CHAPTER SEVEN

Benefits and use of blockchain technology to support supply chain during COVID-19

Giuseppe Ciaburro
Department of Architecture and Industrial Design, Università degli Studi della Campania Luigi Vanvitelli, Borgo San Lorenzo, Aversa, Italy

1. Introduction

Blockchain is a decentralized distributed database consisting of a chain of blocks, containing chronologically correlated transactions validated by a system of cryptographic algorithms and rules. The data, once entered within the blocks, can no longer be modified without the consent of the majority of the system (Nofer et al., 2017). Each record is stored in such a way as to contain a portion of data referable to previous transactions: This connection makes alteration virtually impossible without it being immediately visible to the entire network. In turn, the blocks to become part of the chain are subjected to a validation process based on the principle of distributed consent, a consent that makes superfluous the figure of a supervisor to ensure its legitimacy. The blockchain is therefore a decentralized ledger based on the principle of distributed trust which, thanks to its innovative configuration, does not require a third party who guarantees its incorruptibility because it is its very nature that protects it (Zheng et al., 2018).

Our company is facing an important challenge that no technology has been able to solve so far. This is the so-called trust gap which defines the degree of trust on the part of users in making a transaction. Today, in fact, it is not possible to execute a transaction without the intermediation of a third party in which the contracting parties place their trust (Wüst and Gervais, 2018). But according to some scholars this model, due to its inefficiencies, is doomed to fail. In this regard, there have been numerous crises that have hit the economic system in recent decades, most recently the financial crisis of 2008 which originated from the collapse of the US banking giant Lehman and Brothers. These critical issues have brought user confidence levels to an all-time low in regard to institutions (Li et al., 2020).

Lessons from COVID-19
https://doi.org/10.1016/B978-0-323-99878-9.00003-0

The Internet that once promised to be a strength for democratic information has divided public opinion, facilitated the spread of fake news, and allowed populists to foment contempt for journalists, scientists, and real facts. Until then, the only way to carry out digital transactions of any kind was entrusted to the validation by an intermediary, who confirmed the identity of the contracting parties and the consistency of the declared assets (Klems et al., 2017). Intermediaries such as banks and large social media have thus become the guarantors of trust and consequently the guarantors of the operation. This system has obvious limitations, is senselessly slow, expensive and can suffer cyber-attacks. In addition, the profit created by the digital revolution has been distributed asymmetrically to large intermediaries (Dinh et al., 2018).

Before the birth of the blockchain, any digital asset was infinitely copyable. There was no technological mechanism capable of confirming or not, without the control of an intermediary, that a certain amount of money had not already been spent. To date, when information is exchanged on the Internet, using the http protocol, an exact copy of the data to be transmitted is sent to the recipient (Pilkington, 2016). Obviously, if the transaction or exchange of information has money as its object, this mechanism cannot be adopted unless an intermediary comes into play. This is because, when a transaction is made, it is the single entity, the single information that must be sent and not a copy of it. Thanks to the contribution offered by the distributed database, it is in fact possible to avoid that a given sum of money is the subject of more than a single transaction, thus solving the problem of double spending. Thanks to blockchain technology, a new system has been established in which trust is not in the hands of intermediaries but is established through cryptography and intelligent code: Trust is the basis of this new medium of exchange (Yli-Huumo et al., 2016). A blockchain allows to eliminate the intermediary allowing the parties to trust the system through the mechanism of consent. Consensus is the foundation on which distributed systems are structured. The blockchain is a tool that allows to reach consensus in the execution of a collective activity that involves entities that do not necessarily trust each other, but that have a common goal (Risius and Spohrer, 2017).

A Supply Chain is a network of individuals, organizations, resources, activities, and technologies involved in the processes of creating and selling products or services, from raw materials to the final product (Mentzer et al., 2001). The primary objective of a supply chain is to satisfy demand in the quantities, time and place required with the lowest possible cost, bringing added value to the end customer (Beamon, 1998). Within the supply networks there are a certain number of entities, which have a common interest, but which, at the same time, are separate and therefore do not necessarily trust each other. Supply Chain Management (SCM) is the management of this supply network, which aims to integrate the organizational units along the supply chain and coordinate material, information, and financial flows to satisfy customer requests, improving the competitiveness of the supply chain (Min and Zhou, 2002). The supply chain must be conceived as a value system to which all the players in the chain contribute. The success of the entire system depends on the ability of the individual players to interact with each other. The continuous connection between all the nodes of the network and at the same time between the companies and the final customers becomes an essential element and the basis of a new business model in which the physical and information flows must be extended beyond the boundaries of the company. Blockchain technology has the potential to fundamentally change supply chain management (Casado-Vara et al., 2018). The use of smart contracts to manage supply relationships, the tracking of products and information at every level of the supply chain, the birth of decentralized marketplaces are just some of the applications of this technology (Amr et al., 2019).

In this chapter we will first introduce the basic concepts of blockchain technology, and then move on to the analysis of the essential characteristics of the supply chain. Finally, the applications based on blockchain technology adopted to address the difficult emergency due to COVID-19 will be analyzed, focusing attention on Blockchain-based solutions for the management of the anti-COVID-19 vaccination campaign.

The chapter is organized as follows: In Section 2, Blockchain technologies are described in detail. Fundamental topics such as consent, transaction, smart contract, and proof of work are addressed. Section 3 introduces the essential concepts of the supply chain, analyzing the applications of these concepts in different fields. Section 4 explores examples of applications of Blockchain technology in the management of the COVID-19 pandemic with reference to the administration of vaccines. Finally, Section 5 summarizes the essential points of the work.

2. Introducing blockchain basic concepts

A blockchain is essentially a transactional ledger distributed between nodes connected in a peer-to-peer communications network. To record a transaction, an agreement must be reached between the participants through a consent mechanism: No one will be able to modify the data without the permission of the other participants (Cachin, 2016). By sharing the database across multiple nodes, the blockchain eliminates the need for intermediaries, which were previously required to verify, coordinate and record transactions. Despite its recent history, the blockchain is evolving toward multiple applications and declinations, even moving away from the original concept of Bitcoin, developed by Nakamoto. The birth of Blockchain technology coincides precisely with the appearance of Bitcoin, which constitutes its first historical application. Everything, therefore, begins in November 2008, when the mysterious Satoshi Nakamoto publishes a paper (Nakamoto and Bitcoin, 2008), which illustrates the operation of the Blockchain technology as originally conceived. Bitcoin was born as a tool for the realization of a well-defined project: Creating a virtual payment system independent of institutions. Compared to other virtual currencies, Bitcoin has achieved relatively wide circulation since it was the first to solve the double-spending problem. This consists of making a digital transaction while maintaining the original copy of the exchanged currency (Badertscher et al., 2017). To solve this risk, Bitcoin has exploited distributed ledger technology, which replaces the centralized intermediary in its role of recording each transaction. But since anyone can read and write to the ledger, security issues could arise if any actor attempts to tamper with the ledger. Bitcoin offers a solution to this problem by creating an incentive to behave correctly (Garay et al., 2015). Some actors, called miners, group transactions into blocks by solving a computational problem, called proof of work, which requires hardware with a high computing capacity. Miners who successfully create a block are rewarded with Bitcoin, thus creating a strong incentive to act correctly. In fact, the mining process, in addition to being expensive from a computational point of view, requires an enormous amount of electricity, thus discouraging any hackers to act incorrectly (Calvão, 2019).

A blockchain network is made up of nodes, defined as computational entities that communicate and work jointly with other nodes to complete a transaction: A node can operate on both physical and virtual hardware. In most blockchain networks, each node performs a certain action, such as generating and propagating blocks. In these networks one or more nodes will temporarily assume the role of leader, however, in some networks the nodes play multiple roles instead (Zheng et al., 2017). In a centralized network, all resources, hardware, and software, are stored in a single point. All other systems must connect to this node to have access to resources whenever they need them. While this system offers more control, it is not transparent and furthermore, if you pass this single point of access, you will have access to all data. A decentralized system allocates hardware, software, and computational resources in different workstations. The resources are then divided between the nodes and each node requests the resource it needs to use from the other (Belotti et al., 2019). This structure attributes effective features to the chain (Fig. 1).

The blockchain is therefore a distributed ledger of blocks that holds valid transactions that have been performed on the peer-to-peer network. Each block contains a timestamp of creation and a hash, or pointer, that links each block to the previous one: This continuous link forms a chain. The distributed structure is the key feature concerning the blockchain. A distributed network, unlike centralized and decentralized networks, is a system where data and resources are replicated on various nodes. Each node keeps a record of the transactions between the various nodes on the network. The nodes identify themselves with each other via the IP (Internet Protocol) address, while each node can send a transaction to any other node on the network if it knows the recipient's public key, without any central authority involved in the transaction. The absence of a central server therefore strengthens the security of the system (Aste et al., 2017).

In a peer-to-peer network, nodes can communicate directly with each other without the need for a central authority. There are no hierarchies as each node is at the same level but, depending on the type of blockchain, the nodes can however perform different functions, such as miner, validator, database, etc.

2.1 Distributed databases

Information systems architectures have developed and evolved over the years, passing from centralized schemes to distributed and widespread

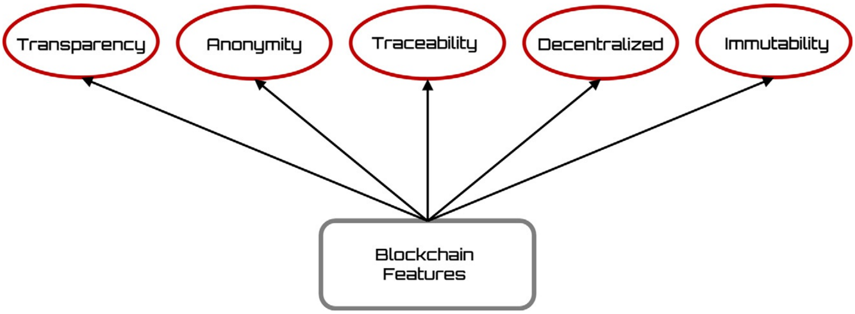

Fig. 1 Blockchain features.

models, more responsive to the decentralization and cooperation needs of modern organizations (Ceri, 2017).

A centralized computer system is therefore characterized by the fact that the data and applications reside in a single processing node, while a distributed computer system is characterized by at least one of the following two conditions:

1. The applications, cooperating with each other, reside on several processing nodes (distributed processing)
2. The unitary information assets are hosted on several processing nodes (distributed database)

When an organization is geographically distributed, it can choose to store its database on a central server or to distribute it to several local servers. A distributed database is a single logical database physically spread over several computers connected to each other by a telematic network. We emphasize that a distributed database is truly a database, not a series of files. The distributed database is still centrally managed as a business asset, providing local flexibility and customization capabilities. The network must allow users to share data, so a user in location A must be able to access the data stored in location B. Sites in a distributed system can be spread over a large area or a small area. Computers can range from PCs to large servers or even supercomputers (Muzammal et al., 2019).

A distributed database requires multiple instances of a Database Management System (DBMS), running on each remote site. The degree to which these different DBMS instances collaborate or work in partnership characterizes the different types of distributed database environments. It is important to distinguish between distributed and decentralized databases. A decentralized database is similarly stored on computers in multiple locations; however, the computers are not linked together by a network to make the data appear to be stored in a single logical database (Fig. 2). Thus, users located at the various sites cannot share data. A decentralized database can be thought of as a collection of independent databases, rather than having the geographic distribution of a single database (Halaburda, 2018).

A distributed system is therefore made up of a set of spatially separated autonomous entities that communicate and coordinate their respective actions with each other through the exchange of messages. The reasons that push an organization to choose to distribute data across multiple sites may be different, and we will analyze some of them below. Modern organizations are often geographically distributed, sometimes even across national borders. In some cases, each unit has the power to create its own information systems,

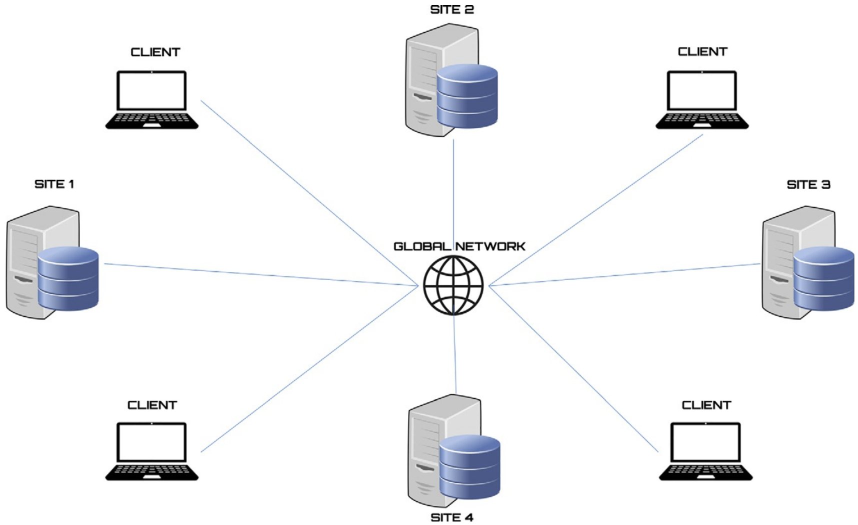

Fig. 2 Distributed database architecture.

and these units process local data over which they cannot have control. Corporate mergers and acquisitions frequently create such conditions (Chowdhury et al., 2018). Another reason is that of the need to share data; decisions in moderately complex business environments require sharing of data between different work units, so it is necessary to consolidate data through local databases accessible on demand. To all this are added economic reasons related to the costs and reliability of the system. The costs of managing large amounts of data across a communications network or managing a large volume of transactions from remote sources can still be high, even though they have dropped significantly recently. So much so that in many cases it can be cheaper to store data and applications where they are needed. Furthermore, the dependence on communication systems by the database always involves an element of risk, which determines the need to have local copies or fragments of data to guarantee the reliability of the system and rapid access to data throughout the organization (Lo et al., 2017).

Today, many organizations purchase packaged application software from various vendors. Each package is designed to work with its own database, and possibly with different database management systems. A distributed database can, in this case, be particularly useful for providing functionality to applications.

Replicating data from distributed databases across several separate computers is a strategy to ensure that a damaged database can be quickly recovered, and users can have access to the data while the primary site is being restored. Replicating data across multiple sites is a natural form of a distributed database. Replication is a typical property of the distributed DBMS that allows you to allocate the same portions of the database on different nodes. Replication is considered useful to reduce the transfer of information between the different nodes within the same transaction or query. The use of replication increases the locality of the data used by each application but introduces the problem of multiple transactions, that is, transactions to be performed on multiple nodes simultaneously (Tapscott and Tapscott, 2017).

2.2 Distributed database security

In recent years, the storage, retrieval, and sorting of information have become increasingly important in many sectors of society, this has led to growing attention to issues related to database security. As regards some fields of use of databases, we can even say that data security is to be considered a priority aspect over others, in fact, while an incorrect design, which provides a very slow but safe database, could also be accepted by a banking institution, a well-optimized database that allows anyone to modify its data would be clearly unacceptable for any company (Rhee et al., 2005).

Data security generally includes two aspects:

1. data protection using encryption techniques
2. control over access to data.

While the problems related to cryptography to secure the storage or sending of data are common to many IT sectors, the problem of controlling access to data, which we will deal with, is more specific to traditional and distributed databases.

We can enumerate three basic security stages for each database:

1. user authentication
2. control authorization to view the data
3. prevention or reduction of attacks through inference channels

The first two points can be shown with a common situation for a database. When a user requests access to the system, the first task of the DBMS is to positively authenticate it, usually via the user-id/password pair; once connected to the system, the user will presumably submit queries to the database, before replying it is again the task of the DBMS to ensure that the user is authorized, by the database administrator, to view the requested data (Bertino and Sandhu, 2005).

The last point is a problem specific to relational databases and is based on the possibility, by unauthorized users, of obtaining confidential information through logical procedures without accessing the protected data.

Generally, we can assert that the problems related to the three stages presented can be solved in traditional databases with common sense, experience and above all with careful planning. As far as distributed databases are concerned, however, the scenario is considerably complicated. In fact, the possibility of designing and implementing a distributed database in various ways means that the resolution of security problems raises conceptual questions even before implementation (Maurya et al., 2020).

Returning to the security stages of a database, user authentication is a prerequisite for each system, correct identification allows, in fact, to determine the user's privileges and group. During the design phase of a distributed database, the first question to ask, regarding security, is who will be responsible for authenticating users.

2.3 Elements of a blockchain

Blockchain technology is characterized by its constituent elements which, through a synergistic process, create a complex system capable of returning an automatic system of transactions (Sherman et al., 2019). The constituent elements of a Blockchain are listed and described in the following list (Fig. 3):

- Transaction: The transaction is that good, value or information that is exchanged between two or more subjects on a blockchain platform and that needs to be approved and verified and archived. It consists of information regarding the transaction and a Cryptographic Key, which is a set of public key cryptographs that allow the verification of users' identity (Durach et al., 2021).
- Cryptography: Cryptography is the discipline that studies how to make information secure, that is, confidential and intact, by taking a plaintext and transforming it into ciphertext, which is incomprehensible to those who do not know the details of the transformation. Confidentiality is a concept like privacy but is only one component of it: it refers to the ability to protect data from those who are not authorized to read it. Integrity, on the other hand, refers to the ability to protect data from unauthorized changes (Fernández-Caramés and Fraga-Lamas, 2020). To protect information with encryption, it must be transformed into something equivalent but not decipherable and not easily traceable to the original: this is

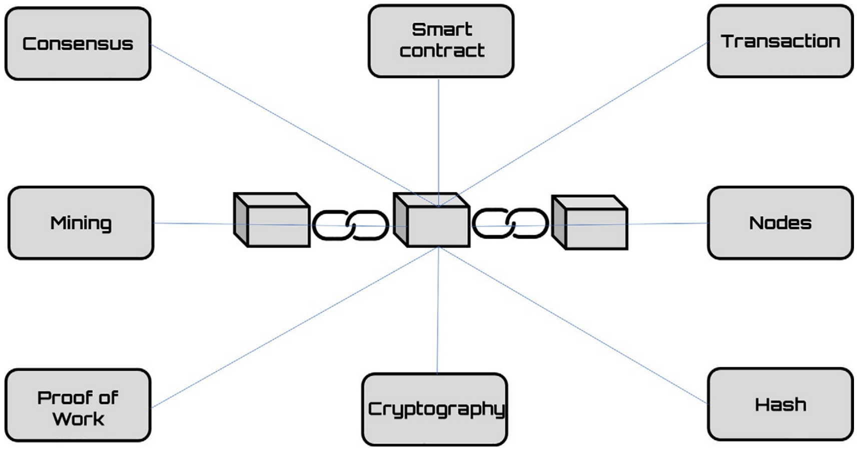

Fig. 3 Key elements of a blockchain.

the act of encryption. Deciphering, on the other hand, is the reverse operation: from an encrypted communication its original, clear, and intelligible form is obtained again. A well-defined procedure for encrypting and decrypting data is called a cryptographic algorithm and, to work, it may require the use of one, no or more keys, conceptually like the passwords we are used to using. A system based on public key cryptography is reliable and secure since it does not require the seller to use the buyer's private information, such as his credit card number. Transactions take place through the exchange of signed information.

- Mining: Mining is the process that creates new blocks, validated, and adds them to the Blockchain; the nodes that carry out the mining process are called miners. Each miner goes through a series of steps that lead to the production of a new block: It collects and decides which information, gathered from the peer-to-peer network, to include in a new block. Verify that all transactions it included in the block are valid. It selects the most recent block in the longest branch of the block chain and inserts a hash of that block into the new block it is creating. He tries to solve the proof of work for the new block and at the same time observes what other new blocks are created by other nodes. If it finds a solution to the proof of work problem, the new block is added to the chosen chain and shared on the network. If another node solves the proof-of-work problem first, its block is subjected to validity checks. If it is valid, it is added to a local copy of the Block Chain and shared on the network, otherwise it is discarded. As miners try to create new blocks simultaneously, with most of their time spent solving the proof of work problem, it happens that there are different versions of the Blockchain at a given time (Wang et al., 2019). This happens because new blocks are created regularly every 10 min, so during this time all nodes try to solve the proof of work. When a node finds a valid solution, it earns a certain number of bitcoins as a reward, provided for by the protocol, shares the block on the network and the nodes that receive the new block, after verifying it, add it to their chain, starting to work on a new block. In this way the nodes synchronize approximately every 10 min.

- Nodes: A node is any hardware device capable of communicating with other devices belonging to the same network. The various nodes are connected to each other and each of them also acts as a server for the management of transactions within the network.
- Consent: Consensus protocols are essential as they allow the proper functioning of any blockchain system. In practice, these are the algorithms that regulate the transaction validation mechanism and establish the rules by which such transactions are transcribed on the latter to form blocks. It is precisely these consensus mechanisms that break the paradigm of the more classic centralized consensus in favor of institutions around the world (Benchoufi et al., 2017). The consensus mechanisms guarantee that the information aggregated to the blocks is true and reliable, two of the most used mechanisms are the proof of work (PoW) and the proof of stake (PoS).
- Proof of work: It plans to put the miners of the network in competition, offering compensation in cryptocurrency for the resolution of a series of very complex computational problems to validate and add a block of transactions within a chain. This approach is characterized at the same time by an almost perfect security, to the detriment of what are perceived as the main limitations of proof of work, that is, slowness and high energy expenditure (Kumar et al., 2019).
- Smart contracts: Indicates computerized contracts programmed to be executed automatically, when preset conditions are fulfilled. Although the smart contract can also be conceived independently of the blockchain, only the characteristics of the latter guarantee that the smart contract cannot be modified and the automatic execution of the computer code that is its essence. In other words, smart contracts do not necessarily have to exist in a blockchain, but only blockchain technology and its platform are, at present, capable of providing them with the security

and reliability that allow them to overcome the need for recourse to a third-party authority and intermediaries. The smart contract, in essence, represents one of the possible applications of the blockchain, among the most advanced and interesting, and it is therefore necessary to treat the two institutions as intimately connected and connected (Singh et al., 2020).

- Hash: The hash code of a block represents its authentication code. It can be considered as the digital signature that determines its uniqueness and ensures the inviolability of the entire block. The hash of the reference block records all the information relating to, while the hash with the information relating to the previous block allows you to create the chain and link one block to another. In practice, it starts from a variable-length data string (input) which is then processed by the hash function, transforming the string to a predefined length (Ren et al., 2020).

2.4 Blockchain architecture

Every single block of a Blockchain is a structure that records transactions that will then be included in the register. A transaction is a change of state that changes blockchain data from one value to another. A block includes the block header, a list of valid transactions, the hash of the previous block and its hash: A single block can contain many transactions. If a block is tampered with, the hash changes and the corresponding hashes of all subsequent blocks in the chain will also need to change for the chain to still be recognized as valid: This waterfall pattern ensures that a block cannot be changed without forcing a change in at least 80% of the blocks of the chain (Syed et al., 2019) (Fig. 4).

The enormous computational and energy power required to carry out this operation makes the blockchain practically immutable: The greater the number of blocks that have been added to the chain, the greater the security of the system. The block header contains three sets of data: the pointer to the previous block (hash), a series of information such as timestamp and proof of work and finally a report of all the transactions contained in the block. The first block in a chain is called the genesis block and each new block is added on top of the previous one. Therefore, each block can be identified in two ways: through its cryptographic hash or through its position in the chain identified by the block height, which defines the number of blocks that precede it in the blockchain (Vincent et al., 2020). The position of a block in the chain or its distance from the genesis block can be used to

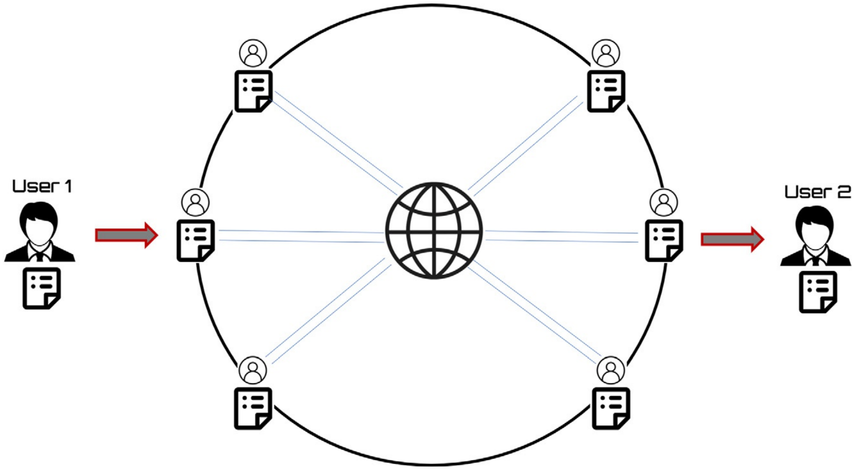

Fig. 4 The Blockchain architecture.

identify the block. However, this position may not be unique due to the presence of bifurcations in the chain (fork). A hard fork occurs when updates are made to the programming language or technology underlying the blockchain. In the context of cryptocurrencies, if the fork were not resolved, it would lead to two different versions of the coin, which could compromise its value. The number of confirmed blocks in the entire Blockchain is called Block Height.

2.5 Blockchain operation

Each node on the network has a set of keys: one private and one public. The private one is used to encrypt the transaction before it is sent. To send a transaction, the sender needs his private key and the recipient's public key. Before being registered on the Blockchain, the transaction must undergo two phases: one for signature and one for verification (Fu and Zhu, 2019). The data encryption by the sender through the private key is defined as the signing phase. The verification phase, on the other hand, consists in the solution of a computational problem (proof of work), which ensures that the same transaction does not occur twice. Proof-of-work involves looking for a value that, once hashed. In this phase, the time stamp of the block also takes place, which further strengthens the security of the chain by associating the block with a legally valid date and time (Niranjanamurthy et al., 2019). The transaction mechanism can be divided into five stages (Fig. 5):

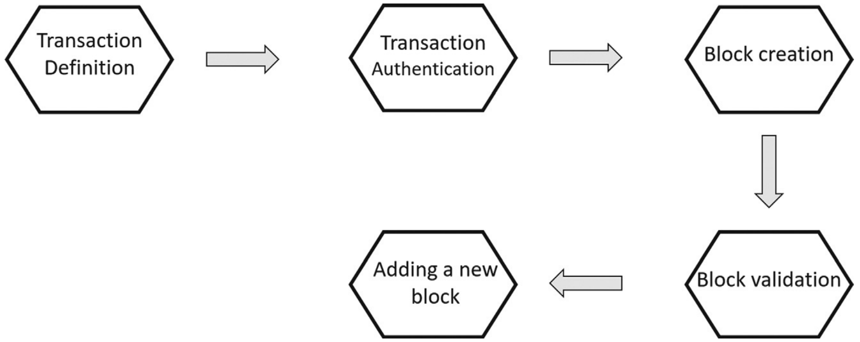

Fig. 5 Transaction mechanism.

1. Transaction definition: The sender generates the transaction by specifying the recipient's public key details and the transaction value. Additionally, this transaction must be authorized with the sender's cryptographic digital signature, which verifies that the transaction is valid and secure.
2. Transaction authentication: Once sent to the network, the transaction is received by the nodes, which authenticate it by decrypting the digital signature. This transaction waits in a pool of pending transactions until a block is created.
3. Block creation: Each node of the network takes charge of the transaction combining it with other pending transactions and creating a block. Subsequently, each node works to solve the proof of work related to its block and, once solved, they transmit it to all the other nodes.
4. Block validation: The nodes in charge of validating the received block accept it only if all the transactions in it are valid and have not already been spent.
5. Block chain: After each transaction recorded in a block has been accepted, the new block is connected to the last block in the chain. The updated version of the chain is then sent to the network, which accepts it as the updated version on which future blocks will be recorded. The nodes express acceptance of the block by attempting to create the next block in the chain, using the hash of the block accepted as the previous hash.

The blockchain is a system that uses cryptography to secure transactions. This concept leads to a redefinition of the intermediary's role as guarantor of the validity of the system. Trust is now based on the consensus mechanism, a process in which most validators in the network come to an agreement regarding the state of the registry (Dogru et al., 2018).

The main elements of a consensus mechanism are:

- Decentralized structure: No central authority can finalize processes or transactions
- Quorum: Nodes exchange messages through a predefined set of steps
- Authentication: This protocol is used to verify the identity of the participants
- Integrity: Strengthens the validation and verification of the integrity of the process
- Nonrepudiation: Used to verify that the sender has sent the message
- Privacy: This protocol ensures that only the actual recipients of a message have access to it
- Error tolerance: Network configuration that ensures that the efficiency and speed of operations are not compromised by the failure of individual nodes or servers.

For example, the consensus mechanism exploited in Bitcoin cryptocurrency is based on the longest chain mechanism, where the chain with the greatest proof of work is defined as the valid one. However, some limitations of the original Blockchain technology have facilitated the exploration of new consensus mechanisms. New platforms have tried to create more scalable and more energy efficient mechanisms to reach consensus among the network nodes. The "proof of work" (PoW) mechanism consists in solving a mathematical computational problem to link the hash related to the transaction with that of the last block registered on the blockchain. However, this computational process must be supported by very powerful hardware, which therefore will require a substantial supply of energy (Dhillon et al., 2017). By multiplying the energy consumed for a single transaction by the total of transactions required per second, there will be a large demand for both electrical and computing energy. To compensate for the increase in hardware speed over time, the difficulty of proof-of-work is determined by a moving average that aims to create an average number of blocks per hour. If the blocks are generated too fast, the difficulty increases. The "proof of stake" (PoS) mechanism represents a valid alternative to the PoW scheme, as it is based on a more efficient computational procedure. Even though the blocks are generated in a similar way to the PoW, the hashing procedure takes place in a limited search space, instead of the unlimited space of the PoW. In this way the transaction can be processed in less time and the system will be faster and require less energy (Kim and Deka, 2020). However, this system is not without risks, in fact, the probability that a miner is chosen for the creation of a block depends on the quantity of "coins" it possesses and not on the computational power.

3. Supply chain explained

A Supply Chain is a network of individuals, organizations, resources, activities, and technologies involved in the processes of creating and selling products or services, from raw materials to the final product (Stevens, 1989). The primary objective of a supply chain is to satisfy demand in the quantities, time and place required with the lowest possible cost, bringing added value to the end customer. Supply Chain Management (SCM) is the management of this supply network, which aims to integrate the organizational units along the supply chain and coordinate materials, information, and financial flows to meet customer requests by improving the competitiveness of the supply chain (Lambert and Cooper, 2000).

Supply Chain Management is a network of distribution facilities and means whose function is to obtain materials, the transformation of these materials into intermediate products and finished products, and the distribution of these finished products to the end user (Fig. 6). Use synchronized and efficient processes that generate value for the company. A supply chain consists of three parts: procurement, production, and distribution (Mentzer et al., 2001). The supply part focuses on how, where and when the raw materials for production and the different services required are purchased and supplied. Supply Chain Management becomes a management model that integrates human capital, processes, and technology. The goal is to synchronize and integrate the flow of materials and services, the flow of information and the flow of money of an organization. Currently, supply chain management is a vital issue in business and is taking on a prominent place

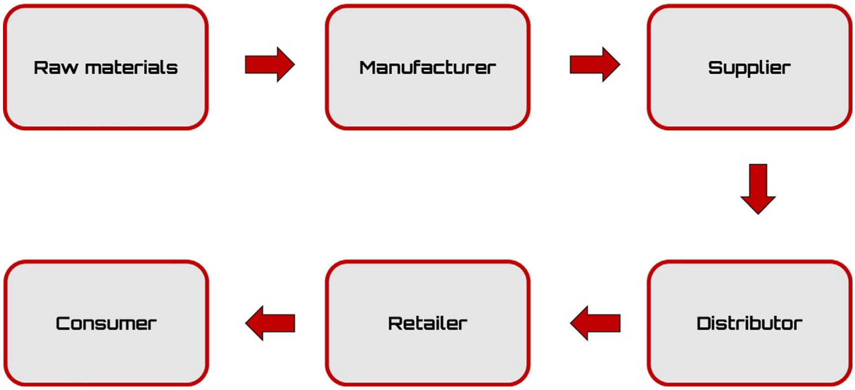

Fig. 6 Supply Chain Management flow.

around the world. With increasingly competitive markets, we need to have a very efficient use of resources. We live in a highly globalized world, where corporate supply chains have improved exponentially. In the past it was believed that the logistics area did not generate value for the company, but today all successful international companies have improved their supply chain through its implementation and, consequently, reduce costs and optimize processes to obtain a worldwide advantage (Davis, 1993).

Crucial in the management of the supply chain is the correct management of the supply chain, which represents a chain in which each node must function and return a product that meets expectations. A problem in the chain gear leads to low product quality that generates a bad reputation of the company, no customer loyalty, poor product acquisition or in the worst-case total rejection by the customer (Beamon, 1998).

It therefore becomes essential to associate the planned activities with a control system of the effectiveness of each step of the process. For this control to be fully effective, it must be carried out by an independent body acting as guarantor. Only in this way will the trust of all components of the supply chain be ensured. In this context, Blockchain-based technologies can provide that added value to ensure technological progress imposed by the new paradigms of Industry 4.0 (Min and Zhou, 2002).

3.1 Supply chain basic concepts

A supply chain is made up of all parties involved, directly or indirectly, in satisfying a customer request. It includes not only the manufacturer and suppliers, but also transport, warehouses, retailers and even the customers themselves. Within each organization, the supply chain includes all the functions necessary to receive and satisfy a customer request. These functions include, but are not limited to, new product development, marketing, operations, distribution, finance, and customer service. All these functions can be summarized in a matrix that highlights the various steps and planning activities necessary for each organization area (Croxton et al., 2001).

This definition highlights two contexts: intraorganizational context and interorganizational context. In the intraorganizational context, decisions are made regarding sales order processes, demand forecasting and planning, distribution, procurement, and production planning. In the interorganizational context, on the other hand, a company is involved in a network of customers and suppliers who exchange flows of materials and information with each other (Hugos, 2018).

The network of a supply chain consists of facilities, transportation resources, storage resources, human capital, and inventory. Its complexity is determined by the fact that each independent organization can have one or more suppliers and customers who in turn could have as many suppliers and as many customers. In addition, logistical third parties may be involved, which can provide goods or services to the company and send them back to the company itself or directly to the customer. Within this network, material, information, and money are exchanged between the various levels. It is precisely because of this high complexity that the complete management of every constituent element of the chain is essential, which also includes cost reduction among the objectives. The supply chain must efficiently integrate all its actors in such a way as to minimize costs at the system level and satisfy high service targets. Regardless of the type of production, industrial sector or size, every company needs to control the flow of materials from the supplier to the end customer as an essential step to achieve a good level of service. Therefore, as a key block in the supplier-customer chain, product distribution and procurement need to be managed properly within companies, without underestimating their importance (Ellram, 1991).

The operations in the modern supply chain are very complex and consist of some phases ranging from the receipt of raw materials to the delivery of the final product to the consumer. The process consists mainly of the following stages:

- Determination of the availability of raw materials and costs. Before the product can begin to be made, it is important to plan where and how the raw materials can be purchased, the time needed to receive them and the quantities available.
- Transformation of raw materials into finished products. This phase varies from company to company, depending on the structure and organization.
- Finished products are shipped to the distribution center through a distribution network planning.
- The distribution facility uses the products to supply a retail store on time.
- The products are delivered into the hands of the consumer with the aim of fully satisfying his needs.

From the procurement of raw materials to the final delivery of goods, companies rely on the supply chain to manage the procedure quickly and efficiently. Supply chains determine when the product must be made, delivered to the warehouse and storage centers, and finally delivered to a retail store or shipped (Simatupang and Sridharan, 2002).

It is a rather complex procedure which, being widely variable, is based on past experiences and future forecasts that try to consider delays and other volatilities. Today's supply chains are under pressure from many points of view, trying to keep up with an increasingly demanding environment. Phenomena such as Industry 4.0, globalization and digitization translate into an increasingly complex, hyperconnected business context, in which data and information are the masters. In today's world, customer service needs, working capital and operating costs are set to rise, and supply chain leaders in many industries are reporting increasing chain complexity. The supply chain landscape is changing faster than ever, leading many companies to reduce investment to survive (Thomas and Griffin, 1996).

Since traditional supply chains are fragmented and operate through independent organizations that focus primarily on local optimization, most of today's supply chains appear as analog machines attempting to solve the problems of a digital world. They appear as decentralized structures, which are unable to survive in the new business environment. The major operational challenges that must be faced are:

- Response times: The current supply chain structure, built on independent silos, ensures that the decision-making process is linear. The passage of information from one functional structure to another is therefore long and laborious, creating wasted time and delays that result in response times to the market that are too high for the current context.
- Lack of visibility: Traditional supply chain processes and the technologies used do not allow for end-to-end visibility along the chain. This lack of visibility is evident at the ordering, production, and shipping level. It therefore results in imprecise and not always consistent planning, which causes an increase in unnecessary costs, as well as a difficulty and inability to detect specific problems that could spread throughout the entire network.
- Conflicts of priorities: Independent organizations in a supply chain are characterized by their metrics, their Key performance indicators (KPIs) and their priorities. Each of these elements is aligned with the business needs of the organization itself. It is complicated within a fragmented global network to coordinate all the priorities of individual independent organizations; this can easily lead to delays, conflicts of interest and inefficiency along the supply chain.
- Inefficient supply model: The new multichannel world is very complex and consequently difficult to manage by the static structure of traditional fragmented supply chains. They were built based on the concept of large volumes and limited number of items. Today's world is instead

characterized by high customization, punctual and rapid orders, which require greater organizational and planning efficiency following a common line from upstream to downstream.

- Inflexible technology: Existing technological platforms for managing supply chains appear to be static and inflexible, too expensive, and complicated. Not agile enough to address the growing demands of todays and future supply chains.
- Lack of advanced transversal skills: In current conditions, there seem to be numerous operational gaps regarding transversal skills between one element of the supply chain and another. The competencies present among supply chain organizations are often too specific and not broad enough to understand end-to-end dependencies.

The extent of the changes required to readjust a company to the new world is significant and requires efforts on the part of individual organizations that must readjust to the complex system situation, forgetting the traditional linear system. The key steps in moving to the next generation of the supply chain, such as, a collaborative digital supply chain, involve the decomposition of functional silos that need to be reorganized into a more efficient structure, the redefinition of priorities and the exchange of data in real time, aimed at to the creation of schedules and synchronized realizations (Bozarth et al., 2008).

The entire Supply Chain sector must necessarily transition from a linear system to a complex system: In the modern industrial sector, the evolution of demand and the increase in competition are pushing producers and distribution to reformulate strategic choices and reorganize processes, operational. To achieve ambitious goals of efficiency and effectiveness in response to market demand, companies are led to seek greater levels of integration between activities. The traditional logic of Supply Chain Thinking and the management rules consolidated up to now are based on the erroneous assumption that supply chains are linear systems. Considering this vision, it would be possible to divide the supply chain into its individual components, optimize the performance of each of them, and obtain an optimized overall system. With a linear view of the supply chain, in which the output is a linear function of the individual inputs, it should be stable and simple to manage and optimize. The reality, however, is different; Complex Adaptive Systems (CAS) science provides a new description of supply chains, according to which the supply chain is a complex and nonlinear system (Chan, 2001). Adaptive complex systems are characterized by groups of agents linked in a process of co-adaptation, in which the adaptation moves of each have consequences for the entire group of individuals. The supply chain must therefore be a nonlinear system, whose behavior is not equal to the sum of the individual parts that compose it, but rather is due to the interactions between them. According to this concept, a small change in initial conditions can lead to large shifts elsewhere. It is essential that the value chain has an efficient organization, because all the links contribute to giving value. The first step necessary to enable the desired progress in the supply chain is to understand this new reality and then apply more efficient solutions and be able to optimize processes. Unfortunately, most supply chains still follow the old style: fragmentation and little flexibility. If previously the focus was on the optimization of some logistic functions within the same company, for example transport and the distribution structure, now the attention must be shifted to the whole of the supply chain processes, functions that in the traditional approach were not so close they must now be strongly linked together.

The integration of the supply chain into a complex ecosystem can take place not only intracompany but also intercompany. In fact, due to the greater dependence on the network, it is now impossible to think of a single company's supply chain strategy. Each of the members of the chain is influenced by the objectives and decisions of all the actors; it is not enough to focus attention only on internal activities, but it is necessary to extend the integration also to all the actors outside the company boundaries who contribute with varying intensity to the achievement of the objectives.

3.2 Blockchain in supply chain management

The importance of distribution, in a world where international trade multiplies and electronic commerce generates an exponentially increasing number of orders, means that many transactions related to transactions are digitized to connect the physical world of the circulation of goods. The supply chain can be made up of many stages and locations, making it increasingly difficult to track each stage in the chain as a result. Furthermore, the lack of transparency on the part of the supply chain hinders the trust between the parties involved in the process, making it impossible for the final consumer to be sure of the true value of the product or service he is purchasing. A series of bad practices occur around the supply chain, such as counterfeiting, the black market, forced labor or poor working conditions, the responsibility of which is very difficult to investigate. Blockchain technology can provide transparency and security to this entire process, thus strengthening the supply chain management (SCM). Even the simplest blockchain application, such as recording all transactions in a distributed ledger, could reveal new data that benefits the supply chain enormously (Francisco and Swanson, 2018).

The technological advances that have characterized the economic and industrial landscape in the last 20 years have led to the end of linear supply chains, giving rise to dynamically connected Digital Supply Networks (DSNs), able to better respond to market dynamics. The introduction of these new configurations has substantially transformed the way in which companies exchange and share information, leading to the birth of complex ecosystems in which processes are integrated with each other. In any case, the management of information and the control of interactions between products and supply chain actors remains a very complex activity. In fact, it requires careful collection of data and their secure archiving to guarantee a continuous and reliable flow of information between the various players involved in the chain. In this regard, although digital technologies have favored and simplified the sharing of information and made it possible to address some of the major problems that characterize the supply chain at various levels, their implementation is not without challenges. In fact, in relation to digital transformation, among the difficulties that businesses must face, there is precisely the understanding of which technologies to invest and at what time. This choice can dictate both the rapid progress of the firm and its differentiation and its collapse and/or exit from the market (Korpela et al., 2017).

Despite the continuous innovations and improvements introduced by digital technologies, there are still many challenges that characterize the current supply networks: paper-based processes are still very widespread, and decision making among the various players in the supply chain is becoming increasingly complex. Due to the presence of separate information systems that provide limited visibility on the individual business functions. These difficulties are affecting all industrial sectors across the board and are leading to the emergence of complex ecosystems that are difficult to manage and coordinate.

But many of the challenges that characterize the SCM cannot be faced with current technologies. In fact, there is currently a lack of solutions that allow to support collaboration and cooperation between the different entities involved. In fact, it is precisely from cooperation that the sharing of information arises. This remains the key element in the supply chain to mark the transition from linear structures to integrated ecosystems in which companies collaborate with each other to optimize the management of flows and intercompany processes. Within this context, it seems clear how the blockchain can play a leading role (Saberi et al., 2019).

Let's see now why blockchain is so important and what deeply distinguishes it from the technologies that preceded it. To date, centralized systems have proved to be the most practical tool for obtaining data security and guaranteeing transparency within the Supply Chains. From a strictly operational point of view, blockchain is not a more efficient technology than current centralized data management platforms. In fact, the distributed database requires greater computational power and consequently a greater energy requirement for the operation of the system. Nevertheless, the advantages that derive from its implementation are innumerable and lie precisely in its infrastructure and in the assumptions that constitute its foundations. The blockchain is a tool that allows to reach consensus in the execution of a collective activity that involves entities that do not necessarily trust each other, but that have a common goal. Trust, which is the essential tool to which companies use, when making an exchange or a transaction, up to the birth of the blockchain, was achieved thanks to the involvement of a centralized intermediary: that is, a central authority in which parties placed their trust and that they assumed the burden and responsibility of verifying the integrity and truthfulness of the transactions. In other words, the blockchain is trustless and, thanks to its distributed nature and consensus mechanisms, it allows the participants of a community to trust each other without resorting to a middleman. In fact, it is not necessary that the individual participants trust a particular node but, it is sufficient, that they place their trust in the system (Schmidt and Wagner, 2019).

The above integrates very well with the supply chain: In fact, within the supply networks there are a certain number of entities, which have a common goal and interest, but which, at the same time, are separate and therefore do not trust necessarily of each other. And it is precisely from trust and the communion of intent that the sharing of information between the players in the supply chain can be achieved. Sharing information in an exchange allows, among other things, to reduce the information asymmetry and the transaction costs associated with it. The reduction of costs that companies must face in resorting to the market can bring business models to a stage in which each company is highly specialized and acquires on the market all the goods and services complementary to the creation of products or the provision of services. The blockchain also allows you to establish trust in all those intercompany relationships characterized by the absence of an intermediary. In fact, in such contexts, the companies involved in an exchange rather than in a transaction do not trust each other and there is information asymmetry, they rely on bargaining. In this regard, to date, when two companies share data, financial information, and intellectual property with each other, the trust they develop in each other in relation to integrity and performance is governed by contracts (Abeyratne and Monfared, 2016).

Contracts make it possible to avoid continuous checks, provide guarantees but, above all, reduce risk. Having said that, defining and structuring a contract that offers complete guarantees and protections to companies, as well as being theoretically impossible, is very complex due to the lack of visibility and sharing of information. In fact, today, due to the elongation that characterizes the productive ecosystems, the participants do not know each other and consequently have no visibility on the activities and data that flow within the system. This causes trust to be built in another way. The blockchain acts as an intermediary or provides the infrastructure on which the parties can build trust and carry out exchanges. To date, digital technologies have removed the physical limits that exist in data transfer. For now, the only barrier that still exists and that does not allow the optimization of the information flow is the lack of trust. Blockchain technology can remove this limit, finally allowing us to exploit the real benefits of this hyperconnected era. Before the blockchain, in fact, the great technological innovations starting from the Internet made it possible to solve some of the great challenges that characterized the corporate and social landscape such as digitization, cloud computing, digital data management. But no technology to date has made it possible to solve the problem of lack of trust. That is, no technology has made it possible to guarantee that the information shared between different partners could be used for one's own advantage rather than for the benefit of one's competitors. The blockchain itself has not introduced any technical innovation. In fact, this is based on the combination of already existing technologies which, however, linked together, allow to create an ecosystem that defines a new concept of trust. And within the supply chains there is no lack of digitalization, there is no lack of data management, there is no lack of distributed systems, but there is no lack of trust (Treiblmaier, 2018). The big challenge lies in understanding when to capitalize on blockchain and how to combine it with other digital technologies to generate important benefits within supply networks.

4. Blockchain-based model for vaccine supply chain

Blockchain technology has already been proposed by several studies as a possible solution to the criticalities connected with the management of problems in the health sector.

4.1 Applications of Blockchain technology in healthcare

Below we will analyze some possible application solutions of Blockchain technology to deal with real cases.

- Patient Medical Records (PHR): There are currently numerous medical records in which patients can store the results of various tests (Ivan, 2016; Dimitrov, 2019). Some of these examples are Apple Health or Microsoft HealthVault, which use centralized systems. Using a Blockchain-based system, the data could be stored in a distributed way, allowing the patient to control which data to share and with whom. The rest of traditional health systems, as well as devices, can be connected to this system to perform any type of test and store the result in the Blockchain. Patients will have full control of their data, as well as having an immutable track that shows when which data was accessed and who accessed it (Esposito et al., 2018).
- Data exchange between traditional care and telemedicine: Telemedicine is gaining popularity among patients who need minor but urgent care and, for whatever reason, must avoid long waits in a traditional medical consultation. The data collected and the treatment delivered through this type of system may be inaccessible to primary care physicians, which in turn will result in an incomplete medical history of the patient. This in turn will generally result in a decrease in the quality of future diagnoses and treatments. Using Blockchain it is possible to eliminate the intermediaries that hinder the exchange of medical data and allow direct relationships between telemedicine and general practitioners. A smart contract can be used to organize exchanges between the various health systems (Ahmad et al., 2021).
- Shared patient data management: Most patients diagnosed with some type of disease want to have a second medical opinion on treatment or diagnosis. At present, this process actively involves the patient, as she must obtain all her medical data and hand it over to the second doctor. This process is by no means recommended considering the patient's situation. A possible solution to this problem would be a

Blockchain-based system that acts as an intermediary between patients and multiple healthcare providers around the world (Tian et al., 2019). This system will give the patient total freedom to decide which medical data to share and with whom.

- Addressing opioid substance abuse: There is a health crisis in the United States due to opioid substance abuse. Currently there is abuse both by health professionals, with unnecessary prescriptions, and by the patient who undergoes a real improvement in the short term at the cost of increasing his dependence on these substances. One possible solution would be to create a trust network consisting of hospitals and pharmacies to store opioid-related transactions (Raghavendra, 2019). For hospitals and pharmacies, the existing incentive would be to be able to compile a data set on opioids and their consumers. Likewise, patients could gain an increase in the quality of their medical care thanks to this large dataset and its possible applications, and they could also be better informed about the risks of these substances.
- Shared registry of a disease: Another interesting use case would be the creation of a distributed and shared registry of the medical data of patients with some type of severely disabling disease. Sharing data on these diseases is critical as treatments are complex and highly personalized. The idea is to build a learning ecosystem that using Blockchain allows to share predictive models, built using shared data and that allow medical professionals to obtain prognosis and improve diagnosis and final treatment (Piccininni et al., 2020).
- Health Insurance Management: Clients of health insurance companies who have an accident that results in permanent disability or even death require a monthly income from their insurance or compensation in the latter case. While it is true that there is a certain percentage of fraud, in most cases it is resolved automatically. To expand and ensure said automation, the use of smart contracts is proposed to orchestrate this process (Radanović and Likić, 2018). The entire award process will be transparent to both the insurer and the client, showing possible errors and fraud that could be investigated in a timely manner. These smart agreements could also be used to ensure awareness and updating of current company policies.
- Pharmaceutical Product Safety: According to the World Health Organization, it is estimated that counterfeit pharmaceuticals worth up to US $ 200 billion are sold globally each year and 50% of these drugs are purchased over the Internet. Counterfeiting, in general, occurs when a

manufacturer or distributor takes back a portion of the manufactured drugs and resells them, or introduces counterfeit drugs into the original batches. The problem is that the technological solutions that are being adopted are unable to dispel these illicit acts. Product traceability refers to the tracking of items at the unit level, from start to finish as they move through the supply chain. Thanks to the Blockchain application, all participants in the exchange can access the origin and location, authenticate the elements that make it up and verify compliance with the requirements and agreements (Nørfeldt et al., 2019).

There are numerous authors who have studied possible solutions of Blockchain technology in the health sector to improve current systems by exploiting its intrinsic characteristics. A first application concerned the management of Electronic Health Records (EHR): Chenthara et al. (2020) proposed a framework based on Blockchain technology for the management of Electronic Health Records (EHR). The framework uses the distributed ledger platform Hyperledger. It is a distributed ledger that is a source of replicated, shared, and synchronized digital data geographically distributed across multiple sites, countries, or institutions. The framework created by the authors then uses InterPlanetary File System (IPFS) to store the EHRs. For transaction security, the framework uses a unique cryptographic public key cryptographic algorithm. Hylock and Zeng (2019) have exploited Blockchains to process patient health data. This is sensitive data that must be treated with great caution, which is why the authors have proposed a new blockchain-based framework called HealthChain. To guarantee the exchange of data, the Health Level-7 Fast Healthcare Interoperability Resources was used, which represents a framework for the electronic exchange of health information. Encryption is guaranteed thanks to the generation of a pair of public and private keys. Public keys are stored in the blockchain and are suitable for securing and verifying transactions. Dubovitskaya et al. (2020) have developed an authorized blockchain-based EHR management system. With the use of this system, the patient will be able to manage their health data also referring to multiple hospitals. The protection of the patient's privacy will be guaranteed, as well as the security of health data management, and it will be possible to control access to the patient so that the latter can know who has had access to her data. Xia et al. (2017) proposed a new system for sharing health data based on Blockchain. The system was called MeDShare and ensures data auditing and control, through continuous monitoring of access to data and the adoption of smart contracts. Other applications of Blockchain technology have concerned the personal health record exchange (Lee et al., 2020), the medical data access and permission management (Azaria et al., 2016), the validation of the patient's identity (Mettler, 2016), a secure supply of drugs (Baunm, 2017).

Since about the end of 2019 the world has been affected by the largest pandemic ever recorded so far due to the uncontrolled spread of the virus called COVID-19. The spread of COVID-19 has caught the world off guard. There are still many questions that do not have an answer and perhaps will not have it for a long period of time. Many of the issues that stakeholders intend to analyze concern the future and are because the main world economies, the ones most involved in global value chains, have suffered. The spread of the pandemic was fast and devastating, catching most of the Western states unprepared that had never had to deal with such an emergency, at least in the last century. Nonexistent or at least outdated pandemic plans did the rest. The inability to contain the spread of the epidemic has prompted many states to impose rigorous lockdown policies that have had very heavy repercussions on economies. The evident need for an effective experimentation to produce an anti-COVID-19 vaccine was immediately understood (Van Bavel et al., 2020).

Research centers around the world immediately took steps to identify the gene of the virus and subsequently some of these centers began an experimentation to produce the vaccine. The use of modern technologies also based on the use of artificial intelligence has made it possible to prepare a vaccine in record time and subject it to an experimental campaign to verify its effects first on animals and then on humans. At the end of this phase, the largest vaccine administration campaign ever carried out in the world was carried out with the use of enormous financial and logistical resources. Given the short duration of the experimentation and given the widespread use of the vaccine on a world scale, some criticalities connected with its use only came to the surface during the administration phase, undermining the confidence of the population on the effective efficacy of the vaccines and the severity of the side effects. To overcome these difficulties, a Blockchain-based technology could have made an important contribution to the effectiveness of the vaccine administration campaign.

4.2 Vaccine characteristics

Some diseases caused by viruses, bacteria or fungi can reach humans due to close contact with various animal species. The passage of microbial agents from one species to another can be the main cause of the spread of new epidemics and pandemics. The diseases that result from this close contact between humans and animals are called zoonoses, or diseases that can be naturally transmitted from vertebrate animals to humans and vice versa. Precisely this animal-human transmission would represent the cause of the outbreak of the COVID-19 pandemic, which since the end of 2019 has caused millions of victims around the world (Le et al., 2020).

Coronaviruses belong to a large family of viruses that can be found both within animals and within humans. They are viruses known for their ability to cause diseases ranging from the more well-known cold to more serious diseases such as SARS and MERS. It defines itself as "new coronavirus," that virus that had never been found inside a human organism, exactly what happened in Wuhan, China, in December 2019. Coronaviruses are so called because they present a particular structure that seems to recall that of a crown, an image due to the tips present on their surface (Corey et al., 2020).

A pandemic can be fought through various forms of prevention:

- Primary prevention, whose task is to prevent the disease from manifesting itself. The restrictive measures of the government, social distancing, hand washing, personal protective equipment (PPE), and disinfection of environments are part of primary prevention.
- Secondary prevention, the task of which is to identify a disease early to limit its evolution as much as possible and limit the damage related to it. This category includes screening with molecular and antigenic swabs and contact tracing systems with COVID-19–positive patients.
- Tertiary prevention, the purpose of which is the earliest possible treatment to limit the impact of complications. This category includes pharmacological and nonpharmacological therapies.

It was immediately evident that there is no therapy that has proven to be certainly effective in the treatment of COVID-19 infection. Vaccines are the most effective tools to prevent, control and eliminate infectious diseases and to minimize their impact on humans. Once administered, the vaccines simulate the first contact with the infectious agent, evoking an immunological response like that caused by natural infection, without however causing the disease and its complications. The principle behind this mechanism is immunological memory: the ability of the immune system to remember which foreign microorganisms have attacked our body in the past and to respond quickly. Without vaccinations, our body can take up to 2 weeks to produce enough antibodies to counter the invader. A time interval during which the microorganism can cause damage to our body (Graham, 2020).

Vaccines are biological preparations consisting of killed or attenuated microorganisms, or by some of their constituents (antigens), or by substances produced by microorganisms and made safe (such as tetanus toxoid which derives from the treatment of tetanus toxin) or, again, from proteins obtained with genetic engineering techniques. Vaccines generally also contain sterile water (or a saline-based physiological solution) and some may also contain, in small quantities, an adjuvant to improve the immune system response, a preservative (or an antibiotic) to prevent contamination of the vaccine by part of bacteria, some stabilizers to keep the properties of the vaccine unaltered during storage (Jeyanathan et al., 2020).

Vaccines are drugs, and as with all drugs there are benefits—which consist in the prevention of a disease—and risks of occurrence of adverse events. As with all drugs, a vaccine only enters the market when international regulatory authorities, such as the European Medicine Agency (EMA) in Europe and the Food and Drug Administration (FDA) in the United States, have verified that the benefits outweigh the risks. Naturally, as for all drugs, the surveillance of the benefit-risk profile continues even after placing on the market, first to check if there are any rare adverse events that cannot be highlighted in the premarketing phase, due to their relative limitation. The number of subjects involved in the studies. Over time, the margins of uncertainty still present at the time of registration also reduce (Knoll and Wonodi, 2021).

4.3 Vaccine trust and the limits of information

Vaccine surveillance is part of drug surveillance activities which, according to the WHO definition, is the set of actions undertaken to collect, archive, identify, analyze, evaluate, and inform about the risks and benefits of medicines, to maintain, modify, suspend, or revoke their marketing authorization or any other regulatory action. Vaccine surveillance allows us to analyze the benefit/risk ratio of each vaccine and ascertain that this ratio remains favorable over time. In the presence of an adverse event that occurred after vaccination this is analyzed because the appearance of an adverse event after the vaccine does not necessarily imply that the cause is the vaccine itself (Malik et al., 2020).

Trust in vaccines is trust in the efficacy and safety of vaccines and in the healthcare system that provides them. Trust in vaccines refers to the belief that vaccination serves the best health interests of the public and its members. Public confidence in vaccination is essential to ensure a high prevalence of vaccination. Over the years, researchers have been involved in combating fake news on vaccines and autism, contesting news stories, and providing references in the literature on the subject.

The benefits of vaccination can be difficult to explain to the public. Healthy people may not recognize the role of vaccines in preventing disease and reducing its spread, because vaccinations prevent infectious diseases rather than treat or control their symptoms in nature and therefore have no visible effect on already ill individuals. Vaccines undergo rigorous scientific evaluation by regulatory authorities. Each vaccine is rigorously evaluated for safety, quality, and efficacy to determine if it can be licensed, using all available scientific evidence from animal data, human clinical studies and manufacturing information to assess its benefits and risks.

The perception of the benefits of vaccinations has weakened precisely because of the successes achieved by vaccination policies: it is said that vaccines are the main victims of their successes. As the frequency of prevented diseases decreases, the perception of their danger is lost, and many are led to think that the vaccine is useless. At the same time, doubts about the safety of vaccines, and therefore about their risk/benefit ratio, increase. Healthy people would, in theory, be willing to undergo prevention only if it has zero risk. Several factors have been identified that undermine trust in vaccines and the propensity to undergo vaccination:

1. Complacency: Perceived risks for vaccine-preventable diseases are low and the vaccine is therefore considered unnecessary. Complacency is the result of the success of vaccines. This barrier breaks down by informing about the still existing risks of pathologies.
2. Confidence: includes confidence in the efficacy and safety of vaccines, but also in the institutions that offer it, in the institutions that produce it, in doctors and health personnel. It is also influenced by political and religious ideologies.
3. Convenience: is understood as the accessibility to vaccines (clinic hours, remoteness of the same, any costs to be borne by the user).

4.4 Blockchain solutions for vaccine administration

The development of a vaccine is a very long process, which takes from 7 to 10 years, during which research is conducted in successive stages that include quality tests, preclinical trials, and stages of clinical trials in humans. The clinical trial includes three phases of studies:

- Phase 1: Studies conducted on healthy volunteers for the identification of the optimal dose and the evaluation of safety in humans.

- Phase 2: Exploratory studies conducted on small groups of people, generally fewer than 100.
- Phase 3: Confirmatory studies conducted on thousands or tens of thousands of people.

The development of vaccines to stop the spread of the COVID-19 virus has highlighted the importance of information data in its digital dimension. To significantly reduce the time needed to develop a vaccine, an extremely complex information management was required. The distributed management of data within a certain community, provided for by the blockchain model, allows for a parallel development of the various phases, guaranteeing a significant reduction in time. But this aspect is only one of the many advantages offered by Blockchain technology, we can highlight the problems connected with respecting the privacy of patients who undergo testing protocols, and those who are subsequently vaccinated. Platforms based on Blockchain technology can be regulated in such a way as to provide for decentralized information management with respect for the principle of privacy by design (Ramirez Lopez and Beltrán Álvarez, 2020).

The development of vaccines against COVID-19 has highlighted the importance of digital data, indissolubly tying the development of a vaccine to the information necessary to produce it: The vaccine contains all the information necessary to design it, to produce it and finally to distribute it. The search for a vaccine against COVID-19 required, in fact, to acquire, sift and correct a huge amount of information quickly and efficiently to forge ahead for its distribution. These are genetic information on the virus, biological and genetic information on how the human body reacts to the virus, health information relating to patients who undergo testing protocols first and then once vaccinated must be considered to identify any effects, long-term vaccine. Information relating to the storage conditions of the vaccine, some vaccines, in fact, must be stored at prohibitive temperatures ranging between −90°C and −60°C. Finally, there is also information relating to logistics to be processed once it must be distributed, because you need to know exactly where each vial is and at what temperature it is in order not to frustrate the vaccination campaign (Antal et al., 2021).

The management of this gigantic amount of information that must be collected, stored safely, quickly, and effectively screened to identify any errors and correct them immediately by identifying the right solutions as soon as possible, requires a radical change of approach and use of innovative technologies. Blockchain technology makes it possible to move from centralized management of information data to decentralized management to ensure transparency, speed, and greater efficiency in the use of information needed for vaccine development. Without this support it is not possible to arrive at a ready response to a pandemic that has developed very quickly, hitting hard every corner of the globe. In fact, if on the one hand the production of vaccines was characterized by short times, the distribution of the same took different times depending on the management policy undertaken by the different countries. Difficulty in procurement, and the complex administration procedure required a long time which often slowed down the effectiveness of the vaccination campaign (Yong et al., 2020).

Also, for the administration of vaccines it is necessary to have a third-party guarantor acting as a central bank to guarantee the value of the securities held; this validation process is assured in an equally secure manner by the entire community. The same goes for information regarding vaccines with blockchain technology. These are no longer managed centrally by a single person who first collects all the information, then processes them and searches for errors and, finally, transmits them all to the relevant agency to request authorization according to a linear time. Instead, this information is immediately made available to the community and the same authority to proceed simultaneously with their validation so as to identify and correct errors and then forward them without delay to the relevant agency so that they can issue the authorization. In other words, all the different phases are merged here and in fact carried out simultaneously, guaranteeing transparency and efficiency (Musamih et al., 2021).

The vaccine development process takes years to go from its conception to the operational phase of commercialization. This is because, for obvious safety reasons, the process for its development is particularly complex and divided into phases, some of which are in turn divided into further subphases. From the comparison of the data collected in the different phases, the level of effectiveness of the vaccine is obtained: After verifying the compliance of all the results produced by the tests with the required standards, the manufacturer then proceeds to send a dossier to the competent authorities to request registration and, obtained official clearance, marketing authorization. But once the authorization is obtained, a further period of control begins, with which the secondary effects on vaccinated people are carefully monitored to test the safety of the vaccine over the years on a growing number of the population. At this point you have a safe vaccine. However, the length of the experimentation process also leads to an exponential increase in costs that not all countries are able to face. The articulation of the process that leads the vaccine to be developed, tested, and then administered is particularly complex, although necessary to have a safe product, it can appear particularly cumbersome. For this reason, also in the scientific field, it was requested to be able to skip the last phase to put countries in competition, thus opening to a sort of mass experimentation, which happened on time for the Russian and Chinese vaccines. Blockchain technology, on the other hand, makes this conceptual leap unnecessary, which simultaneously implies the assumption of an unsustainable series of risks. Because the unification of the phases leads, following a substantially transparent process, to reach a level of efficiency and safety that is far from comparable to any shortcut you plan to take (Omar et al., 2021).

This is because managing billions of information requires a truly radical change of strategy. The blockchain already intervenes in the exploratory phase in which the study of the genetic characteristics of the virus is started to identify the antigen necessary to inhibit its action and thus provoke the response of the immune system. There are hundreds of genetic sequences that need to be compared at this stage and this can be done much more quickly and effectively if a considerable number of scientists all over the world take part in this operation, sharing materials through the blockchain that in this way result in evidence of tampering.

In the next, preclinical phase, in which the possible candidate is tested in vitro and in vivo on guinea pigs, with blockchain technology the information collected is made available to the community of scientists to check all the data, identify any errors and contextually find the most appropriate solutions. This allows biotech companies, among other things, not to lose their intellectual property rights and their competitive advantage over their main competitors.

In the third and last clinical phase, information relating to the trial on thousands and thousands of patients, in particular data on their immune response, adverse effects, clinical conditions etc. These data must be managed in a coordinated and secure manner to be well understood before the authorization process is initiated with the authorities of the various countries. However, patient information must obviously be collected based on an informed consent that must be managed anonymously so as not to be associated with any information leading to their reidentification and this is precisely possible through blockchain platforms which, if managed in a manner safe, they can encourage people to take part in vaccine testing protocols (Hernández-Ramos et al., 2021).

In the authorization phase, data must be shared between the parties in real time to shorten the vaccine approval and marketing process as much as possible. And here, once again, blockchain platforms prove indispensable.

In the vaccine distribution phase, blockchain platforms contribute significantly to the success of the procedure. In fact, it is estimated that up to 30% of the vaccine stocks are lost during the storage phase, because the characteristics of the vaccines require an extremely effective system for controlling the storage conditions of the vaccines. This system requires a precise location of each batch and even of each vial to reconstruct each step up to the moment of its administration. A monitoring system is needed to accompany this very delicate phase on which the success of the vaccination campaign depends. And this not only to optimize the distribution of the vaccine at the level of a single country, but also to allow its distribution all over the world, especially in developing countries so as not to penalize them to avoid, among other things, that they may then constitute a potential site of resurgence of the virus which would risk nullifying the effectiveness of the vaccination campaign (Tsoi et al., 2021).

Ultimately, blockchain technologies allow a truly radical paradigm shift in the field of vaccines whose potential has been tapped by various actors internationally. Given the potential of this technological breakthrough, a conversion of current procedures into truly responsible forms of research and innovation is necessary for its success. Blockchain technology, in fact, with its structural instance of transparency, sharing and control of fully digitized information raises no small questions regarding the respect of privacy.

In general, the idea is to develop tools for implementing the protection of personal data on blockchain platforms, whatever the object. In the mechanisms of collection and data computing of genetic data these cannot be stored in in-house servers and for this reason we often proceed to put all the data on cloud managed by third parties. However, there are several examples of data encryption tools that have been developed for genetic data as an alternative to mechanisms focused instead on the mere compensation of the owners of the personal data. The possibility of implementing certain "privacy enhancing tools" within cloud-based modules and blockchain platforms makes it clear how it is completely feasible to create tools capable of increasing the level of protection of personal data even within distributed systems and based on the transparency of data with respect to a certain community. Provided that these tools are developed by design, that is, at the same time as the design of a platform to be applied to the field of vaccines.

Almost 2 years after the WHO declaration of a COVID-19 pandemic, the inequality between rich and poor countries in access to vaccines is more acute and dramatic than ever. The wealthiest nations have vaccinated most of the population, while most developing countries still have not been able to vaccinate at least 10% of the population, with a structural shortage of medical supplies and oxygen supplies. This is the alarm raised by the World Health Organization. To overcome this criticality, the proposal to overcome the current monopoly held by pharmaceutical companies on vaccine patents has come from many parts of the world. A proposal, which if approved, would allow to increase world production, and start distribution in all poor countries that need it immediately.

5. Conclusion

In this chapter we first introduced the basic concepts of blockchain technology, and then we moved on to the analysis of the essential characteristics of the supply chain. Finally, the applications based on blockchain technology adopted to address the difficult emergency due to COVID-19 were analyzed, focusing attention on Blockchain-based solutions for the management of the anti-COVID-19 vaccination campaign.

We have seen that Blockchain technology proves to be particularly effective in managing the delicate phases of the Supply Chain. Blockchain technology therefore allows you to monitor the process of distribution, storage, and administration of vaccines for COVID-19. The approach is not so different from those already adopted, for example, in the automotive industry to certify the origin of raw materials or in the healthcare sector in the fight against counterfeit drugs. For example, it guarantees to optimize the control of the cold chain necessary to keep the vials of the vaccine required by messenger vaccines at extremely low temperatures. The technological evolution in this case comes to the aid of the world community to face one of the most difficult tests of the modern era.

References

Abeyratne, S.A., Monfared, R.P., 2016. Blockchain ready manufacturing supply chain using distributed ledger. Int. J. Res. Eng. Technol. 5 (9), 1–10.

Ahmad, R.W., Salah, K., Jayaraman, R., Yaqoob, I., Ellahham, S., Omar, M., 2021. The role of blockchain technology in telehealth and telemedicine. Int. J. Med. Inform. 148, 104399.

Amr, M.A., Eljazzar, M.M., Kassem, S.S., Ezzat, M., 2019. Merging supply chain and blockchain technologies. In: The 28th International Conference for the International Association of Management of Technology (IAMOT).

Antal, C.D., Cioara, T., Antal, M., Anghel, I., 2021. Blockchain platform for COVID-19 vaccine supply management. arXiv preprint arXiv:2101.00983.

Aste, T., Tasca, P., Di Matteo, T., 2017. Blockchain technologies: the foreseeable impact on society and industry. Computer 50 (9), 18–28.

Azaria, A., Ekblaw, A., Vieira, T., Lippman, A., 2016. Medrec: using blockchain for medical data access and permission management. In: 2016 2nd International Conference on Open and Big Data (OBD). IEEE, pp. 25–30.

Badertscher, C., Maurer, U., Tschudi, D., Zikas, V., 2017. Bitcoin as a transaction ledger: a composable treatment. In: Annual International Cryptology Conference. Springer, Cham, pp. 324–356.

Baunm, S., 2017. Health IT Startups Working to Secure Pharma Supply Chains? Medcity News. [Online]. Available from: https://medcitynews.com/2017/01/drug-supply-chain-security-and-technology/. (Accessed 12 May 2021).

Beamon, B.M., 1998. Supply chain design and analysis: models and methods. Int. J. Prod. Econ. 55 (3), 281–294.

Belotti, M., Božić, N., Pujolle, G., Secci, S., 2019. A vademecum on blockchain technologies: when, which, and how. IEEE Commun. Surv. Tutorials 21 (4), 3796–3838.

Benchoufi, M., Porcher, R., Ravaud, P., 2017. Blockchain protocols in clinical trials: transparency and traceability of consent. F1000Res. 6, 66.

Bertino, E., Sandhu, R., 2005. Database security-concepts, approaches, and challenges. IEEE Trans. Dependable Secure Comput. 2 (1), 2–19.

Bozarth, C.C., Handfield, R.B., Weiss, H.J., 2008. Introduction to Operations and Supply Chain Management. Pearson Prentice Hall, Upper Saddle River, NJ.

Cachin, C., 2016. Architecture of the hyperledger blockchain fabric. In: Workshop on Distributed Cryptocurrencies and Consensus Ledgers. vol. 310. No. 4.

Calvão, F., 2019. Crypto-miners: digital labor and the power of blockchain technology. Econ. Anthropol. 6 (1), 123–134.

Casado-Vara, R., Prieto, J., De la Prieta, F., Corchado, J.M., 2018. How blockchain improves the supply chain: case study alimentary supply chain. Procedia Comput. Sci. 134, 393–398.

Ceri, S., 2017. Distributed Databases. Tata McGraw-Hill Education.

Chan, S., 2001. Complex adaptive systems. In: ESD. 83 Research Seminar in Engineering Systems. vol. 31, pp. 1–19.

Chenthara, S., Ahmed, K., Wang, H., Whittaker, F., Chen, Z., 2020. Healthchain: a novel framework on privacy preservation of electronic health records using blockchain technology. PLoS One 15 (12), e0243043.

Chowdhury, M.J.M., Colman, A., Kabir, M.A., Han, J., Sarda, P., 2018. Blockchain versus database: a critical analysis. In: 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE). IEEE, pp. 1348–1353.

Corey, L., Mascola, J.R., Fauci, A.S., Collins, F.S., 2020. A strategic approach to COVID-19 vaccine R&D. Science 368 (6494), 948–950.

Croxton, K.L., Garcia-Dastugue, S.J., Lambert, D.M., Rogers, D.S., 2001. The supply chain management processes. Int. J. Logist. Manage. 12 (2), 13–36.

Davis, T., 1993. Effective supply chain management. Sloan Manage. Rev. 34, 35.

Dhillon, V., Metcalf, D., Hooper, M., 2017. Blockchain Enabled Applications. Apress, Berkeley, CA, p. 72.

Dimitrov, D.V., 2019. Blockchain applications for healthcare data management. Healthc. Inform. Res. 25 (1), 51.

Dinh, T.T.A., Liu, R., Zhang, M., Chen, G., Ooi, B.C., Wang, J., 2018. Untangling blockchain: a data processing view of blockchain systems. IEEE Trans. Knowl. Data Eng. 30 (7), 1366–1385.

Dogru, T., Mody, M., Leonardi, C., 2018. Blockchain Technology & Its Implications for the Hospitality Industry. Boston University.

Dubovitskaya, A., Baig, F., Xu, Z., Shukla, R., Zambani, P.S., Swaminathan, A., et al., 2020. ACTION-EHR: patient-centric blockchain-based electronic health record data management for cancer care. J. Med. Internet Res. 22 (8), e13598.

Durach, C.F., Blesik, T., von Düring, M., Bick, M., 2021. Blockchain applications in supply chain transactions. J. Bus. Logist. 42 (1), 7–24.

Ellram, L.M., 1991. Supply-chain management: the industrial organisation perspective. Int. J. Phys. Distrib. Logist. Manage. 21 (1), 13–22. https://doi.org/10.1108/09600039110137082.

Esposito, C., De Santis, A., Tortora, G., Chang, H., Choo, K.K.R., 2018. Blockchain: a panacea for healthcare cloud-based data security and privacy? IEEE Cloud Comput. 5 (1), 31–37.

Fernández-Caramés, T.M., Fraga-Lamas, P., 2020. Towards post-quantum blockchain: a review on blockchain cryptography resistant to quantum computing attacks. IEEE Access 8, 21091–21116.

Francisco, K., Swanson, D., 2018. The supply chain has no clothes: technology adoption of blockchain for supply chain transparency. Logistics 2 (1), 2.

Fu, Y., Zhu, J., 2019. Operation mechanisms for intelligent logistics system: a blockchain perspective. IEEE Access 7, 144202–144213.

Garay, J., Kiayias, A., Leonardos, N., 2015. The bitcoin backbone protocol: analysis and applications. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg, pp. 281–310.

Graham, B.S., 2020. Rapid COVID-19 vaccine development. Science 368 (6494), 945–946.

Halaburda, H., 2018. Blockchain revolution without the blockchain? Commun. ACM 61 (7), 27–29.

Hernández-Ramos, J.L., Karopoulos, G., Geneiatakis, D., Martin, T., Kambourakis, G., Fovino, I.N., 2021. Sharing pandemic vaccination certificates through blockchain: case study and performance evaluation. arXiv preprint arXiv:2101.04575.

Hugos, M.H., 2018. Essentials of Supply Chain Management. John Wiley & Sons.

Hylock, R.H., Zeng, X., 2019. A blockchain framework for patient-centered health records and exchange (HealthChain): evaluation and proof-of-concept study. J. Med. Internet Res. 21 (8), e13592.

Ivan, D., 2016. Moving toward a blockchain-based method for the secure storage of patient records. In: ONC/NIST Use of Blockchain for Healthcare and Research Workshop. ONC/NIST, Gaithersburg, Maryland, United States, pp. 1–11.

Jeyanathan, M., Afkhami, S., Smaill, F., Miller, M.S., Lichty, B.D., Xing, Z., 2020. Immunological considerations for COVID-19 vaccine strategies. Nat. Rev. Immunol. 20 (10), 615–632.

Kim, S., Deka, G.C. (Eds.), 2020. Advanced Applications of Blockchain Technology. Springer.

Klems, M., Eberhardt, J., Tai, S., Härtlein, S., Buchholz, S., Tidjani, A., 2017. Trustless intermediation in blockchain-based decentralized service marketplaces. In: International Conference on Service-Oriented Computing. Springer, Cham, pp. 731–739.

Knoll, M.D., Wonodi, C., 2021. Oxford–AstraZeneca COVID-19 vaccine efficacy. Lancet 397 (10269), 72–74.

Korpela, K., Hallikas, J., Dahlberg, T., 2017. Digital supply chain transformation toward blockchain integration. In: Proceedings of the 50th Hawaii International Conference on System Sciences.

Kumar, G., Saha, R., Rai, M.K., Thomas, R., Kim, T.H., 2019. Proof-of-work consensus approach in blockchain technology for cloud and fog computing using maximization-factorization statistics. IEEE Internet Things J. 6 (4), 6835–6842.

Lambert, D.M., Cooper, M.C., 2000. Issues in supply chain management. Ind. Mark. Manage. 29 (1), 65–83.

Le, T.T., Andreadakis, Z., Kumar, A., Román, R.G., Tollefsen, S., Saville, M., Mayhew, S., 2020. The COVID-19 vaccine development landscape. Nat. Rev. Drug Discov. 19 (5), 305–306.

Lee, H.A., Kung, H.H., Udayasankaran, J.G., Kijsanayotin, B., Marcelo, A.B., Chao, L.R., Hsu, C.Y., 2020. An architecture and management platform for blockchain-based personal health record exchange: development and usability study. J. Med. Internet Res. 22 (6), e16748.

Li, X., Jiang, P., Chen, T., Luo, X., Wen, Q., 2020. A survey on the security of blockchain systems. Futur. Gener. Comput. Syst. 107, 841–853.

Lo, S.K., Xu, X., Chiam, Y.K., Lu, Q., 2017. Evaluating suitability of applying blockchain. In: 2017 22nd International Conference on Engineering of Complex Computer Systems (ICECCS). IEEE, pp. 158–161.

Malik, A.A., McFadden, S.M., Elharake, J., Omer, S.B., 2020. Determinants of COVID-19 vaccine acceptance in the US. EClinicalMedicine 26, 100495.

Maurya, A.K., Singh, A., Tripathi, U.N., Pandey, S., Singh, D., 2020. Security in distributed database system: a survey. J. Comput. Math. Sci. 11 (7), 43–51.

Mentzer, J.T., DeWitt, W., Keebler, J.S., Min, S., Nix, N.W., Smith, C.D., Zacharia, Z.G., 2001. Defining supply chain management. J. Bus. Logist. 22 (2), 1–25.

Mettler, M., 2016. Blockchain technology in healthcare: the revolution starts here. In: 2016 IEEE 18th International Conference on E-Health Networking, Applications and Services (Healthcom). IEEE, pp. 1–3.

Min, H., Zhou, G., 2002. Supply chain modeling: past, present and future. Comput. Ind. Eng. 43 (1–2), 231–249.

Musamih, A., Jayaraman, R., Salah, K., Hasan, H., Yaqoob, I., Al-Hammadi, Y., 2021. Blockchain-based solution for distribution and delivery of COVID-19 vaccines. IEEE Access 9, 71372–71387.

Muzammal, M., Qu, Q., Nasrulin, B., 2019. Renovating blockchain with distributed databases: an open source system. Futur. Gener. Comput. Syst. 90, 105–117.

Nakamoto, S., Bitcoin, A., 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. Available from: https://bitcoin.org/bitcoin.pdf. (Accessed 25 May 2021).

Niranjanamurthy, M., Nithya, B.N., Jagannatha, S., 2019. Analysis of Blockchain technology: pros, cons and SWOT. Clust. Comput. 22 (6), 14743–14757.

Nofer, M., Gomber, P., Hinz, O., Schiereck, D., 2017. Blockchain. Business & information. Syst. Eng. 59 (3), 183–187.

Nørfeldt, L., Bøtker, J., Edinger, M., Genina, N., Rantanen, J., 2019. Cryptopharmaceuticals: increasing the safety of medication by a blockchain of pharmaceutical products. J. Pharm. Sci. 108 (9), 2838–2841.

Omar, I.A., Jayaraman, R., Debe, M.S., Salah, K., Yaqoob, I., Omar, M., 2021. Automating procurement contracts in the healthcare supply chain using blockchain smart contracts. IEEE Access 9, 37397–37409.

Piccininni, M., Rohmann, J.L., Logroscino, G., Kurth, T., 2020. Blockchain-based innovations for population-based registries for rare neurodegenerative diseases. Front. Blockchain 3, 20. https://doi.org/10.3389/fbloc.2020.00020.

Pilkington, M., 2016. Blockchain technology: principles and applications. In: Research Handbook on Digital Transformations. Edward Elgar Publishing.

Radanović, I., Likić, R., 2018. Opportunities for use of blockchain technology in medicine. Appl. Health Econ. Health Policy 16 (5), 583–590.

Raghavendra, M., 2019. Can blockchain technologies help tackle the opioid epidemic: a narrative review. Pain Med. 20 (10), 1884–1889.

Ramirez Lopez, L.J., Beltrán Álvarez, N., 2020. Blockchain application in the distribution chain of the COVID-19 vaccine: a designing understudy. Advance (preprint).

Ren, Y., Zhu, F., Sharma, P.K., Wang, T., Wang, J., Alfarraj, O., Tolba, A., 2020. Data query mechanism based on hash computing power of blockchain in internet of things. Sensors 20 (1), 207.

Rhee, K., Kwak, J., Kim, S., Won, D., 2005. Challenge-response based RFID authentication protocol for distributed database environment. In: International Conference on Security in Pervasive Computing. Springer, Berlin, Heidelberg, pp. 70–84.

Risius, M., Spohrer, K., 2017. A blockchain research framework. Bus. Inform. Syst. Eng. 59 (6), 385–409.

Saberi, S., Kouhizadeh, M., Sarkis, J., Shen, L., 2019. Blockchain technology and its relationships to sustainable supply chain management. Int. J. Prod. Res. 57 (7), 2117–2135.

Schmidt, C.G., Wagner, S.M., 2019. Blockchain and supply chain relations: a transaction cost theory perspective. J. Purch. Supply Manage. 25 (4), 100552.

Sherman, A.T., Javani, F., Zhang, H., Golaszewski, E., 2019. On the origins and variations of Blockchain technologies. IEEE Secur. Priv. 17 (1), 72–77.

Simatupang, T.M., Sridharan, R., 2002. The collaborative supply chain. Int. J. Logist. Manage. 13 (1), 15–30.

Singh, A., Parizi, R.M., Zhang, Q., Choo, K.K.R., Dehghantanha, A., 2020. Blockchain smart contracts formalization: approaches and challenges to address vulnerabilities. Comput. Secur. 88, 101654.

Stevens, G.C., 1989. Integrating the supply chain. Int. J. Phys. Distrib. Mater. Manage. 19 (8), 3–8. https://doi.org/10.12691/ijefm-2-2-2.

Syed, T.A., Alzahrani, A., Jan, S., Siddiqui, M.S., Nadeem, A., Alghamdi, T., 2019. A comparative analysis of blockchain architecture and its applications: problems and recommendations. IEEE Access 7, 176838–176869.

Tapscott, A., Tapscott, D., 2017. How blockchain is changing finance. Harv. Bus. Rev. 1 (9), 2–5.

Thomas, D.J., Griffin, P.M., 1996. Coordinated supply chain management. Eur. J. Oper. Res. 94 (1), 1–15.

Tian, H., He, J., Ding, Y., 2019. Medical data management on blockchain with privacy. J. Med. Syst. 43 (2), 26.

Treiblmaier, H., 2018. The impact of the blockchain on the supply chain: a theory-based research framework and a call for action. Supply Chain Manage. 23 (6), 545–559.

Tsoi, K.K., Sung, J.J., Lee, H.W., Yiu, K.K., Fung, H., Wong, S.Y., 2021. The way forward after COVID-19 vaccination: vaccine passports with blockchain to protect personal privacy. BMJ Innov. 7 (2), 337–341.

Van Bavel, J.J., Baicker, K., Boggio, P.S., Capraro, V., Cichocka, A., Cikara, M., et al., 2020. Using social and behavioural science to support COVID-19 pandemic response. Nat. Hum. Behav. 4 (5), 460–471.

Vincent, N.E., Skjellum, A., Medury, S., 2020. Blockchain architecture: a design that helps CPA firms leverage the technology. Int. J. Account. Inform. Syst. 38, 100466.

Wang, W., Hoang, D.T., Hu, P., Xiong, Z., Niyato, D., Wang, P., et al., 2019. A survey on consensus mechanisms and mining strategy management in blockchain networks. IEEE Access 7, 22328–22370.

Wüst, K., Gervais, A., 2018, June. Do you need a blockchain? In: 2018 Crypto Valley Conference on Blockchain Technology (CVCBT). IEEE, pp. 45–54.

Xia, Q.I., Sifah, E.B., Asamoah, K.O., Gao, J., Du, X., Guizani, M., 2017. MeDShare: trustless medical data sharing among cloud service providers via blockchain. IEEE Access 5, 14757–14767.

Yli-Huumo, J., Ko, D., Choi, S., Park, S., Smolander, K., 2016. Where is current research on blockchain technology?—a systematic review. PLoS One 11 (10), e0163477.

Yong, B., Shen, J., Liu, X., Li, F., Chen, H., Zhou, Q., 2020. An intelligent blockchain-based system for safe vaccine supply and supervision. Int. J. Inform. Manage. 52, 102024.

Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H., 2017. An overview of blockchain technology: architecture, consensus, and future trends. In: 2017 IEEE International Congress on Big Data (BigData Congress). IEEE, pp. 557–564.

Zheng, Z., Xie, S., Dai, H.N., Chen, X., Wang, H., 2018. Blockchain challenges and opportunities: a survey. Int. J. Web Grid Serv. 14 (4), 352–375.