On the exploitation of the blockchain technology in the healthcare sector: a systematic review

Valeria Merlo[a,b], Gianvito Pio[c,d,*], Francesco Giusto[b], Massimo Bilancia[a]

[a]*Ionian Department of Law, Economics and Environment (DJSGE), University of Bari Aldo Moro, Via Duomo 259, 74123 Taranto, Italy*
[b]*Sabanet s.r.l., Via Alberto Sordi 4600, 74121 Taranto, Italy*
[c]*Department of Computer Science, University of Bari Aldo Moro, Via E. Orabona 4, 70125 Bari, Italy*
[d]*Big Data Laboratory, National Interuniversity Consortium for Informatics (CINI), Via Ariosto 25, 00185 Rome, Italy*

---

*Corresponding author.

Email addresses: valeria.merlo@uniba.it (Valeria Merlo), gianvito@pio@uniba.it (Gianvito Pio), francesco.giusto@sabanet.it (Francesco Giusto), massimo.bilancia@uniba.it (Massimo Bilancia)

Abstract

The blockchain is a disruptive technology born in the last few years, which possible applications in different domains are being extensively studied. In this context, healthcare appears to be a very attractive application domain for the blockchain because, due to its characteristics, it can provide the necessary guarantees on the secure processing, sharing and management of sensitive patient data. In this paper, we perform a systematic review of the literature on the adoption of the blockchain technology in healthcare, focusing on applications implemented in real contexts. Our goal is to investigate the current state of the art in this specific field, emphasizing limitations and possible future developments.

Publications extracted from Scopus, PubMed and Web of Science that satisfy some predetermined search criteria were collected by means of appropriate queries. These papers were analyzed and classified into five main categories, based on the specific sub-domain on which the applications were projected.

The performed analysis highlighted that research activities are currently focused on data security and on the implementation of electronic health records through the Blockchain. On the other hand, some other areas are still under-explored, including that related to IoT or to the implementation of automated diagnosis systems.

Keywords

Healthcare, Blockchain, Smart Contracts

1. Introduction

In 2008, Satoshi Nakamoto proposed a solution to the double spending problem (Satoshi Nakamoto, 2008), that refers to the possibility of spending a digital currency multiple times, due to its inherent ease to be duplicated. Nakamoto's innovative idea was to use the blockchain, and proposed the specific blockchain nowadays known as Bitcoin, together with its native cryptocurrency.

A blockchain is a database of sequential blocks containing transactions, distributed in a peer-to-peer network, where each node of the network owns its own copy. The Bitcoin blockchain, like other blockchains subsequently proposed, is *public*. The main advantages of public blockchains are the transparency, the immutability, the traceability and, therefore, the reliability of the stored data. These characteristics make the blockchain applicable in many contexts besides the storage and verification of cryptocurrency transactions.

One of the most interesting applications of the blockchain technology, on which companies and researchers are focusing their efforts, is that of the healthcare. In this context, research activities are being conducted on the design of proper processes to share data, such as records, reports and images, between healthcare institutions without involving third parties that may possibly alter it (Rakic, 2018). Other lines of research include archiving patient health data Shahnaz et al. (2019), enforcing transparency and verifiability of medical experiments (Bell et al., 2018), and supporting the traceability of drugs to prevent counterfeiting issues (Kuo et al., 2017).

In this scenario, the goal of our work is to perform a systematic review of blockchain applications in healthcare that have been proposed in the literature and/or have been actually implemented in real contexts. The motivations of this work live in the need of assessing the current state of the art, outlining challenges and opportunities, as well limitations of current solutions, in order to pave the way for future research activities in this field.

Existing works in the literature have been selected using the PubMed PubReminer tool[1], focusing on Scopus, PubMed, and Web of Science, using *blockchain* as a seed keyword in the title of the articles. We refined the set of identified paper by eliminating duplicates (since copies of the same article can be found in different repositories), and by removing papers without an abstract, a DOI, or keywords provided by the authors. This step was followed by a manual selection based on the abstracts and/or the full content of the articles. In particular, a paper has been included in this review if it describes an application in the healthcare sector that is actually implemented, even through a small prototype. Therefore, papers describing purely theoretical ideas were excluded. This manual selection led to a total of 64 articles, that were subsequently been categorized into research areas, in order to provide researchers with some clues about the challenges, the opportunities and the gaps for which further research activities are needed. The details of the methodology adopted to refine the query are reported in Section 4.

The rest of the paper is organized as follows: Section 2 provides a brief introduction on the blockchain technology; in Section 3, we describe the specific challenges arising while adopting the blockchain for healthcare applications, briefly review existing surveys, and outline the contribution of this paper; in Section 4, we define the methodology we followed to conduct our systematic review; in Section 5 we discuss the outcome of our review, specifically focusing on the identified categories; in Section 6, we outline possible research directions; finally, Section 7 concludes the paper and outline some possible future work.

2. Background on blockchain technology

A blockchain is a database of sequential blocks, stored in multiple decentralized and independent nodes. Chaining is implemented by injecting some information about a given block into the following block. More specifically, the hash of the previous block in the chain is added to the header of the current block (Vujicic et al., 2018). Hashes are strings, of fixed or variable length, generated by an algorithm (SHA256 in the case of the Bitcoin blockchain) which goal is to produce a non-reversible bit sequence that uniquely identifies/represents the entire block data. The peculiarity of hashing algorithms is that the change of a single bit in the input data results in a significant (and unpredictable) change of the returned hash. The *immutability* comes specifically from such hash values. Indeed, it is impossible to alter or tamper any data stored in a previous block, without changing the hashes stored in the next block, which accordingly would alter the hashes of all the subsequent blocks. Therefore, any malicious change to the data in a block would be easily detected by the participant nodes of the blockchain, that would mark such a change as invalid.

When someone submits a transaction (see Figure 1 for a graphical overview), it is broadcasted to the network, and enters into the so-called *transaction pool*, that contains all the unconfirmed transactions. The validation of transactions is based on the process of the generation of blocks, called *mining*. This process is performed by special nodes of the network,

[1] `https://hgserver2.amc.nl/cgi-bin/miner/miner2.cgi`

called *miners*, and consists of *i)* the selection of a subset of transactions from the transaction pool; *ii)* the calculation of a *valid* hash value for the block that is being generated; *iii)* the broadcast of the mined block to the network. Note that the complexity is only in step *ii)*, that is based on the identification of a value to assign to a given variable (called *nonce*) in the block header, such that the hash value of the obtained block is less than a given threshold defined by the protocol. This means that miners proceed by performing several attempts, by varying the value of the nonce, hoping to find a valid hash value. Accordingly, the more computational power a miner allocates to solving such a cryptographic puzzle, the higher the probability to find a valid hash and be able to propagate the block to the network. This process is called Proof-of-Work - PoW (Gervais et al., 2016), and is currently adopted in Bitcoin, in the current version of Ethereum and in several other blockchains.

One may wonder why a miner would spend so many resources to solve such a puzzle and generate a new block. The answer comes from the incentivization mechanism put in place in the blockchain, that rewards a given amount of cryptocurrency to miners who succeed in finding the solution. Note that, due to the decentralized nature of the blockchain, it is possible that two or more miners find a solution at the same time. In this case, a fork of the blockchain is created, where different versions of the chain temporarily live simultaneously. However, each miner continues working on one of the versions, and once a new block is broadcasted, the longest chain[2] is considered as the true one by all the nodes, solving the temporary inconsistency caused by the fork. This strategy, although expensive from a computational viewpoint, is effective against several kinds of attacks (Gervais et al., 2016).

Besides Proof-of-Work consensus algorithm, other approaches have been proposed in other blockchains, including:

- Proof of Stake (PoS), that introduces the concept of cryptocurrencies at *stake* and *coin age*, through which the probability that a miner solves the puzzle and creates a new block depends on the amount of cryptocurrency put at stake, and the amount of time it is at stake (Cao et al., 2020a). PoS will be adopted by the next version of Ethereum.

- Delegated Proof of Stake (DPoS) derives from PoS and consists in delegating the right to create a new block to a subset of representative nodes (Yang et al., 2019). DPoS is currently implemented in Cardano, EOS, and TRON.

- Ripple Protocol Consensus Algorithm (RPCA), that is adopted by Ripple and follows a different approach based on three iterative phases (Chase & MacBrough, 2018).

In general, the goal of a consensus protocol is to keep the status of the blockchain consistent and genuine, avoiding possible attacks, while possibly keeping the needed resources under control. Of course, if the majority of the computational power (in the case of PoW) is in the hands of malicious miners, there is still the possibility of compromising the chain (Saad et al., 2020). This is the motivations behind the need to maximize the decentralization, i.e., the number of nodes acting as miners.

The above-mentioned characteristics make the blockchain a suitable tool for storing not only cryptocurrency transactions, but general-purpose data, without the need of a trusted

[2]This approach is adopted by Bitcoin, but other criteria can generally be used.

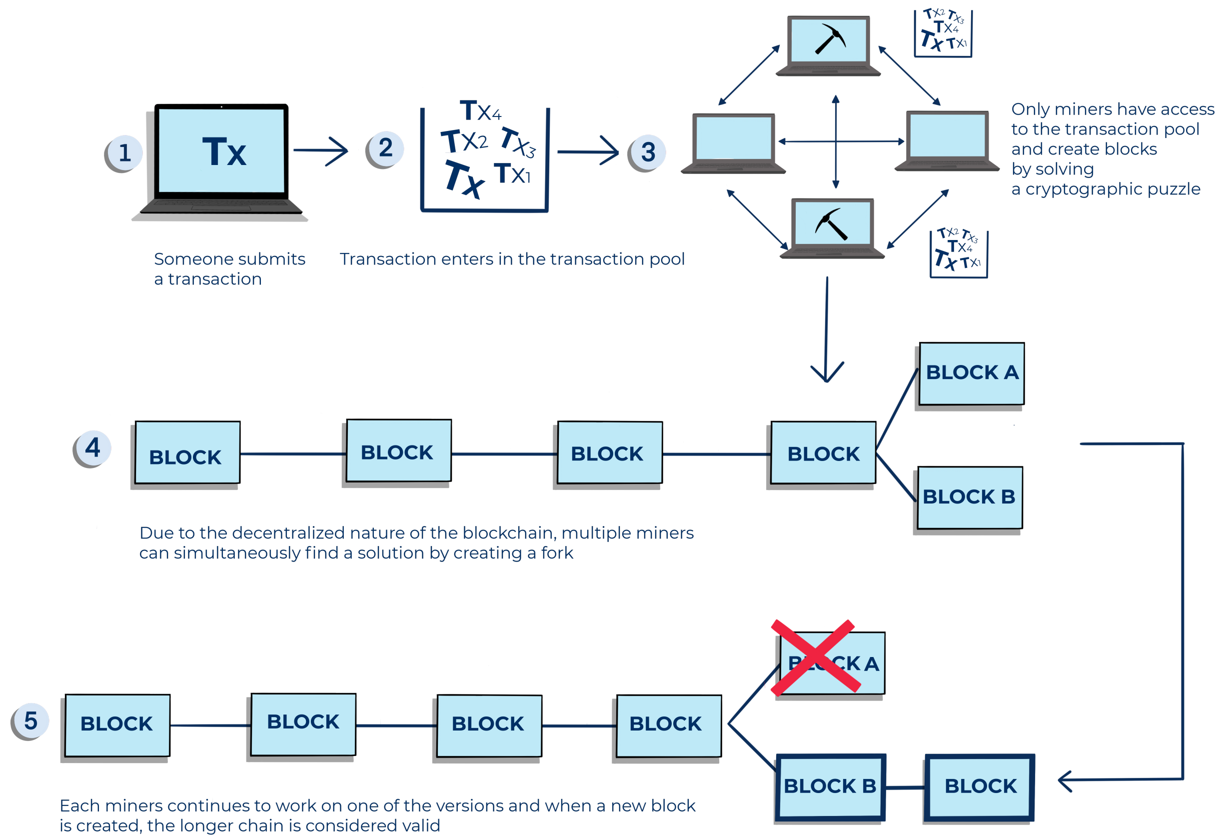

Figure 1: Graphical representation of the general workflow followed to mine new blocks in Bitcoin.

third party, and with strong guarantees in terms of immutability and transparency. This led other blockchain developers to also focus research and development activities on advanced mechanisms to persist data and execute code, through the so-called *smart contracts* introduced in Ethereum.

A smart contract is a collection of functions and data, that define its state, residing at a specific address on the blockchain. In Ethereum, smart contracts represent a specific type of account, with its own balance (in terms of amount of cryptocurrency - ETH), which can also send transactions over the network. However, differently from standard accounts, called Externally Owned Accounts (EOAs), they are not controlled or owned by any user, but act autonomously as they have initially been programmed to. Their functions can be called through a transaction starting from an EOA, or by other smart contracts, provided that the initial trigger comes from an EOA. Smart contracts can define rules and authorizations, and store data in a decentralized manner. The interaction with them is irreversible.

Note that each interaction with the blockchain, both in terms of cryptocurrency transfers and in terms of invocations of smart contract functions, requires a fee (in cryptocurrencies) to be paid to miners, which depend on the complexity of the operations performed and on the amount of data stored/accessed. For this reason, the storage of large amount of data (e.g., images, videos, large textual documents, etc.) on the blockchain is discouraged, and existing solutions generally rely on either centralized/hybrid architectures, or on specific decentralized file systems, like the InterPlanetary File System (IPFS)[3]. IPFS provides a decentralized mean for storing and accessing data, enabling the possibility to download them from multiple locations that are not managed by a single organization. It also improves the resiliency, by distributing data worldwide in multiple nodes owned by multiple entities and individuals. On the contrary, attacks to specific servers of an organization, or accidents (e.g., a fire in a datacenter), may easily compromise centralized data. IPFS also makes censorship actions harder to be applied, since data from IPFS can come from multiple locations. In general, IPFS promotes the possibility to make data permanently available, without the control of a centralized authority. This characteristic made it the most adopted file system for managing large amounts of data in combination with blockchain-based solutions, also in the context of health data.

Another important peculiarity of the blockchain is the possibility of freely taking part to the network: anybody can act as a simple node or as a miner, submit transactions, or read the full history of past transactions, provided that the performed operation conforms to the protocol. This characteristic is specific of the so-called *public* (or *permissionless*) blockchains, like Bitcoin and Ethereum. Note that public blockchains may not be the right solution for all the application domains. This is the case of health data, which, in most cases, are personal and sensitive, and need to be protected and accessed selectively. Therefore, *permissioned* blockchains have been proposed, starting from (the permissioned version of) Ethereum and Hyperledger Fabric. Among permissioned blockchains, we can mainly distinguish two subcategories, namely, *private* and *consortium* blockchains. Private blockchains, also known as *managed* blockchains, are controlled by a single organization, which decides who can act as a node, possibly granting different authorizations. On the other hand, consortium blockchains are governed by a group of organizations, rather than one single entity. Consortium blockchains, therefore, are more decentralized than private blockchains, resulting in higher levels of security. However, setting up consortiums can be problematic because of the initial required cooperation and trust among the participants.

Of course, different hybrid variants of the mentioned types of blockchain are possible, as well as hybrid architectures that put together a private/consortium blockchain with a public blockchain, to identify the best trade-off between data privacy/protection and security/transparency, according to the application scenario at hand.

3. Challenges and contributions

In this section, we briefly discuss the challenges raised by the adoption of the blockchain technology in healthcare. Indeed, although several advantages can be provided by the blockchain technology to different application scenarios in healthcare, mainly due to its inherent reliability, verifiability, and robustness to tampering, it also introduces some criticisms. Among them, the first aspect to consider is the fact that data related to health are generally personal, and possibly sensitive, which introduces additional challenges in terms of data

[3] `https://ipfs.io/`

protection and security. In general, data protection regulations, like the General Data Protection Regulation (GDPR), are considered not fully compatible with public blockchains[4], mainly because of the impossibility to guarantee the right to be forgotten. Therefore, as mentioned in the previous section, the adoption of private/consortium blockchains or hybrid architectures are being considered the right solution. This is the motivation for which most of the works that we will present in Section 4 fall in this category.

The adoption of the blockchain may also introduce inefficiencies in terms of costs and delays. Indeed, while centralized systems may easily (and cheaply) perform complex data consistency checks, perform security checks, store large amounts of data, and provide near real-time responses, the adoption of the blockchain introduces the need to properly check for access authorization in a decentralized manner, as well as storage limitations and latencies, due to the block validation process. Moreover, as mentioned in Section 2, complex transactions may be expensive in terms of miners' fee (in cryptocurrencies), making the whole technology inapplicable in some contexts due to the unacceptable increases of costs.

As a result, the research activities on the adoption of the blockchain in the healthcare sector mainly focused on addressing the above-mentioned challenges. Such challenges have also been considered in other surveys that reviewed existing approaches. A relevant example is the survey by Agbo et al. (2019), where the authors adopted a generic query to select publications including keywords such as *blockchain*, *ledger* or *medic*, without specifically focusing on works presenting implemented solutions. Agbo et al. (2019) classified blockchain applications in healthcare according to different use cases, focusing on commonalities and differences among the existing approaches, without providing specific details about them. Together with the challenges related to the limited speed and scalability, mainly due to the large amount of involved data and the need for short response times, the authors also emphasized an additional issue, namely, the lack of interoperability, as there is no standard for the development of blockchain-based applications for healthcare.

Another relevant survey is the work by Chukwu & Garg (2020). Similarly to the survey by Agbo et al. (2019), the query used to select publications was very generic and without a specific focus on available implementations. The authors analyzed the selected works along three different viewpoints, namely:

- *bibliometric distribution*, i.e., how many works have been published for each type, where the considered types include, for example, studies proposing frameworks, studies discussing prototyping models, or studies implementing real applications;
- *functional distribution*, i.e., the use case considered in the publication, such as the management of electronic medical records, or access control with identity management;
- *technical analysis*, performed only on works actually proposing prototypes and implementations, which focused on the categorization of technical aspects, such as architectures, blockchain platforms, storage schemes, and consensus algorithms.

As stated by the authors, papers proposing models without a working prototype or implementation account for 2/3 of the total number of selected papers. Also in this survey,

[4] https://www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf

communication, scalability and speed issues are emphasized as strong limitations coming from the adoption of the blockchain.

Finally, it is worth mentioning the recent survey by Tandon et al. (2020). The authors used the same search query adopted by Agbo et al. (2019), but did not follow the PRISMA methodology like the previously mentioned surveys. On the contrary, the authors adopted specific selection criteria to determine quality, relevance and robustness (Webster & Watson, 2002), while a meta-ethnographic approach (Noblit & Hare, 1988) was used to review and summarize the studies that qualified for inclusion. Overall, four major families were identified: *i)* conceptual evolution, *ii)* technological advancements (in terms of faced technical challenges, and developed applications), *iii)* efficiency enhancement, and *iv)* data management, including data security and privacy.

As already mentioned, existing surveys did not specifically focused on actually implemented solutions, and mostly collected quantitative statistics along different dimensions of analysis, without providing details on each specific work. Although this strategy may provide a wide overview, it does not allow the reader to focus on ready-to-use (or at least prototyped) solutions. In this respect, in this paper, we provide the following contributions:

- we focus on actually available implementations of blockchain solutions for healthcare;
- we describe the selected publications, providing a clear idea about the contribution they provide to solve typical challenges;
- based on the implemented solutions, as well as on their advantages and limitations, we outline additional research directions.

4. Methodology

We conducted a systematic review of major applications of blockchain technologies in healthcare by performing a set of queries on 3 different repositories, i.e., Pubmed, Web Science and Scopus. We performed the queries in July 2022, and adopted the well-established Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) statement (Moher et al., 2009). In the following, we briefly describe the main steps that we followed, according to the PRISMA statement.

Identification. In order to build a collection of papers to consider, it is first necessary to identify the keywords to define the search query.

At this purpose, we adopted the PubMed PubReminer tool[1] by entering the term *blockchain* as the first word in the title of the articles to be retrieved. The tool returned a total of 353 results, together with a list of the most frequently used words in the abstracts of Pubmed publications, in descending order of occurrence. This list was used to identify additional keywords to refine the query, avoiding general terms like *provide* or *paper*. Specifically, we required the presence of the words *application*, *develop* or *system* (and their variants) to focus on paper discussing actual implementations of blockchain technologies, and added the condition of the presence of at least one of the keywords *clinical*, *doctor*, *patient* and *health* (and their variants), to narrow down the search to the healthcare sector. No time-based filter was imposed on the query, since the blockchain technology has received a huge attention only

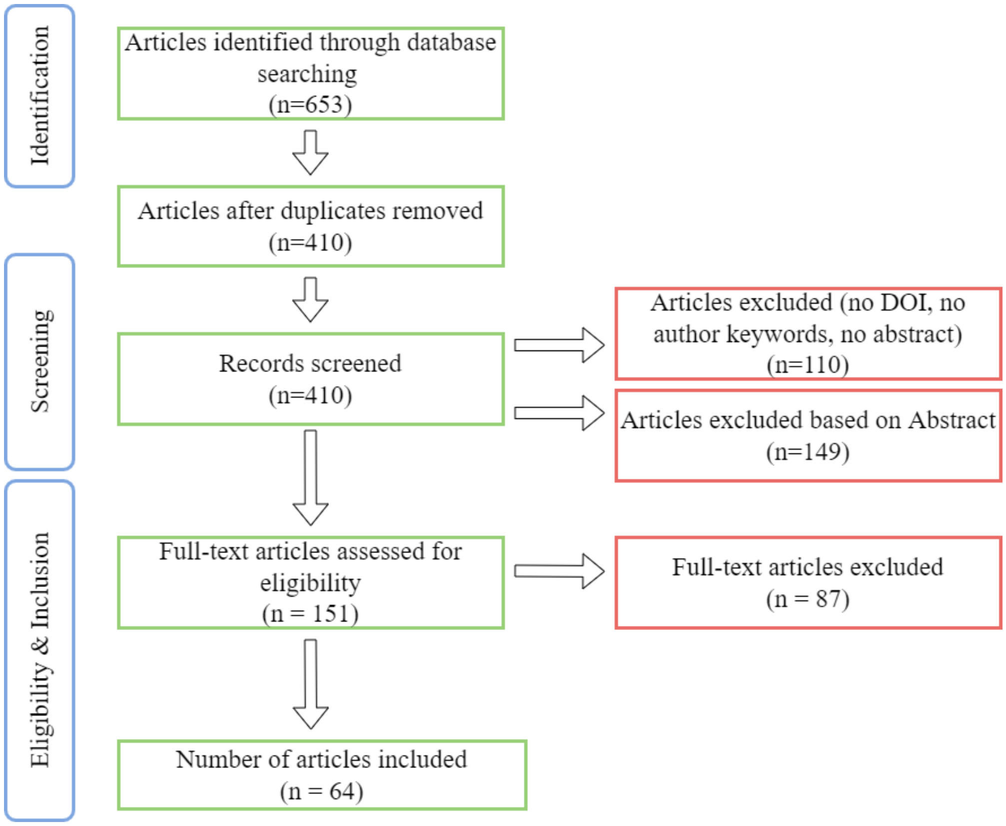

Figure 2: The followed PRISMA flow diagram.

recently. These conditions resulted in the following query, written according to the query language used by Scopus:

```
TITLE (blockchain AND (application OR develop OR system) AND ((clinic OR
clinical OR clinically OR clinics) OR (medic OR medical) OR (patient OR
patients) OR health OR healthcare)) AND (LIMIT-TO (LANGUAGE, "English"))
```

The query returned 479 papers from Scopus, 128 from Web of Science and 46 papers from PubMed, for a total of 653 records. We finally removed 243 duplicate records, leading to a total of 410 articles belonging to the initial database.

Screening. Starting from the 410 selected articles, a first screening step was performed by excluding the documents that did not contain the basic necessary information to perform a descriptive analysis, such as the abstract (12 records excluded), the author's keywords (67 records excluded) and the DOI (31 documents excluded), resulting in 300 articles. The second step was performed through a critical reading of the abstracts. Specifically, we excluded papers describing conceptual models, protocols, or algorithms for which there was no contextual implementation, even through prototypes. Additionally, articles that focus only on the implementation of user interfaces were discarded. At the end of both the screening steps, we obtained 151 eligible articles.

Eligibility & Inclusion. Finally, we critically read all eligible papers, and screened out 87 additional records. The adopted criteria are basically the same as those adopted in

Screening phase, but applied on the entire text of the publication. At the end of the whole process, a final database consisting of 64 articles was obtained.

In Figures 3, 4 and 5 we graphically depict some basic statistics related to three main aspects of the selected papers: the adopted blockchain or tool (based on an existing blockchain), the consensus algorithm, and the blockchain type.

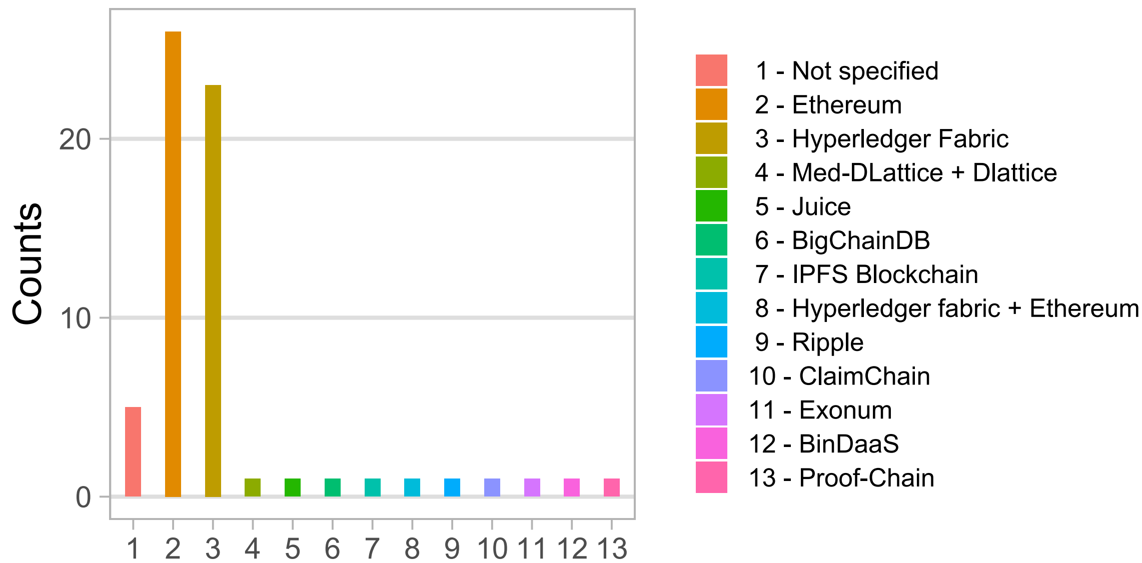

Figure 3: Number of selected papers for each blockchain or blockchain platform.

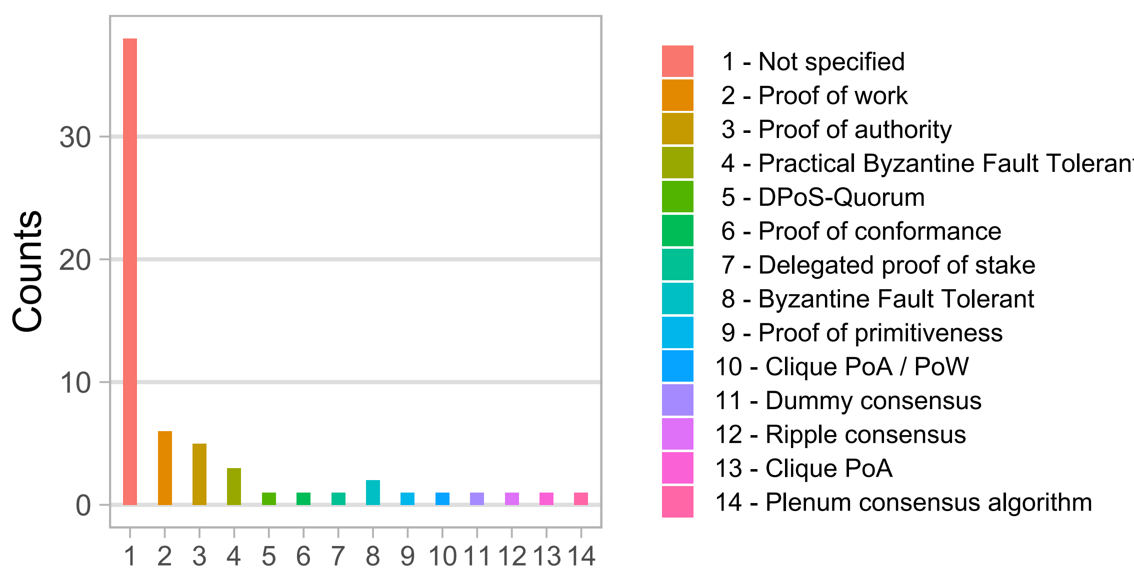

Figure 4: Number of selected papers for each consensus algorithm.

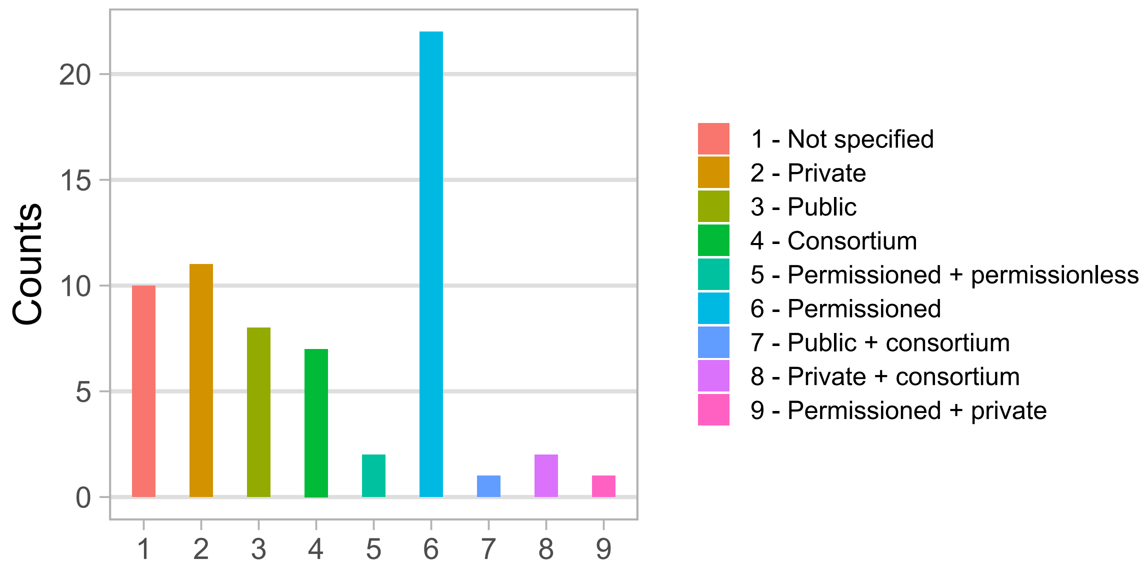

Figure 5: Number of selected papers for each blockchain type.

5. Blockchain-based applications in healthcare

In this section, we present the selected papers. We first classify them according to their main topic, namely according to the specific domain the described applications were designed for. Our ultimate goal is to understand the aspects where blockchain research and development has focused most, achieving interesting results, and to highlight the main gaps where challenges have still to be solved.

In Figure 6, we graphically depict the identified categories, while in Figure 7, we depict the total number of papers appearing yearly for each of them.

In the following subsections we discuss in detail the articles falling into each category.

5.1. Electronic Medical Records

Electronic Medical Records (EMRs) or Elecronic Health Records (EHRs) contain private and sensitive patient data and are usually held by hospital systems. It is often difficult for patients to access their own health data, which may also be distributed among different actors. To alleviate this difficulty, Toshniwal et al. (2019) proposed PACEX, a blockchain-based system that allows patients to have complete control over their EMR. PACEX records all EMR exchanges, stores the hash values of EMRs on the blockchain for integrity verification, while minimizing on-chain data storage. The implementation exploits the Ethereum private blockchain and consists of three main components: the application for patients, the application for hospitals, and the blockchain. The first grants users full authority to access their data and allows for the management of EMRs distributed across multiple hospitals. The second can be adopted by each hospital to process requests of access, or to retrieve EMRs from other hospitals. Each hospital will run an Ethereum node to connect to the private blockchain network. The blockchain records all the interactions that take place between the parties via Smart Contracts. The authors performed a qualitative analysis that proved that the proposed system can meet the requirements of authentication, integrity, access control and traceability. Moreover, the system is user-friendly, as it does not require the patient to have any knowledge related to the blockchain. The main drawback is that PACEX is not able to handle simultaneous multiple requests.

Koushik et al. (2019) developed a decentralized medical service for patients and healthcare providers, based on blockchain. The authors propose a web application that can interact with the blockchain network via REST API calls, providing an easy way for participants to share and/or view medical data. Essentially, the application works as follows: when a doctor visits a patient, prescriptions are added to the user's record along with the necessary observations. When the patient is visited by other doctors, they can easily access the patient's data about previous visits. The application has been implemented using Hyperledger Composer, which enables the creation of a permissioned blockchain network.

The uniqueness of this implementation is the use of Hyperledger Composer, since implementations of medical records management systems prior to this work adopted the Ethereum framework, a public blockchain network that natively cannot preserve the confidentiality of health-related data.

Huang et al. (2019) proposed MedBloc, a blockchain network that consists of multiple nodes which actors are the patients, the healthcare providers, the network administrator, the certificate authority, the authentication service provider, and the client. Since all data on the

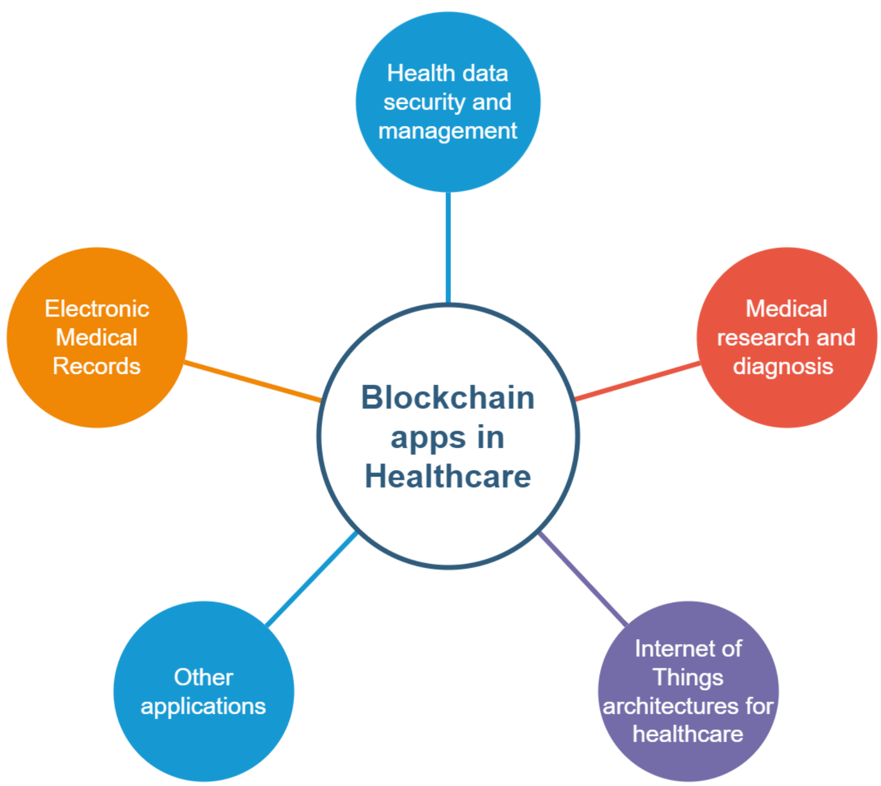

Figure 6: Categorization of the selected papers.

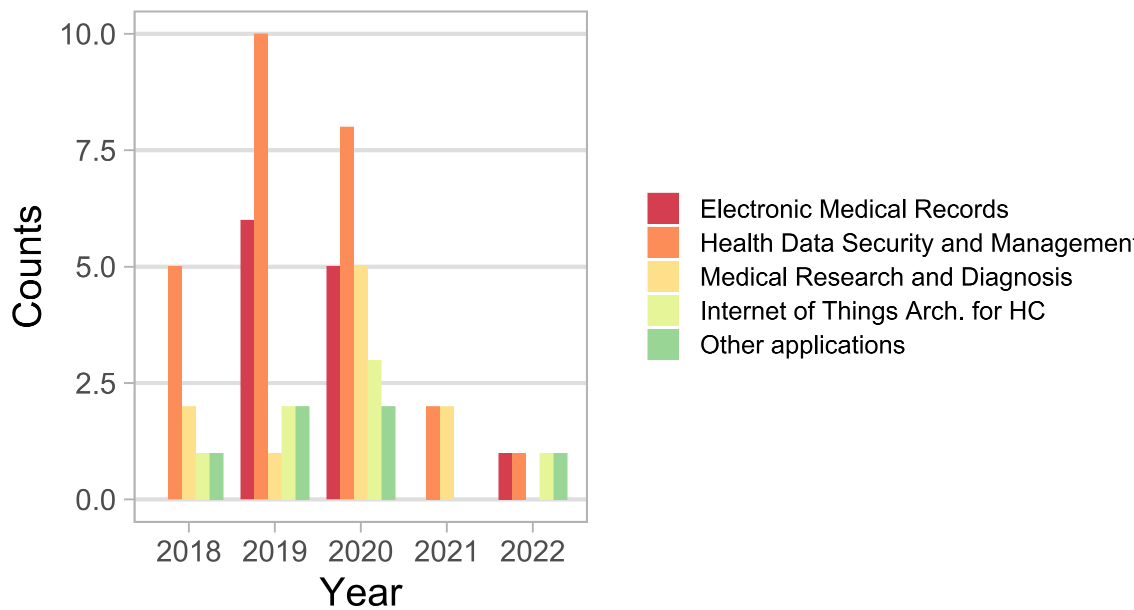

Figure 7: Number of papers appearing each year per category.

blockchain is transparent, the authors proposed to use non-traditional blockchain entities, such as authentication servers and certificate authorities, to provide means for issuing digital identities and protecting the keys used to encrypt all the data on the blockchain. Finally, smart contracts are used to enforce access control rules and protect patients' privacy.

In general, sharing medical records between patients and healthcare facilities, and integrating all EHRs of a group of clinical centers can be achieved using cloud technology. In this context, Rahman et al. (2019) tried to show if it is possible to integrate the blockchain with a traditional cloud-based EHR management system to take advantage of its security and immutability features, and how to choose a specific blockchain network so that the control over the data is fully decentralized. In their paper, they propose a system architecture based on the Ethereum public blockchain. The originality of this study lies in the introduction of the blockchain *handshakers*: every time a transaction is sent to the public blockchain network, it is anonymously validated by them against smart contracts.

Daraghmi et al. (2019) designed the system *MedChain* to improve existing systems by providing interoperable, secure and efficient access to medical records. To reduce the data sent to the blockchain, they are stored in centralized databases while the Ethereum blockchain is used to store all accesses to EMRs, so that the events that happened on EMRs are tracked. The authors propose a new incentive mechanism that is not based on a monetary value, but is welfare-oriented and integrated with the Proof-of-Authority (PoA) consensus algorithm. Specifically, the nodes of the network are associated with a grade indicating the quantity and quality of their medical records in terms of readability, completeness, consistency, correctness and non-redundancy. This grade is assessed by a special tool called *Records Evaluation Manager*. Healthcare providers' nodes with low grades are more likely to be selected to create new blocks, while nodes with higher grades than the average are *voting* nodes, that are responsible for the validation process. The proposed scheme rewards the block creator with an incentive that reduces its probability of creating the next block, thus achieving fairness among providers. Data integrity is ensured by using the SHA-256 hash algorithm, while security is ensured by adopting the distributed ElGamal re-encryption schema (Zhou et al., 2005).

In order to prevent a medication incident in advance, comprehensive management of individual medication history is essential. Kim et al. (2019) has developed a patient-centric medication history recording system using blockchain that captures the QR code printed on the envelope directly based on the prescription. All information is stored in blockchain using the hash value of the data, preventing data tampering.

BiiMed (Jabbar. et al., 2020) is a Blockchain framework, implemented using a private Ethereum blockchain, to improve interoperability and data integrity regarding EHR sharing that is part of a Health Information System (HIS). In the HIS, the data access management module exploits Smart Contracts to support medical facility authentication and authorization. A unique aspect of this work is the introduction of the Trusted Third-Party Auditor (TTPA) based on Blockchain technologies, which validates and stores the shared medical data. Once a medical facility is added to BiiMED, it can add patient records, that are hashed and submitted to the Blockchain framework. The smart contract associated with the TTPA allows records to be added, updated, and removed. The access management system verifies the medical provider's access request and sends a key that enables the communication with the HIS medical provider, i.e., the access to read/write operations on the patient's medical record.

An alternative solution to share EMRs across different systems is proposed by Cao et al. (2020b) in the system HB-EMRS, which adopts a hybrid scheme that combines permissioned and permissionless blockchains for EMR management. Specifically, sensitive parts of EMRs are recorded on the permissioned blockchain, accessible only by the members of the consortium, while non-sensitive data of EMRs are stored on the permissionless blockchain. The participants of the consortium are connected through a set of predefined rules and smart contracts. HB-EMRS also integrates on-chain and off-chain storage to enable the management of large amounts of data. The data is encrypted and stored in a distributed storage system, namely the Inter-Planetary File System (IPFS). The framework also provides backup functionalities: if the EMR data on the consortium blockchain is maliciously tampered with, the full data stored on the IPFS can be used for secure recovery and tracing, ensuring the security of the HB-EMRS solution. The proposed system has been implemented using Hyperledger Fabric and Ethereum, and the latency and throughput tests under different configurations have shown good performances.

It is noteworthy that blockchain-based systems generally lack scalability and require large storage space. Abdul Rahoof & Deepthi (2020) try to solve this problem in the HealthChain system, which provides a health record management system with scalability and small storage space. The system is organized using the so-called *regions*, i.e., subsets of users. HealthChain adopts two types of blockchain networks: a private blockchain for intra-regional communication, and a *consortium* blockchain for inter-regional communication. This system significantly reduces the storage on the ledger since transactions are only stored in the region they belong to. HealthChain is implemented using Ethereum and uses smart contracts to manage information exchanges among all the components.

Fu et al. (2020) developed a novel nesting algorithm for a healthcare-oriented blockchain, to preserve the privacy of the EMR data. It consists in partitioning the l bits of the original EMR into t groups, each having l/t bits. A message sharing scheme splits such t parts into n shares, where $1 \leq t \leq n$. Such shares are then transferred to different nodes in the blockchain, which differs from traditional blockchains since data is not shared by all nodes. Specifically, all nodes can add blocks, that also store hashes that identify the pieces of the EMRs. In the recovery process, authorized data users can collect a set of EMR shares and then reconstruct the EMR, even if a few shares are tampered with or discarded. The security analysis and the simulation results have shown that this architecture makes the EMR storage and sharing processes secure and efficient.

Tith et al. (2020) proposed a decentralized system implemented using Hyperledger Fabric to solve the problem of sharing medical data between EHRs without relying on a centralized system. The key features of the system are a trusted repository of patient data in EHRs that ensures access as well as integrity of the data itself, and enhanced security in handling patient data by using a special encryption scheme in which the data is encrypted with an appropriate symmetric key. Then, the symmetric key is asymmetrically encrypted with the patient's public key and linked to the encrypted data. This hybrid encryption makes the process efficient in terms of both speed and convenience, as encryption of large data can be done faster with the symmetric key than with the asymmetric key, while the latter is more convenient when encrypting smaller data.

Huang et al. (2021) proposed the BCES system, a blockchain-based eHealth system able to ensure that the manipulation of EHRs can be verified. In BCES, every data manipulation is logged on the blockchain as a transaction for permanent storage. Specifically, the authors proposed the adoption of a so-called Proof-Chain to store data manipulation logs, and an attribute-based proxy encryption to achieve fine-grained access control of medical data.

Finally, it is worth mentioning the work by Akhter Md Hasib et al. (2022), who aimed at improving the intelligence and the security of electronic health management. The authors proposed an architecture that provides data immutability and complete transparency of the transactions through the Ethereum blockchain. The main users are the patients, the doctors, and the hospitals. Patients share personal data through a portal, which front-end is implemented using ReactJS, HTML and CSS, while the back-end is represented by smart contracts implemented using the Solidity language. The hospital administration can control the process but cannot access the detailed data. Doctors can access a patient's medical records by submitting a request to the patient. At the end of the consultation, the doctor can update the patient's data and, after a verification step performed by the hospital, the blockchain network is updated.

Table 1 summarizes the main characteristics of the papers described in this section.

Ref.	SC	Blockchain	Major strenghts	Cit.
Toshniwal et al. (2019)	Yes	Ethereum	This work develops PACEX, an application that allows patients to share and have complete control over their data using the Blockchain	5
Koushik et al. (2019)	Yes	H. Composer	The authors propose a patient-centered medical record management system	6
Huang et al. (2019)	Yes	H. Fabric	It proposes a key storage framework that aims to improve usability by leveraging an authentication server for storing the cryptographic material	17
Rahman et al. (2019)	Yes	Ethereum	The authors introduce the use of blockchain handshakers that enable the validation of the submitted transactions	13
Daraghmi et al. (2019)	Yes	Ethereum	It proposes a new incentive mechanism that leverages the degree of health providers regarding their efforts on maintaining medical records and creating new blocks	47
Kim et al. (2019)	-	IPFS	It describes a medication history record system that captures the QR code printed on the envelope directly based on the prescription	4
Jabbar. et al. (2020)	Yes	Ethereum	The originality is the introduction of the Trusted Third-Party Auditor that validates and stores shared data	2
Cao et al. (2020b)	Yes	H. Fabric, Ethereum	It adopts a hybrid scheme that combines permissioned and permissionless blockchains	10
Abdul Rahoof & Deepthi (2020)	Yes	Ethereum	The authors propose a system to solve the scalability problem of blockchain-based systems	2
Fu et al. (2020)	-	-	It proposes a lightweight privacy-preserving cross-institution EMR sharing scheme based on the blockchain technique and a lightweight (t,n)-threshold message sharing scheme	19
Tith et al. (2020)	Yes	H. Fabric	The authors adopt the AES algorithm for symmetric-key encryption of patient data and the Elliptic Curve ElGamal algorithm for asymmetric-key encryption of the symmetric key in the proxy reencryption scheme	15
Huang et al. (2021)	Yes	Proof-Chain	The BCES system adopts the so-called Proof-Chain to store users' manipulations of medical data	16
Akhter Md Hasib et al. (2022)	Yes	Ethereum	The proposed system improves the transparency and the security of electronic health records management, involving patients, doctors and hospitals.	4

Table 1: Summary of the characteristics of the works falling under the category *Electronic Medical Records*. The column *SC* indicates the adoption of Smart Contracts ("-" means that it is not specified). The column *Cit.* refers to the number of citations in Scopus on 19/07/2022.

5.2. Health data security and management

Health information mostly consists of sensitive data, which protection is fundamental. Research activities focused on finding solutions to ensure reliability and privacy, despite the need of sharing information over the network using blockchain and its inherent features.

The system proposed by Zhang & Lin (2018) exploits a combination of two permissioned blockchains. Medical providers' private blockchain stores patients' original medical information (encrypted for security reasons), while the consortium's blockchain only contains index entries to such data. The authors also proposed a secure and privacy-preserving personal health information sharing protocol (BSPP) based on the proposed architecture. Although patient identities are encrypted, authorized doctors can still search for relevant patient indexes using pseudo identities. Furthermore, the doctor can only access the patient's medical history, i.e. the past, while he may not access future data without re-obtaining the patient's consent.

Li et al. (2018) designed a novel blockchain-based data storage system (DPS). Applications mainly interact by submitting, manipulating, querying, and verifying data. Users can submit the data to be stored on the DPS, and can query it and verify its authenticity, based on the so-called concept of *proof of primitiveness*. This system is effective against tampering and deletion, can detect illegal/invalid transactions and report them to users, but needs improvements and optimizations in terms of image management and storage data structures.

Ramani et al. (2018) proposed a system based on 5 main phases to ensure confidentiality, integrity, and authentication. Specifically, the proposed phases are: *i) Registration*: the patient provides his/her data using a mobile device before a visit. *ii) Data appending/adding request*: a doctor requests the update of the patient's data with his/her consent. The doctor encrypts the data using a common key that can be derived from the patient, who ultimately verifies and signs the data. Finally, the doctor approves the patient's signature and transfer the data to the blockchain. *iii) Data appending/adding operation*: before actually storing the data, the blockchain checks the timestamp, looks for the patient's public key and checks the validity of the signature against the declared involved patient and doctor. *iv) Data retrieval request*: the doctor submits a retrieval request to the blockchain at a given time point by attaching the identity of the patient and the identity of the doctor. *v) Data retrieval operation:* the blockchain, upon receiving a request, checks the freshness of the request through the value of T_p, the validity of the signature and whether the patient has given the doctor permission to access the data. Then, it returns patient's data corresponding to that time period.

Peña et al. (2019) focused on protecting patient data in mobile health systems by developing a model for secure data collection, sharing, and integration. The model, which allows patients to access to their data, manages three phases: *i)* data collection through apps or wearable devices, *ii)* data processing on the blockchain and cloud-based systems to ensure privacy and security, and *iii)* a monitoring system to track the system performance. The proposed architecture exploits Hyperledger Composer and, according to the performed tests, ensures authentication, confidentiality, integrity, and availability of data.

Ghaffaripour & Miri (2019) described a framework that improves access control mechanisms in privacy-sensitive medical data management systems. The authors envisioned two levels of privacy preservation in their system. The first is the adoption of a variant of attribute-based encryption, namely Key-Policy Hierarchical Attribute-Based Encryption

(KP-HABE) (Deng et al., 2017) to encrypt user data outside the blockchain. The second level is the benefits brought by the use of blockchain, with Hyperledger Fabric as a reference model.

Recently, there have been several ransomware attacks through which attackers installed malwares on servers of medical organizations, making data inaccessible. To alleviate this problem, Reen et al. (2019) proposed a model that provides absolute privacy and security using cryptography, blockchain and IPFS. The main advantage of using the blockchain in this scenario is the fully decentralized and immutable system of storage, where access controls make possible misuse of data easily identifiable. IPFS ensures immutability of patient records, while the blockchain ensures immutability of recorded transactions. Biometric-based encryption ensures that even in a scenario where patients are in a critical condition and cannot provide access to their records, the latter can be accessed using their fingerprints. However, there are a number of drawbacks that still need to be addressed, such as the limited scalability of the blockchain, and the inability to delete all copies in an IPFS-based network.

Nguyen et al. (2019) analyzed the performance of a different model for sharing patients' data using the blockchain and IPFS. The system is based on a smart contract running on Ethereum, through which authentication and user identification mechanisms are implemented to ensure system integrity. The authors also provided a security analysis and a comprehensive evaluation in terms of several performance metrics to highlight the advantage of the proposed framework over existing solutions.

Andola et al. (2019) proposed the SHEMB system, in which the patient is the sole authority who has complete control over his/her data. Doctors and departments have a common distributed ledger based on Ethereum to share patients' data. However, doctors and patients are not required to store a full copy of the ledger. On the contrary, they coordinates with other departments of the hospital to have access to the full set of patients' data. Moreover, to increase the efficiency of the patient search, symmetric searchable encryption was integrated into the record retrieval component.

In another work (Figueroa et al., 2019), the authors proposed to combine the blockchain technology with RFIDs to support tracking, identification, and communication. However, in order to preserve also privacy and security aspects, the authors rely on an attribute-based access control systems (ABAC). Specifically, Figueroa et al. (2019) implemented a decentralized blockchain-based ABAC model on Ethereum, and considered a specific supply chain for healthcare, where surgical instruments with RFID tags can only access specific areas. A physical node consists of an RFID Reader Control (RFID-RC), a DApp and a Smart Contract. When an RFID-tagged instrument attempts to enter a room, the RFID-RC sends an access request to the DApp, which forwards it to the blockchain, calling the smart contract passing some attributes related with the asset, such as the product type and the serial number. Then, the DApp exploits these attributes to check against the ABAC security policies, that determine whether the access is authorized or not.

A particular scenario can be found in a traditional emergency access system, when the patient cannot give consent to emergency personnel to access their personal health information. Rajput et al. (2019) proposed an emergency access control management system (EACMS) based on a permissioned blockchain built through hyperledger fabric. In EACMS, the patient defines a-priori the access control policy for *non-emergency* doctor and the *emergency* doctor. Experimental results confirmed that this structure ensures the security of sensitive

PHR patient data, and a time-efficient access that also provides privacy, accessibility and granular access control.

Zhou et al. (2019) proposed the system Med-PPPHIS, that exploits a combination of a permissionless blockchain and a permissioned blockchain. The permissioned blockchain is called Med-DLattice and its nodes store and protect data, together with data fingerprint on the chain, and periodically anchor snapshots of the data to the public blockchain. Each consensus node in Med-DLattice is a National Physique Monitoring Station (NPMS), that stores a shared ledger for token assets and medical data of each user. The nodes of Med-DLattice are able to reach consensus efficiently using the proposed DPoS-Quorum algorithm. In the consensus process, NPMSs could use Verifiable Random Functions to check whether they have valid consensus identities to participate in the consensus committee and decide the proposal according to the sum of voting rights they own and represent. If their identities are valid, the consensus vote will be taken. When the number of votes collected by NPMS exceeds the *legal* threshold, consensus is reached and the consensus process ends.

Chenthara et al. (2020) proposed the system HealthChain, a framework that consists of a Distributed Application (dApp), built using Angular, that interacts with the Hyperledger Composer Rest server to show the state of the data stored on a CouchDB database. This application supports four types of users, namely doctors, patients, pharmacists and receptionists. The *Fabric-CA* component provides public key certificates for all the applicants. The *Membership Service Provider* component abstracts all cryptographic mechanisms such as identity validation, signature generation and verification, certificate issuance, and authentication of healthchain users. The user can submit queries through the Fabric SDK, that checks the global state of the permissioned blockchain, built with Hyperledger Fabric, and forward the query to the blockchain. HealthChain also requests the consent to other peers before actually submitting the transaction to the blockchain. Smart contracts are executed during every user interaction to identify the request, validate it, secure the interaction with the doctors, and grant access permissions. The implementation have shown that the proposed architecture also provides a tamper-proof mechanism, thanks to the storage of hash values for each transaction in the blockchain.

Arunkumar & Kousalya (2020) proposed a novel secure decentralized cloud-based medical blockchain (CMBC) to address privacy and security issues in sharing patient health data among different medical organizations. The CMBC architecture adopts a lightweight authentication encryption algorithm to upload encrypted health data to the decentralized cloud-based blockchain. The proposed architecture also adopts a separate key distribution center to generate and exchange the public keys along with the secret keys, used to encrypt and decrypt the data, over an unsecured channel.

Tanwar et al. (2020) proposed an access control system, implemented using Hyperledger Fabric, to improve data accessibility for healthcare providers. In the designed architecture there are 4 main actors: Patient, Clinician, Lab and System administrator. Different activities within the architecture are regulated by different Smart Contracts, that also manage the users' roles and the access to resources according to the permissions associated with the defined roles.

The specific topic of supporting access control has also been considered by other works. Lately, Kumar & Tripathi (2021) emphasized that the adoption of the blockchain for access control introduces scalability issues, due to the tracking of the entire history. To solve this problem, they propose an enhanced Bell-LaPadula model (Liu et al., 2016), according to which access control is based on Smart Contracts and on the categorization of peers with different levels of authorizations and security. It is not required that each peer maintains the complete transaction history, but only the portion satisfying the access control policies. The proposed model is implemented using Hyperledger Fabric, while smart contracts are implemented using Hyperledger Composer, in order to manage access control rules dynamically, overcoming the originally static nature of the Bell-LaPadula model.

The security measures adopted in the implementation of blockchains may not be enough with the advent of quantum computing, which is based on the concept of Q-bits, that provide an overlay state in addition to the values 0 and 1 such that a bit can take on both values simultaneously. This aspect exponentially increases the computational power, introducing additional risks on systems based on traditional encryption strategies. Bhavin et al. (2021) considered these potential issues, and implemented a blockchain for healthcare management via Hyperledger Fabric, managing data access via smart contracts and using quantum blind signature (Lin et al., 2014) for distributing keys. The experimental results in terms oftransaction throughput, resource consumption, and network traffic showed that the proposed scheme improves the performance of the blockchain.

Shah & Rajagopal (2022) proposed an extension of the DPS architecture (Li et al., 2018), called M-DPS. The proposed architecture is based on the Ethereum blockchain and a set of smart contracts. Moreover, contrary to the original DPS architecture, it also exploits the IPFS. The authors compared M-DPS with DPS, showing interesting benefits of the proposed architecture in terms of reduced transaction costs and storage space.

Tang et al. (2018) proposed the system MedImgShr, implemented in Ethereum, which main innovation is the a credit score scheme implemented through a smart contract. When patients or hospitals share medical images, their score changes, influencing their permission to operate.

Upadhyaya et al. (2018) proposed a blockchain-based secure healthcare system specifically for developing countries. Based on various literature reviews, the authors conducted a feasibility study (technical, economic, operational, programmatic) on an automated secure health system in an outreach clinic (ORC) in Chapagaun (Lalitpur) and in the Children Eye ENT and Rehabilitation Service (CHEERS), in Bhaktapur (Nepal). The authors designed the architecture for an optimal health system using the proposed blockchain model, and developed a pilot prototype. Its effectiveness was validated with the balanced scorecard, i.e., a tool usually adopted to evaluate the organization's success according to different aspects.

Ni et al. (2019) proposed Healchain, a consortium blockchain-based architecture consisting of three layers. Each node in Healchain is run by private servers belonging to trusted authorities such as hospitals. These servers are used to validate health records by verifying linked authorization information. Big data can be stored in an off-chain system like IPFS. The hash of data provided by IPFS along with authentication information is packaged into transaction records on Healchain. By using blockchain, the system has a number of advantages such as confidentiality, integrity and traceability. Moreover, a formula is proposed to determine the computational power by trying to maximize the individual economic benefit, i.e. the difference between rewards and costs.

While the idea of using blockchain technology in healthcare is not new, there are still barriers that need to be overcome in order for blockchains to be used on a large scale. One possible solution is the use of the so-called *sidechains*, which are secondary chains connected to the main blockchain. One of the advantages of using sidechains in healthcare is the ability to record transactions and mine blocks simultaneously, as there may be a large amount of patient transactions at the same time. The nature of blockchains requires multiple nodes in the network to reach consensus before a block is created, which in this context can lead to potential bottlenecks. Using secondary chains that are specific to a person/patient on the network can prevent the aforementioned bottlenecks on the main blockchain for the following reasons: *i)* fewer transactions are actually sent on the main chain; *ii)* transactions involving different patients are actually independent of each other, and can be safely added to the sidechain of the respective patient; *iii)* more transactions per seconds can generally be handled. Based on these considerations, Donawa et al. (2019) implemented the so-called Patient-Healthchain architecture, which is based on the use of sidechains.

Another example of a generic three-tier architecture for blockchain-based data management, private in this case, is proposed by Zhuang et al. (2020). The basic idea is to create a generalized architecture that provides functions for data coordination, permission granting, and data sharing. From the bottom to the top, the layers are: *i) transaction* layer, that consists of two smart contracts that specify a metadata model for medical records, and methods that govern data access rights, permission policies, and data encryption; *ii) interfacing* layer, that provides four methods for obtaining health data from different facilities, storing the encrypted data securely, sending metadata or data requests to the blockchain via smart contracts in the transaction layer, and sending the encrypted data to the recipient who obtained the necessary permissions from the data owner; *iii) application* layer, that consists of the healthcare applications that, based on the interfacing layer, securely collect data and analyze it. Using this architecture, the authors developed two example applications for health information exchange that demonstrate the feasibility of adopting blockchain for data management in healthcare.

Among the challenges that need to be addressed when adopting the blockchain, there are the integration, the migration and the synchronization with centralized healthcare systems. Biswas et al. (2020) proposed an architecture based on a unified blockchain network across the country. The central elements are *i)* the certificate authority, which is responsible for registering all the elements that interact in the network by generating certificates and signatures; *ii)* the peers; *iii)* the smart contracts, through which the access and privilege control of the different users is defined in order to maintain the medical records; *iv)* the authorizer, i.e. the main person responsible for creating the blocks, the ledger and the communication channel. The data structures involved are the blocks of the chain and the tables of relational databases, that are adopted to store large data outside the chain.

Thwin & Vasupongayya (2019) proposed a blockchain-based system for managing personal medical records. Considering both the potential benefits and the limitations of the blockchain technology, Thwin & Vasupongayya (2020) focused on analyzing the performance of such a system in a real-world scenario to ensure its usability in practice. The performance of the proposed architecture was evaluated at different request rates, including 1.9, 3.8, and 15.2 per second, which correspond to 165,000, 330,000, and 1,320,000 accesses per day, respectively. The results showed that the system can respond to 165,000 daily accesses within 4 minutes. However, when increasing the rate to 3.8 requests/s, the response time can reach 20 minutes, while 50% of these responses are provided within the 8 minutes. The results with an arrival rate of 15.2 requests/s shows that only 30% of the responses are provided within the 8-minute emergency requirement.

Seo & Cho (2020) proposed a system which involves building a private blockchain for sharing images and supports some rewards for providers. The proposed system is also able to extract the regions of interest of the input images, using some preprocessing algorithms.

Medical data usually include images such as photographs, X-rays, and ultrasound images, which by their nature represent large amounts of data. This aspect clashes with the characteristics of the blockchain, since each block has fixed limited size. Therefore, the challenge is to figure out how to manage image data on the blockchain taking advantage of the guarantees of reliability and immutability that it offers.

Jabarulla & Lee (2021) proposed a new proof of concept for a distributed patient-centric image management (PCIM) system that enforces security without using a centralized structure, exploiting Ethereum and IPFS, as well as an access control protocol based on smart contracts. Each block containing PCIM data is approved and registered by a patient, while transaction validation is performed by the selected consortium and approved by the healthcare ecosystem. Authorized participants follow a protocol based on a smart contract to manage image requests. The network consists of protocol called *Patient-Centric Access Control protocol using a Smart Contract* (PCAC-SC) and a blockchain ledger to manage access control. Medical images are encrypted with the patient's public key and stored in the IPFS network. When an authorized user wants to access the image, he/she simply downloads it from IPFS. The patient, who owns the data, can provide his/her images to other requesters, by signing them with the requester's public key obtained from the blockchain, and uploading them to IPFS and signing the transaction using the requester's public key, his own private key, and the hash provided by IPFS.

Zaabar et al. (2021) proposed HealthBlock, a blockchain-based system for decentralized healthcare management. The HealthBlock architecture exploits the concept of decentralized storage and a permissioned blockchain network as an access control mechanism to monitor patient vital signs information. The authors also proposed the adoption of an OrbitDB database, which is based on IPFS. The HealthBlock users are patients, doctors, pharmacists and laboratory technicians, as well as the administrator of the blockchain network.

According to the GDPR, data must be removed after the agreed period, or whenever a user requests it. As mentioned in Section 3, this privacy regulation is generally incompatible with the blockchain technology, since (also personal) data cannot be deleted from the network once recorded. Kakarlapudi & Mahmoud (2021) presented a private data management system based on blockchain and cloud. The proposed system collects users' consent and stores it on the blockchain network. The system allows users to store their data on a private cloud database, and to approve or revoke data requests. All such operations are recorded on the network through transactions. Moreover, users can keep track of the organizations accessing their data, making the proposed system completely transparent and traceable.

The outlined characteristics of the considered papers are summarized in Table 2.

Ref.	SC	Blockchain	Major strenghts	Cit.
Zhang & Lin (2018)	-	JUICE	The proposed system leverages a combination of two authorized blockchains plus a secure and privacy-preserving personal health information sharing protocol (BSPP)	230
Li et al. (2018)	Yes	Ethereum	It uses the concept of proof of primitiveness to verify the authenticity of the data	138
Ramani et al. (2018)	Yes	Ethereum	The authors focus on building a secure and efficient data accessibility mechanism using the blockchain technology	57
Peña et al. (2019)	Yes	H. Fabric	It proposes a security model to protect patient data on mobile health systems	1
Ghaffaripour & Miri (2019)	Yes	H. Fabric	The authors envisioned two levels of privacy preservation: the adoption of Key-Policy Hierarchical Attribute-Based Encryption(KP-HABE) and the use of blockchain	2
Reen et al. (2019)	Yes	Ethereum	The paper introduces the use of biometric encryption via fingerprints	7
Nguyen et al. (2019)	Yes	Ethereum	The paper proposes a EHRs sharing scheme enabled by mobile cloud computing and blockchain	161
Andola et al. (2019)	Yes	Ethereum	The system uses symmetric searchable encryption technique to speedup the access to the records	2
Figueroa et al. (2019)	Yes	Ethereum	The system is designed for a supply chain environment with a use case suitable for healthcare systems, so that assets such as surgical instruments containing an associated RFID tag can only access specific areas	17
Rajput et al. (2019)	Yes	H. Fabric	The case study considered is a specific healthcare supply chain, where surgical instruments with RFID tags can only access specific areas	59
Zhou et al. (2019)	Yes	Med-DLattice, Dlattice	The authors propose the Med-PPPHIS system, which consists of a permissioonless blockchain called DLattice and a permissioned blockchain called Med-DLattice	28
Chenthara et al. (2020)	Yes	H. Fabric	The blockchain is used to manage emergency access system	2
Arunkumar & Kousalya (2020)	Yes	Ethereum	The system adopts a lightweight authentication encryption algorithm to upload encrypted health data to the decentralized cloud-based blockchain	6
Tanwar et al. (2020)	Yes	H. Fabric	It proposes an algorithm for access control policy for participants to achieve privacy and security	264
Kumar & Tripathi (2021)	Yes	H. Fabric	The authors propose an enhanced Bell-LaPadula model to address the problem of scalability	9
Bhavin et al. (2021)	Yes	H. Fabric	The authors propose to use the Quantum blind signature to protect the traditional encryption system from quantum attacks	11
Shah & Rajagopal (2022)	Yes	Ethereum	The authors propose the M-DPS architecture, as an extension of the work by Li et al. (2018), to reduce transaction costs and storage space.	0

Tang et al. (2018)	Yes	Ethereum	The innovation is the credit scoring scheme implemented	12
Upadhyaya et al. (2018)	Yes	H. Fabric	Through the balanced scorecard, it has been shown that implementation of the proposed health system in a hospital results in 75% customer satisfaction and 63% financial gain	4
Ni et al. (2019)	Yes	-	The proposed system HealChain allows a decentralized and secure data management x	11
Donawa et al. (2019)	Yes	-	It introduces the use of sidechains	8
Zhuang et al. (2020)	Yes	Ethereum	The authors proposed a blockchain system that can be adapted to a wide range of healthcare applications for cross-site data coordination	4
Biswas et al. (2020)	Yes	H. Fabric	The authors propose a unified e-health system based on blockchain	16
Thwin & Vasupongayya (2020)	Yes	H. Fabric	The authors focused on demonstrating the usability of the proposed system in practice	4
Seo & Cho (2020)	Yes	H. Fabric	It covers image sharing and supports some rewards for providers	6
Jabarulla & Lee (2021)	Yes	Ethereum	It proposed a new proof of concept for a distributed patient-centric image management system	13
Zaabar et al. (2021)	Yes	H. Fabric	The authors proposed the system HealthBlock for decentralized health data management	14
Kakarlapudi & Mahmoud (2021)	Yes	H. Fabric	The authors alleviated the GDPR-related issues by storing health data off-chain in a cloud database, and users' consent information on the blockchain	1

Table 2: Summary of the characteristics of the works falling under the category *Health data security and management*. The column *SC* indicates the adoption of Smart Contracts ("-" means that it is not specified). The column *Cit.* refers to the number of citations in Scopus on 19/07/2022.

5.3. Medical research and diagnosis

In this subsection, we discuss existing works dealing with the adoption of the Blockchain to *i)* support research activities, *ii)* facilitate the sharing of medical data to provide doctors with information for diagnoses and research, and *iii)* support emergency situations.

Wang et al. (2018) proposed a parallel health systems (PHS) framework to tackle the problem of sharing cross-border medical knowledge, since doctors usually turn out to be experts in only one field. The PHS framework consists of the physical healthcare system, which includes real doctors and patients, and the artificial system, which includes virtual doctors and patients. Computer-aided diagnosis experiments are conducted according to the principle of evidence-based medicine, which combines clinical knowledge, personal experience, and real patient conditions. Artificial doctors are trained with some diagnostic standards extracted from medical publications, empirical diagnoses from major historical cases, and evidence-based medicine. For diagnosis, the artificial doctor relies on the actual symptoms, medical examination results, medical history, and family medical history. A parallel execution takes place between real doctors and artificial doctors. On the one hand, when the artificial doctors conduct the experiments on computer-aided diagnosis and make the diagnosis of the disease, the real doctor confirms the result to make the final diagnosis. On the other hand, when the artificial doctor selects the best treatment scheme, the real doctor will give his opinion on the result and provide the possible treatment scheme to the real patient. The blockchain is specifically exploited to store all the health data securely.

Medical research activities are strongly dependent on the available data, while patients are usually interested in protecting their privacy. To incentivize data sharing, contribution mechanisms and blockchain can be used. Park et al. (2018) followed this idea, by implementing the CORUS system, which uses crowdsourcing and blockchain to collect data, a cryptocurrency-based system to create research topics and stimulate continuous participation, and cloud computing to evaluate health tools in citizen science fashion. On the same line of research, Lobo et al. (2020) proposed Exonum, an open-source blockchain-based system that facilitate patients' access to their data and encourage them to share it in exchange for some coins of a cryptocurrency, namely *LifeCoins*, to contribute to the research.

Fernández-Caramés et al. (2019) specifically focused on studies about the diabetes. Diabetic patients can nowadays rely on a device called Continuous Glucose Monitor (CGM) that can continuously measure blood glucose levels. In order to share reliable data, the system proposed by Fernández-Caramés et al. (2019) involves the adoption of a decentralized storage system that receives, processes and stores the collected data. To motivate users to add new data, an incentive system based on a digital cryptocurrency called *GlucoCoin* was also developed. Data storage is implemented using the decentralized database OrbitDB running IPFS, while Ethereum was chosen to be able to execute smart contracts.

Khezr et al. (2020) proposed a solution to detect and track the daily activities of over 65s, based on the energy consumption of home devices. To ensure that people's data is protected and accessible to authorized personnel within the healthcare ecosystem, blockchain technology is used as a mean to maintain and share daily activity patterns, discovered through a Bayesian model, with healthcare providers. These activity patterns are stored on the user profile and added to the Hyperledger blockchain. This allows healthcare providers to assess the daily activities of elderly people and make appropriate health assessments.

In the medical research and diagnosis field, the blockchain can be adopted to ensure the immutability of the collected data and the correctness of obtained results. Moreover, the wide adoption of wearable devices that collect real-time health information, such as heartbeat or blood saturation, opens up an infinite number of possibilities for potential applications.

In this context, Neto et al. (2020) implemented a proof of concept to analyze the use of blockchain technology in E-Health applications and, in particular, in genomic applications, like the manipulation of DNA sequence data. Their idea is to use the classical three-tier architecture for IoT devices. In this architecture, the first layer is the *data collection* layer, that is responsible for discovering information sent to the *data storage* layer, i.e. a blockchain-based database called BigchainDB, where only a few nodes are responsible for storing the sequences of transactions. Smart contracts are adopted to enforce access control policies and to ensure the privacy and security of the transmitted information. The final layer is the *application layer*, which access the data stored in the blockchain, using a digital signature which ensures the authentication, and on a relational database to provide services to users (i.e., doctors and patients). Specific applications can range from genomic analysis to real-time monitoring of patients' physiological data. The architecture also relies on a timeout, within which the validation of a block must be completed. Otherwise, if the timeout expires, an empty block is generated. The performed experiments emphasized how a sub-optimal parameter initialization of BigchainDB or a high latency introduced by the network may lead to an excessive production of empty blocks. However, increasing the number of nodes alleviates this issue, even if the validation time can increase up to reach few seconds, that can still be considered reasonable for the adoption of the blockchain in this context.

Peral et al. (2020) proposed a blockchain-based architecture that allows patients to share their health data and organizations to access that data for a fee. The developed architecture uses two web applications: one to create the data for the blockchain, where each node corresponds to different users that participate in sharing the data, and the other to visualize the network created between the different users from an analytical point of view through dashboards. The authors considered the following use case: patients store their data in the blockchain via the system front-end. When a potential buyer decides to access some data, the system checks if he/she has permission to access it. If permission has not yet been granted, the system informs the patient about the buyer's request and the incentive offered. If the patient gives permission, the system stores it in the blockchain and notifies the buyer, who can view the data. The system stores the data access and deducts the payment from the buyer and credits it to the patient.

Gan et al. (2020) suggested storing the data on a Ethereum blockchain network to reduce or eliminate improper or unauthorized use of the information, that is under the total control of the patients. Patients are encouraged to use authentication and encryption protocols to ensure privacy through an incentive mechanism. In addition, the proposed system requires that big data is not stored in the blockchain but in the cloud, being encrypted if sensitive.

Diagnosis does not necessarily have to focus on current conditions, but can also involve the prediction of future diseases, based on indicators and patient characteristics. This concept led to the development of BinDaaS (Bhattacharya et al., 2021), a framework that integrates blockchain and deep learning, to securely protect patient data and make predictions about future diseases. BinDaaS exploits a lattice-based key and a signature verification scheme to resist quantum attacks. Experimental results proved the superiority of the proposed scheme, but also exhibited high communication costs, which can be considered a critical issue.

Along the same line of research, Shynu et al. (2021) proposed a secure and efficient blockchain-based health service for predicting diseases, such as diabetes and cardiovascular diseases in fog computing (Bonomi et al., 2012). The main components of the system are: the sensor devices that track human health parameters; the fog nodes, which can be computers or network devices; the blockchain used to monitor health data; the cloud, used for storage purposes; and the medical analyzer, who is the person authorized to access patients' health information to classify them as healthy or diseased. The authors adopted a rule-based clustering algorithm to group patients, and an adaptive neuro-fuzzy inference system based on feature selection (FS-ANFIS) to automatically classify patients.

Table 3 provides a summary of the characteristics of the papers discussed in this section.

5.4. Internet of Things architectures for healthcare

Monitoring wearables and IoT devices are making patients' lives increasingly convenient, as they can collect, report, and analyze monitoring data, and transmit it to doctors in real time. Moreover, they can also be used to send instant notifications to people via mobile apps or other connected devices. In this context, Attia et al. (2019) designed and implemented a blockchain-based IoT architecture using Hyperledger Fabric to create a secure remote IoT monitoring system. In the proposed architecture, each peer can be part of one or more

Ref.	SC	Blockchain	Major strenghts	Cit.
Wang et al. (2018)	Yes	-	The authors propose an approach consisting of artificial systems-based parallel health care systems + computational experiments + parallel execution to improve the accuracy of diagnosis	120
Park et al. (2018)	Yes	H. fabric	It uses a cryptocurrency-based system to create research topics and stimulate continued participation	10
Fernández-Caramés et al. (2019)	Yes	Ethereum	The authors focus on building an application for the case study related diabetes treatment	53
Khezr et al. (2020)	Yes	H. Fabric	It proposes a solution to track the daily activities of the over-65s in a smart home	5
Neto et al. (2020)	Yes	BigchainDB	This paper proposes an architecture with Blockchain for genomic applications	1
Lobo et al. (2020)	Yes	Exonum	The authors devised a system that encourages patients to share their data in exchange for cryptocurrency	3
Peral et al. (2020)	Yes	H. Fabric	It proposed an architecture that organizations to access patients' health data for a fee	4
Gan et al. (2020)	Yes	Ethereum	The system allows the management of patient data on the blockchain via an incentive-based approach	5
Bhattacharya et al. (2021)	Yes	BinDaaS	It combines blockchain and deep learning	45
Shynu et al. (2021)	Yes	-	It proposes an efficient blockchain-based secure health services for disease prediction	11

Table 3: Summary of the characteristics of the works falling under the category *Medical research and diagnosis*. The column *SC* indicates the adoption of Smart Contracts ("-" means that it is not specified). The column *Cit.* refers to the number of citations in Scopus on 19/07/2022.

channels. A proposal for a transaction, containing data received from the medical devices, is sent to the peers, that approve the proposal by executing the corresponding smart contract code to access the ledger. Then, based on the endorsement policy, certain peers decide whether a transaction is valid or not. If it is valid, the proposal is signed and and a response is sent to the application SDK. Once the application SDK gets enough approvals for the same transaction according to the Practical Byzantine Fault Tolerance algorithm, the transaction is sent to the service which takes the validated transactions from the application SDK, creates blocks and sends them to the commit peers, that update the ledger.

Griggs et al. (2018) proposed the adoption of a consortium-authorized and managed blockchain to execute smart contracts that would evaluate information collected from a patient's IoT healthcare devices based on thresholds defined by experts. The smart contracts trigger alerts for the patient and healthcare providers when necessary, and store the transaction details on the blockchain. The authors also published some demo smart contracts on a github repository (`https://github.com/ckohlios/Healthcare_IoT_Blockchain`).

To specifically address security issues in health information systems, Buzachis et al. (2019) proposed a Blockchain-as-a-Service-based solution for Electronic health Information Exchange (BaaS-HIE). This system is based on a private, consortium-driven blockchain, which means that only authorized users can read blocks and only specific nodes can execute smart contracts and verify new blocks. A typical application scenario is that of a patient being monitored remotely by a doctor, equipped with various Internet of Medical Things (IoMT) devices, including a blood pressure monitor and a pulse oximeter. Each IoMT device must be authenticated with the patient (typically through a smartphone or a tablet) and then through its Identity-Based Signature (IBS) (Hess, 2002).

Therefore, the patient acts as an authority certifying that the node possesses the private key corresponding to its public key. The patient can also decide to share his/her health data with other doctors from different health centers, or deny further access to the doctor(s) once the treatment has been completed. The logic and state transition events are recorded as immutable data in the blockchain.

Another system proposed in this context by Zghaibeh et al. (2020) is Smart-Health (SHealth), a framework for a complete blockchain-based healthcare system, compatible with Hyperledger Fabric, consisting of four tiers. The first is the government layer, which is the highest authority in this system, having the main role of regulating the access to the blockchain. In the second layer we find the users who communicate with the system through *SHealth Wallet*, an application made available to them from trusted SHealth entities, such as providers and partners. The third layer is the IoT terminal layer, followed by the blockchain itself. According to the authors, SHealth is simple, robust, efficient, secure and able to cover all possible scenarios in healthcare systems, some of which are mentioned in the paper such as requesting further tests from a doctor or medication prescribing.

Abou-Nassar et al. (2020) proposed a decentralized and interoperable trust model that exploits the blockchain in healthcare IoT. The architecture consists of a first layer dedicated to information collection and processing, which includes sensors and actuators required for various functions such as retrieving location, temperature, blood pressure, weight, motion, vibration, humidity, etc. The second layer includes gateways and network paths required for the transmission of IoT data. The third layer is a middleware that consists of sub-layers (blockchain decision units, data analytics, and application support) lying between the technology layer and the application layer. According to the authors, the proposed model outperforms other similar approaches in terms of scalability, interoperability, availability, confidentiality and privacy. Moreover, as a future development, they propose to improve the system by using artificial intelligence and deep learning technologies, which will be used in the training phases to identify patterns indicative of specific symptoms from information acquired from wearable sensors.

Rahman et al. (2020) proposed a system with two types of human actors: the IoT provider and the homeowner who wants to safely combine a set of IoT devices. Before using the system, a blockchain profile and a digital wallet must be created for each actor. Multimedia IoT data such as images, audio, and video that cannot be stored on the blockchain due to limited block size are stored in a decentralized repository on IPFS, while a hash is store on the blockchain. After each IoT data transaction, the account balance is updated, notifications are generated, and the status of IoT devices is updated on the blockchain.

Azbeg et al. (2022) designed a healthcare system called BlockMedCare for the management of chronic diseases, and specifically diabetes. The system can collect and share patient data with medical teams. Each patient has a set of IoT medical and electronic wearable devices with embedded sensors. The patient's smartphone is used as intermediate device between the IoT devices and the medical team. Doctors, hospitals, pharmaceutical laboratories and organizations are connected with patients through a blockchain network to access

Ref.	SC	Blockchain	Major strenghts	Cit.
Attia et al. (2019)	Yes	H. Fabric	It proposes an architecture for remote patient monitoring via IoT devices	29
Griggs et al. (2018)	Yes	Ethereum	The system uses smart contracts to assess patient health status by analyzing data collected from IoT health devices and comparing it to personalized threshold values. Available code.	359
Buzachis et al. (2019)	Yes	Ethereum	A platform suitable for overcoming security challenges via blockchain suitable for an EMRs-IoMT scenario has been realized	10
Zghaibeh et al. (2020)	Yes	H. Fabric	SHealth is a private multi-layered blockchain where each layer defines the privileges and permissions of entities in the system	13
Abou-Nassar et al. (2020)	Yes	Ripple	The authors propose a privacy-aware management framework and try to improve IoHT access control methods	102
Rahman et al. (2020)	Yes	H. Fabric	It presents the design of a prototype for secure gesture-based interaction with medical IoT devices in order to remotely protect the health of the elderly or patients with special needs	5
Azbeg et al. (2022)	Yes	Ethereum	It presents BlockMedCare, a system built for chronic disease management through daily data collection and sharing. Data are collected via IoT devices, stored on IPFS, and verified through hashes on the blockchain.	0

Table 4: Summary of the characteristics of the works falling under the category *Internet of Things architectures for healthcare*. The column *SC* indicates the adoption of Smart Contracts ("-" means that it is not specified). The column *Cit.* refers to the number of citations in Scopus on 19/07/2022.

their health data, which are encrypted and stored on the IPFS. The hospitals store an entire copy of the blockchain and participate to the consensus process.

A summary of the features of the described papers is provided in Table 4.

5.5. Other applications

The healthcare system is an ecosystem in which not only medical data must be managed, but also a number of auxiliary data and activities that are necessary for the system to work properly.

Zhou et al. (2018) proposed MIStore, which adopts the blockchain to implement a health insurance billing system that can help insurance companies in obtaining the sum of the patient's medical costs. In general, the process proceeds as follows: *i)* the hospital sends an initialization transaction to the blockchain network so that it can send the patient's medical cost data to the blockchain network through *record-transactions*; *ii)* the insurance company can submit a *query-transaction* to the blockchain, to know the total amount of a patient's cost data; *iii)* servers generate and send responses through *respond-transactions*.

Saeedi et al. (2019) implemented the system ClaimChain to show the potential benefits of adopting the blockchain for billing purposes between healthcare providers and insurance companies. In classical scenarios, an intermediary is responsible for sending invoices to avoid fraudulent transactions. This process is generally inefficient and error prone, since requires manual operations. The proposed application, that aims to overcome these issues, consists of three main components: *Bill Generator*, *Bill Retrieval*, and the blockchain. Bill Generator is a web application for hospitals that allows authorized users to generate customer bills over the blockchain network. Bills over the blockchain can also be viewed by financial officials, that can approve them. On the other hand, Bill Retrieval is a web application that provides access to the billing information and generates reports to verify the budget submitted by healthcare providers. In this process, the blockchain replaces the middleman/agent, with the billing information being encrypted and hashed, and accessible only to the authorized insurance provider.

Another common function of the healthcare system is to transfer the care of a patient from one doctor to another, as needed. This process involves several steps that require provider-to-provider and provider-to-patient communication. In Taiwan, the National Health Insurance Administration (NHIA) has implemented a National Medical Referral (NMR) system that encourages doctors to refer their patients to different healthcare providers to avoid unnecessary hospital visits and financial burdens on the national health insurance system. However, this system lacks scalability and flexibility, and it cannot build trust relationships between patients, primary care doctors, and specialists. Therefore, Lo et al. (2019) developed a blockchain-based system to manage patient referrals. They also developed a decentralized, blockchain-enabled, framework-based personal health data app for patients to collect their data. The developed framework iWellChain has been deployed in an affiliated teaching hospital and four collaborating hospitals. Analysis of access logs revealed that patients were very interested in capturing health data, especially that from lab test reports.

Another context is that of medical procedures, that can be very complex nowadays. Here, the adoption of the blockchain to simplify them has been proposed by Khatoon (2020), who implements a framework with a decentralized application (DApp) supported by a private blockchain network with distributed file system (DFS). The author used Ethereum to implement the smart contracts that are used to create intelligent representations of medical records stored in the network and for various medical workflows, eliminating the need for a centralized control authority. To ensure high performance and efficiency, the data is stored in a local database, while the corresponding hashes are stored in the blocks. In this system, various processes such as issuing medical prescriptions, sharing lab tests, and automatic reimbursement of healthcare services have been implemented.

The Continuing Medical Education (CME) is necessary to ensure the ongoing education of medical staff. Certificates for these activities can sometimes be forged, and medical license renewal is also usually a very time-consuming manual process. By adopting the blockchain technology, the system may become inherently counterfeit-proof, and the management of medical licenses can be automated.

Rathod et al. (2020) proposed a workflow that includes registering users and events, receiving CMEs, and periodically verifying CMEs. When a doctor, organizer, or event needs to be registered, data must be submitted to the appropriate medical board, which stores all data in IPFS. Registering the account of a doctor or of an organizer consists in the invocation of a smart contract that maps the account address to an IPFS hash. If the entity is an event, the medical association assigns it a certain number of CME points after evaluating it. A smart contract is then invoked to verify the validity of the organizer, and to map the IPFS

Ref.	SC	Blockchain	Major strenghts	Cit.
Zhou et al. (2018)	Yes	Ethereum	The proposed system implements a health insurance billing system	91
Saeedi et al. (2019)	Yes	ClaimChain	The system allows you to manage the transition of a patient's care from one doctor to another	0
Lo et al. (2019)	Yes	Ethereum	The system allows you to manage the transition of a patient's care from one doctor to another	10
Khatoon (2020)	Yes	Ethereum	The system is capable of handling complex medical procedures such as surgery and clinical trials	100
Rathod et al. (2020)	Yes	Ethereum	The authors propose a robust system for managing doctors' education certificates	1
Zou et al. (2022)	Yes	H. Fabric	The authors combined distributed identity identifiers (DIDs) and the verifiable credential (VC) using Hyperledger Indy, to build a distributed digital credit system for healthcare.	0

Table 5: Summary of the characteristics of the works falling under the category *Other applications*. The column *SC* indicates the adoption of Smart Contracts ("-" means that it is not specified). The column *Cit.* refers to the number of citations in Scopus on 19/07/2022.

hash of the event with the assigned credits and with the organizer's address. The IPFS hash is provided as a QR code, which in turn is given to a doctor at the end of the event. The doctor's scanning of the QR code invokes a smart contract, which, after verifying data validity, creates and assigns a certificate with a unique ID to the doctor. When the renewal period of the doctor's license expires, a smart contract is invoked, which verifies the validity of the doctor's data, calculates the number of CME credits accumulated and, if this value is sufficient, renews the license; otherwise, it may initiate sanctions or suspension of the license.

Zou et al. (2022) designed a healthcare consumer financing system based on a distributed digital identity architecture, organized in four layers: the *infrastructure* layer, which is responsible for providing the necessary computing and storage resources to the higher layer; the *application support services* layer, which provides basic services such as identity authentication, data encryption and decryption, and the underlying blockchain; the *application* layer, which provides protocols to realize functions, such as verifiable credential management and information maintenance, and an interface to let users interact with the network; the *user* layer, which implements several server-side interfaces that invoke functions of the application layer. The authors innovatively combined distributed identity identifiers (DIDs) and the verifiable credential (VC) model (Consortium, 2019), using the Hyperledger Indy toolkit[5], to build a distributed digital identity credit system. The goal is to support healthcare consumers and healthcare institutions in the collection of credit information, thus simplifying the process of reviewing consumer information by financial institutions.

Table 5 summarizes the characteristics of the papers mentioned above.

[5] `https://www.hyperledger.org/use/hyperledger-indy`

6. Research Directions

As mentioned in Section 3, the adoption of the blockchain in healthcare can introduce additional challenges, some of which have not yet been fully addressed in the literature. Focusing on EMRs (see Section 5.1), the developed systems allow to store and selectively share patients' data, also taking care of their privacy. The main advantage over centralized systems appears to be the robustness to tampering operations, which may affect the possibility to trace the full history of the patients and deeply understand the cause of disease conditions. However, the reluctance to share personal data (from the patient viewpoint) and the full transparency of each update to patients' data (from the medical personnel viewpoint) may discourage the adoption of the developed systems, which may appear as a *strict inspector* ready to accuse of tampering anybody applies updates to data, rather than a tool to transparently and reliably track the full history of the patients. For this reason, more effort should be put on incentivization mechanisms, to promote data sharing and to let the medical personnel feel the technology as a supporting tool, rather than as a continuous inspector on the activities they conduct.

An analogous issue can be observed in the category of *Medical research and diagnosis* (see Section 5.3). In this case, indeed, the effectiveness of statistical analyses and the accuracy of descriptive/predictive models strongly depends on the availability of data, as well as on their correctness. While the latter is generally promoted by the blockchain, the poor availability of data, due to their personal/sensitive nature, may make some approaches totally inapplicable. A relevant example is that of deep learning methods, that, although can be considered the state of the art in several contexts, require a huge amount of data to build accurate models. In this respect, the research should move towards two parallel directions: *i)* the design of incentivization mechanisms to promote data sharing for research purposes; *ii)* the design of specific methods to learn predictive models for healthcare, that can work with small, incomplete and/or unlabeled datasets (e.g., learning methods that work in the semi-supervised setting (Mignone & Pio, 2018; Mignone et al., 2020; Pio et al., 2021)).

As regards *Health data security and management* (Section 5.2), the developed systems combine distributed file systems (e.g., IPFS) and off-chain storage with on-chain solutions for the certification of the data, and resort to hybrid architectures to balance between transparency and privacy preservation. However, considering the recent advances in quantum computing, we expect to see more effort in the research line of quantum encryption (Bhattacharya et al., 2021), which can be considered fundamental to preserve the current security characteristics of the blockchain also with the diffusion of quantum processors.

In the category of *Internet of Things architectures for healthcare* (see Section 5.4), the specific challenges that still need to be addressed are more related to possible communication delays and miners' fees, introduced by the adoption of the blockchain. Indeed, while IoT devices usually need to communicate with low latencies, the validation process of the (specifically, public) blockchains may introduce unreasonable delays. For this reason, more attention should be put on the development of solutions based on specific blockchains that aim to solve these issues[6]

As regards other blockchain applications in healthcare (see Section 5.5), our systematic

[6]https://www.iota.org/.

review also highlighted that there are some areas where there is no solid research. Some relevant examples are the tracking and monitoring of the supply chain within hospitals, or the remote monitoring of fragile patients.

Finally, it is worth mentioning that the majority of the papers did not report a link to public repositories or websites. Although most of the algorithmic approaches are reported in the papers and are, therefore, reproducible, having the systems publicly available would facilitate the integration of contributions from the community and a quicker adoption of the blockchain technology in real-life scenarios in healthcare.

7. Conclusions and Future Work

The purpose of this study was to identify existing blockchain applications in the healthcare sector, that have been implemented in a real-world environment. To achieve this goal, a systematic review was conducted by properly querying three among the major databases, namely Scopus, PubMed, and Web of Science. The results were used to identify current trends in academic research in this area. Specifically, we identified that the research is mostly focused on the exploitation of different blockchain characteristics, such as security and immutability, to protect and manage sensitive patient data. In fact, among the 64 most important publications identified, 28 deal with this topic, followed by 13 publications focused on the implementation of electronic medical records. The remaining 23 papers were distributed among, Internet of Things architectures for healthcare, Medical research and diagnosis, and Other Applications.

For future work, we will investigate possible improvements of the blockchains from a technical viewpoint, to properly face the specific challenges raised by this domain, including the issues related to costs, scalability and latency, that, as stated before, may compromise the applicability of the proposed solutions in several health-related real scenarios.

References

Abdul Rahoof, T. P., & Deepthi, V. R. (2020). Healthchain: A secure scalable health care data management system using blockchain. In D. V. Hung, & M. D´Souza (Eds.), *Distributed Computing and Internet Technology* (pp. 380–391). Cham: Springer International Publishing. doi:http://dx.doi.org/10.1007/978-3-030-36987-3_25.

Abou-Nassar, E. M., Iliyasu, A. M., El-Kafrawy, P. M., Song, O.-Y., Bashir, A. K., & El-Latif, A. A. A. (2020). DITrust Chain: Towards Blockchain-Based Trust Models for Sustainable Healthcare IoT Systems. *IEEE Access*, *8*, 111223–111238. doi:http://dx.doi.org/10.1109/ACCESS.2020.2999468.

Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019). Blockchain technology in healthcare: A systematic review. *Healthcare*, *7*. doi:http://dx.doi.org/10.3390/healthcare7020056.

Akhter Md Hasib, K. T., Chowdhury, I., Sakib, S., Monirujjaman Khan, M., Alsufyani, N., Alsufyani, A., & Bourouis, S. (2022). Electronic health record monitoring system and data security using blockchain technology. *Security and Communication Networks*, *2022*, 2366632. URL: https://doi.org/10.1155/2022/2366632. doi:10.1155/2022/2366632.

Andola, N., Raghav, Prakash, S., Venkatesan, S., & Verma, S. (2019). Shemb:a secure approach for healthcare management system using blockchain. In *2019 IEEE Conference on Information and Communication Technology* (pp. 1–6). doi:http://dx.doi.org/10.1109/CICT48419.2019.9066237.

Arunkumar, B., & Kousalya, G. (2020). Blockchain-based decentralized and secure lightweight e-health system for electronic health records. In S. M. Thampi, L. Trajkovic, S. Mitra, P. Nagabhushan, Z. El-Alfy, El-Sayed M.and Bojkovic, & D. Mishra (Eds.), *Intelligent Systems, Technologies and Applications* (pp. 273–289). Singapore: Springer Singapore. doi:http://dx.doi.org/10.1007/978-981-15-3914-5_21.

Attia, O., Khoufi, I., Laouiti, A., & Adjih, C. (2019). An iot-blockchain architecture based on hyperledger framework for health care monitoring application. In *NTMS 2019-10th IFIP International Conference on New Technologies, Mobility and Security* (pp. 1–5). IEEE Computer Society. doi:http://dx.doi.org/10.1109/NTMS.2019.8763849.

Azbeg, K., Ouchetto, O., & Jai Andaloussi, S. (2022). Blockmedcare: A healthcare system based on iot, blockchain and ipfs for data management security. *Egyptian Informatics Journal*, *23*, 329–343. doi:https://doi.org/10.1016/j.eij.2022.02.004.

Bell, L., Buchanan, W. J., Cameron, J., & Lo, O. (2018). Applications of Blockchain Within Healthcare. *Blockchain in Healthcare Today*, *1*. doi:http://dx.doi.org/10.30953/bhty.v1.8.

Bhattacharya, P., Tanwar, S., Bodkhe, U., Tyagi, S., & Kumar, N. (2021). Bindaas: Blockchain-based deep-learning as-a-service in healthcare 4.0 applications. *IEEE Transactions on Network Science and Engineering*, *8*, 1242–1255. doi:http://dx.doi.org/10.1109/TNSE.2019.2961932.

Bhavin, M., Tanwar, S., Sharma, N., Tyagi, S., & Kumar, N. (2021). Blockchain and quantum blind signature-based hybrid scheme for healthcare 5.0 applications. *Journal of Information Security and Applications*, *56*, 102673. doi:http://dx.doi.org/10.1016/j.jisa.2020.102673.

Biswas, S., Sharif, K., Li, F., Latif, Z., Kanhere, S. S., & Mohanty, S. P. (2020). Interoperability and synchronization management of blockchain-based decentralized e-health systems. *IEEE Transactions on Engineering Management*, *67*, 1363–1376. doi:http://dx.doi.org/10.1109/TEM.2020.2989779.

Bonomi, F., Milito, R., Zhu, J., & Addepalli, S. (2012). Fog computing and its role in the internet of things. In *Proceedings of the first edition of the MCC workshop on Mobile cloud computing* (pp. 13–16). doi:https://doi.org/10.1145/2342509.2342513.

Buzachis, A., Celesti, A., Fazio, M., & Villari, M. (2019). On the design of a blockchain-as-a-service-based health information exchange (baas-hie) system for patient monitoring. In *2019 IEEE Symposium on Computers and Communications (ISCC)* (pp. 1–6). doi:http://dx.doi.org/10.1109/ISCC47284.2019.8969718.

Cao, B., Zhang, Z., Feng, D., Zhang, S., Zhang, L., Peng, M., & Li, Y. (2020a). Performance analysis and comparison of pow, pos and dag based blockchains. *Digital Communications and Networks*, *6*, 480–485. doi:http://dx.doi.org/10.1016/j.dcan.2019.12.001.

Cao, Y., Sun, Y., & Min, J. (2020b). Hybrid blockchain–based privacy-preserving electronic medical records sharing scheme across medical information control system. *Measurement and Control*, *53*, 1286–1299. doi:http://dx.doi.org/10.1177/0020294020926636.

Chase, B., & MacBrough, E. (2018). Analysis of the xrp ledger consensus protocol. doi:http://dx.doi.org/10.48550/arXiv.1802.07242. arXiv:1802.07242.

Chenthara, S., Ahmed, K., Wang, H., & Whittaker, F. (2020). A novel blockchain based smart contract system for ereferral in healthcare: Healthchain. In Z. Huang, S. Siuly, H. Wang, R. Zhou, & Y. Zhang (Eds.), *Health Information Science* (pp. 91–102). Cham: Springer International Publishing. doi:http://dx.doi.org/10.1007/978-3-030-61951-0_9.

Chukwu, E., & Garg, L. (2020). A systematic review of blockchain in healthcare: frameworks, prototypes, and implementations. *Ieee Access*, *8*, 21196–21214. doi:http://dx.doi.org/10.1109/ACCESS.2020.2969881.

Consortium, W. W. W. (2019). Verifiable credentials data model 1.0: Expressing verifiable information on the web. URL: https://www.w3.org/TR/vc-data-model/?#core-data-model.

Daraghmi, E.-Y., Daraghmi, Y.-A., & Yuan, S.-M. (2019). Medchain: A design of blockchain-based system for medical records access and permissions management. *IEEE Access*, *7*, 164595–164613. doi:http://dx.doi.org/10.1109/ACCESS.2019.2952942.

Deng, Y.-q., Ge, S., & Wen, Y.-m. (2017). Kp-habe: A fully secure key-policy hierarchical attribute-based encryption. *DEStech Transactions on Computer Science and Engineering*, . doi:http://dx.doi.org/10.12783/dtcse/cnsce2017/8882.

Donawa, A., Orukari, I., & Baker, C. E. (2019). Scaling blockchains to support electronic health records for hospital systems. In *2019 IEEE 10th Annual Ubiquitous Computing, Electronics Mobile Communication Conference (UEMCON)* (pp. 0550–0556). doi:http://dx.doi.org/10.1109/UEMCON47517.2019.8993101.

Fernández-Caramés, T. M., Froiz-Míguez, I., Blanco-Novoa, O., & Fraga-Lamas, P. (2019). Enabling the internet of mobile crowdsourcing health things: A mobile fog computing, blockchain and iot based continuous glucose monitoring system for diabetes mellitus research and care. *Sensors*, *19*. doi:http://dx.doi.org/10.3390/s19153319.

Figueroa, S., Añorga, J., & Arrizabalaga, S. (2019). An attribute-based access control model in rfid systems based on blockchain decentralized applications for healthcare environments. *Computers*, *8*. doi:http://dx.doi.org/10.3390/computers8030057.

Fu, J., Wang, N., & Cai, Y. (2020). Privacy-preserving in healthcare blockchain systems based on lightweight message sharing. *Sensors*, *20*. doi:http://dx.doi.org/10.3390/s20071898.

Gan, C., Saini, A., Qingyi, Z., Xiang, Y., & Zhang, Z. (2020). Blockchain-based access control scheme with incentive mechanism for ehealth systems: patient as supervisor. *Multimedia Tools and Applications*, . doi:http://dx.doi.org/10.1007/s11042-020-09322-6.

Gervais, A., Karame, G., Wüst, K., Glykantzis, V., Ritzdorf, H., & Capkun, S. (2016). On the security and performance of proof of work blockchains. (pp. 3–16). doi:http://dx.doi.org/10.1145/2976749.2978341.

Ghaffaripour, S., & Miri, A. (2019). Application of blockchain to patient-centric access control in medical data management systems. In *2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)* (pp. 0190–0196). doi:http://dx.doi.org/10.1109/IEMCON.2019.8936186.

Griggs, K. N., Ossipova, O., Kohlios, C. P., Baccarini, A. N., Howson, E. A., & Hayajneh, T. (2018). Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *Journal of Medical Systems*, *42*, 1–7. doi:http://dx.doi.org/10.1007/s10916-018-0982-x.

Hess, F. (2002). Efficient identity based signature schemes based on pairings. In *International Workshop on Selected Areas in Cryptography* (pp. 310–324). Springer. doi:http://dx.doi.org/10.1007/3-540-36492-7_20.

Huang, H., Sun, X., Xiao, F., Zhu, P., & Wang, W. (2021). Blockchain-based eHealth system for auditable EHRs manipulation in cloud environments. *Journal of Parallel and Distributed Computing*, *148*, 46–57. doi:https://doi.org/10.1016/j.jpdc.2020.10.002.

Huang, J., Qi, Y. W., Asghar, M. R., Meads, A., & Tu, Y.-C. (2019). Medbloc: A blockchain-based secure ehr system for sharing and accessing medical data. In *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)* (pp. 594–601). doi:http://dx.doi.org/10.1109/TrustCom/BigDataSE.2019.00085.

Jabarulla, M. Y., & Lee, H.-N. (2021). Blockchain-based distributed patient-centric image management system. *Applied Sciences*, *11*. doi:https://doi.org/10.3390/app11010196.

Jabbar., R., Krichen., M., Fetais., N., & Barkaoui., K. (2020). Adopting formal verification and model-based testing techniques for validating a blockchain-based healthcare records sharing system. In *Proceedings of the 22nd International Conference on Enterprise Information Systems - Volume 1: ICEIS,* (pp. 261–268). INSTICC SciTePress. doi:http://dx.doi.org/10.5220/0009592102610268.

Kakarlapudi, P. V., & Mahmoud, Q. H. (2021). Design and Development of a Blockchain-Based System for Private Data Management. *Electronics*, *10*. doi:10.3390/electronics10243131.

Khatoon, A. (2020). A blockchain-based smart contract system for healthcare management. *Electronics*, *9*. doi:http://dx.doi.org/10.3390/electronics9010094.

Khezr, S., Benlamri, R., & Yassine, A. (2020). Blockchain-based model for sharing activities of daily living in healthcare applications. In *2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)* (pp. 627–633). doi:http://dx.doi.org/10.1109/DASC-PICom-CBDCom-CyberSciTech49142.2020.00109.

Kim, J. W., Lee, A. R., Kim, M. G., Kim, I. K., & Lee, E. J. (2019). Patient-centric medication history recording system using blockchain. In *2019 IEEE International Conference on Bioinformatics and Biomedicine (BIBM)* (pp. 1513–1517). doi:http://dx.doi.org/10.1109/BIBM47256.2019.8983032.

Koushik, A. S., Jain, B., Menon, N., Lohia, D., Chaudhari, S., & B.P, V. K. (2019). Performance analysis of blockchain-based medical records management system. In *2019 4th International Conference on Recent Trends on Electronics, Information, Communication Technology (RTEICT)* (pp. 985–989). doi:http://dx.doi.org/10.1109/RTEICT46194.2019.9016812.

Kumar, R., & Tripathi, R. (2021). Scalable and secure access control policy for healthcare system using blockchain and enhanced bell–lapadula model. *Journal of Ambient Intelligence and Humanized Computing*, *12*. doi:http://dx.doi.org/10.1007/s12652-020-02346-8.

Kuo, T.-T., Kim, H.-E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association*, *24*, 1211–1220. doi:http://dx.doi.org/10.1093/jamia/ocx068.

Li, H., Zhu, L., Shen, M., Gao, F., Tao, X., & Liu, S. (2018). Blockchain-based data preservation system for medical data. *Journal of Medical Systems*, *42*. doi:http://dx.doi.org/10.1007/s10916-018-0997-3.

Lin, T.-S., Chen, Y., Chang, T.-H., Lu, C.-Y., & Kuo, S.-Y. (2014). Quantum blind signature based on quantum circuit. In *14th IEEE International Conference on Nanotechnology* (pp. 868–872). doi:http://dx.doi.org/10.1109/NANO.2014.6968020.

Liu, H., Dai, Z., Li, J., & Zhou, Y. (2016). An improved mls policy model. In *2016 10th IEEE International Conference on Anti-counterfeiting, Security, and Identification (ASID)* (pp. 47–52). doi:http://dx.doi.org/10.1109/ICASID.2016.7873915.

Lo, Y.-S., Yang, C.-Y., Chien, H.-F., Chang, S.-S., Lu, C.-Y., & Chen, R.-J. (2019). Blockchain-enabled iwellchain framework integration with the national medical referral system: Implementation and preliminary results (preprint). *Journal of Medical Internet Research*, *21*. doi:https://doi.org/10.2196/13563.

Lobo, V. B., Analin, J., Laban, R. M., & More, S. S. (2020). Convergence of blockchain and artificial intelligence to decentralize healthcare systems. In *2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC)* (pp. 925–931). doi:http://dx.doi.org/10.1109/ICCMC48092.2020.ICCMC-000171.

Mignone, P., & Pio, G. (2018). Positive unlabeled link prediction via transfer learning for gene network reconstruction. In M. Ceci, N. Japkowicz, J. Liu, G. A. Papadopoulos, & Z. W. Raś (Eds.), *Foundations of Intelligent Systems* (pp. 13–23). Cham: Springer International Publishing. doi:10.1007/978-3-030-01851-1_2.

Mignone, P., Pio, G., Džeroski, S., & Ceci, M. (2020). Multi-task learning for the simultaneous reconstruction of the human and mouse gene regulatory networks. *Scientific Reports*, *10*, 22295. doi:10.1038/s41598-020-78033-7.

Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G., , & the PRISMA Group (2009). Reprint—Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement. *Physical Therapy*, *89*, 873–880. doi:http://dx.doi.org/10.1093/ptj/89.9.873.

Neto, M. M., S.Marinho, C. S. d., Coutinho, E. F., Moreira, L. O., Machado, J. d. C., & Souza, J. N. d. (2020). Research opportunities for e-health applications with dna sequence data using blockchain technology. In *2020 IEEE International Conference on Software Architecture Companion (ICSA-C)* (pp. 95–102). doi:http://dx.doi.org/10.1109/ICSA-C50368.2020.00027.

Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2019). Blockchain for secure ehrs sharing of mobile cloud based e-health systems. *IEEE Access*, *7*, 66792–66806. doi:http://dx.doi.org/10.1109/ACCESS.2019.2917555.

Ni, W., Huang, X., Zhang, J., & Yu, R. (2019). Healchain: A decentralized data management system for mobile healthcare using consortium blockchain. In *2019 Chinese Control Conference (CCC)* (pp. 6333–6338). doi:http://dx.doi.org/10.23919/ChiCC.2019.8865388.

Noblit, G., & Hare, R. (1988). A meta-ethnographic approach. *Meta-Ethnography*, (pp. 27–37). doi:http://dx.doi.org/10.4135/9781412985000.n2.

Park, J., Park, S., Kim, K., & Lee, D. (2018). Corus: Blockchain-based trustworthy evaluation system for efficacy of healthcare remedies. In *2018 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)* (pp. 181–184). doi:http://dx.doi.org/10.1109/CloudCom2018.2018.00044.

Peña, C. A. N., Díaz, A. E. G., Aguirre, J. A. A., & Molina, J. M. M. (2019). Security model to protect patient data in mhealth systems through a blockchain network. In *Proceedings of the LACCEI international Multiconference for Engineering, Education and Technology*. doi:http://dx.doi.org/10.18687/LACCEI2019.1.1.285.

Peral, J., Gallego, E., Gil, D., Tanniru, M., & Khambekar, P. (2020). Using visualization to build transparency in a healthcare blockchain application. *Sustainability*, *12*. doi:http://dx.doi.org/10.3390/su12176768.

Pio, G., Mignone, P., Magazzù, G., Zampieri, G., Ceci, M., & Angione, C. (2021). Integrating genome-scale metabolic modelling and transfer learning for human gene regulatory network reconstruction. *Bioinformatics*, *38*, 487–493. doi:10.1093/bioinformatics/btab647.

Rahman, M. A., Abualsaud, K., Barnes, S., Rashid, M., & Abdullah, S. M. (2020). A natural user interface and blockchain-based in-home smart health monitoring system. In *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)* (pp. 262–266). doi:http://dx.doi.org/10.1109/ICIoT48696.2020.9089613.

Rahman, M. S., Khalil, I., Mahawaga Arachchige, P. C., Bouras, A., & Yi, X. (2019). A novel architecture for tamper proof electronic health record management system using blockchain wrapper. In *Proceedings of the 2019 ACM International Symposium on Blockchain and Secure Critical Infrastructure* BSCI '19 (p. 97–105). New York, NY, USA: ACM. doi:http://dx.doi.org/10.1145/3327960.3332392.

Rajput, A. R., Li, Q., Taleby Ahvanooey, M., & Masood, I. (2019). Eacms: Emergency access control management system for personal health record based on blockchain. *IEEE Access*, *7*, 84304–84317. doi:http://dx.doi.org/10.1109/ACCESS.2019.2917976.

Rakic, D. (2018). Blockchain Technology in Healthcare. In *Proceedings of the 4th International Conference on Information and Communication Technologies for Ageing Well and e-Health* (pp. 13–20). SCITEPRESS - Science and Technology Publications volume 2018-March. doi:http://dx.doi.org/10.5220/0006531600130020.

Ramani, V., Kumar, T., Bracken, A., Liyanage, M., & Ylianttila, M. (2018). Secure and efficient data accessibility in blockchain based healthcare systems. In *2018 IEEE Global Communications Conference (GLOBECOM)* (pp. 206–212). doi:http://dx.doi.org/10.1109/GLOCOM.2018.8647221.

Rathod, J., Gupta, A., & Patel, D. (2020). Using blockchain technology for continuing medical education credits system. In *2020 Seventh International Conference on Software Defined Systems (SDS)* (pp. 214–219). doi:http://dx.doi.org/10.1109/SDS49854.2020.9143876.

Reen, G. S., Mohandas, M., & Venkatesan, S. (2019). Decentralized patient centric e-health record management system using blockchain and ipfs. In *2019 IEEE Conference on Information and Communication Technology* (pp. 1–7). doi:http://dx.doi.org/10.1109/CICT48419.2019.9066212.

Saad, M., Spaulding, J., Njilla, L., Kamhoua, C., Shetty, S., Nyang, D. H., & Mohaisen, D. (2020). Exploring the Attack Surface of Blockchain: A Comprehensive Survey. *IEEE Communications Surveys and Tutorials*, *22*, 1977–2008. doi:http://dx.doi.org/10.1109/COMST.2020.2975999.

Saeedi, K., Wali, A., Alahmadi, D., Babour, A., AlQahtani, F., AlQahtani, R., Khawaja, R., & Rabah, Z. (2019). Building a blockchain application: A show case for healthcare providers and insurance companies. In *Proceedings of the Future Technologies Conference* (pp. 785–801). Springer. doi:http://dx.doi.org/10.1007/978-3-030-32520-6_57.

Satoshi Nakamoto (2008). Bitcoin: A Peer-to-Peer Electronic Cash System, .

Seo, J., & Cho, Y. (2020). Medical image sharing system using hyperledger fabric blockchain. In *2020 22nd International Conference on Advanced Communication Technology (ICACT)* (pp. 62–64). doi:http://dx.doi.org/10.23919/ICACT48636.2020.9061384.

Shah, R., & Rajagopal, S. (2022). M-dps: a blockchain-based efficient and cost-effective architecture for medical applications. *International Journal of Information Technology*, *14*, 1909–1921. doi:http://dx.doi.org/10.1007/s41870-022-00912-1.

Shahnaz, A., Qamar, U., & Khalid, A. (2019). Using Blockchain for Electronic Health Records. *IEEE Access*, *7*, 147782–147795. doi:http://dx.doi.org/10.1109/ACCESS.2019.2946373.

Shynu, P. G., Menon, V. G., Kumar, R. L., Kadry, S., & Nam, Y. (2021). Blockchain-based secure healthcare application for diabetic-cardio disease prediction in fog computing. *IEEE Access*, *9*, 45706–45720. doi:http://dx.doi.org/10.1109/ACCESS.2021.3065440.

Tandon, A., Dhir, A., Islam, A. N., & Mäntymäki, M. (2020). Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda. *Computers in Industry*, *122*, 103290. doi:https://doi.org/10.1016/j.compind.2020.103290.

Tang, H., Tong, N., & Ouyang, J. (2018). Medical images sharing system based on blockchain and smart contract of credit scores. In *2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN)* (pp. 240–241). doi:http://dx.doi.org/10.1109/HOTICN.2018.8605956.

Tanwar, S., Parekh, K., & Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *Journal of Information Security and Applications*, *50*, 102407. doi:http://dx.doi.org/10.1016/j.jisa.2019.102407.

Thwin, T., & Vasupongayya, S. (2019). Blockchain-based access control model to preserve privacy for personal health record systems. *Security and Communication Networks*, *2019*, 1–15. doi:http://dx.doi.org/10.1155/2019/8315614.

Thwin, T. T., & Vasupongayya, S. (2020). Performance analysis of blockchain-based access control model for personal health record system with architectural modelling and simulation. *International Journal of Networked and Distributed Computing*, *8*, 139–151. doi:http://dx.doi.org/10.2991/ijndc.k.200515.002.

Tith, D., Lee, J.-S., Suzuki, H., Wijesundara, W. M. A. B., Taira, N., Obi, T., & Ohyama, N. (2020). Application of blockchain to maintaining patient records in electronic health record for enhanced privacy, scalability, and availability. *Healthcare Informatics Research*, *26*, 3. doi:http://dx.doi.org/10.4258/hir.2020.26.1.3.

Toshniwal, B., Podili, P., Reddy, R. J., & Kataoka, K. (2019). Pacex: Patient-centric emr exchange in healthcare systems using blockchain. In *2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)* (pp. 0954–0960). doi:http://dx.doi.org/10.1109/IEMCON.2019.8936258.

Upadhyaya, P., Kumar Upadhyay, S., Subedi, B., Subedi, B., & Gaire, A. (2018). Revolutionizing healthcare systems of a developing country using blockchain. In *2018 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)* (pp. 1–6). doi:http://dx.doi.org/10.1109/ICCIC.2018.8782417.

Vujicic, D., Jagodic, D., & Randic, S. (2018). Blockchain technology, bitcoin, and Ethereum: A brief overview. In *2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH)* (pp. 1–6). IEEE. doi:http://dx.doi.org/10.1109/INFOTEH.2018.8345547.

Wang, S., Wang, J., Wang, X., Qiu, T., Yuan, Y., Ouyang, L., Guo, Y., & Wang, F.-Y. (2018). Blockchain-powered parallel healthcare systems based on the acp approach. *IEEE Transactions on Computational Social Systems*, *5*, 942–950. doi:http://dx.doi.org/10.1109/TCSS.2018.2865526.

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, *26*, xiii–xxiii. URL: http://www.jstor.org/stable/4132319. doi:http://dx.doi.org/10.2307/4132319.

Yang, F., Zhou, W., Wu, Q., Long, R., Xiong, N. N., & Zhou, M. (2019). Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism. *IEEE Access*, *7*, 118541–118555. doi:http://dx.doi.org/10.1109/ACCESS.2019.2935149.

Zaabar, B., Cheikhrouhou, O., Jamil, F., Ammi, M., & Abid, M. (2021). HealthBlock: A secure blockchain-based healthcare data management system. *Computer Networks*, *200*, 108500. doi:https://doi.org/10.1016/j.comnet.2021.108500.

Zghaibeh, M., Farooq, U., Hasan, N. U., & Baig, I. (2020). Shealth: A blockchain-based health system with smart contracts capabilities. *IEEE Access*, *8*, 70030–70043. doi:http://dx.doi.org/10.1109/ACCESS.2020.2986789.

Zhang, A., & Lin, X. (2018). Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. *Journal of Medical Systems*, *42*. doi:http://dx.doi.org/10.1007/s10916-018-0995-5.

Zhou, L., Marsh, M. A., Schneider, F. B., & Redz, A. (2005). Distributed blinding for distributed elgamal re-encryption. In *25th IEEE International Conference on Distributed Computing Systems (ICDCS'05)* (pp. 824–824). IEEE. doi:https://doi.org/10.1109/ICDCS.2005.24.

Zhou, L., Wang, L., & Sun, Y. (2018). Mistore: A blockchain-based medical insurance storage system. *J. Med. Syst.*, *42*, 1–17. doi:http://dx.doi.org/10.1007/s10916-018-0996-4.

Zhou, T., Li, X., & Zhao, H. (2019). Med-ppphis: Blockchain-based personal healthcare information system for national physique monitoring and scientific exercise guiding. *Journal of Medical Systems*, *43*, 305. doi:http://dx.doi.org/10.1007/s10916-019-1430-2.

Zhuang, Y., Chen, Y.-W., Shae, Z.-Y., & Shyu, C.-R. (2020). Generalizable layered blockchain architecture for health care applications: Development, case studies, and evaluation. *J Med Internet Res*, *22*, e19029. doi:http://dx.doi.org/10.2196/19029.

Zou, L., Chen, J., Lan, Q., Zhou, Z., Ma, C., & Yang, Z. (2022). Application of blockchain digital identity technology in healthcare consumer finance system. In *2022 IEEE 2nd International Conference on Power, Electronics and Computer Applications (ICPECA)* (pp. 1212–1219). doi:http://dx.doi.org/10.1109/ICPECA53709.2022.9719286.