Blockchain technology – support for collaborative systems

Gheorghe MATEI
Bucharest, Romania
mgm1802@yahoo.com

Blockchain technology is one of the most promising new technology, a new approach in data registration and distribution, and represents a new paradigm for how information is shared. Blockchain technology gained attention after the first application of this technology – Bitcoin blockchain – was deployed. The tech community considers that blockchain is one of the most disruptive technologies and saw more possibilities of using it in many other sectors. The technology can create trusted, secured, transparent, verifiable, real-time communication networks capable to support almost everything, from payments networks to supply chains, real estate deals, healthcare data sharing, voting systems protected from falsification, etc.

This paper aims to briefly present the blockchain technology and how it could be applied in a collaborative system in the healthcare industry.

Keywords*: blockchain, Bitcoin, hash, peer-to-peer, proof-of-work, proof-of-stake, private key, public key*

DOI: 10.24818/issn14531305/24.2.2020.02

1 A short presentation of the blockchain technology

Blockchain is the name of a relatively new technology. Many experts consider it is the most promising new technology, the next *big thing,* probably the biggest since the appearance of the internet. As the name states, blockchain is a sequence of blocks containing one or more transactions. The blocks are chained together and distributed to the users.

It is accepted that the blockchain concept occurred in 1991 when Stuart Haber and W. Scott Stornetta published "**How to Time-Stamp a Digital Document**" in the Journal of Cryptology. This was the first work on a secured chain of blocks. They proposed a system where document timestamps could not be tampered with. One year later, together with Dave Bayer, they proposed Merkle trees as a solution to store more documents into one block, which improved the system's efficiency [1].

In 2002, David Maziers and Dennis Shasha formulated the concept of decentralized trust within a network system.

In 2005, Nick Szabo proposed Bitgold, a protocol for decentralized property titles that incorporated a blockchain system. This protocol involved *proof-of-work* and *timestamping* features but, unfortunately, it also had a fatal weakness. It was discovered that someone who held a balance of Bitgold could spend his/her virtual coins twice without being "caught". This weakness became known as the *double-spending problem* [2].

The work of the researchers mentioned above stopped at a conceptual level. A real live blockchain was created only in 2008. In this year, Satoshi Nakamoto (a pseudonym of a person or a group of people) published "**Bitcoin: A Peer-to-Peer Electronic Cash System**". In this paper, he proposed a solution that would solve the double-spending problem that led to the abandonment of the Bitgold project. That was a peer-to-peer network that would timestamp transactions "*by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work*" [3].

The purpose of the system proposed by Satoshi Nakamoto was to allow online payments to be signed digitally and sent directly from one party to another without needing the authorization of a trusted third party, as a bank or other financial institution. The electronic payment system was based on "*cryptographic proof instead of trust, allowing two willing parties to transact* *directly with each other without the need for a trusted third party*” [3].

This document became the white paper for the first working blockchain, Bitcoin. Bitcoin was the first cryptocurrency, that is a digital coin that runs on a blockchain. A cryptocurrency is a currency that is is not issued and controlled by a central bank. It can be used instead of fiat money for trading, and it uses an encrypted mathematical blockchain model to track the exchange of value or ownership.

Although in Nakamoto’s paper the virtual currency database was not referred to as a blockchain, it was so named over time because all the transactions generated onto the network were grouped into blocks of data and then chained together using sophisticated mathematical algorithms.

As mentioned above, Bitcoin was the first application using blockchain technology. Since then, many other cryptocurrencies were launched, as well as numerous applications developed for different social or economical sectors. All those applications are based on blockchain technology.

In the simplest terms, blockchain can be defined as a linear data structure that stores transactional records chronologically, ensuring decentralization, security, and transparency. As mentioned in [4], blockchain is not a single technology. Rather it is an architecture that allows disparate users to make transactions and then create unchangeable and secure records of those transactions.

Sometimes referred to distributed ledger technology, blockchain is a distributed database stored on lots of computers at the same time. It applies to both static data (a registry), and dynamic data (transactions).

A blockchain is a digital ledger of linked batches of transactions, a chain of blocks containing digital data or information, every block being dependent on the previous one. The blocks and their contents are protected by powerful cryptography, that branch of mathematics which deals with information securitization and authentication, as well as the limitation of the access to an informatics system. When a block is completed, a unique security code is generated by using a cryptographic method called hashing, in combination with a consolidating data structure known as the Merkle tree.

A hash is a unique code which is the result of applying a special mathematical function to a set of elements – in blockchain case, the transactions contained in a block. In simple terms, hashing means taking an input string of any length and giving out an output of a fixed length [5].

When a transaction has been verified and is ready to be added to a block, it is converted through a hash algorithm into a string of digits and letters having a fixed length. Then two transaction hashes are combined and, through the same hash algorithm, another hash will be generated. This process is repeated with all transactions in the block until remains just one hash, the *root hash* of the block.

A hash algorithm is working only one way. The results of this algorithm are deterministic, always generating the same unique hash when using the same input. So it’s impossible to reverse the process, to “un-hash” it, to decode the original data [6].

Due to its uniqueness, any change made to the information inside the block will modify the hash of that transaction, affecting every iteration to the root hash. This is known as a *Merkle tree,* and a simplified diagram is shown in figure 1. By summarizing hashed transactions into a single root hash, a Merkle tree reduces significantly the amount of data required to be stored and transmitted over the network.

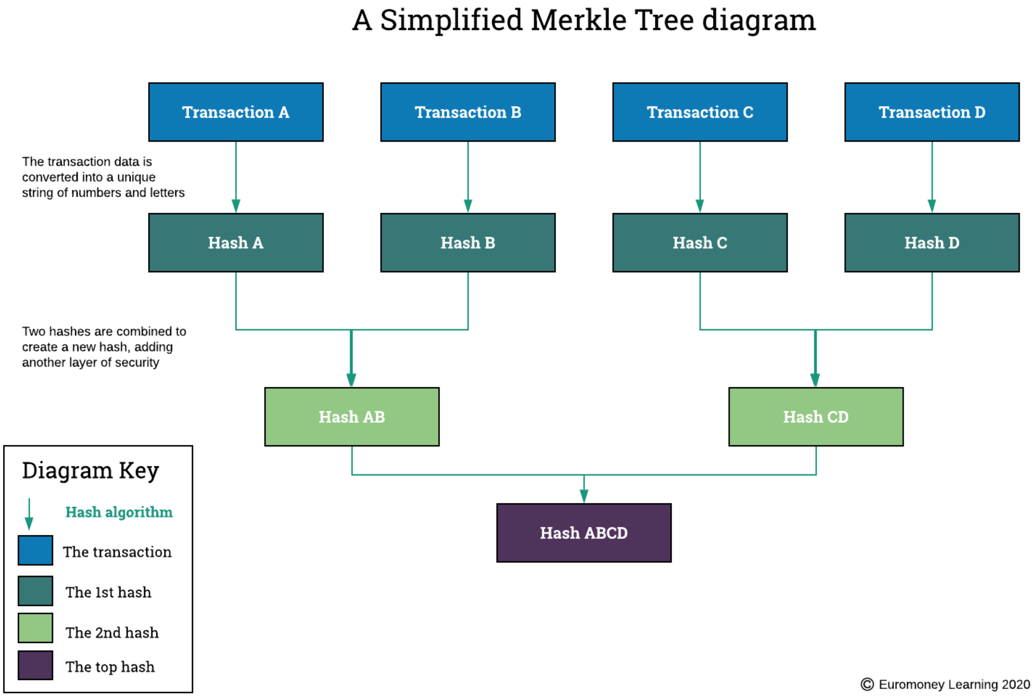

A Simplified Merkle Tree diagram
Transaction A
Transaction B
Transaction C
Transaction D
The transaction data is converted into a unique string of numbers and letters
Hash A
Hash B
Hash C
Hash D
Two hashes are combined to create a new hash, adding another layer of security
Hash AB
Hash CD
Hash ABCD
Diagram Key
Hash algorithm
The transaction
The 1st hash
The 2nd hash
The top hash
© Euromoney Learning 2020

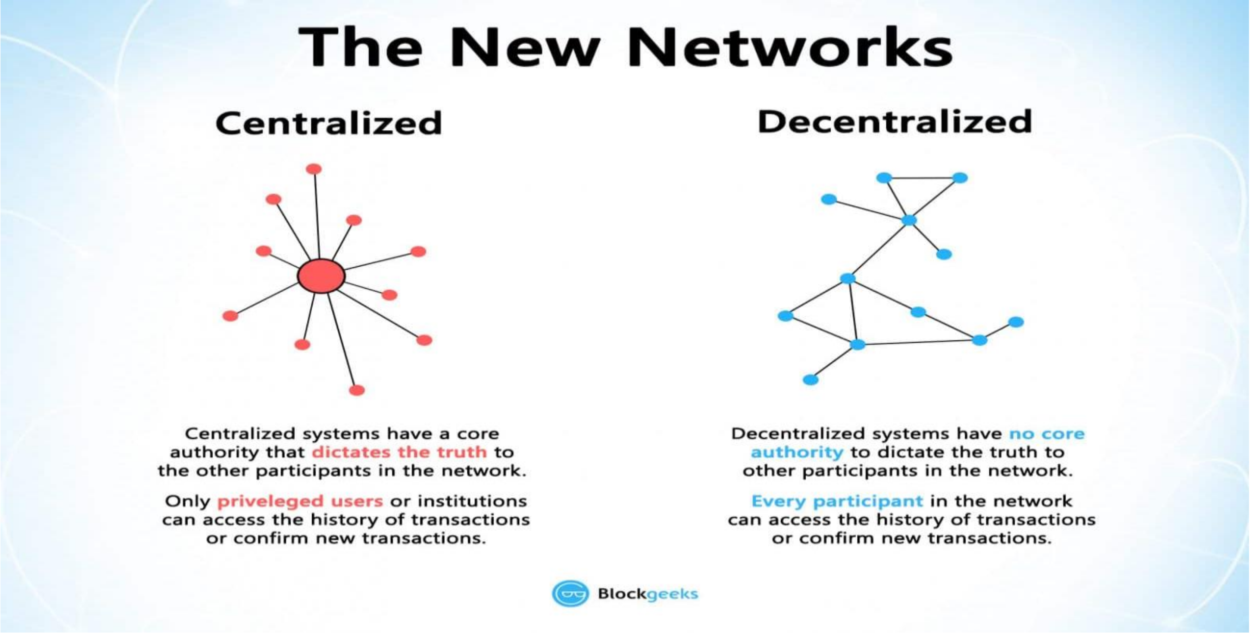
Fig. 1. A simplified Merkle tree diagram
(source [6])

The connection of blocks through unique hash keys ensure blockchain security. The hash code – that is part of the block – contains a link to the previous block, creating a chain of blocks, that is a blockchain. Each block also contains a timestamp which shows the moment when that block was created.

Blockchain is based on a *peer-to-peer* topology, which is a distributed architecture that partitions tasks or workloads between interconnected computers, called *peers*. A blockchain is a distributed ledger of transactions, that is completely open to everyone on the network. Those transactions may refer to money transfers, in the case of blockchain currencies such as Bitcoin, exchange of goods or services between two parties, or ownership rights, when the blockchain records who owns what.

A blockchain runs onto a decentralized network of computers – called *nodes* – interconnected to one another, unlike a centralized network built around a central authority. Nodes can be any kind of electronic device and are not given any special privileges. The network has a flat topology, with no centralized authority nor any hierarchy. Figure 2 shows some differences between a centralized network and a decentralized one.

A centralized system has a core authority that dictates the truth to the other participants in the network. Nodes are connected to a central server, which is responsible for all communications between them and is hosting the database. Moreover, only privileged users can access the history of transactions or confirm new transactions.



The New Networks

Centralized

Centralized systems have a core authority that dictates the truth to the other participants in the network.

Only priveleged users or institutions can access the history of transactions or confirm new transactions.

Decentralized

Decentralized systems have no core authority to dictate the truth to other participants in the network.

Every participant in the network can access the history of transactions or confirm new transactions.

Fig. 2. Types of networks
(source: [5]))

As shown in the picture above, a centralized system has a core authority that dictates the truth to the other participants in the network. Nodes are connected to a central server, which is responsible for all communications between them and is hosting the database. Moreover, only privileged users can access the history of transactions or confirm new transactions.

Decentralized systems have no core authority to dictate the truth to other participants in the network. Instead of trusting a third party, users trust a program with preset rules. Nodes communicate directly with each other without needing a central server. All participants are equally privileged and everyone can access the history of transactions or confirm new ones, as everyone is hosting a copy of the database (blockchain), an identical copy for all nodes. All copies are updated automatically whenever a new block is added to the blockchain.

In a blockchain network there could be hundreds or thousands of nodes, maybe millions in the case of Bitcoin. So, there is a huge number of copies of the same blockchain distributed into the network. That makes the information stored in the blockchain very difficult to be hacked, as a hacker would need to manipulate every copy of the blockchain on the network. Moreover, changing the content of a block will automatically generate a new hash for that block. But the next block in the chain still contains the old hash, so that the hacker would need to change the content of this block too. And so on, until the end of the chain. Therefore, to change or delete a single block, a hacker needs to change every block after in on the blockchain, and this would have to be done on the majority of the network's nodes, a thing practically impossible to be done.

The blockchain software is run by each computer connected to the network. Computers may be located all over the world, but each computer is running the same software. If one is hacked or disconnected, the network does not collapse, it remains operational and the other computers can go on without it. Compared to a decentralized system, it has no weak point and it is more cost-effective.

As mentioned in [2], the blockchain is a method of trustless digital exchange, spread across lots of computers running the same program. By distributing ledger across every computer running the protocol, blockchains remove the need for a centralized authority or any third party, and users can interact with each other directly. They are responsible for handling their records, thus getting the overall control of their data. It can be said that this brings freedom to the digital world on an individual level.

2 Blockchain features and operation

Although it is mainly used by cryptocurrencies, blockchain technology is not limited to their support. It is not just a backup network for digital currencies, but it can offer much more. It has several features that give it robustness and safety in operation. Its features and mode of operation give it large possibilities to penetrate in many other fields.

2.1 Blockchain features

Blockchain has several features that make it a strong instrument, a revolutionary one as many scientists stated. These features are closely related and influence each other. Here are some of the most important features:

- it’s a decentralized system;
- runs on a peer-to-peer network;
- it’s immutable;
- it’s tamper-proof;
- ensures privacy but transparency too;
- it’s based on a consensus protocol.

Blockchains are **decentralized systems**. Because of this, no single entity holds the authority of the overall network. Information is not stored by one single entity; everyone in the network owns the information. The blockchain is multiplied, in its entirely, across all computers in the network. It puts users in a straightforward position. Interaction between any two nodes can be made directly, not through a third party. While everybody in the network has an identical copy of the distributed ledger, no one can modify it on his/her own.

With the use of a blockchain, the interaction between two parties through a **peer-to-peer** model is easily accomplished without the requirement of any third party. Blockchain does not need any third trusted party, internal or external, to authorize its activity. This is possible because the blockchain is distributed among all its users. Every user has its copy of transactions and hashed blocks, and they spread the information of any new transaction to the entire network. This way, it is not possible for anyone to alter the information in the blockchain since it is not stored by an individual entity but for an entire network of node users. Once a block of transactions is validated, it is added to the blockchain and every user updates their local information. Even an attack was to modify a local ledger, the network will not accept any block from the altered blockchain. This is possible due to the peer-to-peer protocol used by blockchain which allows all the network participants to hold an identical copy of transactions, enabling approval through a machine consensus.

The **immutability** feature of a blockchain refers to the fact that any data once written on the blockchain becomes permanent and cannot be altered or changed anymore. Immutability is given by the mechanism of chaining the blocks into blockchain through a cryptographic hash function. Cryptography, which is a complex mathematical algorithm, acts as a firewall for attacks so, along with decentralization, it is another layer of protection. Every block has its unique hash and it also contains the hash of the previous block. Modifying the content of a block generates a new hash for that block, which leads to breaking the connection with the next block, which still contains the old hash. It is not possible to modify any block without changing all the blocks that follow it. Due to the blockchain’s immutability, data stored in it is not susceptible to hacker attacks. Hence, the blockchain works as an immutable ledger.

With the property of immutability embedded in blockchains, it becomes easier to detect the tampering of any data. Blockchains are considered **tamper-proof** as any change in even one block can be detected and addressed immediately. There are two key ways of detecting tampering, namely hashes and blocks.

As described earlier, each hash function associated with a block is unique. Any change in the data will lead to a change in the hash function. Since the hash function of the block is linked to the next block, for a hacker to make any changes, he/she will have to change hashes of all the blocks after that block, which is quite difficult to do.

Although the real identity of a person who generates a transaction is hidden through complex cryptographic algorithms and is represented only by his/her public address, which ensures that person's **privacy**, blockchains are **transparent** systems, allowing any participant to see all the transactions made by a certain public address.

A **consensus** algorithm is the core of the blockchain architecture. To keep the network decentralization, every blockchain must have a consensus algorithm, or else its value is lost. It uses a consensus to help the network make decisions. Editing the blockchain is only possible if there is a consensus between the network of computers storing separate but identical versions of the blockchain. Users need to meet an agreement about the validity of the chain before adding more blocks. Every time a node adds a new block, all the users have to validate the block by using a common protocol. The consensus is responsible for the network being trustless. Nodes might not trust each other, but they can trust the algorithm that runs on the network. Typically, the nodes reach a consensus about the correctness of a new block by proof-of-work or proof-of-stake mechanism.

Proof-of-work is a consensus mechanism that demands some work from the service requester, usually meaning processing time by a computer. It is based on solving a complex mathematical puzzle that requires great computational power to validate transactions and create new blocks.

Proof-of-stake is a consensus algorithm through which the creator of the next block to be added in the blockchain is chosen by various combinations of random selections. Regardless of the mechanism used, the nodes check that the new block meets the requisites of their proof method, including validation for all the transactions inside the block. If the block is valid, they consider it as a part of the blockchain and keep adding new blocks [7] [8] [9].

2.2 Blockchain operation

Each block in the chain contains several transactions, and every time a new transaction occurs on the blockchain, a record of that transaction is added to every node's ledger. Each transaction is secured with a digital signature that proves its authenticity. The construction of this signature is based on two keys, namely the sender's *private key* – that allows the sender to make transactions – and the receiver's *public key* – that allows the receiver to access transactions. The transaction is verified by the nodes in the network, which has to confirm its details, including the transaction's time and its participants. Transactions are stored in a block. When all the transactions in the block have been verified and the majority of nodes in the network reached a consensus and agreed with the validation and approval process, the block is timestamped and gets a unique identifying code which is named a hash, as presented in section 1. The hash of the previous block added in the blockchain is stored in the current block too. Once the new block is added to the blockchain, it becomes public and available for anyone to view.

This is the general model of a blockchain operation. It can have certain particularities specific to each blockchain. For example, a transaction made on the Bitcoin blockchain goes, from a sender to a receiver, through the steps shown in figure 3.

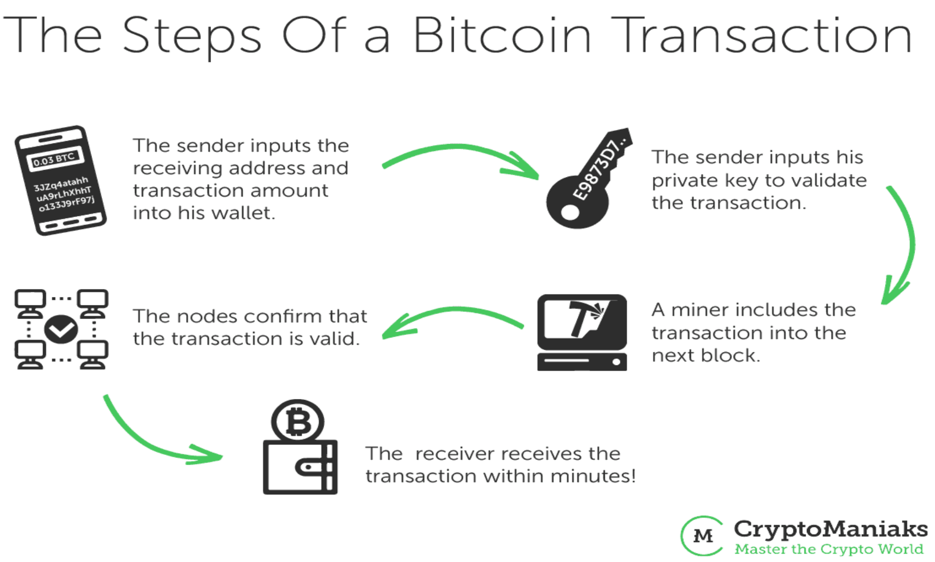

The Steps Of a Bitcoin Transaction
0.03 BTC
3JZq4atahh uA9rLhXhhT o133J9rF97j
The sender inputs the receiving address and transaction amount into his wallet.
E9873D7..
The sender inputs his private key to validate the transaction.
A miner includes the transaction into the next block.
The nodes confirm that the transaction is valid.
The receiver receives the transaction within minutes!
CryptoManiaks
Master the Crypto World

Fig. 3. The steps of a Bitcoin transactions
(source: [2])

i. The sender inputs the receiving address – that is the receiver's public key – and the transaction amount into his wallet, which is a device running special software that identifies the owner and allows him/her to sign online transactions.
ii. The sender inputs his/her private key for validating the transaction.
iii. A miner, that is a special node in the Bitcoin blockchain aiming to validate transactions, includes the transaction into the next block. To do so, the miner has to solve a complex mathematical puzzle known as the proof-of-work problem. Miners in the network compete to solve the problem. The first miner who solves it announces this to the whole network at the same time and receives, as a reward, an amount of bitcoins provided by the protocol.
iv. The other nodes on the network confirm the transaction validity.
v. After a short time, the receiver can access the transaction and use the money.

3. Types of blockchains

As per the requirements and access permissions for the network participants, there are two broad categories in which blockchains can by classified: public and private blockchains. Both types have certain similarities, such as:

- both of them have a peer-to-peer decentralized network;
- all the participants in the network have their copy of the distributed ledger;
- transactions are processed through consensus;
- the network maintains copies of the ledger and synchronizes the latest update on every node through the consensus of the majority of participants;
- both of them use rules for the immutability and safety of the ledger to prevent malicious attacks [10].

In addition to these features, several characteristics make them different.

In a **public blockchain**, open-source software is used by everyone participating in the network. A public blockchain is a ledger that can be accessed by any participant. Just an internet connection will allow him/her to access the blockchain, to interact with other participants, to send or validate transactions with no restrictions and without the need to have someone's permission. It is managed autonomously to exchange information between parties. That is why it is called a *permissionless blockchain*. Anyone with access to the internet might join and become a participant in the blockchain network That means he/she can see the history of the blockchain, as well as make transactions on it. Public blockchains allow participants all over the world to exchange data and information in a direct, open, and secure way.

An example of a public blockchain is the Bitcoin and the other cryptocurrencies blockchains. In these blockchains, there is very little chance that the rules decided and applied initially will be changed in the latter stage.

Private blockchains use the same principles as public ones, but the software is proprietary and hosted on private servers. They are shared only among trusted participants who are allowed to access the blockchain, on a permission basis. That is why it is also called a *permissioned blockchain*.

Contrary to public blockchains, the overall control of the network of a private blockchain is in the hands of its owners. Participants' access is restricted. No one can join the blockchain without the permission of network administrators. Moreover, the rules of a private blockchain can be changed according to different levels of permission, exposure, risks, number of members, authorization, etc.

Private blockchains are usually used by companies and organizations to create and centrally administrate their transactional networks. Usually, they can run independently on a closed network, but they can be integrated with other blockchains too. Because only certain people can access a private blockchain, depending on its system of permissions, the level of trust required amongst the participants is higher than in a public one.

4 Blockchains in healthcare

The healthcare industry is one of the sectors that may see important changes as a result of blockchain technology. Blockchain technology can give healthcare support for increasing the quality of the services offered to patients, as well as for improving the collaboration between doctors, patients, pharmacists, and insurance companies. Moreover, the landscape of the healthcare system is moving towards a more patient-centric approach which focuses on two major elements, namely affordable treatment and suitable healthcare facilities at all times.

4.1 The existing healthcare system

The current healthcare sector cannot be considered complete because there are many actors in this field that do not have a proper system for efficiently managing their processes. Moreover, it is inadequate for managing the exchange of information between participants and that is why it requires certain major changes. The wrong usage of available data is preventing healthcare organizations to deliver appropriate patient care and high-quality services, to ensure a better health. Often, these organizations are not able to fulfill the needs of patients, causing their dissatisfaction.

Many healthcare entities today are still dependent on old, outdated, and susceptible to failure systems for keeping patient records. These systems store patient data in a local database, managed by a certain entity. Although patient data may be duplicated in multiple local databases, none of them contains complete information. This can make it difficult for a doctor to make a proper diagnosis, which is time-consuming for him, but also boring for the patient. Moreover, every system is a potential point of failure which could be damaged by technical problems or hacker attacks. Due to this, the cost of maintaining a patient-oriented business is increased considerably [11].

The current system is not able to collect, analyze, secure, and exchange data coherently and consistently. That is why a new system is needed, a system that is transparent, efficient, and easily operable.

4.2 A possible next system

The potential of blockchain technology for the healthcare sector highly depends on its acceptance by the decision-makers in the system.

As already mentioned, a blockchain is a distributed ledger that keeps track of transactions and activities happening throughout the network. The data stored on a blockchain is secure in its entirety. Blockchain can bring out a major development in the healthcare sector because it can bring several changes that can improve the healthcare management of patients. The technology holds the ability to improve the quality of care services provided to patients while keeping the necessary funds at a reasonable level.

To fundamentally change the healthcare sector in the coming times, blockchain must prove that can solve all the problems of the current system and to transform it into a system where all the information is easily accessible, at any given time, by doctors, pharmacists, researchers, and patients as well. Blockchain can act as a collaborative network, enabling different parties to exchange and add information in the system. Mainly, the information refers to patients' electronic healthcare records and can be seen or modified only by authorized users: doctors, pharmacists, insurance providers, or patients themselves

Blockchain allows the creation and distribution of a single common database of patients' health information. This system would be accessible by all the entities involved in the process, no matter what electronic medical system they use. Healthcare providers can leverage blockchain to securely store their patients' medical records. When a medical record is generated and signed, it can be written into the blockchain. This provides patients with proof and guarantees that their records will never be changed. These personal medical records could be store on the blockchain in an encoded form so that only certain people can access them [12]. This offers higher security and transparency while allowing doctors to spend more time on patient care and their treatments. Moreover, it will also enable better sharing of studies, reports, analyzes, and statistics of researches which could process huge amounts of data and, in turn, would facilitate clinical trials and treatment therapies for different diseases.

In a healthcare system, facilitating data sharing between the providers of healthcare solution can lead to accuracy in diagnosis, effective treatments may decrease costs per patient, contributing to a more efficient system. As patient data is constantly growing, all available resources must be used efficiently, to make the most effective utilization of the insights discovered through it. Blockchain for healthcare allows all entities interested in the healthcare sector to stay in sync and share data on a commonly distributed ledger. Having such a system available, the participants can share and keep a track of their data and other activities happening in the system without worrying about their integrity and security and without needing any intermediaries or trusted third parties.

The blockchain technology can offer to the healthcare sector an efficient, secure, and reliable system to optimize current workflows and make the right decisions. Having properties like immutability, trustworthiness, and decentralization, the distributed technology of blockchain provides the healthcare sector with opportunities to detect fraud, reduce operational costs, facilitate processes, remove duplication of work and apply transparency in the healthcare sector.

Specialists in the healthcare sector need to have access to scientific studies regarding population health by groups of ages, diseases, or other criteria. In such studies, the patient data has to be provided in an anonymous form, without revealing patients' names or other particular information. Those who conduct such studies should have access to as much data as possible. If the patient data is isolated and stored on multiple systems that do not allow the information to be shared, really relevant studies are very difficult to be achieved. Blockchain provides a reliable solution to this specific challenge. When applied correctly, blockchain will allow improved security, data sharing, interoperability, data integrity, and real-time update and access [11].

An important problem facing the healthcare system is the quality and authenticity of medicines and medical materials purchased through various supply chains. Counterfeit or fake medicines represent a serious problem in the pharmaceutical space and may constitute a major financial loss and, worse, they can endanger patients' health. A blockchain-based supply chain would solve such problems.

A supply chain system involves the flow of goods and products from the initial stage to the final one. Usually, there are more entities involved in this route, and therefore the proper operation of a supply chain is crucial for businesses.

In a blockchain-based system, provenance tracking becomes easy and possible at any time, as well as the history of a product from its origin to where it is at a certain moment. Such a system ensures an accurate provenance tracking traceability across the supply chain and can detect possible frauds in any part of it, reducing the risk of spreading counterfeit products.

One may ask which type of blockchains is best suited for the healthcare sector. A proper solution could be a set of integrated private blockchains. Hospitals, clinics, medical offices and laboratories, rehabilitation sanatoriums, researchers in the health field could be the users of a blockchain storing patients' medical records: the history of diseases from birth to the present, current symptoms, recommended analyzes and their results, imaging investigations, established diagnosis, treatments, prescriptions, disease evolution, etc. This blockchain could be connected to the blockchain of medical insurance companies and with that of the pharmaceutical industry, which users are manufacturers of medicines and medical products and pharmacies that sell these goods to the population. In turn, the pharma blockchain should be connected to the supply chains of raw materials, from origin points to manufacturing companies, including all intermediaries on this route.

In this way a complex collaborative system would be created that would be beneficial to all participants and, finally, would provide high-quality services to its end-users, patients.

5 Conclusions

"*The blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value.*" [13]

Blockchain technology is based on the idea of a distributed database where trust is established through mass collaboration and clever code rather than a single authority that is responsible for authentication, validation, and settlement. It is an advanced technology that is expected to alter almost every industry in the coming years. By allowing digital information to be distributed but not copied, altered, or deleted, it might be considered the foundation of a new type of internet.

Blockchain is a technology allowing users to create a transparent, secure, and immutable system that can record any kind of transactions or information. There is no need for a third trusted party; users rely on the technology itself, following predefined rules to meet consensus.

Blockchain technology could revolutionize the way that health data is stored and transmitted. With blockchain, healthcare systems can store medical records confidential and secure-.

In the financial sector, blockchain is expected to change the way stock exchanges work, loans are bundled and insurances are contracted. Because they will not need any third party, any intermediaries, they will give up all services offered by banks. This will lead to cost decreasing, by fees elimination.

The technology can be used to track raw materials or products across a supply chain, or to track ownership of assets. The transparency of a blockchain-based system can help to see the complete product's route from its origin, thus helping in eradicating the circulation of fake products. Assets as diamonds, fine art, or property titles are susceptible to be counterfeit, but a blockchain can ensure their authenticity.

A distributed ledger of certificates and degrees issued by universities would lead to the detection of false diplomas and would be able to check and certify somebody's qualification.

Copyrights can be protected by a blockchain-based system. A blockchain for the intellectual property could help authors, owners or users to get clarity of copyright. Once they register their work in the blockchain, they will own the evidence which will be tamper-proof. As once entered in the blockchain the content of a block cannot be modified, the owner of the work will have the overall authority over the ownership, as well as the distribution of the content [10].

In an electronic voting system, blockchain technology can provide transparency and can ensure that the election was fair and legitimate, eliminating potential frauds or human errors. Each vote would be stored as a block on the blockchain, making them almost impossible to modify. The blockchain protocol would also maintain transparency in the electoral process, reducing the personnel needed to conduct the elections and provide officials with real-time results [12]. Furthermore, its resilience is determinant in preventing cyber-attacks against the voting system.

A blockchain acts as a decentralized system that records and documents transactions. It's a distributed transaction ledger that maintains identical copies across each node within a network, which facilitates the security of the blockchain.

Blockchain-based systems have all essential security needs covered. Because it operates in a distributed network, a blockchain cannot be affected by hackers, who can only disrupt a single node and not the functionality of the whole network. Thanks to decentralized hosting and encryption, such a system is entirely self-sustained [14].

We can assume that blockchain technology is here to stay. Blockchain will not replace traditional relational databases that companies exploit nowadays, but it opens new doors for the storage and distribution of transactional data inside and outside them. What must not be forgotten is that any blockchain project is a long-term strategic initiative.

References

[1] D. Bayer, S. Haber, W. S. Stornetta: "Improving the Efficiencies and Reliability of Digital Time-Stamping", *Sequences 2*, pp. 329-334, 1992, available at https://link.springer.com/chapter/10.1007/978-1-4613-9323-8_24

[2] Blockchain For Dummies: The Ultimate Guide (2020). Available at https://cryptomaniaks.com/guides/blockchain-for-dummies-ultimate-blockchain-101-guide

[3] S. Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System (2008). Available at https://bitcoin.org/bitcoin.pdf

[4] L. Mearian: What is blockchain? The complete guide (2019). Available at https://www.computerworld.com/article/3191077/what-is-blockchain-the-complete-guide.html

[5] A. Rosic: What is Blockchain Technology? A Step-by-Step Guide For Beginners (2016). Available at https://blockgeeks.com/guides/what-is-blockchain-technology/

[6] What is blockchain? Available at https://www.euromoney.com/learning/blockchain-explained/what-is-blockchain

[7] T. S. Rodriguez: Blockchain for Dummies. The five keys to understanding what is the Blockchain (2018). Available at https://medium.com/swlh/blockchain-for-dummies-d3daf2170068

[8] B. Marr: What is Blockchain? Available at https://www.bernardmarr.com/default.asp?contentID=1389

[9] H. Anwar: 6 Key Blockchain Features You Need to Know About (2018). Available at https://101blockchains.com/introduction-to-blockchain-features/

[10] M. Pratap: Blockchain Technology Explained: Introduction, Meaning, and Applications (2018). Available at https://hackernoon.com/blockchain-technology-explained-introduction-meaning-and-applications-edbd6759a2b2

[11] M. Pratap: Blockchain in Healthcare: Opportunities, Challenges, and

Applications. Available at https://engineerbabu.com/blog/blockchain-in-healthcare-opportunities-challenges-and-applications/

[12] Blockchain Explained. Available at https://www.investopedia.com/terms/b/blockchain.asp

[13] Tapscott, Don; Tapscott, Alex: Here’s Why Blockchains Will Change the World (2016). Available at https://fortune.com/2016/05/08

[14] N. Reif: How Does Blockchain Work? (2020). Available at https://www.investopedia.com/tech/how-does-blockchain-work/

Gheorghe MATEI has graduated from the Faculty of Planning and Economic Cybernetics in 1978. He achieved a Ph.D. in Economic Cybernetics and Statistics in 2009, with a thesis on Business Intelligence systems in the banking industry. His fields of interest include Business Intelligence systems, data warehousing, decision support systems, as well as innovative technologies such as blockchain and the Internet of Things. He is a co-author of the book “*Business Intelligence Technology*” (2010), as well as author and co-author of several articles in journals, international databases, and proceedings of national and international conferences in the mentioned domains.