. Such contracts are merely minor players in the overall scenario. Where the execution requires the formation of subsidiary contracts to perform the main contract, they are nothing more than a means of declaring the user's intent, and they have no independent initiative or freedom of will compared to the human agent who concluded the principal, master contract. (Norton Rose Fulbright, 2016b)

Although in French law the "subjective" theory of intent has traditionally been accepted and the actual intention of the parties is of serious and fundamental importance in contract formation, French jurists have gradually inclined toward the "objective" theory of intent. From this perspective, the use of blockchain based smart contracts can reflect the user's intent in concluding an intermediate contract during the execution process. In French law, it has also gained acceptance that electronic agents lack independent intent and personality, and are therefore regarded merely as tools to assist in the formation and execution of ancillary smart contracts. (Yu, 2018)

Smart contracts are indeed examples of increasingly intelligent automated systems. By employing artificial intelligence and blockchain technologies, they demonstrate how technological progress can be used to secure global transactions. For example, a person can authorise software controlled by blockchain based smart contracts to sell a specified number of shares in Company X at a predetermined price.

If blockchain enables smart contracts and the robots based on them to operate with complete freedom from centralised control, new challenges arise regarding how to regulate them and allocate responsibility for these devices.

Currently, the approaches considered for regulating autonomous systems and devices are rooted fundamentally in institutional legal thinking. Institutions presuppose that these contracts and software/hardware devices act as tools for third party operators who have the power to control these systems to modify risks (both physical and economic) and may generate the next generation. As David Vladeck, former Director of the Bureau of Consumer Protection at the US Federal Trade Commission, says: "Where human intervention in machine decision making is very clear, there is no need to reconsider liability rules." (Demeyer, 2018)

Any person (or company) that has played a role in developing a contract or its executing machine, and has contributed to its decision making, is potentially liable for its wrongful acts—whether intentional or negligent. If smart contracts and their based devices become increasingly independent of third party operators, new ethical, legal, and juridical questions arise: should the owners and creators of those devices be responsible for their actions or not? If they are not qualified as electronic representatives with the authority to validate capacity—since they operate independently of any centralised control—can they enter into credible commercial transactions, and to what extent? If an autonomous smart contract does not act as an agent for a person or a third party, who is responsible for the harm it causes to humans or machines? And if the actions of this smart contract are too unpredictable, who should be liable for its crimes?

According to statistics from the US Department of Defense, with the deployment of killer robots and other autonomous weapons systems and self operating smart contracts, similar questions have arisen in this field: whether, once activated, they can select targets without requiring human operator intervention. Several organisations support the prohibition of autonomous devices that can choose and strike targets on their own. These include the Campaign to Stop Killer Robots, launched in April 2013, which has garnered support from organisations worldwide.

If society does not succeed in banning such robots and smart contracts, laws might confer "legal personhood" on autonomous devices or machines—i.e., enact rules for them just as for humans. As can be seen explicitly in paragraph (m) of Article 2 of Iran's Electronic Commerce Law. Consequently, they would be granted the capacity to acquire specific rights and obligations enforceable under the law. Such an approach was proposed by Lawrence Solum in 1991, and in 2017 the European Parliament's Committee on Legal Affairs proposed a new regulatory framework to control and assign responsibilities for smart contracts based on artificial intelligence. The proposed framework includes the introduction of an "electronic personality" for autonomous devices, enabling them to participate in legal proceedings, whether as plaintiffs or defendants.

This is largely analogous to the way laws have historically assumed legal and juridical personality. However, even if autonomous blockchain based smart contracts were to possess legal personality, cryptographic laws would bring about new consequences that do not exist in the context of centralised, controlled machines and smart contracts. For example, if an autonomous smart contract is held responsible for causing harm to a third party—whether contractual harm or physical damage—a court might not have the necessary and appropriate power to compel it to pay damages. As long as that autonomous smart contract relies solely on code, it is the code that can control access to the contract's financial resources and the devices dependent on it, unless other relevant functions have also been defined in the smart contract's code to facilitate payment upon a court order. In reality, no one has the authority to seize or confiscate the assets of such contracts and the machines based on them.

Table 1

Table 1 Research Findings

Topic	Main Finding	Documentation / Reasons	Legal Consequence
Legal nature of blockchain	Blockchain lacks legal personality and is purely technical in nature.	Assets on the blockchain do not belong to the network itself; predominance of technical aspect over legal aspect; focus on consensus protocols and decentralised data storage.	Blockchain cannot be made a party to an obligation or contract; applicable laws mainly concern technical and security aspects.
Legal nature of smart contract	A smart contract possesses independent legal personality.	Self-execution (automatic performance), fully automated operation, no need for human intermediary in execution, independence from the contracting parties.	A smart contract can be attributed rights, obligations, and liability; it can sue or be sued.
Suitable platform for smart contract	Blockchain (especially public and permissionless) is the best platform for concluding and executing smart contracts.	Decentralised, peer-to-peer features, inherent transparency, removal of intermediaries, prevention of monopoly	Increased commercial efficiency, reduced execution costs, possibility of automatic enforcement without

		and tampering, reduction of fraud from beginning to end of contract.	judicial or administrative intervention.
Privacy on blockchain	Concluding a smart contract on a blockchain does not mean complete protection of privacy.	Use of semi-anonymous public addresses; possibility of re-identifying individuals through complex data analysis (big data techniques); impossibility of unilateral correction or erasure of information after storage.	Private and governmental entities may gain access to individuals' financial, contractual, and confidential details.
Scalability and security challenges	For widespread adoption, blockchain must manage a high volume of transactions while maintaining speed and security.	Emerging nature of the technology; government intervention through restrictive or supportive regulations; making cryptocurrency use or smart contract code deployment expensive or difficult.	Need for balanced regulation that both supports innovation and ensures security and public order.
Legislative approaches	Governments can influence blockchain through three means: market regulation, reliance on legislative levers, and enacting laws governing software development.	Regulating digital currency value on secondary markets; shaping social norms in blockchain communities; requiring developers to embed specific features in the core protocol.	Possibility of controlling, restricting, or directing technological development; however, due to decentralised and semi-anonymous nature, full government oversight is difficult.
Primary nature of smart contract	In its primary nature, a smart contract is itself a "contract" and does not require entirely new laws.	Possesses traditional elements of a contract: parties, capacity, mutual consent, enforceability; can be aligned with principles of electronic transactions law.	Existing legal principles (with regulatory or judicial adjustments) can address the needs of such contracts, albeit with a time lag between technology adoption and legal reform.
Secondary nature of smart contract	A smart contract is merely an instrument for execution; will and intent belong to the human/manager behind it.	Lacks independent will and personality; every action originates from human management; its role is like that of a telephone or fax in transmitting intent.	Human actors (user, developer, operator) are liable for wrongful acts of the smart contract (whether intentional or negligent).
Possibility of granting electronic personality	In the future, autonomous smart contracts may be granted "electronic personality."	European Parliament proposal in 2017; Iran's Electronic Commerce Law (Article 2, paragraph (m)); Lawrence Solum's theory (1991).	Smart contract may participate in legal proceedings (as plaintiff or defendant); capacity to acquire rights and obligations under the law.
Tort and criminal liability challenges	If a smart contract becomes completely independent of human control, new issues arise in allocating responsibility.	Example: damage caused by an autonomous smart contract; court may lack power to compel it to pay damages (unless the contract code includes a mechanism to enforce a judgment).	Need to redefine liability rules; impossibility of seizing smart contract assets because they are purely code-based.

3. CONCLUSION

In the twenty first century, we have so far witnessed the emergence of several new, innovative, and highly influential technologies affecting all aspects of human life. Among the most important of these is the emerging technology of blockchain. Blockchain—now common in various forms such as public, private, permissioned, and permissionless—initially appeared only in a public form to complete the puzzle of the cryptocurrency Bitcoin. Over time, however, it demonstrated its power in other economic, social, and legal fields and came to be utilised. Many countries have been spending enormous sums on studying the executive infrastructures and ideation of this platform, because they have realised its power; some even consider its impact to be greater than that of the internet and describe it as revolutionary. One of the fields influenced by this technology is the operational domain of smart contracts.

Smart contracts, which represent a new and advanced form of electronic contracts, can showcase their many advantages even more brilliantly by relying on this network. It is the automatic and self executing nature of such contracts that has secured the interest of businesses in using them. By relying on blockchain technology, they provide the highest level of security in every respect—both in terms of accidental risks and intentional manipulation—for the parties involved.

Given the widespread use of these two technologies (blockchain and smart contracts), it is imperative that the legal community and legislators examine the limits and gaps in their consequences and effects as soon as possible, and set

about enacting a body of regulations before something undesirable happens. Because anything that is beneficial can also, to the same extent, be subject to abuse and unfortunate outcomes. The prerequisite for any study in this field, especially legal studies, is first to understand the nature and technical landscape of the two, then to explore their appropriate legal nature, and only thereafter to undertake legislative action. Accordingly, in this paper, after examining these two technologies and their interrelationship in achieving combined achievements, the technical and then legal nature has been analysed from the perspective of contract law and Iran's Electronic Commerce Law, and various appropriate scenarios for legislation have been presented.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

Azizi, A. (2018). Daramadi bar chalesh ha ye mogharerat gozari marbot ba fanavari ye zanjireh ye blocki [An introduction to regulatory challenges related to blockchain technology]. (Report No. 1051/11/97/1397). Markaz e Pajouhesh ha ye Tose'e va Ayandeh Negari, Sazman e Barnameh va Budjeh ye Keshvar.

Chohn, A., West, T., & Parker, C. (2017). Smart after all: Blockchain, smart contracts, parametric insurance, and smart energy grids.

Clack, C. D., Bakshi, V. A., & Braine, L. (2016). Smart contracts technology: Foundations, design landscape and research directions.

Demeyer, M. (2018). Blockchain technology and smart contracts from a financial law perspective (Master's thesis). Faculty of Law and Criminology, Ghent University.

Feizi Chekab, G. N. (2024). Zaman e voqu e aqd az tarighe vaseteh ha ye elektronik [Time of contract conclusion through electronic intermediaries]. Pajouhesh e Hoquq va Siasat, 13.

Honarmand, M. (2011). Tejarat e elektronik va qarardad ha ye elektroniki [Electronic commerce and electronic contracts]. Mahnameh ye Dadrasi, 85.

Kissinger, H. (2019). Negarani ha ye Henry Kissinger darbare ye hush e masnooei [Henry Kissinger's concerns about artificial intelligence] (M. Azami Maram, Trans.). Faslnameh ye Motarjem e Olum e Ensani, 4(10).

Norton Rose Fulbright. (2016a). Can smart contracts be legally binding contracts? An R3 and Norton Rose Fulbright white paper.

Norton Rose Fulbright. (2016b). Unlocking the blockchain: A global legal and regulatory guide.

Norton Rose Fulbright. (2018). Legal analysis of the governed blockchain.

Raskin, M. (2017). The law and legality of smart contract. Georgetown Law Technology Review, 1(2).

Savarayi, P. (n.d.). Tahlil e hoquqi e sanad e elektronik [Legal analysis of electronic document]. Majaleh ye Tahghighat e Hoquqi, 65.

Szabo, N. (2024). Smart contracts.

Vasali, N. (2006). Qarardad e elektronik va mabani ye e'tebar e an [Electronic contract and foundations of its validity]. Mahnameh ye Kanun, 66.

Wang, W. (2019). A survey on consensus mechanisms strategy management in blockchain networks. IEEE, 7.

Wrede, P. (2018). How technology can make insurance more inclusive (Fintech Note No. 2). World Bank Group.

Yu, Q. (2018). Design, implementation, and evaluation of blockchain enabled multi energy transaction system for district energy system (Master's thesis). Swiss Federal Institute of Technology (ETH) Zurich.