# Chapter 12
# Blockchain Technology in Healthcare: Use Cases Study


**Halima Mhamdi, Soufiene Ben Othman, Ahmed Zouinkhi, and Hedi Sakli**

**Abstract** Blockchain technology is now regarded as one of the most interesting and possibly innovative technologies. It enables information to be stored and exchanged securely and transparently without the need for a centralized authority to regulate it. A few of the primary benefits of this technology is the atomicity of the stored data. Given its features, this technology has the potential to give answers to challenges encountered in a very sensitive sector, notably healthcare. The medical field is dealing with several issues that some are attempting to address today. The most important are the administration of medical records and the claims process, the acceleration of clinical and biomedical research, and the advancement of the biomedical and health data registry. The major challenge is the processing and analysis of patient records due to the large amount of data collected. The security of this data is another challenge to consider. Due to the high connectivity, these systems are prone to malicious attacks. In addition, it is difficult to ensure confidentiality due to the exchange of sensitive data. This chapter discusses the use of blockchain technology in healthcare sector. The purpose of this survey was to provide an overview of the features and concepts related to security requirements of blockchain in a healthcare system. It shows that this technology has a major role in terms of security of patient's medical data.

H. Mhamdi · A. Zouinkhi
MACS Research Laboratory, National Engineering School of Gabes, Gabes University, Gabes, Tunisia
e-mail: ahmed.zouinkhi@enig.rnu.tn

S. B. Othman
PRINCE Laboratory Research, ISITcom, Hammam Sousse, University of Sousse, Sousse, Tunisia

H. Sakli (✉)
MACS Research Laboratory, National Engineering School of Gabes, Gabes University, Gabes, Tunisia

EITA Consulting, Montesson, France
e-mail: hedi.s@eitaconsulting.fr



C. Chakraborty, M. R. Khosravi (eds.), *Intelligent Healthcare*,
https://doi.org/10.1007/978-981-16-8150-9_12

**Keywords** Blockchain · Smart healthcare · Secure data management · Internet of medical things · Electronic healthcare record · Drug supply chain · Clinical trials · Security · Privacy

## 12.1 Introduction

The Internet of Things (IoT) is described as a network of identifiable and unique components that interact even without human assistance via Internet connectivity [1]. This new idea encompasses numerous areas: energy [2], smart home [3], agriculture [4], healthcare [5–7], industry [8] and etc.

The incorporation of IoT in the healthcare field is fostering a new approach known as the Internet of Medical Things (IoMT). This term refers to a connected infrastructure of devices and software applications that can communicate with various IT systems to provide health-related services [9]. Telemonitoring for patients with chronic or long-term diseases is one instance of IoMT. This sort of therapy eliminates the need for patients to visit the hospital or doctor's office every time they have a medical concern or a change in their health, as well as inpatient wearable mHealth devices that can communicate data to nurses. Another example, in the pharmaceutical sector, is drug tracking. However, it is important to note that the healthcare sector faces many challenges. The major challenge is the processing and analysis of patient records due to the large amount of data collected. The security of this data is another challenge to consider. These systems are vulnerable to malicious assaults due of their high connection. Furthermore, due to the sharing of sensitive data, it is difficult to maintain privacy.

Healthcare sector faces many challenges. The first one is Patient records management. Currently, information is not shared between doctors, and the patient must carry over the reports of his previous consultations to each new specialist. This mission is more difficult for an uninformed patient who does not master the medical discussion and does not have a precise idea of the content of his file. With the rise of telemedicine, visits to the doctor are made through multiple channels, making it more difficult for healthcare professionals to update patients' medical records. Therefore, it will be vital for this industry to create a way to record and update medical records for both in-person and virtual visits. This means digitizing these records and sharing them, after patient consent, with healthcare professionals to be updated in real time. Clinical trial certification is another one. Clinical trials involving drugs are intended to establish or verify a certain amount of data. The sharing of this data including confidentiality, integrity, record keeping, and patient enrollment is often used by researchers in a secure manner. Sharing research between different scientists and organizations could lead to better and more rapid progress on specific topics. Also, the lack of drug traceability is another issue to which a distributed and public database could provide a start. Securing access to health data is a major issue in network-to-network data transmission. The dependence of IoMT applications and platforms on a centralized cloud puts security at risk.

Blockchain is a new technology that is gaining traction in a variety of industries and offers several benefits and prospects. Blockchain technology is characterized by the immutability of stored data, decentralization, and privacy. Integrated in the health sector, it helps to overcome the problems encountered in the latter.

The purpose of this chapter is to review the current literature on the challenges and approaches to security and privacy in Blockchain Healthcare applications. To provide the reader with the Blockchain necessary background for a better understanding of this area, we outline the various aspects of Blockchain technology, including basic concepts, features, smart contracts, and blockchain types. We also examine current academic chapters that make advantage of Blockchain in various fields. The study of the bibliography is in relation with security from 2018 to 2021. Then, an interest is devoted to the integration of blockchain technology in healthcare. We present existing applications around blockchain to increase healthcare security. Also, we give an overview of the solutions offered by researchers to secure patients' medical data.

The remainder of this chapter is organized as follows. In the second section we discuss the blockchain technology, its function mode, its characteristics as well as the smart contracts. Section 12.3 presents the application of this technology in the healthcare field. In Sect. 12.4, we present the solutions proposed by the researchers in this axis. Finally, we conclude the chapter in Sect. 12.5.

## 12.2 Fundamentals of Blockchain Technology

Machines and devices connect with each other without the use of intermediaries in a peer-to-peer network, resulting in a decentralized network known as Blockchain. It is in fact a set of connected nodes that share and record transactions. Each node in the network keeps a copy to avoid having a single point of failure. The data shared through the blockchain is structured in blocks that are linked together forming a distributed ledger (DLT). The security and immutability of this data is ensured through cryptographic functions. The concept of blockchain is introduced by Satoshi Nakamoto in 2008 [10].

Blockchain technology is mainly characterized by major elements: decentralized, transparent, autonomous, secure, and immutable [11, 12]. Blockchain is decentralized. It is a distributed database where data is stored in all nodes of the network. All nodes can manipulate access and update transactions simultaneously and without intermediary via a well-defined protocol. This data is not all held on a central intermediary's server, but instead is "distributed", i.e. hosted by each participant. Since their creation, the transactions in the blockchain are accessible by all users. But they are extended by cryptographic functions so that they cannot be modified. That is to say that the addition of transactions is allowed and not their modification or deletion. As in the Bitcoin network, all transactions are public and verifiable by everyone through a consensus mechanism, which will allow everyone to ensure that each participant owns the Bitcoins they are spending and that they are

spending them only once. The transparent nature of blockchain could certainly prevent the modification or theft of this data. The blockchain corresponds to a history of transactions on which everyone agrees. This consensus on the sequencing of transactions solves the so-called "double spending" problem: A Bitcoin spent in one transaction cannot be spent a second time in a transaction that would later be broadcast on the network. The second transaction would be rejected by the network. Once recorded in the blockchain, it is impossible to delete or modify a transaction since there are several copies in different nodes of the network. Therefore, the blocks can be extended and not modified. This gives the blockchain a high level of security and makes it more complicated to attack the blocks of information. In the blockchain network, the handling of transactions is no longer concentrated in a central organization but is spread over all participants of the network. Transactions can be consulted and stored by each node and even transferred and updated. In this way, the blockchain functions autonomously without the intervention of a trusted third party and keeping the identity of the node anonymous and secure.

### *12.2.1 Blockchain Operations and Classifications*

Once we begin the blockchain operating procedure, we must specify a transaction. This is the process by which Blockchain nodes exchange and share information. Transactions are really data exchanges between network members that are saved in files called blocks. These data are encrypted before being linked to the previous block to form a chain. Each time a transaction is added to the blockchain, it develops. Transactions must be checked and validated ahead of time.

The function process of blockchain transactions begins when someone B requests a transaction from A. The data requested by the other party B will form a new block and will be distributed on the different nodes of the blockchain network. In order to be transferred, the new block is verified and validated by the network nodes using cryptographic techniques. After being validated, it is added to the previous blocks in chronological order. The added block is chained in such a way that it cannot be modified or deleted. At the final stage, user B receives the transaction from A which ends successfully.

According to its characteristics and functionalities, the blockchain is classified into three categories: public blockchain, private blockchain and consortium blockchain [13]. In the public blockchain network, transactions are managed by all participants without central control organs. They have the right to consult and even modify the exchanged data. The use of consensus mechanism guarantees the security and immutability of this type of network. The most famous example of public blockchain is Ethereum and Bitcoin. In the private blockchain network only authorized participants can access it. The access is done by invitation from the entities controlling the network. Therefore, in order to carry out transactions, participants must request permission from third parties. This type of network is usually applied between companies of the same type. Hyperledger Fabric is an example of a private

blockchain. The consortium blockchain is the fusion between the public and private blockchain. The reading and writing of transactions in this type is both allowed for some nodes and restricted for others. The consensus is the most noticeable distinction between the two systems. Instead of an open system in which anybody may validate blocks or a closed system in which only one entity appoints block producers, a consortium chain includes a number of equally powerful parties that serve as validators and producers at the same time. BigchainD B is an example of a consortium blockchain.

### *12.2.2 Smart Contracts and Ethereum Platform*

The use of smart contracts and decentralized applications (DApp) is one of blockchain's most valuable assets. Their primary function is to facilitate the exchange of goods and services, as well as monetary transactions, without the need of a third-party authority.

Nick Szabo defines smart contracts in 1994 as "a computerized transaction protocol that performs the provisions of a contract" [14]. The smart contract performs transactions automatically, with no human intervention required. The information handled by the smart contract is transmitted via linked items and other measurement equipment. Miners in the blockchain examine the transactions [15, 16] and update them in order for them to be stored in the blockchain. Blockchain systems such as Ethereum are used to create smart contracts. This is the most promising blockchain platform. It can handle sophisticated bespoke smart contracts written in Turing-complete code. Solidity, a high-level programming language, is used to create smart contract code, which is subsequently translated into Ethereum Virtual Machine (EVM) byte code. In the EVM, the quantity of gas is the cost or execution fee for each transaction. This fee is calculated as follows:

$$Fee = gasPrice \times \min(gasLimit, gasUsed) \tag{12.1}$$

where *gasPrice* is the amount of Gwei, as a form of remuneration, received by the miners, *gasLimit* is the maximum gas amount to complete a transaction and *gasUsed* is defined depending on the storage and processing quantity for each transaction.

A decentralized application is an application deployed on blockchain and is generally based on smart contracts. It aims to improve the transparency and traceability of the collected information. Given the number of researchers and developers who are attracted to DApp, various sites gather statistics on the different DApp applications.

### *12.2.3 Blockchain Applications*

Blockchain technology attracts the interest of several researchers in different fields. B. Bhushan et al. [17, 18] and Saxena et al. [19] presented an in-depth study on the combination of blockchain technology and IoT. They focused on IoT applications by ensuring security, confidentiality, and privacy in IoT systems. They also investigated the future challenges in this sector. Authors in their article [20], with the same aim guarantee security and confidentiality, have exposed the contribution of this technology in the design and development of smart city. Other researchers have exploited the use of blockchain in the supply chain [21, 22]. This use aims to solve the problem of reliability and access to manufacturer information. The proposed solution is based on the use of the Ethereum blockchain and the ERC20 interface. It guarantees data security and traceability as well as interoperability by reducing the cost and making exchanges automatic in the supply chain and manufacturing. Authors in [23] addressed the security and privacy issue in Internet of vehicle using blockchain. In addition, Halima et al. [24] exploited the decentralized feature to ensure communication between vehicles and service providers. To protect and secure the flow of financial data on mobile banking platforms, the authors in Ref. [25] propose architecture based on a multilevel authentication mechanism that produces a unique time-based password. This solution ensures the security and confidentiality of banking transactions.

To study the impact of blockchain technology in various sectors: Healthcare, smart cities, Internet of Vehicles, agriculture, ... in terms of security, statistics concerning articles published in this context are made. The queries used are "blockchain and security", "blockchain and security and Healthcare", "Blockchain and security and smart cities", "Blockchain and security and Internet of Vehicles"... The data is collected from IEEE explore, Springer, Science Direct and MDPI, etc. databases from 2018 to 2021. Figure 12.1 depicts the number of articles by year

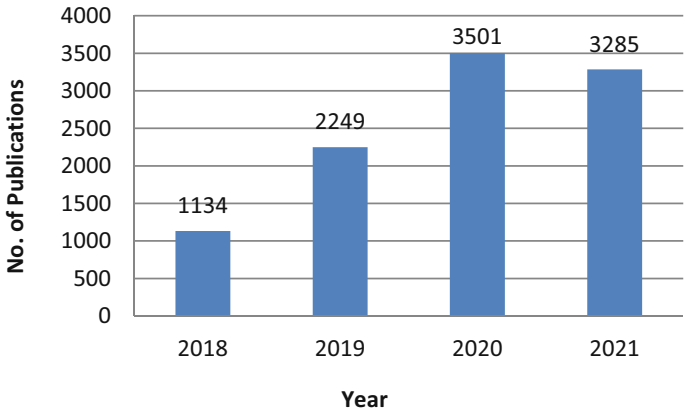



**Fig. 12.1** Number of publications from 2018 to 2021

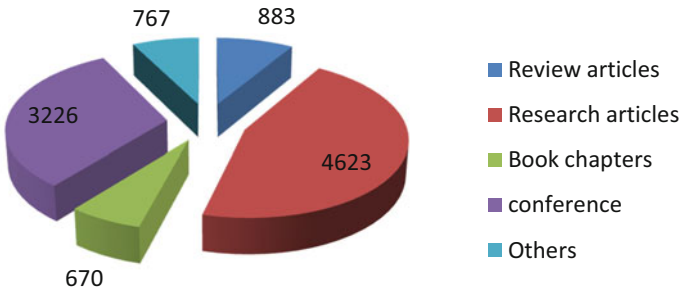
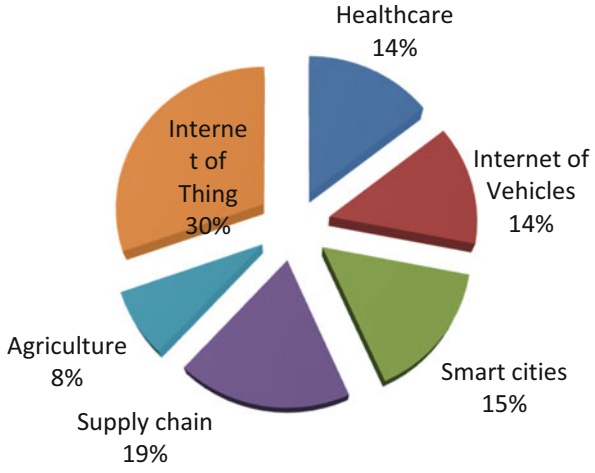



**Fig. 12.2** Number of publications according to article type

**Fig. 12.3** Distribution of publications according to application sector




during the last 4 years. We discovered about 10,169 publications in total. This number is growing more and more, which shows the interest of this technology in improving security in various sectors. As shown in Fig. 12.2, analyses made on the number of articles according to the type of publication show that research articles exceed 45% of the publications followed by conference papers of 31%.

We have reported the data from the evaluated publications regarding the implication of blockchain technology in the different sectors in Fig. 12.3. This graph reveals that the highest percentages of research articles were obtained in Internet of things, while the second-highest percentages of publications were obtained in supply chain then Healthcare and internet of Vehicles.

Figure 12.4 illustrates the numbers of published studies based on applicable disciplines and Blockchain roles in various applications, where the majority of articles are from Blockchain IoT and the second-highest number of articles cover supply chain applications. Healthcare sector the field of health is ranked as the third most important. These statistics are for articles published in 2021.

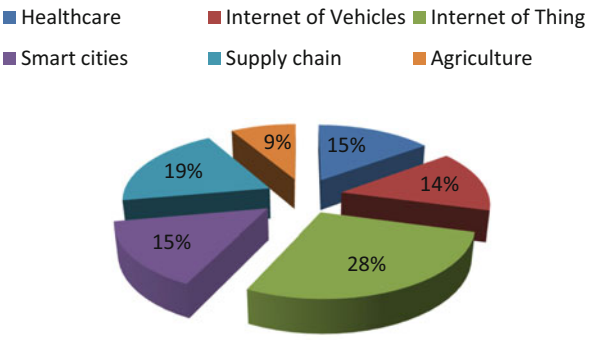



**Fig. 12.4** Distribution publications according to application sector in 2021

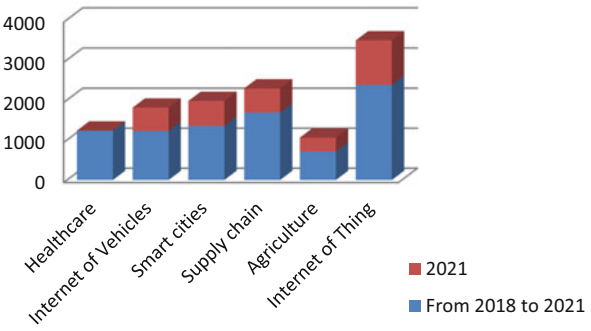



**Fig. 12.5** Distribution Journal articles according to application sector

While Fig. 12.5 shows the number of publications by type of domain during the last 4 years compared to the year 2021. Taking the list of research publications, we can see that the Internet of Things still occupies the first place since it groups the other domains.

In the rest of this chapter, we will focus on the exploitation of blockchain technology in the health care sector. More precisely, how to use this new concept to secure medical data. We will expose the existing works in this context.

## 12.3 Blockchain for Smart Healthcare

Because of blockchain's potential and features, this technology is seen as a critical answer to challenges encountered in the Healthcare sector. It piques the curiosity of many healthcare experts. 7 out of 10 anticipate blockchain's major benefits to apply to clinical trials and medical records, and 6 out of 10 believe blockchain will enable them access new markets and new reliable and secure information [26]. The application of blockchain in the healthcare sector can be classified into many axes. The most relevant one is patient data management which includes electronic healthcare record sharing and access. Counterfeit drugs and pharmaceutical supply chain are the second axes in drug supply chain. Clinical trials are another use cases that need

security and privacy manipulation. Table 12.1 presents a summary of the integration of blockchain technology in the healthcare field. It groups different use cases with various types of blockchain with the use of smart contracts.

Bakhtawar et al. [27] suggested a method to protect individuals from the Corona virus. The created architecture is built on blockchain technology and ANFIS (Adaptive Neuro-Fuzzy Interference System). The connection between these two ideas and the KNN (K Nearest Neighbor) method ensures patient privacy while increasing the detection probability of those infected with Covid19. The mobile application ensures the traceability of patient interactions through bluetooth, and the data acquired is kept on the cloud.

In Ref. [28], the authors proposed a platform named BiiMed. This solution aims at sharing the patient's electronic health record between different stakeholders. It ensures data integrity and interoperability thanks to the blockchain. The proposed architecture is composed of two parts: Health Information System and BiiMed blockchain. HIS consists in gathering, saving, and sharing medical data while the BiiMed platform manages the shared data. It is based on the Ethereum blockchain and the smart contract.

MedChain [29] is another platform that works on the same principle of sharing data by storing them immutably in the blockchain. In their work [30], test scenarios are designed and implemented. They are based on HyperLedger Fabric to examine various identification criteria in the health sector. The authors have exploited blockchain technology to ensure security, privacy and confidentiality of data. The health sector is a very sensitive area and therefore these criteria must be present in any application in this sector. Analyses made show that blockchain technology ensures authenticity by avoiding attacks through its encryption capacity. Moreover, and most importantly, access to patient medical data is controlled. Only authorized persons are able to consult this data. However, the private blockchain, HyperLedger Fabric, ensures the security, confidentiality and transparency of data for healthcare. These criteria can be extended to other blockchain platforms with performance evaluation as well as energy consumption while ensuring security.

The authors of Ref. [31] have proposed a system called MeDShare. This system allows the exchange of medical data and keeps electronic medical records secure. The participants in this system are hospitals, service providers and health research. They use medical data shared by MeDshare. Data confidentiality is ensured by a customized audit control. In the same sense of sharing medical information, the authors have developed the Medblock prototype [32] based on the blockchain. This prototype allows secure access to electronic medical records.

H. S. Z. Kazmi et al. [33] have exploited smart contracts to design a system for remote patient monitoring and alerting health specialists in case of emergency. This remote monitoring system guarantees the security and privacy of the patient through blockchain.

To solve the interoperability problem, authors [34] implemented a blockchain-based system. It allows patients to share their clinical data with healthcare providers. The patient has the right to choose the person with whom he shares his data. Access

**Table 12.1** Summarized literature review

| Problem addressed | | | | | |
|---|---|---|---|---|---|
| Uses Cases | Ref | Year | Framework | Smart contract | Contribution |
| Patient data management | [27] | 2021 | NM | No | - Share the patient's electronic health record between different stakeholders.<br>- Ensures integrity, confidentiality and interoperability of the data shared<br>- Resolved the problem of large-scale data management and sharing in an EHR system.<br>- Remote monitoring system guarantees the security and privacy of the patient. |
| | [28] | 2020 | NM | Yes | |
| | [29] | 2019 | Ethereum | | |
| | [30] | 2021 | Ethereum | | |
| | [31] | 2018 | NM | No | |
| | [32] | 2018 | NM | | |
| | [33] | 2020 | Proprietary | | |
| | [34] | 2019 | NM | | |
| Security and privacy in blockchain-healthcare | [35] | 2018 | NM | NM | - Allows the sharing of patient data by controlling the access to these sensitive data.<br>- Ensure the security of private data.<br>- Ensure the confidentiality of messages on the blockchain.<br>- Provides access at different levels of granularity without the need for a public key infrastructure (PKI).<br>- Ensures the integrity, security, and confidentiality of private patient data. |
| | [36] | 2018 | NM | NM | |
| | [37] | 2017 | NM | NM | |
| | [38] | 2018 | NM | NM | |
| | [39] | 2018 | NM | NM | |
| | [40] | 2021 | NM | Yes | |
| | [41] | 2021 | NM | NM | |
| Drug/pharmaceutical supply chain management | [42] | 2020 | NM | NM | - Product identification and tracking in pharmaceutical supply chains.<br>- Maintain security, traceability, and visibility in the pharmaceutical supply chain.<br>- Tracking of pharmaceutical products during distribution.<br>- Monitor drug files to ensure the confidentiality, security and transparency of the management process and the sharing of the drug life cycle. |
| | [43] | 2010 | NM | Yes | |
| | [44] | 2019 | NM | | |
| | [45] | 2019 | NM | | |
| | [46] | 2019 | NM | | |
| Clinical trial certification | [47, 48] | 2019, 2018 | Bitcoin | NM | - Avoid undesirable consequences of drug use.<br>- Development of platforms and systems for collecting and sharing patient data in clinical trials.<br>- Support the transparency of the data and documents retrieved during clinical research.<br>- Ensure traceability of clinical data. |
| | [49] | 2018 | NM | NM | |
| | [50] | 2017 | NM | NM | |
| | [51] | 2019 | NM | NM | |
| | [52] | 2021 | Ethereum | Yes | |

to the data in a secure way is ensured by the identification and authentication of the user. Once identified, they can access and update the patients' data.

The authors of [35] tackled the problem of security and patient privacy. They proposed a system based on the immutability and autonomy of the blockchain. This system allows the sharing of patient data by controlling the access to these sensitive data. Discrete wavelets transform and genetic algorithm are the basis of the proposed scheme.

To ensure the security of private data, the authors of Refs. [36, 37] proposed a key management scheme to ensure the confidentiality of messages on the blockchain. In the same context, Zhang and Poslad [38] suggest an access authorization model and scheme called Granular Access Authorization supporting Flexible Queries (GAA-FQ) using encryption and decryption algorithms. This scheme provides access at different levels of granularity without the need for a public key infrastructure (PKI).

The signature scheme proposed in Ref. [39] is a solution ensuring security and trust. Thanks to the attribute with multiple authorities, which is the backbone of this solution, the patient's public/private keys are not generated and shared.

The solution proposed by the authors [40] deals with contract automation in the healthcare supply chain. It brings together all parties involved in the purchasing process of medical products. The manufacturer, the distributor as well as the Group Purchasing Organization (GPO) and the healthcare provider interact with each other using smart contracts. For storage of large amounts of information, transactions and data exchange are stored in a distributed storage system such as Interplanetary File System (IPFS) or Filecoin. Then a link between Ethereum blockchain and the storage system is established in order to keep the data secure via cryptographic functions. Therefore, the result is a more secure, feasible and cost-minimizing automatic health supply chain management system.

The authors proposed [41] a system named "Internet-of-Healthcare Systems" (IoHCS). This system saves patient medical data on the distributed blockchain system. In this way, all participants: doctor, nurse or a member of the medical staff, can access the patient's electronic records in real time and securely. As illustrated in the following figure, the developed model is composed by six elements: Hospital Information system HIS, The Central Server, Web / Software Agents, Message Queuing Telemetry Transport (MQTT) Broker, Mobile Device Systems and blockchain. The components of the system work together to ensure the proper functioning of the process of access to the electronic medical record in a way that guarantees the security, confidentiality, and integrity of data.

The traceability of drugs and the fight against counterfeiting is another concrete case of blockchain and IoMT. According to the World Health Organization, 1 in 10 pharmaceutical products are counterfeit. This figure reaches 30% of medicines in developing countries, which represents a market of 200 billion dollars. Moreover 25 million counterfeit drugs are distributed on the Internet with a value of 43 million Euros [42].

Drug traceability is a very sensitive area that needs an urgent solution as it affects the lives of individuals. The use of blockchain technology brings advantages in this

context especially in the tracking of pharmaceutical products during distribution. For this use case, the different supply chain actors are identified in the blockchain network. Pharmaceutical companies register their products with a unique identifier. Stores reselling the drugs or pharmacists could check upon receipt of stocks of drugs that they come from valid laboratories; the information related to each drug is updated in the blockchain each time.

Clauson et al. [43] present a detailed study on the application of blockchain technology in pharmaceutical supply chains. This study includes product identification and tracking as well as validity verification.

To manage medical data, the authors [44] proposed a decentralized application (Dapp) based on blockchain technology in particular Ethereum blockchain and smart contracts. The developed solution handles various medical cases including patient, doctor, pharmacies, laboratory and any other service provider. The application includes the management of medical prescriptions, tests and analysis results from the laboratory. The communication between the different actors of the system and the reimbursement of health care are also covered. The authors did not forget the cases of clinical trials and surgical procedure in their study. They used different smart contracts for each study case based on the consensus mechanism and a distributed file system (DFS). The cost of deploying smart contracts varies between the developed services. It depends on the number of actors in the platform and the complexity of the process required such as surgery and pediatrics.

In their article [45], authors exploit the notion of smart contracts and multi-agents 'system. They propose a platform allowing the storage of transactions between the different actors of the system in the blockchain. The smart contracts ensure the management of these transactions.

To maintain security, traceability and visibility in the pharmaceutical supply chain, the authors [46] designed a private blockchain platform to fight drug counterfeiting. Similarly, a proof-of-concept application has been developed by Jamil et al. [47]. This platform consists of a web application whose role is to monitor drug files between doctors, patients, pharmacists, etc. in a decentralized manner. The smart contracts guarantee the confidentiality, security and transparency of the management process and the sharing of the drug life cycle.

In order to develop medical and biological insights, biomedical research called a clinical trial is done on humans. The objective of these clinical trials is to develop and verify a series of data. They allow, but are not limited to, demonstrating the efficacy, relevance and safety of a drug in relation to a disease. Indeed, the objective of these studies is to demonstrate causality between the favorable evolution of a disease and the taking of a specific treatment.

Several studies have exploited blockchain in clinical research to avoid undesirable consequences of drug use [48]. The characteristics of blockchain, notably its immutability, transparency, and decentralization, encourage the development of platforms and systems for collecting and sharing patient data in clinical trials [49].

The authors of [50] use the Ethereum Blockchain platform and smart contracts. The results found support the transparency of the data and documents retrieved during clinical research. In the same context, use of smart contracts and blockchain,

Zhuang et al. [51, 52] presented an automatic and secure validation system for unmediated clinical trials via distributed databases.

## 12.4 Discussion and Solutions

Healthcare is not like any other field, and it must adhere to extremely stringent confidentiality regulations. To work in the healthcare sector, a blockchain must first and foremost provide data confidentiality and patient data privacy.

While handling health records, the patient, the physicians, the hospital, the pharmacists, or the medical analysis laboratories all seem to be sources of data that must be seen and shared in a straightforward manner. This is a common issue when a patient is admitted to the hospital. Health practitioners do not always have access to the patient's past and do not have comprehensive insight into the therapies he/she is receiving, the history of his/her disease, or the history of his/her family. The optimal solution would be to have a list of all the locations where a patient's medical data may be found so that it can be accessed promptly. With the patient's permission, this list would be available to any health practitioner who requested it. As a result, rather than having access just to the database of the establishment where one is, one might have access to all of the sources of information spread across the network's databases. Blockchain technology, in the form of a distributed and secure registry, presents precisely such a solution, allowing patients to not only see their data, but also manage access to it. As a result, we assure the interoperability of the platform utilized by the various health players using blockchain technology. Similarly, the emergency service can have access to patient data without requiring a request from the patient.

The MyHealthMyDataproject in Europe creates a health blockchain model that is consistent with medical privacy since no information is kept directly on the blockchain: only links to its information are saved. MyHealthMyData, a Siemens partner, strives to improve access to and exchange of health data in clinical studies. If a person wishes to delete his or her data from the blockchain, he or she will be able to break the links to his or her information, without having to break the chain. The different blocks will remain in place in the chain but will be permanently deactivated.

The characteristics of blockchain technology allow it to play a prominent role in the certification of clinical trials. Indeed, blockchain could be used to ensure that data is collected and exchanged, when necessary, while respecting patient privacy or proprietary information. The use of this technology allows saving the results found as well as the data and reports from the clinical research in an immutable way. This property overcomes the problems of changing results, thus reducing the incidence of fraud and error in clinical trial records. Blockchain brings transparency to clinical trials. Also, the pharmaceutical industry could use blockchain to authenticate clinical trial results.

**Table 12.2** Security solutions in IoT smart healthcare systems

| Reference | Problem addressed | Technology used | Solution |
|---|---|---|---|
| [53–56] | Patient data security and privacy | Multi-agents system and Blockchain | Use of patient agent-assisted end-to-end, patient centric agent, smart contracts and consensus algorithm. |
| [57–59] | Respect patients' privacy | Artificial intelligence | Develop protocol and deep learning-based algorithm to ensure patient privacy that authenticate |
| [60–63] | Data integrity and privacy of the patient | Lightweight cryptography | Propose an EPPDA scheme: An efficient and privacy-preserving data aggregation scheme with authentication for IoT-based healthcare applications. |
| [64–66] | Control and management of IoT data | Software defined networking | Combine SDN with data generated by smart healthcare applications to improve the flexibility and intelligence of IoT supervision and control. |

To overcome gaps in secure patients' healthcare data, many solutions are proposed in the literature. Table 12.2 summarizes this several works.

Authors in [53–56] suggest the use of Multi-agents system with blockchain. In this solution, autonomous agents can execute action in place of users. For constructing secure intelligent healthcare systems, Smart agents are used with smart contracts to combine Blockchain technology with Body Area Sensor Networks (BASN). Smart contracts implemented on the Blockchain may automatically analyze health data based on threshold levels and store transaction logs in the Blockchain's immutable ledger to provide direction regarding for nurses or doctors. Nevertheless, nothing is known about the archival management of medical records, the security and privacy of the patient end-devices, and processing organization for the Blockchain in present IoT eHealth and Blockchain research. Authors in [54] suggested a Patient Agent-assisted End-to-End decentralized Blockchain-enabled eHealth architecture. By combining Blockchain, machine learning, and artificial intelligence technologies. The agent can handle the issues highlighted by combining wireless body sensors with Blockchain. Other solutions [55] consist of developing Patient Centric Agent (PCA) based on consensus algorithm. It maintains the patient's safety and privacy. It also identifies the streaming data storage and security requirements.

Other researchers are using artificial intelligence (AI), in particular machine learning (ML), to ensure security and privacy in the smart healthcare. In their article [57], the authors have gone over the key applications and systems where AI and IoT are being advocated for a safer, more accurate, and predictive healthcare system. The protocol defined by Gope et al. [58] allows to respect patients' privacy by authenticating IoT devices. Security is provided against machine learning or modeling attacks. Using a deep learning-based algorithm, authors [59] create an IoT-based automated noninvasive patient pain detection/monitoring system. To monitor patient

pain, the proposed system does not require any wearable bothersome sensing devices, line-of-sight cameras, or any specialized/constrained surroundings.

Many approaches based on Cryptography were built to detect and block attacks in the healthcare application using IoT. Several security schemes to protect healthcare systems based-IoT using Cryptographic solutions are available in the literature [60–63].

In the literature, there are several security approaches for IoT-based healthcare systems that use Software Defined Networking (SDN) [64–66]. SDN allows healthcare businesses to benefit from virtualization, resulting in greater network agility and lower total cost of ownership. SDN delivers security benefits as a result of its architecture. Because the SDN controller can view all network data at the same time, it's simpler to identify unusual behavior in intruder-generated network traffic. Rather of waiting for an operating system or application software update for manufacturer-proprietary equipment, once a new threat has been detected, operators can quickly build new software to analyze and mitigate the risk.

## 12.5 Conclusion

This chapter presents a state of the art on the impact of blockchain technology in the healthcare sector. The most relevant applications in this area are electronic patient record sharing, and pharmaceutical tracking, clinical trial, and security in healthcare. Blockchain brings security, integrity, and transparency to the healthcare field. Despite the promising offers of blockchain in terms of confidentiality and efficiency, there is a lack of realization of solutions proposed by researchers. It is therefore necessary to carry out an important upstream work of data digitization, process automation, staff education and regulatory supervision.

**Conflict of Interest**
There is no conflict of interests.

**Funding**
There is no funding support.

**Data Availability**
Not applicable.

## References

1. Farooq, M., Waseem, M., Mazhar, S., et al. (2015). A review on internet of things (IoT). *International Journal of Computers and Applications, 113*(1), 36–54.
2. Zouinkhi, A., Ayadi, H., Val, T., Boussaid, B., & Abdelkrim, M. N. (2020). Auto-management of energy in IoT networks. *International Journal of Communication System, 33*(1), e4168.

3. Malcheand, T., & Maheshwary, P. (2017). Internet of things (IoT) for building smart home system. In *Proceedings of the 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India* (pp. 65–70). IEEE.
4. Minbo, L., Zhu, Z., & Guangyu, C. (2013). Informat ion service system of agriculture IoT. *Automatika, 54*(4), 415–426.
5. George, G., & Thampi, S. M. (2019). Securing smart healthcare systems from vulnerability exploitation. In G. Wang, A. El Saddik, X. Lai, G. MartInez Perez, & K. K. Choo (Eds.), *Smart city and informatization. iSCI* (Communications in computer and information science) (Vol. 1122). Springer.
6. Almalki, F. A., Othman, S. B., Almalki, F. A., & Sakli, H. (2021). EERP-DPM: Energy efficient routing protocol using dual prediction model for healthcare using IoT. *Journal of Healthcare Engineering, 15*, 9988038.
7. Almalki, F. A., & Othman, S. B. (2021). EPPDA: An efficient and privacy-preserving data aggregation scheme with authentication and authorization for IoT-based healthcare applications. *Wireless Communications and Mobile Computing, 2021*, 5594159.
8. Trab, S., Bajic, E., Zouinkhi, A., Abdelkrim, M. N., & Chekir, H. (2018). RFID IoT-enabled warehouse for safety management using product class-based storage and potential fields methods. *International Journal of Embedded Systems, 10*(1), 71–88.
9. Mohd Aman, A. H., Hassan, W. H., Sameen, S., et al. (2021). IoMT amid COVID-19 pandemic: Application, architecture, technology, and security. *Journal of Network and Computer Applications, 174*, 102886.
10. Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. Retrieved from https://bitcoin.org/bitcoin.pdf.
11. Tasca, P., & Tessone, C. J. *A taxonomy of blockchain technologies: Principles of identification and classification* (p. 4). Ledger. https://doi.org/10.5195/ledger.2019.140
12. Manpreet, K., Mohammad, Z. K., Shikha, G., Abdulfattah, N., Chinmay, C., & Subhendu, K. P. (2021). MBCP: Performance analysis of large scale mainstream Blockchain consensus protocols. *IEEE Access, 9*, 1–14. https://doi.org/10.1109/ACCESS.2021.3085187
13. Hong-Ning, D., Zibin, Z., & Zhang, Y. (2019). Blockchain for Internet of Things: A survey. *IEEE Internet of Things Journal, 6*(5), 8076–8094.
14. Szabo, N. (1997). Smart contracts: Formalizing and securing relationships on public networks. *First Monday, 2*, 9–1.
15. Wang, S., Yuan, Y., Wang, X., Li, J., & Qin, R. (2018). *An overview of smart contract: Architecture, applications, and future trends* (pp. 108–113). IEEE.
16. Riabi, I., Ayed, H. K. B., & Saidane, L. A. (2019). A survey on Blockchain based access control for internet of things. In *15th International Wireless Communications & Mobile Computing Conference (IWCMC)* (pp. 502–507). Tangier.
17. Bhushan, B., Sahoo, C., Sinha, P., & Khamparia, A. (2020). *Unification of Blockchain and Internet of Things (BIoT): Requirements, working model, challenges and future directions*. Wireless Networks. https://doi.org/10.1007/s11276-020-02445-6
18. Bhushan, B., Sinha, P., Sagayam, K. M., & J, A. (2021). Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions. *Computers & Electrical Engineering, 90*, 106897. https://doi.org/10.1016/j.compeleceng.2020.106897
19. Saxena, S., Bhushan, B., & Ahad, M. A. (2021). Blockchain based solutions to secure IoT: Background, integration trends and a way forward. *Journal of Network and Computer Applications, 181*(5), 103050. https://doi.org/10.1016/j.jnca.2021.10305
20. Haque, A. K., Bhushan, B., & Dhiman, G. (2021). *Conceptualizing smart city applications: Requirements, architecture, security issues, and emerging trends*. Expert Systems. https://doi.org/10.1111/exsy.12753
21. Ajay, K., Kumar, A., Bharat, B., & Chinmay, C. (2021., [SCI, IF 2.79]). Secure access control for manufacturing sector with application of Ethereum blockchain. *Peer-to-Peer Networking and Applications, 14*, 3058–3074. https://doi.org/10.1007/s12083-021-01108-3

22. Hong-Ning, D., Zibin, Z., & Zhang, Y. (2019). Blockchain for Internet of Things: A survey. *IEEE Internet of Things Journal, 6*(5), 8076–8094.
23. Ramaguru, R., Sindhu, M., & Sethumadhavan, M. (2019). Blockchain for the internet of vehicles. In M. Singh, P. Gupta, V. Tyagi, J. Flusser, T. Ören, & R. Kashyap (Eds.), *Advances in computing and data sciences. ICACDS* (Communications in computer and information science) (Vol. 1045). Springer.
24. Mhamdi, H., Zouinkhi, A., & Sakli, H. (2020). Multi-agents system of vehicle services based on Blockchain. In *20th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA)* (pp. 291–296). Monastir.
25. Joseph, B. A., Chinmay, C., & Sakinat, O. F. (2021). A secured transaction based on Blockchain architecture in Mobile banking platform. *International Journal of Internet Technology and Secured Transactions, 2021*, 1–12. https://doi.org/10.1504/IJITST.2021.10039177
26. IBM Institute for Business Value. In *Healthcare rallies for blockchains*. IBM. https://www.ibm.com/downloads/cas/BBRQK3WY
27. Bakhtawar, A., Abdul, R. J., Chinmay, C., Jamel, N., Saira, R., & Muhammad, R. (2021). Blockchain and ANFIS empowered IoMT application for privacy preserved contact tracing in COVID-19 pandemic. *Personal and Ubiquitous Computing, 2021*, 1–17. https://doi.org/10.1007/s00779-021-01596-3
28. Jabbar, R., Fetais, N., Krichen, M., & Barkaoui, K. (2020). Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity. In *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)* (pp. 310–317). IEEE.
29. Bingqing, S., Guo, J., & Yang, Y. (2019). MedChain: Efficient healthcare data sharing via Blockchain. *Applied Sciences, 9*(6), 1207.
30. Antwi, M. S., Adnane, A., Ahmad, F., Hussain, R., Rehman, M. H. u., & Kerrache, C. A. (2021). The case of HyperLedger fabric as a blockchain solution for healthcare applications. *Blockchain: Research and Applications, 2*(1), 100012. https://doi.org/10.1016/j.bcra.2021.100012
31. Yang, Y., et al. (2018). Medshare: A novel hybrid cloud for medical resource sharing among autonomous healthcare providers. *IEEE Access, 6*, 46949–46961.
32. Fan, K., et al. (2018). Medblock: Efficient and secure medical data sharing via blockchain. *Journal of Medical Systems, 42*(8), 136.
33. Syeda, K., Faiza, N., Sahrish, M., et al. (2020). In L. Barolli et al. (Eds.), *Trusted remote patient monitoring using blockchain-based smart contracts* (BWCCA 2019, LNNS) (Vol. 97, pp. 765–776). Springer Nature.
34. Ullah Khan, A., Shahid, A., Tariq, F., et al. (2020). In L. Barolli et al. (Eds.), *Enhanced decentralized management of patient-driven interoperability based on blockchain* (BWCCA 2019, LNNS) (Vol. 97, pp. 815–827). Springer Nature.
35. Hussein, A. F., Kumar, N. A., Ramirez-Gonzalez, G., Abdulhay, E., Tavares, J. M. R. S., & de Albuquerque, V. H. C. (2018). A medical records managing and securing blockchain based system supported by a genetic algorithm and discrete wavelet transform. *Cognitive Systems Research, 52*, 1–11.
36. Zhao, H., Bai, P., Peng, Y., & Xu, R. (2018). Efficient key management scheme for health blockchain. *CAAI Transactions on Intelligence Technology, 3*, 114–118.
37. Zhao, H., Zhang, Y., Peng, Y., & Xu, R. (2017, March 22–24). Lightweight backup and efficient recovery scheme for health blockchain keys. In *Proceedings of the 2017 IEEE 13th International Symposium on Autonomous Decentralized System (ISADS), Bangkok, Thailand* (pp. 229–234). IEEE.
38. Zhang, X., & Poslad, S. (2018, May 20–24). Blockchain support for flexible queries with granular access control to Electronic Medical Records (EMR). In *Proceedings of the 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA*.

39. Guo, R., Shi, H., Zhao, Q., & Zheng, D. (2018). Secure attribute-based signature scheme with multiple authorities for Blockchain in electronic health records systems. *IEEE Access, 6*, 11676–11686. https://doi.org/10.1109/ACCESS.2018.2801266
40. 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. https://doi.org/10.1109/ACCESS.2021.3062471
41. Yongjoh, S., So-In, C., Kompunt, P., Muneesawang, P., & Morien, R. I. *Development of an internet-of-healthcare system using blockchain*. IEEE Access. https://doi.org/10.1109/ACCESS.2021.3103443
42. du LEEM, R. (2017). *Contrefaçon de médicaments, une atteinte à la santépublique*. Leem, juin. http://www.leem.org/sites/default/files/DP-contrefacon-06-07-2017.pdf
43. Clauson, A., Breeden, A., Davidson, C., & Mackey, K. *Leveraging blockchain technology to enhance supply chain management in healthcare: An exploration of challenges and opportunities in the health supply chain*. Blockchain in Healthcare Today™. ISSN 2573-8240. https://doi.org/10.30953/bhty.v1.20
44. Khatoon, A. (2020). A Blockchain-based smart contract system for healthcare management. *Electronics, 9*(1), 94. https://doi.org/10.3390/electronics9010094
45. Casado-Vara, R., González Briones, A., Prieto, J., & Corchado Rodríguez, J. (2019, June). Smart contract for monitoring and control of logistics activities: Pharmaceutical utilities case study. In *Advances in intelligent systems and computing*. IEEE.
46. Raj, R., Rai, N., & Agarwal, S. (2019). Anticounterfeiting in pharmaceutical supply chain by establishing proof of ownership. In *TENCON 2019–2019 IEEE Region 10 Conference (TENCON)* (pp. 1572–1577). IEEE.
47. Jamil, F., Hang, L., Kim, K., & Kim, D. (2019). A novel medical blockchain model for drug supply chain integrity management in a smart hospital. *Electronics, 8*(5), 505.
48. Radanović, I., & Likić, R. (2018). Opportunities for use of blockchain technology in medicine. *Applied Health Economics and Health Policy, 16*, 583–590. https://doi.org/10.1007/s40258-018-0412-8
49. Roman-Belmonte, J. M., De la Corte-Rodriguez, H., Rodriguez-Merchan, E. C. C., la Corte-Rodriguez, H., & Carlos Rodriguez-Merchan, E. (2018). How Blockchain technology can change medicine. *Postgraduate Medicine, 130*, 420–427.
50. Mytis-Gkometh, P., Efraimidis, P. S., Kaldoudi, E., & Drosatos, G. (2017). Notarization of knowledge retrieval from biomedical repositories using Blockchain technology. In *IFMBE Proceedings* (Vol. 66, pp. 69–73). Springer Nature.
51. Zhuang, Y., Sheets, L. R., Shae, Z., Chen, Y. W., Tsai, J. J. P., & Shyu, C. R. (2019). Applying Blockchain technology to enhance clinical trial recruitment. *AMIA Annual Symposium Proceedings AMIA Symposium., 2019*, 1276–1285.
52. Zhuang, Y., Sheets, L., Gao, X., Shen, Y., Shae, Z. Y., Tsai, J. J. P., & Shyu, C. R. (2021 January 25). Development of A blockchain framework for virtual clinical trials. *AMIA Annual Symposium Proceedings, 2020*, 1412–1420.
53. Cha, S.-C., Chen, J.-F., Chunhua, S., & Yeh, K.-H. (2018). A blockchain connected gateway for ble-based devices in the internet of things. *IEEE Access, 6*, 24639–24649.
54. Uddin, M. A., Stranieri, A., Gondal, I., & Balasubramanian, V. (2020). Blockchain leveraged decentralized iot ehealth framework. *Internet of Things, 9*, 100159.
55. Uddin, M. A., Stranieri, A., Gondal, I., & Balasubramanian, V. (2019). Blockchain leveraged task migration in body area sensor networks. In *25th Asia-Pacific Conference on Communications (APCC)* (Vol. 2019, pp. 177–184). IEEE.
56. Uddin, M. A., Stranieri, A., Gondal, I., & Balasubramanian, V. (2020). Dynamically recommending repositories for health data: A machine learning model. In *Proceedings of the Australasian Computer Science Week Multiconference* (pp. 1–10). IEEE.
57. Bharadwaj, H. K., et al. (2021). A review on the role of machine learning in enabling IoT based healthcare applications. *IEEE Access, 9*, 38859–38890. https://doi.org/10.1109/ACCESS.2021.3059858

58. Gope, P., Sikdar, B., & Millwood, O. A scalable protocol level approach to prevent machine learning attacks on PUF-based authentication mechanisms for internet-of-medical-things. In *IEEE Transactions on Industrial Informatics*. IEEE. https://doi.org/10.1109/TII.2021.3096048
59. I. Ahmed, G. Jeon and F. Piccialli, "A deep-learning-based smart healthcare system for patient's discomfort detection at the edge of internet of things," in *IEEE Internet of Things Journal*, vol. 8, 13, pp. 10318–10326, 2021, doi: https://doi.org/10.1109/JIOT.2021.3052067.
60. Sujata, D., Chinmay, C., Sourav, K. G., Subhendu, K. P., & Jaroslav, F. (2021). *BIFM: Big-data driven intelligent forecasting model for COVID-19* (pp. 1–13). IEEE Access. https://doi.org/10.1109/ACCESS.2021.3094658
61. Almalki, F. A., & Soufiene, B. O. (2021). EPPDA: An efficient and privacy-preserving data aggregation scheme with authentication and authorization for IoT-based healthcare applications. *Wireless Communications and Mobile Computing, 2021*, 5594159., 18 pages. https://doi.org/10.1155/2021/5594159
62. Almalki, F. A., Othman, S. B., Almalki, F. A., & Sakli, H. (2021). EERP-DPM: Energy efficient routing protocol using dual prediction model for healthcare using IoT. *Journal of Healthcare Engineering, 2021*, 9988038., 15 pages. https://doi.org/10.1155/2021/9988038
63. Soufiene, B. O., Bahattab, A. A., Trad, A., & Youssef, H. (2020). PEERP: An priority-based energy-efficient routing protocol for reliable data transmission in healthcare using the IoT. *Procedia Computer Science, 175*, 373–378. https://doi.org/10.1016/j.procs.2020.07.053
64. Wang, T., & Chen, H. (2021). A lightweight SDN fingerprint attack defense mechanism based on probabilistic scrambling and controller dynamic scheduling strategies. *Security and Communication Networks, 2021*, 6688489., 23 pages. https://doi.org/10.1155/2021/6688489
65. Ahvar, E., Ahvar, S., Raza, S. M., Manuel Sanchez Vilchez, J., & Lee, G. M. (2021). Next generation of SDN in cloud-fog for 5G and beyond-enabled applications: Opportunities and challenges. *Network, 1*, 28–49. https://doi.org/10.3390/network1010004
66. Li, Y., Su, X., Ding, A. Y., Lindgren, A., Liu, X., Prehofer, C., Riekki, J., Rahmani, R., Tarkoma, S., & Hui, P. (2020). Enhancing the internet of things with knowledge-driven software-defined networking technology: Future perspectives. *Sensors, 20*, 3459. https://doi.org/10.3390/s20123459