2528-9705

Örgütsel Davranış Araştırmaları Dergisi

Journal Of Organizational Behavior Research

Cilt / Vol.: 7, Sayı / Is.: S, Yıl/Year: 2022, Kod/ID: 22S0-785

# Examining the Relationship between the Underlying Blockchain Mechanism of Digital Currencies and Its Distribution Properties

Parmida Najmi*

graduated in  business of administration at the university of Qom for my bachelor degree

*Corresponding Author
E-mail:  parmda.najmi@gmail.com

## ABSTRACT

*After the emergence of blockchain as an independent technology applicable in various banking and financial domains, many people in different countries quickly started using blockchain as an infrastructure technology. The advanced blockchain technology provides a new data storage format in the database, and the pattern of transaction processing in this technology enables a high level of decentralization. Therefore, applying this technology in various fields provides safe, scalable, and efficient management of resources due to distributed and decentralized data control. The present research describes its unique properties, such as distribution, after a brief introduction to blockchain and its framework and components. According to the accomplished research, blockchain is a distributed ledger that uses cryptographic and algorithmic approaches to build and verify an extensive data structure. This is the first and most important difference between blockchain and distributed ledger. The blockchain data structure consists of a chain of blocks comprising transaction information recorded on a ledger. A blockchain consists of a sequence of blocks, while a distributed ledger does not necessarily require a chain or sequence.*
*Further, distributed ledgers do not require proof of work. Principally, DLT does not require a block data structure. This ledger is just a database model distributed across several places or regions. Although DLT and blockchain have many similarities, they are two different concepts.*

**Keywords:** *Blockchain, Digital Currency, Bitcoin, Ethereum, Distribution Properties.*

## 1. INTRODUCTION

Digital currencies are considered emerging phenomena of the global economy. After the emergence of blockchain or distributed ledger as an independent technology applicable in various financial and banking domains, many people in different countries quickly started using blockchain as their infrastructure technology [1].
Bitcoin is one of the digital currencies. This decentralized cryptocurrency produced by participant nodes with a determined rate in the system is a peer-to-peer network that needs no permission to allow any user to connect to the network and create a new transaction. In this network, every user can send a new transaction to validate and create a new block. SHA-2 is the algorithm used for Bitcoin encryption. Authentication is done using BitID as a decentralized authentication protocol. This protocol allows users to access the network by Bitcoin. Transactions are also carried out by the ECDSA cryptographic algorithm to ensure that authorized individuals have access to funds. Bitcoin uses digital signatures for the transactions' integrity to ensure that transactions cannot be changed after their fulfillment [2].

Blockchain is a distributed ledger used to exchange digital currencies and make transactions. Each member in the blockchain network has a copy of the most up-to-date encrypted ledger and can validate it and create a new transaction. A distributed database facilitates this scenario. This database contains a considerable number of validated growing data blocks. Completed blocks are linearly added to the ledger in terms of confirmation time. Each block has metadata, including a time tag and an address that points to the previously completed block. The blockchain database stores information on all the accomplished transactions. This database allows network users to change ledger information securely. To change the current block data, all network users apply a validation algorithm to validate it against the history existing in the ledger. If most users agree with the information, the block is approved and added to other approved blocks. Each block is identified by a phrase hashed by the SHA-256 cryptographic hash algorithm. Each block can have a parent and several children that refer to the same parent block. Therefore, they contain the same previous hash phrase. Indeed, each block has its parent's hash expression in its hash expression, and this sequence of expressions that connects individual blocks to their parent forms a large chain of blocks referring to the first block. This chain is known as blockchain [3].

## 2. Research methodology

The present study is applied research conducted as a systematic review, and the required data were collected using by library method. For better inclusion of related literature, this research was searched in valid journals by searching Persian equivalents of keywords, including "blockchain, digital currency, bitcoin, and distribution properties" on Persian databases such as Magiran, SID, and IranMedex. Further, these keywords were searched on the English language databases of Wiley, Central Biomed, PubMed Library, and Science Direct. In addition, an advanced search was done in Google Scholar in Farsi and English. The interval was considered 2016 to 2022 was considered. The research inclusion and exclusion criteria have been presented in Table 1. Searching databases revealed that the related studies had been carried out mostly in America, China, Iran, India, Russia, and England on a small scale.

The present research aims to answer this question: What is the relationship between blockchain and its distribution property, and what is the role of digital currencies? The sensitive search strategy was applied to collect all the research related to blockchain and its distribution. After selecting the databases, the strategy was applied using the selected keywords. In the first stage, the most important and relevant articles were used. The keywords were related to each other using AND to include the articles containing all the keywords.

Further, the capabilities of databases were noticed to include the search results related to the interval of 2016 to 2022. After applying these considerations, the number of found articles was reduced to an acceptable level. The search had optimal results, and those articles, sufficient information, were checked. It should be noted that most of the studies on this issue have been done since 2016 onwards and the use of the results of this research sounds necessary.

**Table 1:** inclusion and exclusion criteria of research

| Inclusion criteria | Exclusion criteria |
|---|---|
| The articles include the concepts of Blockchain, digital currency, bitcoin, and distribution properties. | The articles include the concepts of Blockchain, digital currency, and undistributed properties. |

| | |
|---|---|
| Research and review articles | |

After searching the mentioned websites and databases, 70 articles were found. By removing repetitive items and applying inclusion and exclusion criteria included in Table 1, 50 articles that were not related to "blockchain, digital currency, bitcoin, and distribution properties" and their full text were not accessible were removed. Finally, 12 and 6 articles were used as the main and secondary sources to cover the investigated subject in this research. The process of article searching and inclusion has been presented in Figure 1.

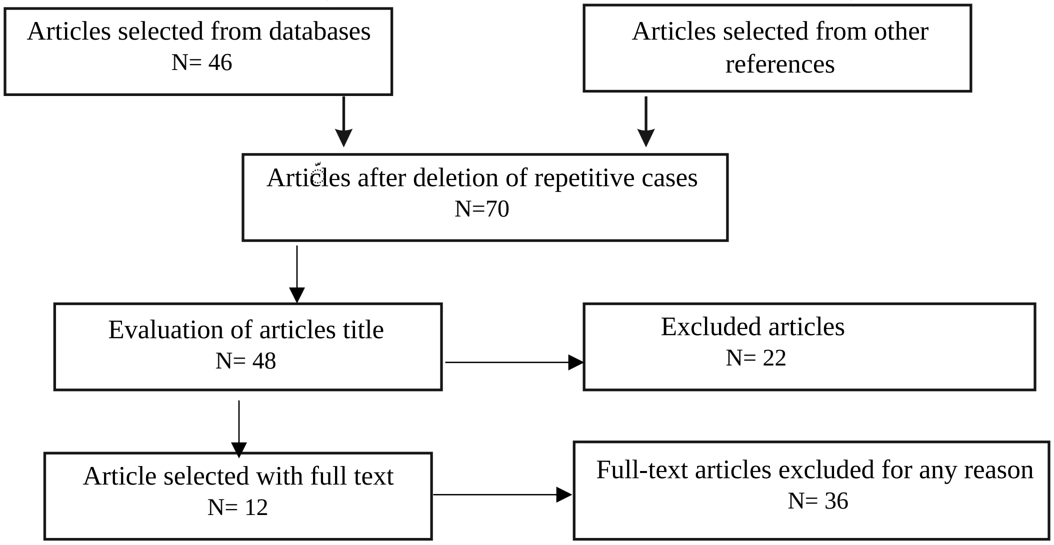
Articles selected from databases
N= 46
Articles selected from other references
Articles after deletion of repetitive cases
N=70
Evaluation of articles title
N= 48
Excluded articles
N= 22
Article selected with full text
N= 12
Full-text articles excluded for any reason
N= 36

Figure 1-1. Process of articles searching and inclusion

## 3. Blockchain and distribution properties

### 3-1. A brief introduction to Blockchain technology

Different companies attempt to make information reception easier and increase their security. New software emerges with different algorithms that do not last long and will soon be obsolete. Human beings are looking for a comprehensive, stable, and flexible system to be used in different environments with impenetrable security. Such a system can develop a great evolution in human life and affect everything from television to social networks and banking systems. Nowadays, there has been a discussion at various conferences about a new technology that has the desired properties and is applicable; A new technology called blockchain [2].

Blockchain can considerably change our world. We are all familiar with today's administrative systems. The insurance renewal process takes a whole day; we need to do much paperwork to buy a car or house, and tracing a medical record is time-consuming. Blockchain is one of the ways that facilitate the administrative system. Of course, blockchain is not only used in these systems but is widely used wherever there is a need to send or receive information. This system facilitates the process of recording and tracking the assets in a business network. Assets can include real estate, land, cars, and cash, or even intangible assets such as intellectual property, patents, copyrights, or trademark registrations. Almost any Valuable thing can be traded and traced on the blockchain since it reduces risks and costs for both sides of the transaction.

As the name suggests, Blockchain consists of blocks (blocks of information storage) and chains. Indeed, the blocks containing information are linked like an unbreakable chain, which greatly contributes to the stability and security of this system as its important feature. The more recorded information (such as transactions or transfers) in this network, the more blocks would be formed. Therefore, we are involved in a bigger system. We will perceive the development of blockchain as growing information technology.

Nevertheless, each block includes a "hash". It is a digital fingerprint or a unique identification code that makes each block unique. Each block contains its unique hash and the unique hash of the block before it. This element is the chain that links the blocks together. With the existence of the hash of the previous block, the order of the blocks is completely determined and links the blocks together like a string.

It is worth mentioning that the hash would be changed by changing the information in each block, and since the hash of each block is stored in previous blocks, they must also change, and this process must continue in the same way, which would be impossible. For this reason, any change in this system is easily revealed. This would make the blockchain network strong and immutable. This impenetrability makes currency, banking, transactions, and assets system or any other thing recorded in this system unalterable and unhackable [3].

Look at Figure 1-2. This figure represents the outline of three blocks connected in a string. If we want to change the information of block 1969, its hash will also change, and if we want to hack this field and change the amount of money transfer from 4900000 Rials to 10 million Rials, the "1969A" field will change. Accordingly, the "1970B" field must be modified as well. Along with this modification and considering the rule (change in block = change in the hash), the hash of block 1970 will automatically change, and the fields of block 1971 must also be hacked and changed. Further, the entire network blocks must be hacked and modified in the same way, which is it is impossible.

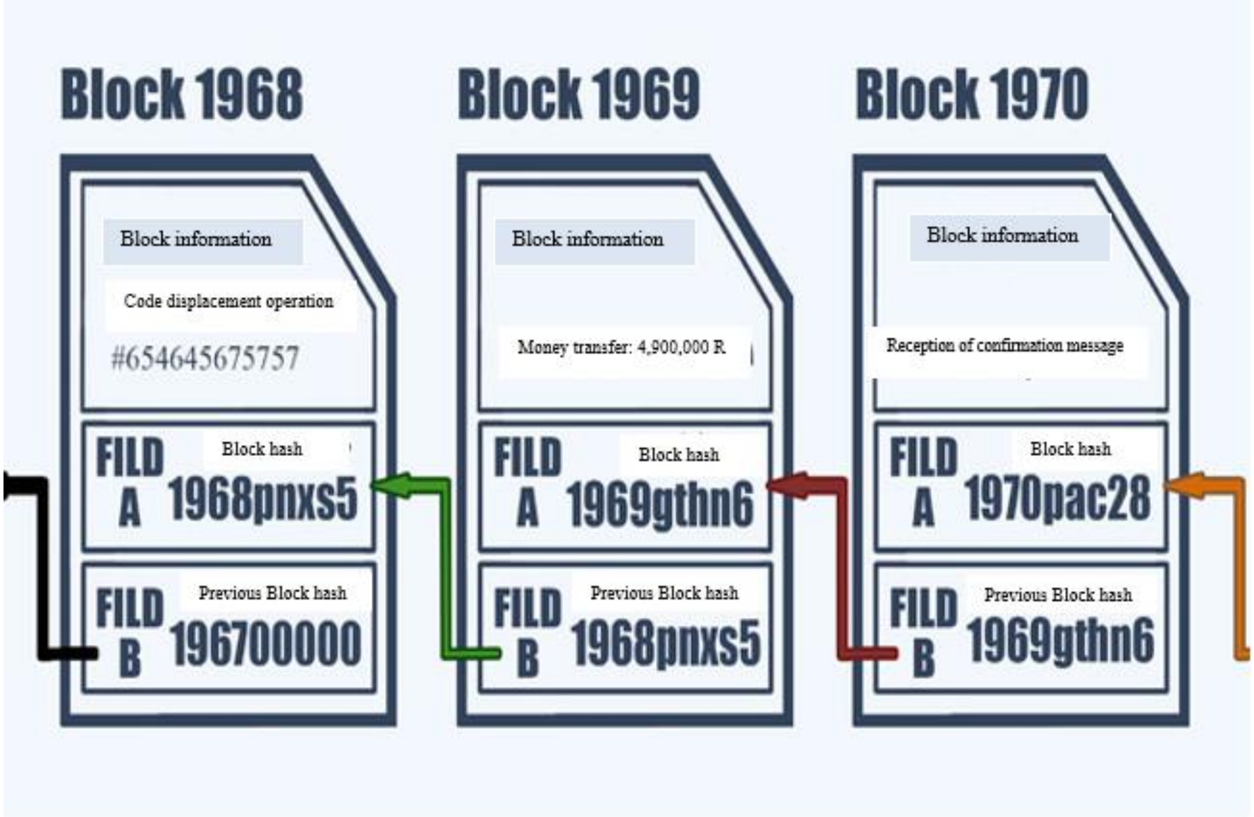

**Figure 1-2.** Blocks chain in the blockchain network

For a detailed examination of the blockchain system, it should be said that when you do an action in a blockchain system through a digital currency or a messaging app, the information of that action is stored in a block. Each block has its unique code constructed by mathematical functions. This code completely changes with a slight change in the block information. Further, each block includes the codes of the previous and next blocks. Therefore, if the information and code of a block change, all its previous and subsequent blocks must also be changed since all these blocks are linked together like a chain; therefore, it is impossible to change all the blocks of a string. Even if all the blocks of a thread change, it would only change its related thread. As it was mentioned, the information is shared between all members of the system [2].

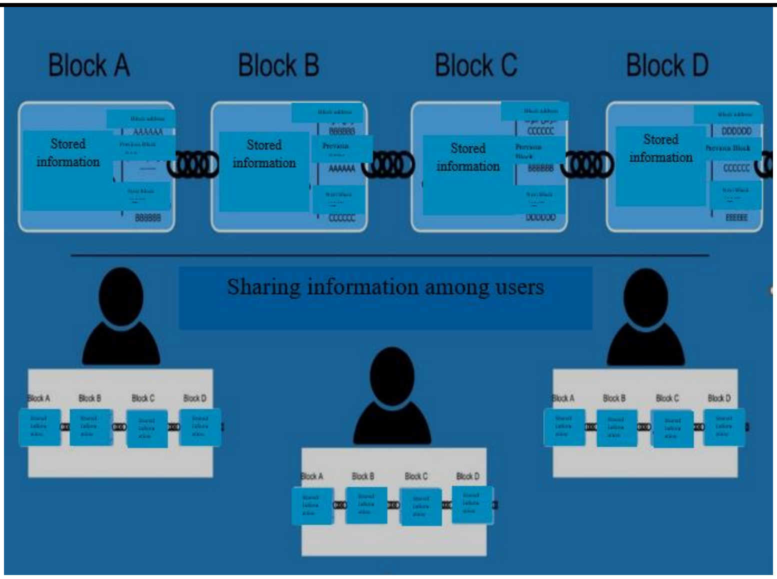

**Figure 1-3.** Sharing information among blockchain users

### 2-3. Blockchain distribution properties in digital currencies

The terms “decentralized” and “distributed” are usually used when speaking about blockchains, which are often confusing since their difference is not always obvious. For instance, the Bitcoin blockchain protocol is a decentralized system used for exchanging digital cash; but this is also a sample of distributed ledger technology. The centralized system is only controlled by an entity, such as a person or company.

There is no controlling entity in the decentralized systems. Instead, the control operation is divided between several independent entities; No entity controls the blockchain; rather, a network of nodes decides to add a transaction to the chain by consensus. The distributed concept refers to the difference in locations [4].

In a non-distributed (shared) system, all the components are located in the same physical location despite the distributed systems. In the blockchain, as a distributed system, the network nodes belong to different locations around the world.

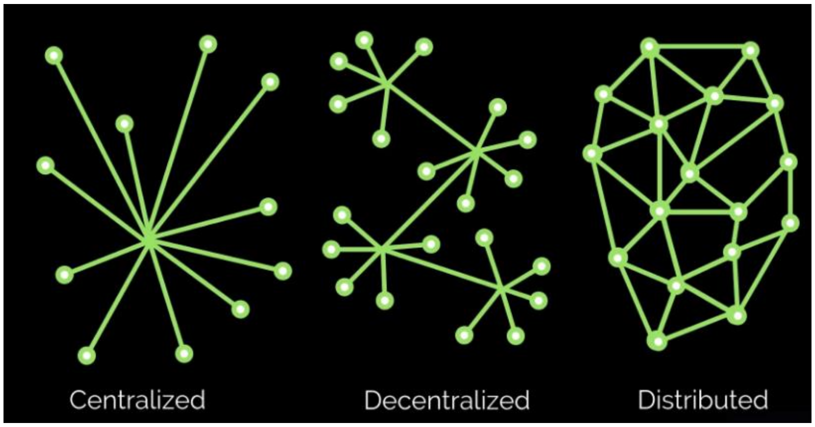

**Figure 1-4.** Distributed system

Imagine you are writing a document using the Microsoft Word application on a PC running the Microsoft Windows operating system. This setup is both centralized and non-distributed. One entity, Microsoft, controls your application and operating system (centralized). Both the application and the operating system are located on your PC, i.e., in one physical location (non-distributed). Now, suppose you run an open-source operating system like Linux on your PC with open-source word-processing software. Different people and organizations contribute to the evolution of both items (the setup is now decentralized). On the other hand, you are still using one physical PC to run all the software (it's still non-distributed).

A distributed but centralized system may sound contradictory, but if we use the definitions above based on control and location, we'll see how this works. Consider a cloud service provider offering a data storage service. Physically, your data could be shared and replicated on different machines according to resource availability and resiliency (distributed). However, wherever the machines and data storage facilities happen to be, the cloud service provider still controls them all (centralized). Bitcoin is a blockchain system that cannot be altered by any one entity (decentralized). It also runs as a peer-to-peer network of independent computers spread across the globe (distributed).

[4-5].

### 3-3. Distributed ledger and blockchain

Distributed ledger technology (DLT) can be considered one of the foundations of blockchain technology, but it is different from the blockchain in that entity. Therefore, to understand blockchain technology and decentralized networks, which is the basis of many digital currency projects, you must have a correct understanding of this technology. To continue, this will be discussed in detail. DLT stands for Distributed Ledger Technology, known as "shared ledger" or simply distributed ledger. The ledger is a digital system in which the users and systems can record transactions of assets in multiple places at the same time [5-6].

Blockchain is the most prevalent type of distributed ledger technology that is currently in use. Blockchain is a ledger more developed than a database which is an entire system with moving parts and components that work together [7].

Blockchain technology developed with the emergence of Bitcoin as a peer-to-peer cryptocurrency. In Blockchain technology, all nodes in the network must agree and come to a consensus. This means that when a transaction is sent to the network, it must be confirmed by the network nodes. Every time the authenticity of transactions is verified by the blockchain network, they are placed in the next block of the chain and recorded in the history of the network [8-9]. A block is a piece of data structure where transactions are recorded. In other words, if a person sends you a bitcoin, you have to wait for the transaction to be validated and recorded on the network's transaction ledger. In the Bitcoin network, a series of new transactions are hashed or compressed into a small data set every ten minutes to create the next block. For this reason, it is called blockchain technology since it is essentially a chain of blocks. The users who are responsible for creating new blocks are called miners, which receive the reward for mining; new coins are created with each new block which is called the block rewards and serves as an incentive for miners to generate the network. Without miners, the network will not be available [10-11].

### 3-4. Difference between blockchain and distributed system

Distributed ledger and blockchain have many similarities. Both are a digital, decentralized list of records. Despite the similarities, they are different. Indeed, the distributed ledger can have different forms, one type of which is the blockchain. Many of us have been guilty of confusing these two terms and using them interchangeably. But even though their meanings overlap in some areas, and even though they've both reached similar levels of public notoriety since the 2017 cryptocurrency bull market, they aren't quite identical. They both generally refer to a record of information that's distributed across a network, and yes, they both foster a greater degree of transparency and openness than had been enabled by earlier centralized databases or digital records. But this is where the analogies end since blockchains and distributed ledger technology (DLT) each come with their own important distinguishing properties. [12-13].

### Openness, decentralization, cryptography

There are two big distinctions, and depending on where you sit on the Bitcoin vs. blockchain spectrum, some qualify Bitcoin-style blockchains as largely superior to and more innovative than their distributed ledger counterparts, while others qualify DLT as more useful for everyday commercial purposes [14]. The illustration below outlines how the two technologies relate to each other, showing that one way to implement DLT is through a blockchain:

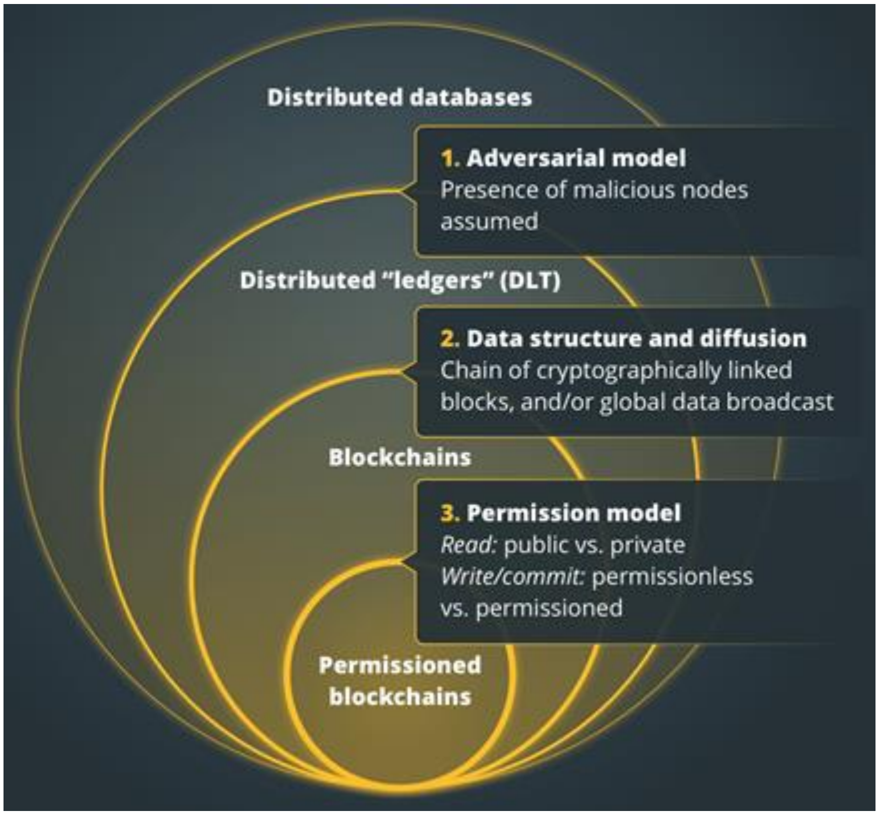
Distributed databases
1. Adversarial model
Presence of malicious nodes assumed
Distributed "ledgers" (DLT)
2. Data structure and diffusion
Chain of cryptographically linked blocks, and/or global data broadcast
Blockchains
3. Permission model
Read: public vs. private
Write/commit: permissionless vs. permissioned
Permissioned blockchains

**Figure 1-5.** The relationship between blockchain and DLT:

### Examining the relationship between blockchain and DLT

Firstly, blockchains are generally public, meaning that anyone can view their transaction histories and that anyone can participate in their operations by becoming a node. They are, as cryptocurrency parlance puts it, "permissionless." This is the key feature pointed out to

Cointelegraph by Marta Piekarska, the director of the ecosystem at Hyperledger. According to Piekarska:

"First and foremost: one is permissionless, the other is permissioned. This means that in the first case, anyone can participate in the network; in the other: only chosen participants have access to it. This also determined the size of the network: Bitcoin wants to grow infinitely, while in a permissioned blockchain space, the number of parties is smaller."

Put simply, the public aspect of blockchains generally implies three interrelated things: 1) Anyone can use the blockchain, 2) anyone can serve as a validating node of the blockchain, and 3) anyone who becomes a node can, in turn, act as part of that blockchain's governance mechanism. In theory, this makes blockchains decentralized and democratic structures resistant to undue control or influence from any single party.

By contrast, a distributed ledger generally doesn't enable any or most of these public features. It restricts who can use and access it (hence the "permissioned" terminology), and it also restricts who can operate as a node. And in many cases, governance decisions are left to a single centralized company or body. Compared to the ideal of a public, decentralized blockchain, it exists solely to serve the interests of a concentrated group of commercial players and interests [15].

Below is an image detailing how the centralized, decentralized, and distributed networks are structured:

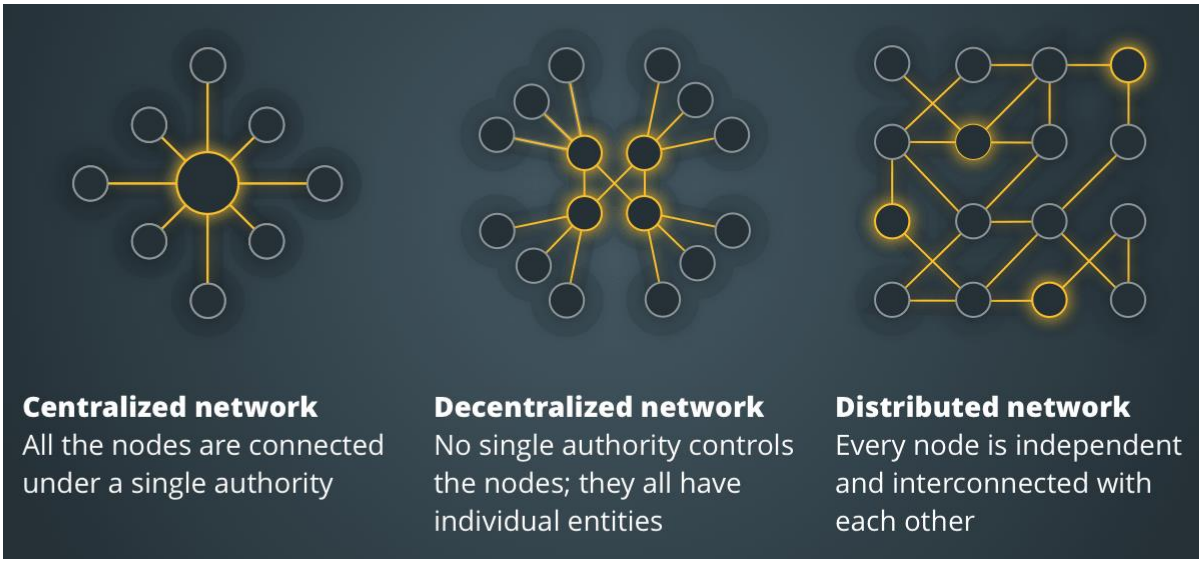
Centralized network
All the nodes are connected under a single authority
Decentralized network
No single authority controls the nodes; they all have individual entities
Distributed network
Every node is independent and interconnected with each other

**Figure 1-6.** Different network types

And then there's the second main difference. As the name implies, blockchains consist of a series of time-stamped blocks, and the information inside the blocks is stored in a chain in such a way that each block is dependent on its previous block, as well as new information in the block. New blocks are stored and linked to the previous blocks; hence it is called blockchain technology. This ensures a greater level of security for the blockchain insofar as the need for cryptographic consensus makes it very difficult to fake transactions.

However, while some distributed ledgers aren't cryptographically validated chains of blocks, it's worth stressing that some are. Because of this, it should be emphasized that there's only one essential difference between blockchains and distributed ledgers, which is simply that one is permissionless, and the other is permissioned.

"The only difference between private and public blockchains is the range of availability. I can easily imagine deploying the Bitcoin protocol in a private cloud serving just a small group of users. The fundamental difference here is between permissionless blockchains — like Bitcoin and permissioned ones. For permissionless ones, we do not need to trust any third-party company to run it fairly and honestly."

But assuming that a distributed ledger is private and not a chain of time-stamped blocks driven by cryptographic consensus, it often becomes a fairly conventional database that exists only among a select group of participants. In the enterprise space, people are talking about private blockchains, which technically are not blockchains but better database management systems. Nevertheless, it does have productivity gains; I call it a 9 to 10 innovation, whereas public blockchains like Bitcoin and Ethereum are 0 to 1 innovations that completely change the way we think and use money and computation. Bitcoin is a true public blockchain that is open, neutral, censorship-resistant, and borderless. And distributed ledgers are simply permissioned databases [16].

**Privacy and scalability**

Even though blockchains are arguably superior to distributed ledgers, DLT can still be a useful addition to the global economy's technological arsenal, particularly in cases in which it would be unwise to harness a truly public and decentralized blockchain.

"The strongest argument for a private blockchain seems to be when a bunch of banks get together to create a system for transferring money between each other. In this case, no bank would be content letting any of the other banks 'maintain' the database on their own, so a shared blockchain controlled by no one would make sense."

Added to this, the privacy of private ledgers is an obvious benefit for any company protective of its business or customer data. Still, the chief commercial officer at the Energy Web Foundation, Jesse Morris, contends that, even here, the privacy of public blockchains can be much stronger than some people realize. A common criticism of public chains has to do with privacy (e.g., the details of every transaction are known to all). This criticism does not recognize two simple facts: 1) any decentralized applications can shield certain transactional details by only transmitting the bare minimum of information necessary across any blockchain while keeping sensitive data off-chain, and 2) even in private networks, privacy-preserving features are applied to protect sensitive information from participants on a private blockchain, and these same privacy preservation measures are beginning to be utilized on public blockchains as well [17].

In other words, there is a recognition that public blockchains potentially offer many of the privacy benefits promised by their more private rivals. Of course, private ledgers still generally have the advantage of being controlled by the companies that use them. This is obviously a big plus for big multinational banks that want to have control over their processes.

There is also the very salient benefit of improved scalability since, as mentioned above, distributed ledgers are often shared yet largely centralized databases. As such, they can process thousands — if not hundreds— of transactions per second, while decentralized blockchains such as Bitcoin struggle to top seven transactions per second, all the while consuming vast quantities of electricity. This is perhaps the main benefit offered by distributed ledgers, and even if they don't offer much decentralization and transparency beyond previous database systems, it's one reason why they'll continue being used in the future [18].

## 4. Suggestions

In Iran, like many other countries, the final decision has not been made yet about the use and production of this type of currency. Of course, cryptocurrency mining has been officially considered an industry, and Hassan Rouhani, the former president of the Islamic Republic of Iran, talked about regulating cryptocurrencies and producing a national cryptocurrency. The Department of Payment Systems of the Central Bank's New Technologies posted the 0.0 version of the cryptocurrency rules on its website. These rules are compiled in 13 pages and 7 headings, including:

- Requirements for the field of universal cryptocurrencies
- ICO requirements
- Requirements for the central bank's cryptocurrency, as well as the regional cryptocurrency fields
- General requirements for exchanges
- General requirements for cryptocurrency wallets
- Mining

According to the accomplished research, some suggestions are made as follows, represented in Table 2, for further research to improve studies and a better understanding of blockchain, digital currencies, and the distribution properties in the country.

**Table 2.** Suggestions for research

| Row | Research suggestion | Explanations |
|---|---|---|
| 1 | Presenting a secure digital currency based on blockchain technology and distributed system in Iran | If the country's central bank diagnose that it is necessary to regulate a digital currency to carry out future transactions, the initial mining and doing transactions would be facilitated, and this requires more studies about the manner of development of digital currencies so that the precise application and gaps are recognized and removed. |
| 2 | Investigating cryptographic algorithms used in the digital currencies process | Considering the wide usage of cryptographic algorithms used in the process of digital currencies development, it is necessary to examine these algorithms in the specification and creation of a secure framework for these currencies, and further research would play a determinative role in facilitating this process. |

## 5. Conclusion

According to the accomplished studies, blockchain is one of the distributed ledgers which uses cryptographic and algorithmic approaches to build and verify an extensive data structure. This is the first and most important difference between blockchain and distributed ledger. The blockchain data structure consists of a chain of blocks comprising transaction information recorded on a ledger. A blockchain consists of a sequence of blocks, while a distributed ledger does not necessarily require a chain or sequence. Further, distributed ledgers do not require proof of work and provide better options, at least for scalability on paper. Principally, DLT does not require a block data structure. This ledger is just a database model distributed across several places or regions. Although DLT and blockchain have many similarities, they are two different concepts. Put simply, every blockchain is a distributed ledger, but not every distributed ledger is a blockchain. A distributed ledger is a decentralized version of an accounting ledger that eliminates the intermediary or centralized entity. Distributed ledgers are used for the decentralized recording of various data and information. In DLT, all the network members or nodes agree to a consensus to record records, and it is impossible to change information and data without their consensus.

Blockchains are a type of distributed ledger that are used to record financial information such as transaction details. Despite the developments created in the digital industry, distributed ledgers still have to cope with various challenges to pave their way on the intricate path of widespread global use in this industry. Of course, these challenges should not weaken the hopes for this technology. Understanding the challenges is the first step in problem-solving.

**Acknowledgment:Non**

**Conflict of Interest: Non**

**Funding: Non**

**Ethical statements Non**

## References

[1] H. Akbari; M. Amiri; "Scenarios of Global Economy Facing the Basic Cryptocurrencies", Ministry of Economic Affairs and Finance, Future Research Studies, Modeling and Management of Economic Information. 2016.

[2] M. Seyyed Hosseini; M. Doaei; "Bitcoin, the first Virtual Currency", Bors Monthly, No. 114-115. 2013.

[3] S. Singh. “Blockchain: Future of Financial and Cyber Security”. 2016 2nd International Conference on Contemporary Computing and Informatics (ic3i), IEEE. 2016.

[4] Distributed Ledger Technology: beyond block chain (PDF) (Report). Government Office for Science (UK). January 2016. Retrieved 29 August 2016.

[5] Sadeghi, Mahsa; Mahmoudi, Amin; Deng, Xiaopeng (2022-02-01). "Adopting distributed ledger technology for the sustainable construction industry: evaluating the barriers using Ordinal Priority Approach". Environmental Science and Pollution Research. 29 (7): 10495–10520. Doi:10.1007/s11356-021-16376-y. ISSN 1614-7499. PMC 8443118. PMID 34528198.

[6] S, Surbhi (26 Jul 2018). "Difference between Journal and Ledger". Developer works. Retrieved 22 Dec 2020.

[7] Maull, Roger; Godsiff, Phil; Mulligan, Catherine; Brown, Alan; Kewell, Beth (21 Sep 2017). "Distributed ledger technology: Applications and implications". FINRA. 26 (5): 481–89. Doi**:** 10.1002/jsc.2148.

[8] Ray, Shaan (2018-02-20). "The Difference between Blockchains & Distributed Ledger Technology". Towards Data Science. Retrieved 25 September 2018.

[9] "Distributed Ledger Technology: beyond block chain" (Press release). Government Office for Science (UK). 19 January 2016. Retrieved 25 September 2018.

[10] Brakeville, Sloane; Perepa, Bhargav (18 Mar 2018). "Blockchain basics: Introduction to distributed ledgers". Developer works. IBM. Retrieved 25 Sep 2018.

[11] "Central banks look to the future of money with blockchain technology trial". Australian Financial Review. Fairfax Media Publications. 21 November 2016. Retrieved 7 December 2016.

[12] "Citi and Goldman Sachs go live with blockchain equity swaps platform-The TRADE". Www.thetradenews.com. Retrieved 2022-05-20.

[13] "BlackRock Joins Blockchain Platform Axoni for Equity Swap Trades". Bloomberg.com. 2021-09-07. Retrieved 2022-05-20.

[14]"Crypto FAQ: What is Distributed Ledger Technology (DLT)" Cryptocurrency Works. Retrieved 2022-07-28.

[15]"Blockchains & Distributed Ledger Technologies" . Blockchainhub Berlin. Retrieved 2022-07-28.

[16] ^ "Crypto FAQ: What is Distributed Ledger Technology (DLT)?" Cryptocurrency Works. Retrieved 2022-07-28.

[17] Pervez, H. (2018). "A Comparative Analysis of DAG-Based Blockchain Architectures". ICOSST 2018.

[18] "Crypto FAQ: What is Distributed Ledger Technology (DLT)?" Cryptocurrency Works. Retrieved 2022-07-28.