A Survey of Blockchain-Based Strategies for Healthcare

ERIKSON JÚLIO DE AGUIAR and BRUNO S. FAIÇAL, University of São Paulo
BHASKAR KRISHNAMACHARI, University of Southern California
JÓ UEYAMA, University of São Paulo

Blockchain technology has been gaining visibility owing to its ability to enhance the security, reliability, and robustness of distributed systems. Several areas have benefited from research based on this technology, such as finance, remote sensing, data analysis, and healthcare. Data immutability, privacy, transparency, decentralization, and distributed ledgers are the main features that make blockchain an attractive technology. However, healthcare records that contain confidential patient data make this system very complicated because there is a risk of a privacy breach. This study aims to address research into the applications of the blockchain healthcare area. It sets out by discussing the management of medical information, as well as the sharing of medical records, image sharing, and log management. We also discuss papers that intersect with other areas, such as the Internet of Things, the management of information, tracking of drugs along their supply chain, and aspects of security and privacy. As we are aware that there are other surveys of blockchain in healthcare, we analyze and compare both the positive and negative aspects of their papers. Finally, we seek to examine the concepts of blockchain in the medical area, by assessing their benefits and drawbacks and thus giving guidance to other researchers in the area. Additionally, we summarize the methods used in healthcare per application area and show their pros and cons.

CCS Concepts: • **Distributed Systems** → **Networks P2P**; • **Blockchain** → *Distributed Ledger Technology*;

Additional Key Words and Phrases: Distributed systems, blockchain, distributed ledger technology, healthcare, medical, survey

ACM Reference format:
Erikson Júlio de Aguiar, Bruno S. Faiçal, Bhaskar Krishnamachari, and Jó Ueyama. 2020. A Survey of Blockchain-Based Strategies for Healthcare. *ACM Comput. Surv.* 53, 2, Article 27 (March 2020), 27 pages.
https://doi.org/10.1145/3376915

1 INTRODUCTION

The Healthcare area is of great social importance because the issues it addresses are directly concerned with improving the quality of life which it can achieve by overcoming real health problems

Erikson Júlio de Aguiar would like to thank the supporting organizations for funding this work: The Agency *Coordenação de Aperfeiçoamento Pessoal de Nível Superior* - CAPES - Brazil - Finance Code 001 and grant no. 2018/18187-3 from São Paulo Research Foundation – FAPESP. Jó Ueyama would like to thank FAPESP for funding the bulk of his research work through grant no. 2018/17335-9.
Authors' addresses: E. Júlio de Aguiar, B. S. Faiçal, and J. Ueyama, University of São Paulo, São Carlos, SP 13566-590, Brazil; email: erjulioaguiar@usp.br, bsfaical@alumni.usp.br, joueyama@icmc.usp.br; B. Krishnamachari, University of Southern California, Los Angeles, CA; email: bkrishna@usc.edu.
Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
© 2020 Association for Computing Machinery.
0360-0300/2020/03-ART27 $15.00
https://doi.org/10.1145/3376915

[91]. In light of this, the computer has been used to carry out tasks that have led to significant progress in healthcare, such as (i) an automated healthcare record system; (ii) sharing reliable information; (iii) analysis in Big Data; and (iv) collaboration in clinical practice and diagnosis [13, 106, 108].

Healthcare systems have advanced over the years and brought about greater competitiveness in the pharmaceutical industry and helped overcome difficulties in the field [83]. As a result, the users (e.g., physicians, nurses, and social workers) are able to work in an environment that can improve patient care, because there is a better management of healthcare records. Computing provides an opportunity to assist the whole process of patient care, by organizing and managing the information that is required [16, 83, 106].

Historical data stored in computerized healthcare systems can provide valuable information about the health of a patient. In addition, it can be collated and used to analyze epidemics and the healthcare services of both cities and rural areas [45]. These data are of great value for researchers in various fields, and can assist in understanding phenomena and overcoming particular challenges [106]. But, this information must be treated as confidential because it refers to the patients' personal data. Unauthorized disclosure of the personal information of patients may have an adverse effect and tarnish the image of healthcare institutions vis-à-vis society [106]. It is necessary to protect the clinical information of patients and prevent its dissemination, so as to avoid unethical or embarrassing situations [45].

After following the emergence of blockchain technology, some authors have sought to tackle the problems involving reliability and safety in the healthcare system [4, 37, 108]. By having this decentralized architecture, it can now be managed by the users themselves, and it is possible to have more reliable systems. The blockchain can mitigate problems arising from the privacy and integrity of patient information, owing to the features of blockchain, such as immutability, transparency and reliability, and other factors [4, 65]. Another key point is that blockchain assists in the management of logs and the auditing of the data. However, blockchain-based healthcare systems still face challenges that have to be overcome [100]. One of them is the fact that the internal features of the network are anonymous, and this anonymity of the nodes makes it difficult to trace the connections that allow the information to be made available [43].

One of the various areas where the blockchain can be applied is the control and management of drug distribution, and as shown in this article, this involves going through all the stages in the supply chain [57, 66, 86]. Blockchain systems also can assist in combating drug counterfeiters, such as the diversion of pharmaceutical products and theft [66]. It is also worth noting that according to Pratap [85], in a study conducted on behalf of International Business Machines Corporation (IBM), around 16% of healthcare executives plan to implement a blockchain solution in their work environment, and more than 56% expect to do this by 2020.

In short, blockchain can operate in different scenarios in the healthcare field and has been inspired by the work of [38]. An analysis is needed of its following strengths, weaknesses, opportunities, and threats (SWOT). This analysis is intended to investigate the value of blockchain in healthcare settings, so as to select any key points that can be explored by future researchers [40]. Figure 1 illustrates the points selected in the SWOT analysis to describe its main features.

Highlights of this survey. Unlike the current surveys available, this article aims to explore the state-of-the-art in blockchain-based applications for the healthcare area. Exploring a wide range of scenarios such as the supply chain, sharing information, patient monitoring, and privacy assurance with blockchain in healthcare settings. It also sets out the main trends in the area, which can serve as a basis for other researchers. Below are highlighted some key differences of this survey compared with others that can be found in the literature:

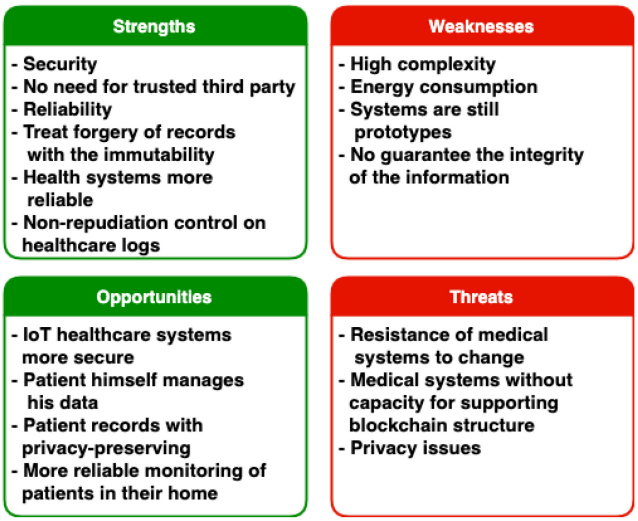

Fig. 1. SWOT analysis of blockchain-based applications in the healthcare context. Adapted from [38].

1. This survey provides a more detailed and up-to-date discussion related to the current works on the blockchain when applied to the healthcare area. It is thus unlike other works in the literature that only provide a systematic review of how blockchain can be employed for a diverse range of applications, such as [87], [54], [111], [67], [62], [9], and [68].
2. It gives an overview of the tools that have been employed by the industry for the construction of blockchain networks.
3. It shows how Internet of Things (IoT) and blockchain technology can complement each other in offering assistance to the healthcare field.
4. It discusses the use of privacy techniques in the healthcare field and how blockchain can improve it.
5. There is a discussion about aspects of data access control in healthcare records and how the blockchain can make an improvement.
6. It provides use cases for monitoring patients in healthcare or remote care environments that are aided by blockchain.

These are all displayed in Table 1 which was inspired by the work of Zheng et al. [111], and is designed to explore some works in the literature that investigate the field of healthcare. Table 1 summarizes some of the research into the healthcare environment and compares the concepts adopted with the perspectives of this study.

It should be noted that this article is concerned with the blockchain applications in the field of healthcare that are currently being discussed in the literature. However, it seeks to examine these systems more broadly by describing each of their benefits and limitations. That is, unlike the work of Hölbl et al. [54], which provides (i) a brief systematic review of the field; (ii) some related works to the topic, and (iii) the adopted search parameters followed by a brief discussion.

This article is also different because it surveys efforts with IoT technology in the healthcare area with blockchain. When compared with the work of [87], it includes several different features, such as IoT and logs management. Unlike the paper in Cai et al. [25], this survey examines some key features of blockchain and includes discussions about Decentralized Applications (Dapps) with various deployment scenarios, in particular cryptocurrencies. Apart from this, this article offers some blockchain applications for this environment in the field of healthcare and Dapps.

Table 1. The Table Shows a Comparison of the Main Features Found in Literature with Those of This Survey

Features	[54]	[87]	[68]	This survey
Presents consensus protocols used in the medical area	X			X
Cite papers about log management and auditing	X	X	X	X
Introduces blockchain systems for supply chain in healthcare	X	X	X	X
Addresses the limitations of the use of the PoW protocol in the health area	X		X	X
Presents bibliographic data used in the review	X		X	X
Benefits and limitations of the blockchain in the healthcare			X	X
Provides a more detailed and up-to-date works on the blockchain applied to healthcare				X
It gives an overview of the tools employed by industry for the construction of blockchain networks				X
It presents how IoT and blockchain work together				X
Discusses the use of privacy techniques in the healthcare field and how blockchain can improve it				X
Discusses data access control in healthcare records and how the blockchain can make an improvement				X
Presents use cases for monitoring patients in healthcare or remote care aided by blockchain				X

It is also worth mentioning that numbers in the features' column refer to the six highlights topics above that serve as differentials for this work, as outlined in the previous paragraph.

This article was structured as follows. Section 2 provides an overview of the main concepts underlying the blockchain technology. Section 3 examines some of the tasks that must be carried out, including: (a) the management of the healthcare records that must be shared; (b) the management of logs; and (c) industrial strategies; as well as this, we show how the IoT, blockchain, and medicine intersect. In Section 4, the blockchain technology is applied to the management of drug supply chains. Section 5 defines some concepts about security and privacy for the healthcare systems. Finally, Section 6 concludes this article.

2 OVERVIEW ON THE USE OF BLOCKCHAIN IN HEALTHCARE

This section sets out by addressing some of the motivational factors for the use of blockchain in the healthcare field. In addition, the main concepts that are embedded in the blockchain are introduced and examined in this section.

2.1 The Need for Technology in the Area of Healthcare

The healthcare area is increasingly requiring more assistance from other fields, such as Computer Science, which can make a significant contribution in this area [106]. This includes, for example, the management of electronic healthcare records, designing tools that can assist in the diagnosis of diseases, gene prediction for genomes, and other examples [13, 35, 93].

Within public health organizations (as well as private organizations) the systems store a large amount of patient data every day; and this fact raises the question about how to handle all of this data. In recent years, this challenge has been met by employing a common concept—the Big Data Analysis—that can be defined as a set of new approaches used in large datasets of

high complexity, in which the standard architectures cannot be supported [60]. Big Data has the potential to be applied to healthcare areas, and make the following improvements: prediction in healthcare diagnosis, analysis in magnetic resonance imaging, and other applications [81].

Computing is a multidisciplinary area that can be applied to various fields of knowledge, with the aim of strengthening and automating the process in each particular field. The set of tools that computing provides can be useful for tackling different problems in the world of medicine. It could result in improved quality, efficiency, and cost savings for healthcare systems [30].

2.2 The Blockchain Technology

Blockchain is an innovative technology originated as from the cryptocurrencies, around 2008/2009 [74, 76]. Currently, it carries out specific tasks, whether they are in the area of finance, healthcare, transport, government, or other areas. This new technology can provide more efficient and secure ways of recording assets [100]. Moreover, it can also be understood as a technology based on decentralized peer-to-peer (P2P) networks, with a replicated and distributed ledger (Rifi et al. [90]). Figure 2 represents the blockchain data structure, where each block is connected to the previous one by means of cryptographic hash pointers to the genesis block (the first block of the structure). Thus, the transactions are grouped within the blocks from the root node of the Merkle tree, where they are distributed [36].

The distributed ledger approach has some components as shown in Section 2; these aspects are the core for running the blockchain network. All these components are described in the paper in [76] and we are not covering them as they are out of the scope of this article.

This article gives an account of the concepts that operate behind the Bitcoin cryptocurrency, and the cryptocurrencies have led to the blockchain technology being disclosed to the public. Other types of cryptocurrency and technologies based on blockchain have emerged from these ideas. As shown by Swan [100] and Hoy [53], these advances were classified as blockchain 1.0, 2.0, and 3.0. Blockchain 1.0 is the first phase, and is characterized by the emergence of the cryptocurrency with Nakamoto [76] and their roll-out alongside simple transfers of assets.

Blockchain 2.0 is defined as the emergence of smart contracts [22] and by the advances made in the way it works, jumping from simple transactions to loans, real estate funds, and others.

Blockchain 3.0 is the evolutionary stage we are currently observing, with the application of this technology not only to finance but also to other sectors of society such as medicine, science, and the arts. According to Lin and Liao [63] and Zheng et al. [111], the blockchain has the following features: (i) Decentralization, (ii) Transparency, (iii) Immutability, (iv) Privacy, (v) Distributed ledger, and (vi) Smart contacts. Besides that, one more detailed definition for blockchain features can be found in other papers in literature, such as Zheng et al. [111], Swan [100], and Hoy [53].

2.3 Types of Blockchain Networks

Blockchain can be divided into a few distinct groups, which have their own characteristics, and directly reflect the network behavior. These types of blockchain can be classified as (based on the features described by Zheng et al. [111] and Alhadhrami et al. [7]) follows:

- **Public blockchain:** The transactions are transparent to all the nodes. When published, any network node can participate in blockchain consensus mechanisms to validate the transaction. The node does not require permission and is unknown in the network. In this type of network, nodes can act on a large scale and support each other. An example of this type of network is Bitcoin and Ether cryptocurrencies [111].
- **Permissioned blockchain:** It is managed by an organization whose nodes require permission to join the structure and in which the transactions of these systems are controlled

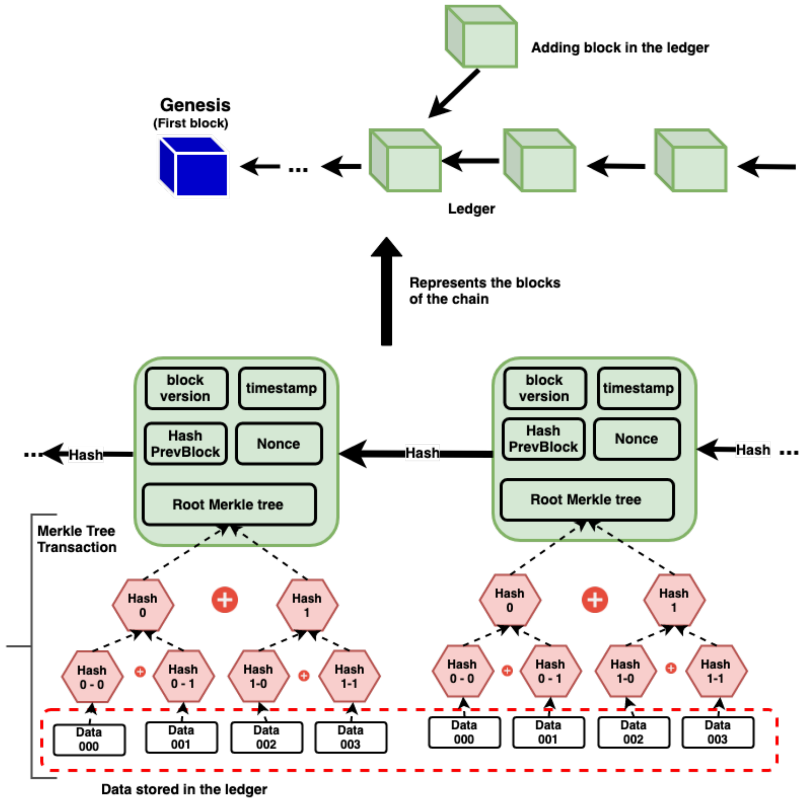

Fig. 2. The primary blockchain structure, adapted from [36, 103]. The figure shows the way the ledger is structured in blockchain networks and describes the components that are inside the distributed ledger. The genesis block is assigned automatically when the network is started, with hash default values, and other blocks are inserted in the ledger following the genesis. In block structures, one could include components such as hash from the previous block, nonce, timestamp, block version, and the value known as the root of the Merkle tree. The Merkle tree is used to organize transactions into a blockchain network, and store them with security, as shown in the red line. The attributes allocated into the block could be modified depending on the consensus protocol used; in summary, this figure presents the characteristics inserted in blockchain structure like Ethereum and Bitcoin implementations.

[111]. The advantage of this type of network is that it ensures a higher degree of privacy because it requires authentication to access the content. An example of a platform of this type is MultiChain [47].

— **Consortium blockchain:** It shares some of the Permissioned blockchain since it is usually managed by a group and it requires authentication to join the network. The distinction of this type of network is that the validating nodes consist of a small number of nodes with pre-established features, that enable them to validate a transaction. When validating the transaction in this type of network, the chosen nodes must reach a consensus, create a new block, and finalize the process [97].

2.4 Validation Process in Blockchain

The validation process in blockchain is also known as mining by some algorithms, such as proof-of-work [76]. That process is usually performed by a consensus algorithm which also establishes

what rules the nodes will follow to validate the blocks. The consensus protocol ensures that the nodes participating in the validation obtain a satisfactory response to all of them, by following the order in which the transactions should take place. This means that they can decide if the block will be inserted in the chain [84, 97].

For blocks validation in the blockchain are designed consensus protocols that providing a more reliable network. We outline the following main protocols founds in the literature for blockchain in healthcare:

— **Proof-of-work (PoW):** The nodes involved in this validation process (i.e., the miners) compete with each other to solve a cryptography puzzle. The node that is first to find a solution obtains the right to validate the block in order to create a new block that implements a transaction. It is also worth noting that some implementations of the PoW algorithm, such as Bitcoin, offer a reward to the winner [76].
— **Proof-of-stake (PoS):** The validations are chosen from the number of participants in the network. Hence, the more coins it has, the more likely one will have to validate the blocks and thus this node will determine the authenticity of the block [56, 73].
— **Practical Byzantine Fault Tolerance (PBFT):** It consists of two types of nodes, the client and the server. When validating the transactions, the PBFT follows a number of stages: (i) the client node sends a request to the server node; (ii) the server node transmits the transaction to the other server nodes, which will decide whether they are valid or not; (iii) if a server node accepts the transaction, that node transmits a readiness message to the others. Provided that a large number of the nodes confirm the transaction, it will be in "confirmation alert"; (iv) each confirmed node sends a broadcast message to the network in order to attest its action; and (v) the node that sent the transaction receives the response, whether it was validated or not [27, 73].

2.5 Smart Contracts

Smart contracts have emerged on blockchain 2.0, with the implementation of framework Ethereum [22]. It is trendy today because of the tools available to build a Blockchain-based application with smart contracts in the Solidity language. A smart contract is a protocol that establishes the rules that a transaction must follow in an automated and electronic way [29, 102].

The implementation of smart contracts in trade can contribute to bring greater security, reliability and ease in purchases. Whether they use cryptocurrency, or even, exchange of other assets. Contracts are executed automatically when a given transaction value matches some rule established in it. This fact can contribute to identifying inconsistencies (such as violations) automatically. The smart contracts can provide greater flexibility to electronic transactions, as a role can provide to the legal environment [42, 78].

2.6 Challenges of Using the Blockchain in Healthcare

Blockchain can be applied to several areas, even though it is a multidisciplinary concept that poses challenges and is subject to limitations [100]. Researchers in this area are attempting to overcome or reduce the impact of these adverse factors. We list some issues (i.e., technical challenges) of the blockchain technology, when employed in the healthcare area [53, 68, 100, 110]:

— **Throughput:** As a result of the increase in the number of transactions and nodes in the network, more checks will have to be carried out, which can cause a network bottleneck. When working with healthcare systems, high throughput is a problem; because unless there is fast access, this might adversely affect a diagnosis which could save someone's life.

— **Latency:** The process of validating a block takes about 10 minutes; this can be detrimental to system security services since there might be successful attacks within that time frame. Healthcare systems are dynamic and should be accessed all the time, since any delay can adversely affect the analysis of an exam.
— **Security:** This can be compromised if an entity is able to seize control of 51% of the network computational power. This matter requires a good deal of attention because a healthcare system that is impaired can mean that the healthcare organizations lose credibility.
— **Resource consumption:** The use of this technology threatens to involve a serious loss of resources, mainly because a lot of energy is spent on the mining process. In a healthcare environment, the energy costs are very high, since several devices are needed to monitor the patients; however, the use of the blockchain might also entail high computing and energy costs. It is a problem for organizations to manage these costs.
— **Usability:** Usability is also a problem in these types of systems because they are very complex to handle. In addition, it is necessary to create an API (Application Programming Interface) with user-friendly features for users. Since health professionals do not have the same degree of technical knowledge as IT professionals, the systems should be easy and intuitive.
— **Centralization:** Although blockchain is a decentralized architecture, some approaches tend to centralize the miners and as a result, this reduces the level of network reliability. Since this central node is vulnerable and can be violated, the information that it stores can be accessed through malicious attacks [111].
— **Privacy:** It is widely believed that the Bitcoin framework enables blockchain to ensure the privacy of its nodes. However, this assumption has been refuted by the findings of [111]. In addition, strategies are needed to offer this capacity to blockchain-based systems [111]. Owing to privacy laws and regulations, the blockchain-based systems have to comply with the General Data Protection Regulation (GDPR).

3 HEALTH INFORMATION MANAGEMENT

After discussing the basic concepts of blockchain technology, this section aims to address how this technology can be employed in the field of medicine—involving investigating the management of healthcare information, which is something of great value to the healthcare field because it deals with sensitive patient data.

In the healthcare area it is of great social importance because its advances can lead to an improvement in the quality of life. Following this line of reasoning, the computation can assist in reducing the effects of some problems in this area. For instance, informatics assist in the automation of healthcare records by ensuring more secure data sharing, log management, and uses in other areas [13, 106, 108].

For the management of healthcare information, whether through healthcare records or by other means, has a direct bearing on the quality of patient care. The collation of the information can speed up the time needed for treatment, as well as assisting the decision-making of the doctor after diagnosing the patient's symptoms [72].

This section aims to discuss matters concerning managing healthcare information. It will address how blockchain technology can assist in sharing and managing medical information, such as sharing and managing information of patient monitoring coming from IoT devices.

3.1 Sharing of Healthcare Records

The sharing of health records is one of the first and most common healthcare applications with blockchain. To share health information is difficult because it is classified as sensitive information and deals with the personal data of the patients. Among the key works in the literature that discuss

this application of blockchain technology are Dubovitskaya et al. [37], Azaria et al. [13], and Xia et al. [108].

Blockchain-based architectures for the sharing of electronic healthcare records may have different characteristics. One of the most classic systems in the literature is discussed in the work of Azaria et al. [13]. That has been cited by several current papers in the literature, which use it as a basis for the construction of other similar architectures. Azaria et al. [13] inspires some of these architectures, cited in [11, 58, 61, 77].

The first sharing architecture to be discussed will be MedRec, which adopts a blockchain-based framework for storing electronic healthcare records. The MedRec aims to tackle problems such as response time in data access, interoperability, and better data quality for healthcare research [13].

It is worth examining the tools used in the construction of the architecture of MedRec, since it implements a private P2P network (Permissioned blockchain), as well as using smart contracts through the Ethereum framework to enable one to manage and track state transitions in the network.

One of the hallmarks of the MedRec architecture is that it provides patients with a consultation agency with records of their healthcare history so that they can be kept informed about health decisions.

Another differential is that they allow standardization of health data since they are flexible and offer open data standards that come in many different shapes. This type of architecture adopts an exciting approach to the application of health data management systems by providing greater security and a common language for data sharing for research purposes [13], although the paper of Azaria et al. [13] also intends to carry out the tests and analysis with a wide range of users.

In brief, MedRec is a viable proposition for use in sharing healthcare records and can be used to integrate healthcare with patients, the hospital, and physicians. In this way, the registered data may reduce inconsistencies in different hospital systems.

As mentioned by Dubovitskaya et al. [37], the approach presents a subject of Cloud computing, which can also assist in the development of new architectures for sharing healthcare records through blockchain by creating safer and more reliable healthcare systems which are used in clinical practice. The authors propose a cloud-based architecture, which adopted the data structure blockchain-based, to connect a network of communication with nodes. The paper by Dubovitskaya et al. [37] demonstrates the application of a blockchain architecture, that is, the fact that it employs the concepts of intelligent contracts and transparent, immutable bookkeeping to manage the sharing of healthcare information.

In addition, Dubovitskaya et al. [37] points out the architectures Cloud Junction and blockchain together to improve management "access control" for systems. For example, the author used data from the Department of Radiation Oncology for testing. It defines access control policies with two essential functions (doctor and patient), as well as using intelligent contracts to define transaction logic. One of the future goals for these types of architecture is to share radiology images and perhaps carry out testing with real patients [37]. The current papers related to blockchain in healthcare presents a network or system prototype, besides they hope in futures works develop a functional system for being tested with real users.

As well as investigating matters related to blockchain architectures for the sharing of healthcare records aided by cloud technology, there is also a need to discuss areas such as auditing information [108]. One of the authors who address this question is Xia et al. [108] (with MedShare), where there is a discussion about finding a blockchain-based solution for record-sharing among healthcare cloud service providers. The solution aims at helping to provide better environment auditing and controlling access to records, as well as creating a query layer (a graphical environment for

querying databases) to connect to the blockchain network when using activation triggers to perform the tasks with the smart contracts [108].

The MedShare-based solution involves a system consisting of four layers: (i) **User layer**: the data will be accessed through a graphical interface; (ii) **Data query layer**: a group of structures that process and respond to query requests in the system; (iii) **Database infrastructure**: a layer composed of the system databases, in which only a few specialist institutions can have access; (iv) **Data structuring and provenance layer**: responsible for processing within the system; in other words, it is the layer which contains the following: the adopted blockchain network structure, consensus protocol, node authenticator, and smart contracts [108].

The main purpose of the type of solution like MedShare, is to enable some features of the healthcare systems to be adopted. The features might include the following: data provenance, auditing, and greater security for the systems. Further, the solution allows the control and revocation of access rights to users and perhaps a repository of healthcare information to be formed, which can be useful for the analysis of Big Data. Therefore, if the system uses cloud processing, it may be suitable for meeting the high demand for data [108].

It is also worth noting what technologies are employed in the construction of these architectures. The language used in the implementations is usually Python, with the aid of t Flask library,[1] which is used to build web pages in Python. The reason for using this technology was that a wide range of devices can be deployed in these environments. Another key technology worth mentioning here is the database; an example of typical use is the SQLite.[2]

3.2 Sharing Imaging in Healthcare

Healthcare information can be characterized by all types of data as well as by images. Currently, some problems in sharing healthcare records may also occur in images [15]. An architecture working with this type of information can be found in [82], with some definitions underlying this concept. From this work, they intend to basically propose an architecture for sharing images. The patient can share their healthcare images in a safe and controlled way.

The structure is based on a centralized network developed by the Radiological Society of North America (RSNA), but is built in a decentralized way. The idea of the Image Share Network (ISN) is to solve the problems presented in the RSNA networks: Registering the images in repositories for study, which can be consulted safely. Images can be viewed as long as the owner of the stored images grants access [82].

Exploring the architecture of [82], it was structured as a set of nodes forming a P2P network of the Chord type, in which each node of the network is represented by an actor in the healthcare system defined by it. The network consists of (i) **center of images:** that serves as an intermediate node to access the images; (ii) **patient:** which has the full access level under his/her images, so he/she can decide with whom to share them; (iii) **health:** has the level of read-only access in the images that the patient specifies; and (iv) **personal healthcare records:** represents the healthcare records and all kinds of records associated with the patient when conducting a consultation in a hospital or clinic.

The main task of the image sharing architecture revolves around the concepts employed in the validation process. Its process is carried out by the consensus algorithm Proof-of-stake since it has the advantage of low load for the participants. And for secure transfer, the concepts of public and private cryptographic keys are used. After all, the proposed architecture can benefit health systems, providing greater security and reliability with the aid of blockchain technology. However,

[1] https://www.fullstackpython.com/flask.html.
[2] https://www.sqlite.org/index.html.

it has limitations, mainly associated with the privacy of images because they are sensitive data. The authors hope that future researchers are cautious on this point [82].

Shortly, the method proposed by [82] may be an advantageous approach because it does not require an intermediary and the patients themselves can manage the distribution of their data and their keys. The architecture of [82] could be compared to the work of [44], which presents a framework for the sharing of patient-oriented images (i.e., own patients manage the sharing of their images). However, it depends on a central unit that transfers the data to the other nodes of the network. The central server can suffer attacks or failures, hindering the good performance of the network.

3.3 Log Management in Healthcare Systems

Log management is an important concept for computational systems since logs enable historical data to be generated that assist in error analysis, intrusion detection, and other services [49]. Healthcare systems also need this kind of management to ensure greater control for users when accessing patient information [106].

However, since the logs generated by the conventional systems that we use today risk being tampered with, there is a need for a technological system that can overcome this problem and this is provided by blockchain. In the case of stored data (such as the logs themselves), the immutability characteristics of blockchain can ensure they are not tampered with in the ledger. The application of these concepts in the healthcare environment was explored in the work of Anderson [12]. It adopts a blockchain-based approach to control the logs generated by the access of information. The strategy adopted also seeks to perform audit control, standardize data, and make sharing easier by employing a Permissioned blockchain structure. The security audit logging is somewhat complex because the collation of the information obtained may sometimes be of no use or lack essential pieces of information [12, 106].

In Anderson [12], they explored a log control approach, called AuditChain, and is basically an application that addresses issues related to interoperability, while providing facilities for sharing electronic healthcare records. The following components were used when adopting this approach: the IBM framework, and the Hyperledger Fabric[3] facilitating the process of building applications based on blockchain.

The application can be accessed through a user interface, but this involves making use of a web service implemented in Node.js,[4] and for this reason an application is defined that assists in the management of audit logs, as well as provides multilevel access control, for the authors, that is, the physician, nurses, and patients. It should be pointed out that AuditChain focuses on the management of personal healthcare records, and the patients themselves can obtain and manage their own information [12].

The audit logs generated by AuditChain are inserted in the ledger so that they can be replicated and distributed to the network nodes. However, it is not only the concept of the ledger that is employed but also the smart contracts needed to define the transaction logic. Such a contract is known as Chaincode in the Hyperledger Fabric framework [12].

When working with a blockchain-based framework, the Auditchain uses asymmetric encryption with a pair of keys, for the purpose of encrypting the data involved in the transaction. Even when the blockchain network is facing a security-related risk, the users who are allowed to join the system have a virtual token in the JavaScript Object Notation (JSON) format. This will be adopted as a digital signature for the user's transaction.

[3] https://www.hyperledger.org/projects/fabric.
[4] https://nodejs.org/en/.

Nonetheless, there are limitations to the use of AuditChain, such as the difficulty in finding logs related to a specific user. Also, when carrying out the procedure, it is necessary to create the query script, which means it is not a very intuitive process. Another significant factor is that the tests conducted with the systems have not been implemented in the real world, and thus the metrics that are used may not be the most appropriate to be operated in a real-world environment [12].

3.4 Approaches Used in the Industry

The previous sections examined some policies for the management of electronic healthcare records. Since the blockchain concept is gaining popularity today, there is a need to investigate some applications that are specifically targeted at industry. Industry strategies involve measures for tackling particular market-oriented problems and boosting profits.

Two strategies involving industry in the blockchain-based healthcare environment are [5] and [96]. Our research also encountered a survey on strategies aimed at industry using the Sandgaard and Wishstar [96] tool that is geared toward the healthcare environment.

The first approach to consider is the work of [96], known as Medicalchain, which was built with the aid of a Permissioned blockchain from the Hyperledger Fabric. The application enables patients to have access controls for all their information as well as being able to handle their healthcare data in a personalized way. Medicalchain uses tokens to access information and also provides access controls, by defining some key figures such as the doctor, research group, and patient.

Medicalchain differs from other approaches adopted in the literature, one of them being that it has a store of healthcare data. Research groups, for example, can draw on this store to exchange information for monetary assets that can be used within the network. When the patient offers some information to the network, he/she receives a reward in the form of coins that can be used in the system—the cryptocurrency used in this system is called Medtoken. As well as this, there is an integration of the blockchain network which enables data to be stored from a patient's wearable devices. They may be employed to check blood pressure, alcohol consumption, physical activities that are carried out, and in other areas which may provide doctors with useful information when diagnosing the patient [5].

In short, the Medicalchain scheme can be very useful and offers valuable prospects for the healthcare systems. However, it suffers from some limitations, insofar as the process of information exchange is bureaucratic and requires a monetary exchange to obtain information from the system. Another limitation applies to Medtoken, since its use is restricted to the system. In addition, the cost of each Medtoken is $0.25. It should be noted that the project is still in its Beta version and there are some problems in the modules [5].

With regard to the applications used in industry, attention should be drawn to the work of Sandgaard and Wishstar [96] which recommends a blockchain-based platform for the management of electronic healthcare records. In this way, it seeks to provide greater security and transparency, while constructing healthcare applications. Medchain, as it is called, assists in the management of electronic healthcare records, in two key areas: safety and interoperability of systems that use this tool.

Medchain, in its architectural applications, adopts a modular approach since some layers plugged into it. One of the main layers that the tool has is the standard data layer (a chain for securing healthcare records) since it serves as the basis for all the others. This layer allows other software to be connected so that its functions can be used in the future. The standard data layer also provides support for applications with Distributed Features (DApps) that assist the patients in accessing their healthcare files. These are obtained from a user interface application that communicates with DApp [96].

In order to use blockchain technology in the healthcare area, in which some papers work aims to propose structures that protect the privacy of patient's healthcare data, follow the standard for Healthcare Insurance Portability and Accountability Act (HIPAA). The papers are [70], Clinicoin [32], Medibloc [69], and MedX [71].

Medchain shares Medicalchain's features, as it also works within a token system, which is composed of two distinct types: (i) MedCoin: also called an external token, which is used in trade exchange. (ii) Internal token: has the functionality to create the hash of the block, which serves as a pointer to connect the distributed records which might be located anywhere in the network with the owner patient of information. Another feature of Medchain is linked to the question of the structure offered by the network, blockchain as a Service (BaaS). To allows any electronic healthcare records system to be integrated with blockchain and ensures its users can have a better level of security, reliability, and the other benefits that a blockchain network can offer [96].

A use case associated blockchain in healthcare, the GovTech program from Estonia (starting in 2011) which contribute the governmental process joining emergent technologies to solve issues. Likewise, blockchain technology assists in ensuring the security and reliability of governmental healthcare systems. The use case of the blockchain in healthcare, according to the paper by Heston [51], presents some benefits when used in this context, such as for storing and managing the healthcare records. Blockchain offers security, tamper-proof, scalability and does not need a third trusted part. Also, this technology can improve audibility from the creation of immutable logs, provide privacy to healthcare records, and even decrease costs in healthcare. Another issue is Estonia's challenges with the deployment of this technology, such as the suitability for its users (patients, physicians, health care providers), provides an incentive to use the system with blockchain technology. In summary, the blockchain at Estonia can improve medical care as well as the quality of life of healthcare system users and also ensure the privacy of patients records [51].

3.5 Consensus Protocols Used on Healthcare Systems

Consensus protocols are necessary structures for the operation of the transaction environment in blockchain networks. These protocols assist in coordinating the validation of the transactions by following some specific rule defined by the algorithm. Basically, they help the validating nodes to reach an agreement, since there is a risk that transactions sent to the network originate from a malicious node. Hence, the validation process can assist in the rejection of the malicious transactions [24].

Among the protocols examined in Section 2.4, it is also worth mentioning the platform of IBM Hyperledger Fabric, which is often adopted in works within the context of blockchain in healthcare systems. It also supports tools for building a complete blockchain network, employing the PBFT consensus protocol [23]. On the basis of the concepts mentioned above, a literature review was carried out to select the consensus protocols in the healthcare systems. In Table 2 is shown the result of this research.

Based on the exploration conducted in this survey, the previous table shown presents data related to the most widely adopted protocols in healthcare approaches that are (i) proof-of-work and (ii) PBFT, the former due to its popularity in various areas and also because it was the first to emerge. The latter is due to the low latency it provides to the network, and because it forms the basis of the IBM Hyperledger platform, which is very popular and supports the blockchain networking process.

There are two protocols explored in industry that are known as proof of accessibility and proof of time and space. For accessibility proof, the algorithm is intended to guarantee that access is provided to the data even if the node that stores it is removed from the network. The protocol uses data

Table 2. Consensus Algorithms Used in Studies that Address the Healthcare Context

Consensus Protocol	Paper	Overview
Proof of Work	MedRec [13]	Sharing healthcare records
	MediBChain [4]	Sharing healthcare records
	[48]	Privacy in the sharing of healthcare information
	[34]	Sharing healthcare records privately and user-friendly
Proof of Stake	[82]	Sharing healthcare imaging
PBFT	[37]	Sharing safe and reliable healthcare records
	[12]	Management and audit of access logs from healthcare records
	MediChain [96]	Sharing healthcare records
	Medicalchain [5]	Exchange healthcare information at a marketplace through MedTokens

backup, replication, and fragmentation techniques to carry out this procedure. The data fragmentation technique employs the data fragments that are replicated to different storage nodes in the network, where each node is unable to store more than 50% of the fragments of a given database.

The protocol of proof of time and space examines if the data were stored, and requests a proof of space in periodic intervals of time. These requirements check the integrity of the stored healthcare records, while the nodes that take part in these processes earn a reward in MedCoins [96].

Furthermore, the consensus protocols presented is also explored in other fields, such as IoT and Supply Chain. IoT needs light consensus protocols due to devices with limited hardware; for instance, PBFT, modified PoS, Stellar Consensus Procol (SCP), and others [95, 105]. Related to Supply Chain, the choice of the protocol depends on the applications; however, in this article, we focused on healthcare applications.

3.6 Patient Monitoring

Since the IoT and the use of sensors operate in various environments, as well as clinics, hospitals, and other medical centers, there is a need to improve the level of security of these sensors [28]. The sensors are either smart bracelets or some other devices within the hospital that can be implanted in patients.

Blockchain is a technology that can help to improve the security of these devices because, when monitoring patients, sensitive personal data are generated by the sensors. There is a need to comply with regulations, such as *Lei Geral de Proteção a Dados* (LGPD) in Brazil [75], General Data Protection Regulation (GDPR) in Europe [6], and the HIPAA in USA [52], for the protection of personal data. These rules stipulate that the systems must guarantee the privacy of patient information, and the blockchain can also help by ensuring the privacy of healthcare information.

Several technologies have emerged to improve and empower traditional systems. Some examples of these technologies are the IoT, networks of sensors, and wearable devices. Medicine can also benefit from these advances; for example, in the use of the Wireless Body Area Networks (WBANs) principle. This principle applies to a personal network composed of several sensors that are implanted or wearable, and where there is unit central for data transfer [8]. Figure 3 displays the simplified structure of a WBAN network for patient monitoring with blockchain [94].

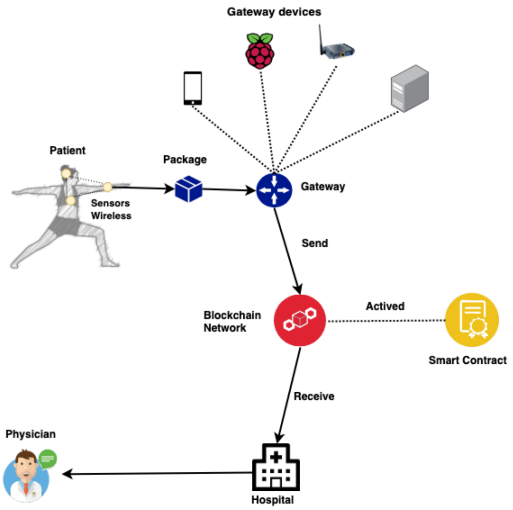

Fig. 3. Structure of Wireless Body Area Networks (WBANs) for patient monitoring, adapted from [8, 89]. This shows the patient doing physical exercise, during which the doctor has to check the heart rate while the task is being carried out. As a result, the sensors that are in the patient's body send a packet to the gateway device. The packages are then sent to the blockchain network, where they interact with smart contracts to carry out the tasks and store the data. The data in the blockchain are sent to a hospital so that physicians can obtain more queries with secure data. Moreover, the figure shows some devices that can be used as gateways to send data via blockchain.

Patient monitoring is an essential procedure within the healthcare system since it can assist the healthcare professional during the follow-up of the patient's treatment. It means that the essential features of WBANS and their protocols, such as wearable device technologies and gateways, can improve the quality of monitoring. However, there are some limitations concerning reliability, efficiency, and consistency to the ability to share patient information over a secure channel [89]; although, other emerging technologies can help overcome these problems, one of which is blockchain. Because it offers a reliable manner of exchanging information between the nodes of the network and employs concepts like immutability and data privacy, in this way, this technology can enhance the level of security in the transfer of information.

Based on the factors outlined above, blockchain can assist in the monitoring of the patients by forming structures that can make the process more reliable. Linn and Koo [65] present in their paper a blockchain-based framework established for sharing healthcare information obtained from sensors, that has all the advantages that blockchain can provide. Nevertheless, the patient himself will be able to manage the information generated by the sensors when combined, such as the heartbeats measured by a cardiac monitor [65].

In Linn and Koo [65], the authors propose the creation of a blockchain-based shared repository of information. This can be useful for various purposes in healthcare research. The data generated helps in the follow-up of patients, and may even accelerate the diagnosis and treatment of diseases [65].

Another example of patient monitoring using blockchain technology has been addressed by [104]. They investigate the remote monitoring of patients using personal sensor networks. Also, this system uses blockchain technology to transfer data generated by the sensors, so that they pass through the various levels of the proposed architecture. The advantage of this technology is that it reduces communication overhead, and can transfer records without the need for a trusted third party, as well as offering transparency and immutability [50, 99].

The architecture designed by Uddin et al. [104] is composed of two layers: (i) the first controls the flow and storage of the data; (ii) the second controls the central healthcare data unit. The architecture operates from a personal network of patient sensors, in which the generated data is sent to a healthcare data provider (this might be the Smartphone). The produced data is sent to a server that acts as the patient data agent and is responsible for data module management, the data mining module, and data security. It also can notice that when transferring data, it is necessary to traverse a blockchain network structure before they reach the end users, to ensure greater security and reliability [104].

The architecture formed by Uddin et al. [104] carries out tests to measure its performance in different situations. One of the analyses conducted was concerned with certain types of attacks, such as man-in-the-middle attacks and denial of service attacks and their impact on patient privacy. Before the tests are carried out, many factors were defined, starting with the mining and mining selection algorithms.

The set of analyses demonstrated the usage of about 25% of the processor and 98 MB of memory when there were three miners in the network. On the other hand, the tests related to security matters were based on the previously mentioned attacks and compared to the works of Gope and Hwang [46] and Balasubramanian et al. [14] as a baseline, intending to analyze the security protocols used. They also tested the physical characteristics of the network, such as the following: processing time, overhead, and throughput in Kbps. The results showed lower processing costs and lower overhead than other works used as the baseline and occupied 45% of the network with 26 nodes and a transfer rate lower than the other works taken as baseline [104].

Finally, this section aims to set out some principles and examine some studies that examine how patients can be monitored with the aid of personal sensors. This study also investigates measures to improve the quality and security of data transfer, as well as make a reduction in energy costs.

3.7 Discussion

This section examined the concepts employed for healthcare information management using blockchain technology and, based on this knowledge, it uses protocols to control transactions. These concepts also assist the process of sharing electronic health records, increased security, the immutability of data, and privacy. The primary protocol that is involved in the network trust-building processes is the consensus protocol, such as Proof-of-work, Proof-of-stake, and PBFT. Moreover, when implementing blockchain-based applications, we encountered some studies relying on the Hyperledger Fabric framework and employing PBFT consensus protocols.

Other factors discussed in this section are the prospect of sharing healthcare records, sharing images in healthcare, managing healthcare application logs, and managing healthcare information for industry-wide bargaining proposals. Each of them points out different ways of tackling problems and addresses the advantages of this type of solution in the healthcare environment.

Lastly, we discussed some principles and analyzed some studies that examine how patients are monitored with the aid of personal sensors. This study also investigated measures to improve the quality and security of data transfer, as well as the reduction of energy costs. It should stress that since blockchain is a newly emerging concept in computing today, it can assist in improving reliability and monitoring patients through sensors with limited hardware. Moreover, as the consensus protocols are becoming more advanced, they can be used in resource-constrained devices (e.g., IoT), as from light consensus protocols such as PBFT and SCP [67].

4 SUPPLY CHAIN MANAGEMENT

One of the managerial processes for the development of an organization is supply chain management (SCM), insofar as it connects a network of partners, ranging from the producer of the

raw material to the distribution organization. SCM systems include several industries, such as the healthcare industry, and as a result of technological advances, other devices integrated into this environment, including blockchain technology [59]. In this way, it can assist in tracking and logging assets in the supply chain. For this reason, this section aims to discuss some positive ways in which blockchain can support the management of supply chains when applied to the healthcare industry.

The supply chain management involves handling assets from the production line to their distribution so that they reach the end consumer in a state of good quality and on time [59]. Business strategy is a critical factor for some companies, such as healthcare and the pharmaceutical industry. Given this, this type of company needs to provide higher quality in the manufacture, transport, and delivery of medicines since the lack of assets can disrupt the social environment, for example, some medications are essential to the quality of life of some people; without them, they could not carry out their normal activities [98]. This article will focus on two points: (i) blockchain and IoT for supply chain in the drug monitoring and (ii) blockchain-based health asset tracking in the supply chain.

4.1 Blockchain and IoT for Supply Chain

The IoT technology can be applied to several applications and this includes transmitting real-time information and monitoring the assets throughout the chain [109]. In addition, other technologies integrated with IoT, such as blockchain, can serve to improve the security and reliability of these assets. This section seeks to show how these technologies combined can better perform. We also discuss the case of the Modum company that works mainly in this area.

The healthcare industry is generating considerable interest in terms of the use of IoT to assist patients and physicians due to sensors that can be integrated with small devices for monitoring patient's health conditions, and generate reports for analysis [88]. With the IoT, hospitals could become smart hospitals facilitating some processes for healthcare professionals [88].

The Modum company is a use case that illustrates blockchain and IoT in the same application, which, according to Kshetri [57], was founded through a partnership with the University of Zurich. The companies seek to create a drug- sharing network that is integrated with the blockchain technology. The objective of the company is to combine IoT concepts, to monitor the changes in the condition of the drugs (Kshetri [57] and Campbell [26]). The technology checks if the specific transport standards are met to ensure quality is maintained until the goods reach their destination. The Modum operates a system based on blockchain Ethereum, through a smart contract, checks at strategic stages if the state of the drug conforms to the required standard. If there are any problems in the transaction when checked, the medication will be refused, and an alert will be sent to the control panel to take any necessary action [57].

Since Modum is concerned with the transporting of medicines, it has to monitor several factors such as temperature. It means that the customer will be able to check the status of the drug until it reaches its destination through a secure and decentralized network—blockchain [21]. The technical details for further specifying the construction of the Modum platform are as follows: (i) blockchain-based Ethereum network; (ii) Bluetooth sensors, for IoT devices; (iii) PostgreSQL database to store asset data; (iv) REST API platform to service a JSON; (v) intelligent contract to define the stages of the transactions; and (vi) mobile application to read the bar codes of the medicines and make the necessary checks.

4.2 Health Asset Tracking in the Supply Chain

To address the process of tracking health assets in the supply chain using blockchain, we discussed concerns about drug theft and falsification, which must be investigated more carefully because of

the large number of cases in recent years [107]. These crimes have caused significant financial losses in the healthcare system, and it is necessary to take new measures to combat them, such as tracking the supply chain of medicines [86]. According to the World Health Organization (WHO), in 2017, 1 in 10 medicines in developing countries were either counterfeit or of poor quality [107]. The WHO also points out that the use of this type of medication risks aggravating the symptoms of the disease or causes severe side effects [107].

The paper of Erhun et al. [41] examines the importance of drug delivery management in Nigeria, where there is a lack of medicines since the country can only supply 30% of its needs from local manufacturers, and to overcome the problem, it has to rely on imported medicines [41]. However, this policy requires proper management to carry out the correct distribution of the medicines to ensure that only legitimate medicines are supplied. Usually, many traders sell medicines of doubtful origins on the streets that are thus exposed to the sun all day. One way to control this problem is through the management of the supply chains [41, 79]. Not only this, one of the most modern ways to help combat this problem is through the management of supply chains based on blockchain.

A use case regarding poor managed drug control occurred in Nigeria in 1990, and according to Alubo [10], it is known as the "Paracetamol Tragedy." During this tragic episode, several children under four years old died after taking a dose of paracetamol that had an uncontrolled mixture of compounds. The drugs had toxic effects on the children who died later. This case illustrates the urgent need to control the compounds that are added to the drugs through poorly managed supply chains.

Thus, one point that should be addressed accordingly in the drug distribution is the traceability of these assets. This is because there is a risk that they can be diverted and used for other purposes depending on the type of medicine, or even stolen for illegal sale. However, blockchain is a valid scheme for overcoming this problem, as is shown in the work by Bell et al. [16]. The paper examines how a company called Chronicled developed a structure based on blockchain, in which the drug is traced from the time it leaves its manufacturer until it reaches the end consumer. This process assists in monitoring the distribution of fake medicines, as well as the problem of drug diversion [16]. It ensures that all the assets that are distributed are recorded in the blockchain ledger (i.e., the drug log records), therefore once the data is stored it can no longer suffer changes.

4.3 Discussion

This section addressed different topics concerning the management of drug supply chains, where some different applications were supported by blockchain technology, to take advantage of its benefits. It was evident that a common problem in the distribution of medicines is their falsification—with tragic consequences for the population—as in the case of Nigeria. Blockchain can assist in this area, mainly because of its immutability characteristics, which make drug falsification more challenging.

Another aspect of blockchain technology is that it can play a crucial role in monitoring the distribution of drugs, and check that the assets follow the supply chain pattern correctly. Combining the blockchain technology with IoT, it can enhance the reliability of the information conveyed in real time. The drug-related information supplied to the recipients (customers), for example, may be more reliable because of the immutability of the data provided by the blockchain network.

5 PRIVACY AND SECURITY IN BLOCKCHAIN FOR HEALTHCARE

Currently, there is an increase in health data since physical documents are digitized, and sensors and other technological devices uses generating health data [1]. Data is produced from various sources in the healthcare area, such as hospital records, radiography images, and monitoring sensors [80].

There are several databases with information about patients, although some of this may be sensitive, since it is patient's information. However, one of the ways to ensure greater security in these environments is the use of blockchain technology, which can be very useful because of certain features it has, such as immutability and data traceability tools. The following paragraphs discuss some factors that apply to blockchain with regard to security in healthcare systems. First of all, the healthcare systems with blockchain can improve systems linked to cryptography. The paper by [31] sets out a strategy for searching the best cryptography models for smart contracts.

Nevertheless, privacy issues with blockchain is not fully addressed. There is a need to examine some areas of privacy when sending information and the transaction link with the data of the patient [43]. The challenges about privacy in the blockchain include the following [43]:

- **Identity privacy:** maintaining the user's private identity and not relating it to the transaction.
- **Transaction privacy:** ensuring that the transaction content is not accessed by non-authorized users.

The use of patient healthcare records gives rise to a concern about patient privacy since the data aggregated in these records contain personal information. These records might consist of a personal registration number, the number of the credit card that the patient uses to make a payment in the private network, and other items. Many techniques in the literature that can help to address these problems, such as k-anonymity or zero-knowledge proof, is examined by [101]. Authors show a formal model for ensuring privacy, which involves using a technique to prove that information is valid without revealing it to other nodes.

The privacy techniques that should be noted include the following: (i) trusted execution environments (TEE) [92], (ii) homomorphic cryptography [2], (iii) zk-snarks [17] (derived from the zero-knowledge proof), and (iv) differential privacy [39].

Here, we will discuss one of the strategies that may be useful for ensuring privacy in the healthcare area. The TEE is a security technique hardware-supported that has a separate module designed to provide greater security and privacy to the system. Thus, it relies on the CPU to perform code execution reliably and exploited in environments that employ blockchain and can be used to ensure greater security, such as healthcare environments [64, 92]. All the previously defined concepts can be used for blockchain technology when applied to the healthcare area.

As well as this, there is another factor that can ensure greater privacy of healthcare information; this is the Healthcare Insurance Portability and Accountability Act (HIPAA) [52], which is a privacy rule drawn up by the United States. The HIPAA rule assists in (a) improving information sharing within the healthcare environments, (b) defining national standards, and (c) protecting personal healthcare data. The HIPAA privacy rules cover the following: (i) healthcare plans; (ii) healthcare provision; (iii) Healthcare Clearinghouses; and (iv) Business Associates.

In summary, these rules provide users of healthcare systems with greater reliability and personal data security. With the support of the privacy rules, blockchain technology can improve the security and reliability of patient personal information in the healthcare environment [52]. It is also worth noting that HIPAA rules restrict access to information, insofar as this factor is linked to the technology that uses this type of information to find solutions that can benefit the healthcare environment. Due to restrictions, the process becomes more bureaucratic, and some of the technological operations may become inactive.

Another technique that can be employed to enhance privacy when sharing healthcare information is the use of blockchain. Since according to Bethencourt et al. [18], it is an attribute-based encryption, it is a cryptographic public-key method, which has attributes that are important for first-generation techniques and also for policies needed to access encrypted data.

An architecture that explores this concept can be found in the work of [33], and is called Decentralized Sharing of Healthcare Records (DSHR). In this, a set of tools was used for establishing it, which included the following: (i) Ethereum: to define the blockchain rules and smart contracts; (ii) InterPlanetary File System (IPFS): to form the P2P network for the exchange of information; and (iii) attribute-based encryption: to encrypt healthcare records as a means of ensuring their privacy. However, privacy technique must be used with caution because it can result in a high computational cost for the sharing of records.

One way to ensure privacy in the healthcare environment is the creation of data access logs repositories blockchain-based for healthcare records for Big Data. For instance, in Karafiloski and Mishev [55] draw our attention to a tool that builds data repositories, which provides a secure way of generating bases for the analysis of Big Data by using blockchain in the area of healthcare.

With the aid of this framework, healthcare agencies will not have to worry about the reliability of the data since they are derived from the blockchain network, and thus, the users themselves will be able to manage them. Moreover, the blockchain can help by improving the reliability and security of Big Data environments [55].

As discussed earlier, one type of healthcare data is multimedia data (e.g., images, sounds, and videos). The paper by Patel [82] addresses digital imaging making a connection with the blockchain.

On the other hand, in regard to ensuring the data privacy, the first approach that can help overcome security problems is to employ the Off-chain network for storing multimedia blockchain data and preserving privacy by complying with the GDPR [112]. Another means of ensuring multimedia data security might be to embed a watermark to register the copyright for sharing security. This registration means that the accessed data that is stored in the blockchain is immutable. This effort is found in [19, 20].

Finally, privacy issues in healthcare environments where there is a sharing of records can be mitigated by techniques such as zero-knowledge proof and attribute-based encryption, where they can be employed directly by referring to the health record file, or to data that is stored in a database.

It should be emphasized that data privacy is essential in a health setting, and blockchain technology can assist in ensuring security for this environment. Moreover, there is a current trend to employ cryptography techniques to improve the privacy level in healthcare systems, which involves a blockchain based on differential privacy [39, 112]. The differential privacy protects the data against linkage attacks, where related data in two databases might be linked, or for inferring and discovering patient sensitive data [39].

6 CONCLUSION

This survey carried out an analysis in some aspects of the literature that are concerned with the use of blockchain technology in the healthcare area. The investigation has covered other co-related areas such as privacy and safety of healthcare information. Blockchain technology is a recent concept, and its application in the field of healthcare with the most significant publications in this area only appeared between 2016 and 2019. Therefore, studies in the area initially only defined general terms. Subsequently, initial attempts have been made so far to apply this technology to the sharing of healthcare information, the management of drug supply chains, and patient monitoring systems.

The strategy that has been discussed is guaranteeing privacy when sharing health records, which has been a growing trend in recent years (2017, 2018, and 2019). Privacy is a question that is gaining traction and has exciting research prospects, especially with the emergence of the personal data protection laws (LGPD, GDPR, and HIPAA). Privacy laws determine the rights and responsibilities that organizations have when protecting the personal data of their clients. Blockchain can

Table 3. Summary of the Methods Used on Blockchain to Healthcare with Pros and Cons Per Application Area

Area	Methods	Pros	Cons
Sharing health information	MedRec [13]	Improve data quality for medical researches	Not have contract encryption
		System interoperability	It's just a prototype
	MediChain [96]	Could use mobile interface and a web application	Loss of patient access key
		Reduces risk to identify the patient from data leaked	Problems with privacy
	Medicalchain [5]	Health data marketplace	Tokens could be used just within Medicalchain
		Patient control access with MedTokens	There are risks for acquiring the MedTokens
Remote care with IoT	Patient centric agent (PCA) [104]	Provide access control role-based	Requires devices with high power processing for encryption
		Uses a protocol to improve security and authentication of patient's smartphone	Vulnerable to man in middle attack
Supply chain for healthcare	Modum [3]	Uses good practice of the GDPR	Business oriented
		Monitors the pharma chain with NFC	Poor documentation and complex
Security and privacy	Decentralized Sharing of Health Records (DSHR) [33]	Uses attribute-based encryption to ensure privacy	Complexity to use
		Stores sensitive data in off-chain	Increases cost as the number of attributes increases
	[31]	Scheme for searching the cryptography strategies to blockchain	Uses the synthetic environment
		Encrypts smart contracts	High cost to mine the blocks

make a valuable contribution to guaranteeing privacy by using techniques such as the following: immutability of data, attribute-based encryption, zero-knowledge proof, and other approaches.

The range of consensus protocols used for blockchain-based healthcare applications is a highlight of this study. The most widely used was the Proof-of-Work (PoW) and Practical Byzantine Fault-Tolerance (PBFT) because they can be adopted in platforms such as Ethereum and Hyperledger Fabric. An analysis of these protocols (beginning with the PoW), showed that it has a high computational cost and would be impracticable for the healthcare environment. Hospitals would have to spend much money on infrastructure to maintain this service in the network, and since it is a permissionless protocol, the privacy of information could be compromised. Even as concerning PoW, it should stress that most of the papers that discuss this protocol are theoretical, with implementation remaining a hypothetical possibility. Thus, a protocol suitable for use in healthcare applications would be PBFT, because it is permissioned protocol and has another consensus rationale, with lower computational costs and without miners.

In short, this study aimed to present a number of works for researchers interested in implementing blockchain-based healthcare systems. We also discussed some of the platforms for building blockchain-based healthcare applications, presenting their limitations and advantages. As a result, we concluded that a line of research is the sharing of healthcare information and the use of

the PBFT consensus algorithm, as well as the use of the Hyperledger Fabric platform. However, if the researcher is concerned about the future outcome that will emerge, he/she should pay attention to the drug supply chain and patient monitoring where blockchain and IoT can be combined.

From the development of this study, we can observe that blockchain technology can be applied to different perspectives within the healthcare field. One of them worth exploring more deeply is the healthcare equipment monitoring integrated with the IoT. With these technologies together, it is interesting to cite the possibilities of providing more safety to the fitness and mental healthcare monitoring environments due to the full range of smart health devices that are currently emerging. With the support of blockchain technology, some problems involving the reliability and security of patients' data could be mitigated.

Finally, we summarized some methods and applications used by blockchain for healthcare, which are related to each knowledge area cited in this survey. Table 3 sets out the pros and cons of these methods to form a point of comparison between these methods. A baseline can be used for future research.

REFERENCES

[1] Karim Abouelmehdi, Abderrahim Beni-Hssane, Hayat Khaloufi, and Mostafa Saadi. 2017. Big data security and privacy in healthcare: A Review. *Procedia Computer Science* 113 (2017), 73–80. DOI: https://doi.org/10.1016/j.procs.2017.08.292

[2] Abbas Acar, Hidayet Aksu, A. Selcuk Uluagac, and Mauro Conti. 2018. A survey on homomorphic encryption schemes: Theory and implementation. *ACM Computing Surveys* 51, 4 (July 2018), Article 79, 35 pages. DOI: https://doi.org/10.1145/3214303

[3] Modum.io AG. 2017. Whitepaper: TECHNOLOGY Data Integrity For Supply Chain Operations, Powered By Blokchain. Retrieved October 1, 2018 from https://assets.modum.io/wp-content/uploads/2017/08/modum_whitepaper_0.9.pdf.

[4] Abdullah Al Omar, Mohammad Shahriar Rahman, Anirban Basu, and Shinsaku Kiyomoto. 2017. MediBchain: A blockchain based privacy preserving platform for healthcare data. In *Security, Privacy, and Anonymity in Computation, Communication, and Storage*. Springer International Publishing, Cham, 534–543. https://link.springer.com/chapter/10.1007/978-3-319-72395-2_49

[5] Abdullah Albeyatti. 2018. Meddicalchain. Retrieved September 30, 2018 from https://medicalchain.com/Medicalchain-Whitepaper-EN.pdf [White paper].

[6] Jan Philipp Albrecht. 2016. How the GDPR will change the world. *European Data Protection Law Review* 2 (2016), 287.

[7] Zainab Alhadhrami, Salma Alghfeli, Mariam Alghfeli, Juhar Ahmed Abedlla, and Khaled Shuaib. 2017. Introducing blockchains for healthcare. In *2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA)*. IEEE, 1–4. DOI: https://doi.org/10.1109/ICECTA.2017.8252043

[8] Aftab Ali and Farrukh Aslam Khan. 2015. Key agreement schemes in wireless body area networks: Taxonomy and state-of-the-art. *Journal of Medical Systems* 39, 10 (Aug. 2015), 115. DOI: https://doi.org/10.1007/s10916-015-0272-9

[9] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani. 2018. Applications of blockchains in the Internet of Things: A comprehensive survey. *IEEE Communications Surveys Tutorials* 21 (2018), 1–1. DOI: https://doi.org/10.1109/COMST.2018.2886932

[10] S. Ogoh Alubo. 1994. Death for sale: A study of drug poisoning and deaths in Nigeria. *Social Science & Medicine* 38, 1 (1994), 97–103. DOI: https://doi.org/10.1016/0277-9536(94)90304-2

[11] Joel Alwen, Jeremiah Blocki, and Ben Harsha. 2017. Practical Graphs for Optimal Side-Channel Resistant Memory-Hard Functions. Cryptology ePrint Archive, Report 2017/443. Retrieved September 20, 2018 from https://eprint.iacr.org/2017/443.

[12] Jessie Anderson. 2018. *Securing, Standardizing, and Simplifying Electronic Health Record Audit Logs through Permissioned Blockchain Technology*. Ph.D. Dissertation. Dartmouth College. https://www.cs.dartmouth.edu/~trdata/reports/abstracts/TR2018-854/.

[13] Asaph Azaria, Ariel Ekblaw, Thiago Vieira, and Andrew Lippman. 2016. MedRec: Using blockchain for medical data access and permission management. In *2016 2nd International Conference on Open and Big Data (OBD)*. IEEE, 25–30. DOI: https://doi.org/10.1109/OBD.2016.11

[14] V. Balasubramanian, D. B. Hoang, and T. A. Zia. 2011. Addressing the confidentiality and integrity of assistive care loop framework using wireless sensor networks. In *2011 21st International Conference on Systems Engineering*. IEEE, 416–421. DOI: https://doi.org/10.1109/ICSEng.2011.82

[15] Ana Sofia de Oliveira Guedes Bastos. 2011. *Quality of Health Information on Acute Myocardial Infarction and Stroke in the World Wide Web*. Master's Thesis. Universidade do Porto.

[16] Liam Bell, William J. Buchanan, Jonathan Cameron, and Owen Lo. 2018. Applications of blockchain within healthcare. *Blockchain in Healthcare Today* 1 (2018), 1–7. DOI: https://doi.org/10.30953/bhty.v1.8

[17] Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Virza Madars. 2014. Zerocash: Decentralized Anonymous Payments from Bitcoin (extended version). Retrieved February 5, 2018 from http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf.

[18] J. Bethencourt, A. Sahai, and B. Waters. 2007. Ciphertext-policy attribute-based encryption. In *IEEE Symposium on Security and Privacy (SP'07)*. IEEE, 321–334. DOI: https://doi.org/10.1109/SP.2007.11

[19] D. Bhowmik and T. Feng. 2017. The multimedia blockchain: A distributed and tamper-proof media transaction framework. In *2017 22nd International Conference on Digital Signal Processing (DSP'17)*. IEEE, 1–5. DOI: https://doi.org/10.1109/ICDSP.2017.8096051

[20] D. Bhowmik, A. Natu, T. Ishikawa, T. Feng, and C. Abhayaratne. 2018. The Jpeg-Blockchain framework for glam services. In *2018 IEEE International Conference on Multimedia Expo Workshops (ICMEW'18)*. IEEE, 1–6. DOI: https://doi.org/10.1109/ICMEW.2018.8551519

[21] T. Bocek, B. B. Rodrigues, T. Strasser, and B. Stiller. 2017. Blockchains everywhere—A use-case of blockchains in the pharma supply-chain. In *2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM'17)*. IEEE, 772–777. DOI: https://doi.org/10.23919/INM.2017.7987376

[22] Vitalik Buterin. 2014. A Next-Generation Smart Contract and Decentralized Application Platform. Retrieved August 20, 2018 from https://github.com/ethereum/wiki/wiki/White-Paper.

[23] Christian Cachin. 2016. Architecture of the Hyperledger Blockchain Fabric. Retrieved August 31, 2018 from https://www.zurich.ibm.com/dccl/papers/cachin_dccl.pdf.

[24] Christian Cachin and Marko Vukolic. 2017. Blockchain consensus protocols in the wild. *CoRR* abs/1707.01873 (2017), 1–24. arxiv:1707.01873 http://arxiv.org/abs/1707.01873

[25] W. Cai, Z. Wang, J. B. Ernst, Z. Hong, C. Feng, and V. C. M. Leung. 2018. Decentralized applications: The blockchain-empowered software system. *IEEE Access* 6 (2018), 53019–53033. DOI: https://doi.org/10.1109/ACCESS.2018.2870644

[26] Rebecca Campbell. 2016. Modum.io's Tempurature-Tracking Blockchain Solution Wins Accolades at Kickstarter Accelerator 2016. https://bitcoinmagazine.com/articles/modum-io-s-tempurature-tracking-blockchain-solution-wins-accolades-at-kickstarter-accelerator-1479162773/.

[27] Miguel Castro and Barbara Liskov. 1999. Practical byzantine fault tolerance. In *Proceedings of the T3rd Symposium on Operating Systems Design and Implementation (OSDI'99)*. USENIX Association, Berkeley, CA, 173–186. http://dl.acm.org/citation.cfm?id=296806.296824

[28] S. Cha, J. Chen, C. Su, and K. Yeh. 2018. A blockchain connected gateway for BLE-based devices in the Internet of Things. *IEEE Access* 6 (2018), 24639–24649. DOI: https://doi.org/10.1109/ACCESS.2018.2799942

[29] Krishnendu Chatterjee, Amir Kafshdar Goharshady, and Yaron Velner. 2018. Quantitative analysis of smart contracts. In *Programming Languages and Systems*, Amal Ahmed (Ed.). Springer International Publishing, Cham, 739–767.

[30] Basit Chaudhry, Jerome Wang, Shinyi Wu, Margaret Maglione, Walter Mojica, Elizabeth Roth, Sally Morton, and Paul Shekelle. 2006. Systematic review: Impact of health information technology on quality, efficiency, and costs of medical care. *Annals of Internal Medicine* 144, 10 (2006), 742–752. DOI: https://doi.org/10.7326/0003-4819-144-10-200605160-00125 arXiv:/data/journals/aim/20115/0000605-200605160-00125.pdf

[31] Lanxiang Chen, Wai-Kong Lee, Chin-Chen Chang, and Raymond Kim-Kwang Choo. 2019. Blockchain based searchable encryption for electronic health record sharing. *Future Generation Computer Systems* 95 (2019), 420–429. DOI: https://doi.org/10.1016/j.future.2019.01.018

[32] Clinicoin. 2018. Clinicoin—Blockchain Powered Global Wellness. Retrieved February 5, 2019 from https://icorating.com/upload/whitepaper/pTpjzwFCNILrde22da7EQfxVpJZoDKCoLx22yavq.pdf.

[33] Leonardo Costa, Billy Pinheiro, Roberto Araújo, and Antonio Abelém. 2018. Compartilhamento seguro de arquivos de Saúde usando criptografia baseada em atributos e redes descentralizadas. In *Anais do XVIII Simpósio Brasileiro de Computação Aplicada a Saúde (SBCAS'18)*, Vol. 18. SBC, Natal, RN, Brazil, 1–12. http://portaldeconteudo.sbc.org.br/index.php/sbcas/article/view/3682.

[34] Arlindo F. da Conceição, Flavio S. Correa da Silva, Vladimir Rocha Locoro, Angela, and João Marcos M. Barguil. 2018. Electronic health records using blockchain technology. In *Anais do I Workshop em Blockchain: Teoria, Tecnologias e Aplicações (WBlockchain - SBRC 2018)*, Vol. 1. SBC, 1–14. https://portaldeconteudo.sbc.org.br/index.php/wblockchain/article/view/2357.

[35] Ulisses Martins Dias et al. 2007. *Predição da Função das Proteínas sem Alinhamentos Usando Máquinas de Vetor de Suporte*. Master's Thesis. Universidade Federal de Alagoas.

[36] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang. 2018. Untangling blockchain: A data processing view of blockchain systems. *IEEE Transactions on Knowledge and Data Engineering* 30, 7 (July 2018), 1366–1385. DOI: https://doi.org/10.1109/TKDE.2017.2781227

[37] Alevtina Dubovitskaya, Zhigang Xu, Samuel Ryu, Michael Schumacher, and Fusheng Wang. 2017. Secure and trustable electronic medical records sharing using blockchain. *CoRR* abs/1709.06528 (2017), 1–10. arxiv:1709.06528 http://arxiv.org/abs/1709.06528

[38] Davor Dujak and Domagoj Sajter. 2018. *Blockchain Applications in Supply Chain*. Springer International Publishing, Cham, 21–46. DOI: https://doi.org/10.1007/978-3-319-91668-2_2

[39] Cynthia Dwork and Aaron Roth. 2014. The algorithmic foundations of differential privacy. *Foundations and Trends in Theoretical Computer Science* 9, 3–4 (Aug. 2014), 211–407. DOI: https://doi.org/10.1561/0400000042

[40] Robert G. Dyson. 2004. Strategic development and SWOT analysis at the University of Warwick. *European Journal of Operational Research* 152, 3 (2004), 631–640. DOI: https://doi.org/10.1016/S0377-2217(03)00062-6

[41] W. O. Erhun, O. O. Babalola, and M. O. Erhun. 2001. Drug regulation and control in Nigeria: The challenge of counterfeit drugs. *Journal of Health & Population in Developing Countries* 4, 2 (2001), 23–34. http://www.nigeriapharm.com/Library/Drug_regulation.pdf.

[42] Joshua A. T. Fairfield. 2014. Smart contracts, bitcoin bots, and consumer protection. *Washington and Lee Law Review Online* 71, 2 (2014), 36. https://scholarlycommons.law.wlu.edu/wlulr-online/vol71/iss2/3/.

[43] Qi Feng, Debiao He, Sherali Zeadally, Muhammad Khurram Khan, and Neeraj Kumar. 2019. A survey on privacy protection in blockchain system. *Journal of Network and Computer Applications* 126 (2019), 45–58. DOI: https://doi.org/10.1016/j.jnca.2018.10.020

[44] Yaorong Ge, David K. Ahn, Bhagyashree Unde, H. Donald Gage, and J. Jeffrey Carr. 2013. Patient-controlled sharing of medical imaging data across unaffiliated healthcare organizations. *Journal of the American Medical Informatics Association: JAMIA* 20, 1 (Jan. 2013), 157–163. DOI: https://doi.org/10.1136/amiajnl-2012-001146

[45] João Paulo Pereira Gonçalves, Larice Rodrigues Batista, Larissa Mendes Carvalho, Michelle Pimenta Oliveira, Kênia Souto Moreira, and Maísa Tavares de Souza Leite. 2013. Prontuário Eletrônico: Uma ferramenta que pode contribuir para a integração das Redes de Atenção à Saúde. *Saúde em Debate* 37 (2013), 43–50. http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0103-11042013000100006.

[46] P. Gope and T. Hwang. 2016. BSN-Care: A secure IoT-based modern healthcare system using body sensor network. *IEEE Sensors Journal* 16, 5 (March 2016), 1368–1376. DOI: https://doi.org/10.1109/JSEN.2015.2502401

[47] Gideon Greenspan. 2015. MultiChain Private Blockchain, White Paper. Retrieved September 10, 2018 from http://www.multichain.com/download/MultiChain-White-Paper.pdf.

[48] Rui Guo, Huixian Shi, Qinglan Zhao, and Dong Zheng. 2018. Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems. *IEEE Access* 6 (2018), 11676–11686. DOI: https://doi.org/10.1109/ACCESS.2018.2801266

[49] Udit Gupta. 2015. Secure management of logs in internet of things. *CoRR* abs/1507.05085 (2015), 1–6. arxiv:1507.05085 http://arxiv.org/abs/1507.05085

[50] J. D. Halamka, A. Lippman, and A. Ekblaw. 2017. The Potential for Blockchain to Transform Electronic Health Records. Retrieved September 30, 2018 from https://hbr.org/2017/03/the-potential-for-blockchain-to-transform-electronic-health-records.

[51] Thomas F. Heston. 2017. A case study in blockchain health care innovation. *International Journal of Current Research* 9 (2017), 1–2. https://www.journalcra.com/article/case-study-blockchain-health-care-innovation.

[52] U.S. Department of Health & Human Services (HHS). 2013. Summary of the HIPAA Privacy Rule. Retrieved February 4, 2019 from https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

[53] Matthew B. Hoy. 2017. An introduction to the blockchain and its implications for libraries and medicine. *Medical Reference Services Quarterly* 36, 3 (2017), 273–279. DOI: https://doi.org/10.1080/02763869.2017.1332261

[54] Marko Hölbl, Marko Kompara, Aida Kamišalić, and Lili Nemec Zlatolas. 2018. A systematic review of the use of blockchain in healthcare. *Symmetry* 10, 10 (2018), 1–22. DOI: https://doi.org/10.3390/sym10100470

[55] E. Karafiloski and A. Mishev. 2017. Blockchain solutions for big data challenges: A literature review. In *17th International Conference on Smart Technologies (IEEE EUROCON'17)*. IEEE, 763–768. DOI: https://doi.org/10.1109/EUROCON.2017.8011213

[56] Sunny King and Scott Nadal. 2012. Ppcoin: Peer-to-peer Crypto-Currency with Proof-of-Stake. Retrieved October 31, 2018 from https://peercoin.net/960assets/paper/peercoin-paper.pdf.

[57] Nir Kshetri. 2018. Blockchain's roles in meeting key supply chain management objectives. *International Journal of Information Management* 39 (2018), 80–89. DOI: https://doi.org/10.1016/j.ijinfomgt.2017.12.005

[58] Tsung-Ting Kuo, Hyeon-Eui Kim, and Lucila Ohno-Machado. 2017. Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association* 24, 6 (Nov. 2017), 1211–1220. DOI: https://doi.org/10.1093/jamia/ocx068

[59] Douglas M. Lambert, Martha C. Cooper, and Janus D. Pagh. 1998. Supply chain management: Implementation issues and research opportunities. *The International Journal of Logistics Management* 9, 2 (1998), 1–20. DOI: https://doi.org/10.1108/09574099810805807 arXiv:https://doi.org/10.1108/09574099810805807

[60] Choong Ho Lee and Hyung-Jin Yoon. 2017. Medical big data: Promise and challenges. *Kidney Research and Clinical Practice* 36, 1 (2017), 3. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5331970/.

[61] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun. 2017. Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. *IEEE Internet of Things Journal* 4, 6 (Dec. 2017), 1832–1843. DOI: https://doi.org/10.1109/JIOT.2017.2740569

[62] Xiaoqi Li, Peng Jiang, Ting Chen, Xiapu Luo, and Qiaoyan Wen. 2017. A survey on the security of blockchain systems. *Future Generation Computer Systems* (2017), 1–13. DOI: https://doi.org/10.1016/j.future.2017.08.020

[63] Iuon-Chang Lin and Tzu-Chun Liao. 2017. A survey of blockchain security issues and challenges. *International Journal of Network Security* 19, 55 (2017), 653–65901. DOI: https://doi.org/10.6633/IJNS.201709.19(5).01

[64] Joshua Lind, Ittay Eyal, Florian Kelbert, Oded Naor, Peter R. Pietzuch, and Emin Gün Sirer. 2017. Teechain: Scalable blockchain payments using trusted execution environments. *CoRR* abs/1707.05454 (2017). arxiv:1707.05454 http://arxiv.org/abs/1707.05454

[65] L. A. Linn and M. B. Koo. 2016. Blockchain for Health Data and Its Potential Use in Health IT and Health Care Related Research. Retrieved August 25, 2018 from https://www.healthit.gov/sites/default/files/11-74-ablockchainforhealthcare.pdf.

[66] Tim K. Mackey and Gaurvika Nayyar. 2017. A review of existing and emerging digital technologies to combat the global trade in fake medicines. *Expert Opinion on Drug Safety* 16, 5 (2017), 587–602. https://www.tandfonline.com/doi/abs/10.1080/14740338.2017.1313227?journalCode=ieds20.

[67] Imran Makhdoom, Mehran Abolhasan, Haider Abbas, and Wei Ni. 2019. Blockchain's adoption in IoT: The challenges, and a way forward. *Journal of Network and Computer Applications* 125 (2019), 251–279. DOI: https://doi.org/10.1016/j.jnca.2018.10.019

[68] Thomas McGhin, Kim-Kwang Raymond Choo, Charles Zhechao Liu, and Debiao He. 2019. Blockchain in healthcare applications: Research challenges and opportunities. *Journal of Network and Computer Applications* 135 (2019), 62–75. DOI: https://doi.org/10.1016/j.jnca.2019.02.027

[69] Medibloc. 2017. Medibloc Whitepaper. Retrieved February 5, 2019 from https://medibloc-homepage.oss-us-west-1.aliyuncs.com/whitepaper/medibloc_whitepaper_en.pdf.

[70] Medicohealth. 2018. The Biggest Doctor-Patient Environment Based on Blockchain. Retrieved February 5, 2019 from https://medicohealth.io/supporters/documents/wp_beta.pdf.

[71] MedX. 2018. MedX Protocol—Launch Unstoppable Medical Apps. Retrieved February 5, 2019 from https://medcredits.io/pdfs/medx-protocol–project-slides.pdf.

[72] Robert H. Miller and Ida Sim. 2004. Physicians' use of electronic medical records: Barriers and solutions. *Health Affairs* 23, 2 (2004), 116–126. DOI: https://doi.org/10.1377/hlthaff.23.2.116 arXiv:https://doi.org/10.1377/hlthaff.23.2.116 PMID: 15046136.

[73] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun. 2017. A review on consensus algorithm of blockchain. In *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC'17)*. IEEE, 2567–2572. DOI: https://doi.org/10.1109/SMC.2017.8123011

[74] U. Mukhopadhyay, A. Skjellum, O. Hambolu, J. Oakley, L. Yu, and R. Brooks. 2016. A brief survey of Cryptocurrency systems. In *2016 14th Annual Conference on Privacy, Security and Trust (PST'16)*. IEEE, 745–752. DOI: https://doi.org/10.1109/PST.2016.7906988

[75] Caitlin Sampaio Mulholland. 2018. Dados pessoais sensíveis e a tutela de direitos fundamentais: Uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). *Revista de Direitos e Garantias Fundamentais* 19, 3 (2018), 159–180.

[76] Satoshi Nakamoto. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved August 20, 2018 from https://bitcoin.org/bitcoin.pdf.

[77] Ricardo Neisse, Gary Steri, and Igor Nai-Fovino. 2017. A blockchain-based approach for data accountability and provenance tracking. In *Proceedings of the 12th International Conference on Availability, Reliability and Security (ARES'17)*. ACM, New York, NY, Article 14, 10 pages. DOI: https://doi.org/10.1145/3098954.3098958

[78] Steve Omohundro. 2014. Cryptocurrencies, smart contracts, and artificial intelligence. *AI Matters* 1, 2 (Dec. 2014), 19–21. DOI: https://doi.org/10.1145/2685328.2685334

[79] Ogbonna Brian Onyebuchi. 2016. National drug distribution in Nigeria; implications for the goals of national drug policy. *European Journal of Pharmaceutical and Medical Research (EJPMR)* 3, 1 (2016), 1–4.

[80] E. R. Onyejekwe. 2014. Big data in health informatics architecture. In *2014 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM'14)*. IEEE, 728–736. DOI: https://doi.org/10.1109/ASONAM.2014.6921667

[81] P. Otero, W. Hersh, and A. U. Jai Ganesh. 2014. Big data: Are biomedical and health informatics training programs ready?: Contribution of the IMIA working group for health and medical informatics education. *Yearbook of Medical Informatics* 9, 1 (2014), 177. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4287071/.

[82] Vishal Patel. 2018. A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. *Health Informatics Journal* 25, 4 (2018), 1398–1411. DOI: https://doi.org/10.1177/1460458218769699 arXiv:https://doi.org/10.1177/1460458218769699 PMID: 29692204.

[83] Gilberto Perez, Ronaldo Zwicker, et al. 2010. Fatores determinantes da adoção de sistemas de informação na área de saúde: Um estudo sobre o prontuário médico eletrônico. *RAM. Revista de Administração Mackenzie (Online)* 11, 1 (2010), 174–200.

[84] George Pîrlea and Ilya Sergey. 2018. Mechanising blockchain consensus. In *Proceedings of the 7th ACM SIGPLAN International Conference on Certified Programs and Proofs*. ACM, 78–90. DOI: https://doi.org/10.1145/3167086

[85] Mayank Pratap. 2018. Blockchain in Healthcare: Opportunities, Challenges, and Applications. Retrieved from https://hackernoon.com/blockchain-in-healthcare-opportunities-challenges-and-applications-d6b286da6e1f.

[86] Kefa Rabah. 2017. Challenges and opportunities for blockchain powered healthcare systems: A review. *Mara Research Journal of Medicine & Health Sciences* 1, 1 (Oct. 2017), 45–52. http://medicine.mrjournals.org/index.php/medicine/article/view/6https://medicine.mrjournals.org/index.php/medicine/article/view/6.

[87] Igor Radanović and Robert Likić. 2018. Opportunities for use of blockchain technology in medicine. *Applied Health Economics and Health Policy* 16, 5 (Oct. 2018), 583–590. DOI: https://doi.org/10.1007/s40258-018-0412-8

[88] Amir M. Rahmani, Tuan Nguyen Gia, Behailu Negash, Arman Anzanpour, Iman Azimi, Mingzhe Jiang, and Pasi Liljeberg. 2018. Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach. *Future Generation Computer Systems* 78 (2018), 641–658. DOI: https://doi.org/10.1016/j.future.2017.02.014

[89] Y. Ren, R. Werner, N. Pazzi, and A. Boukerche. 2010. Monitoring patients via a secure and mobile healthcare system. *IEEE Wireless Communications* 17, 1 (2010), 59–65. DOI: https://doi.org/10.1109/MWC.2010.5416351

[90] Nabil Rifi, Elie Rachkidi, Nazim Agoulmine, and Nada Chendeb Taher. 2017. Towards using blockchain technology for eHealth data access management. In *2017 4th International Conference on Advances in Biomedical Engineering (ICABME'17)*. IEEE, 1–4. DOI: https://doi.org/10.1109/ICABME.2017.8167555

[91] Juan M. Roman-Belmonte, Hortensia De la Corte-Rodriguez, and E. Carlos Rodriguez-Merchan. 2018. How blockchain technology can change medicine. *Postgraduate Medicine* 130, 4 (2018), 420–427. DOI: https://doi.org/10.1080/00325481.2018.1472996

[92] M. Sabt, M. Achemlal, and A. Bouabdallah. 2015. Trusted execution environment: What it is, and what it is not. In *2015 IEEE Trustcom/BigDataSE/ISPA*, Vol. 1. IEEE, 57–64. DOI: https://doi.org/10.1109/Trustcom.2015.357

[93] André Hideaki Saheki. 2005. *Construção de Uma Rede Bayesiana Aplicada ao Diagnóstico de Doenças Cardíacas*. Ph.D. Dissertation. Universidade de São Paulo. http://www.teses.usp.br/teses/disponiveis/3/3132/tde-06042005-203820/es.php.

[94] O. Salem, Y. Liu, A. Mehaoua, and R. Boutaba. 2014. Online anomaly detection in wireless body area networks for reliable healthcare monitoring. *IEEE Journal of Biomedical and Health Informatics* 18, 5 (Sept. 2014), 1541–1551. DOI: https://doi.org/10.1109/JBHI.2014.2312214

[95] Mehrdad Salimitari and Mainak Chatterjee. 2018. An overview of blockchain and consensus protocols for IoT networks. *CoRR* abs/1809.05613 (2018), 1–15. arxiv:1809.05613 http://arxiv.org/abs/1809.05613

[96] Joachim Sandgaard and Steve Wishstar. 2018. MedChain. Retrieved September 30, 2018 from http://medchain.us/doc/Medchain%20Whitepaper%20v1.0.pdf [White Paper].

[97] L. S. Sankar, M. Sindhu, and M. Sethumadhavan. 2017. Survey of consensus protocols on blockchain applications. In *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS'17)*. IEEE, 1–5. DOI: https://doi.org/10.1109/ICACCS.2017.8014672

[98] Rui T. Sousa, Songsong Liu, Lazaros G. Papageorgiou, and Nilay Shah. 2011. Global supply chain planning for pharmaceuticals. *Chemical Engineering Research and Design* 89, 11 (2011), 2396–2409. DOI: https://doi.org/10.1016/j.cherd.2011.04.005

[99] Chet Stagnaro. 2017. White Paper: Innovative Blockchain Uses in Health Care. Retrieved September 28, 2018 from https://www.freedassociates.com/wp-content/uploads/2017/08/Blockchain_White_Paper.pdf.

[100] Melanie Swan. 2015. *Blockchain: Blueprint for a New Economy* (1st ed.). O'Reilly Media, Inc., Sebastopol, CA.

[101] Latanya Sweeney. 2002. K-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems* 10, 5 (Oct. 2002), 557–570. DOI: https://doi.org/10.1142/S0218488502001648

[102] Nick Szabo. 1997. Formalizing and securing relationships on public networks. *First Monday* 2, 9 (1997), 22. DOI: https://doi.org/10.5210/fm.v2i9.548

[103] Thein Than Thwin and Sangsuree Vasupongayya. 2019. Blockchain-based access control model to preserve privacy for personal health record systems. *Security and Communication Networks* 2019 (2019), 1–15. DOI: https://doi.org/10.1155/2019/8315614

[104] Md. Ashraf Uddin, Andrew Stranieri, Iqbal Gondal, and Venki Balasubramanian. 2018. Continuous patient monitoring with a patient centric agent: A block architecture. *IEEE Access* 6 (2018), 32700–32726. DOI: https://doi.org/10.1109/ACCESS.2018.2846779

[105] Xu Wang, Xuan Zha, Wei Ni, Ren Ping Liu, Y. Jay Guo, Xinxin Niu, and Kangfeng Zheng. 2019. Survey on blockchain for Internet of Things. *Computer Communications* 136 (2019), 10–29. DOI: https://doi.org/10.1016/j.comcom.2019.01.006

[106] R. Wechsler, M. S. Anção, C. J. R. de Campos, and D. Sigulem. 2003. A Informática no consultório Médico. *Jornal de Pediatria* 79 (2003), 1–10. DOI: https://doi.org/10.1590/S0021-75572003000700002

[107] WHO. 2017. Substandard and Falsified Medical Products. Retrieved October 8, 2018 from http://www.who.int/news-room/fact-sheets/detail/substandard-and-falsified-medical-products.

[108] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani. 2017. MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. *IEEE Access* 5 (2017), 14757–14767. DOI: https://doi.org/10.1109/ACCESS.2017.2730843

[109] B. Yan and G. Huang. 2009. Supply chain information transmission based on RFID and internet of things. In *2009 ISECS International Colloquium on Computing, Communication, Control, and Management*, Vol. 4. IEEE, 166–169. DOI: https://doi.org/10.1109/CCCM.2009.5267755

[110] Jesse Yli-Huumo, Deokyoon Ko, Sujin Choi, Sooyong Park, and Kari Smolander. 2016. Where is current research on blockchain technology?—A systematic review. *PLoS One* 11 (2016), 1–27. DOI: https://doi.org/10.1371/journal.pone.0163477

[111] Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Xiangping Chen, and Huaimin Wang. 2018. Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services* 14, 4 (2018), 352–375.

[112] G. Zyskind, O. Nathan, and A. Pentland. 2015. Decentralizing privacy: Using blockchain to protect personal data. In *2015 IEEE Security and Privacy Workshops*. IEEE, 180–184. DOI: https://doi.org/10.1109/SPW.2015.27

Received February 2019; revised October 2019; accepted December 2019