PRAGUE UNIVERSITY
OF ECONOMICS
AND BUSINESS

Acta Informatica Pragensia
2023, Volume 12, Issue 1, pp. 160–178
Special Issue: Deep Learning Blockchain-enabled Technology
for Improved Healthcare Industrial Systems
https://doi.org/10.18267/j.aip.187

Review Open Access

Survey on Security and Interoperability of Electronic Health Record Sharing Using Blockchain Technology

Reval Prabhu Puneeth [1,2], Govindaswamy Parthasarathy [2]

[1] Department of Computer Science and Engineering, NMAM Institute of Technology, Nitte, India
[2] School of Computing and Information Technology, REVA University, Karnataka, India

Corresponding author: Reval Prabhu Puneeth (Puneeth.reval313@gmail.com)

Abstract

Blockchain is regarded as a significant innovation and shows a set of promising features that can certainly address existing issues in real time applications. Decentralization, greater transparency, improved traceability and secure architecture can revolutionize healthcare systems. With the help of advancement in computer technologies, most healthcare institutions try to store patient data digitally rather than on paper. Electronic health records are regarded as some of the most important assets in healthcare system and are required to be shared among different hospitals and other organizations to improve diagnosis efficiency. While sharing patients' details, certain basic standards such as integrity and confidentiality of the information need to be considered. Blockchain technology provides the above standards with features of immutability and granting access to stored information only to authorized users. The examination approach depends on the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (or PRISMA) rules and an efficient planned search convention is utilized to look through multiple scientific databases to recognize, investigate and separate every important publication. In this paper, we present a solid systematic review on the blockchain and healthcare domain to identify the existing challenges and benefits of applying blockchain technology in healthcare systems. More than 150 scientific papers published in the last ten years are surveyed, resulting in the identifications and summarization of observations made on the different privacy-preserving approaches and also assessment of their performances. We also present a significant architectural solutions of blockchain to achieve interoperability. Thereby, we attempt to analyse the ideas of blockchain in the medical domain, by assessing the advantages and limitations, subsequently giving guidance to other researchers in the area.

Keywords

Electronic healthcare records; EHR; Blockchain; Data privacy; Decentralize technology; Security; Interoperability.

Citation: Puneeth, R. P., & Parthasarathy, G. (2023). A Survey on Security and Interoperability of Electronic Health Records Sharing Using Blockchain Technology. *Acta Informatica Pragensia*, 12(1), 160–178. https://doi.org/10.18267/j.aip.187

Special Issue Editors: Mazin Abed Mohammed, University of Anbar, Iraq
Seifedine Kadry, Noroff University College, Norway
Oana Geman, Ștefan cel Mare University of Suceava, Romania

Academic Editor: Zdenek Smutny, Prague University of Economics and Business, Czech Republic

1 Introduction

Blockchain technology is decentralized, immutable and tamper-proof in nature. The technology is known from the 1990s, but it has gained popularity based on the idea of a distributed ledger approach where each node associated in the network keeps a duplicate of the record (Dubovitskaya et al., 2019). Actually, it came into light in the year 2008, when Satoshi Nakamoto published the idea of digital forms of money and the idea was executed in 2009. Therefore, blockchain technology has advanced greatly and as a result of many benefits, the technology is now utilized in numerous areas. Numerous associations are benefiting from safety and security with the execution of blockchain technology. Blockchain technology guarantees the integrity of the information stored and guarantees that once the information is stored in the blockchain it cannot be changed (Zhuang et al., 2020).

The first implementation of the Bitcoin code was released as open-source, which enabled others to contribute by modifying the code and create different blockchain generations. Blockchain 1.0 includes technologies such as Monero, Dash, Litecoin with its main aim to bring public access and transparency to the financial system. Smart contacts are a new feature in Blockchain 2.0. This layer consists of a variety of financial assets, including derivatives, options, swaps, and bonds. At this level, applications that go beyond money, finance, and markets are included. Some framework examples of these generations are Ethereum, Hyperledger, NEO, QTUM and Ethereum Classic (Tanwar et al., 2020).

Blockchain 3.0 technology was intended for non-financial blockchain applications such as healthcare, media, the arts, justice and government-related applications; it emerged around 2012. The latest generation of Blockchain X.0 addresses a dream of blockchain uniqueness where there would be a public blockchain administration that would be similar to a Google search engine that anyone can use. The future applications would be artificial intelligence-enabled blockchain (Mahajan et al., 2022).

Healthcare applications have been considered the main region where a greater number of purpose cases have been distinguished. However, it needs to be investigated what blockchain-based healthcare applications have been created. This paper explains the constraints and the significant difficulties of the blockchain-based-healthcare framework and distinguishes how these difficulties are presently being addressed and their importance including some of the important points to that may not be known yet. Moreover, the existing traditional approach of the healthcare industry is considered rigid, and it is recommended to measure the facts of change and resistance to the adoption of new innovative practices. Some of the issues in the traditional centralized approach that have drawn attention of researchers worldwide are privacy, information security, third-party dependence and interoperability (Hathaliya and Tanwar, 2020). The HIPAA (Health Insurance Portability and Accountability Act) rules put restrictions on usage of patient health information, but privacy is victimized in many ways.

For example, a patient may visit multiple healthcare centres for medical treatments due to availability of good healthcare infrastructure. As most healthcare service providers follow the centralized storage approach, patients do not have any control over their own data, and moreover they cannot share their medical history with other doctors, so it is important to share patient health information among different healthcare centres by maintaining integrity and confidentiality standards. That could reduce redundant diagnosis that may be done on the patient and in turn this saves doctors’ time to make a decision about the patient as well as expenses incurred by the patient. Other cloud-based solutions are available, but the challenge is all about the credibility of the third party. As such, blockchain technology provides a solution to the above issue in a better and efficient way that leads to a smart and efficient healthcare system.

Interoperability in the medical service area is the capacity of medical service frameworks to share, interpret and utilize Electronic Healthcare Records (EHRs) seamlessly (Fang et al., 2021). EHR management and interoperability solutions are important for consistent exchanging of patients medical details, which can improve the effectiveness of healthcare services with decreased costs and time.

Moreover, the EHR guidelines of various medical care associations are not uniform, causing a low level of interoperability in medical care data frameworks among the associations (Rajput et al., 2021; Cunha et al., 2021); thus, interoperable EHR aims to maintain identical EHR structure. EHR sharing and interoperability among different medical care associations is an open research area.

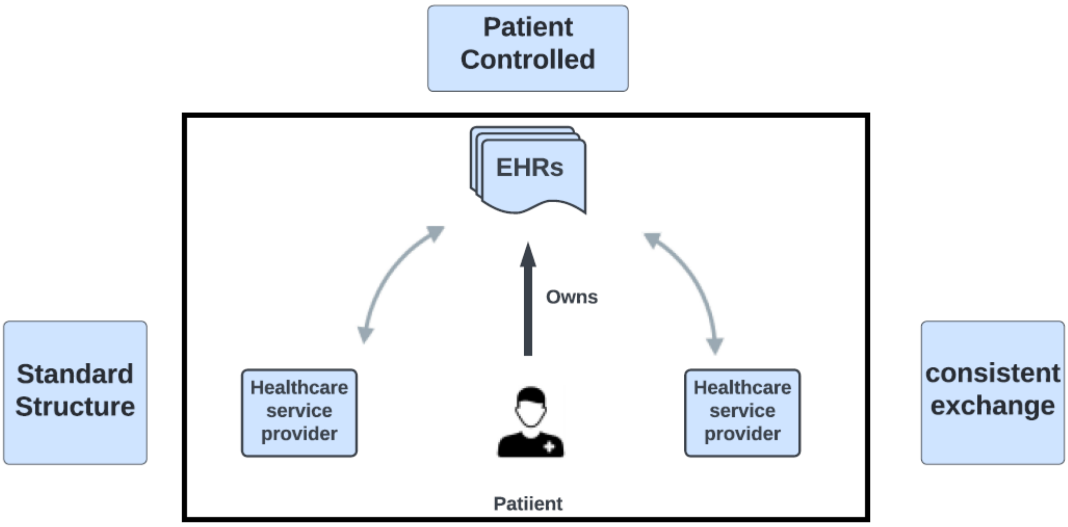

Figure 1. *Goals of EHR interoperability.*

Patient-controlled interoperable solutions mean that EHRs are controlled by patients, and they grant or deny access to their records to different partners (Mayer et al., 2019). Consistent EHR sharing among various medical service partners is fundamental for superior medical services. The three main goals of EHR interoperability are shown in Figure 1.

In summary, this survey aims to provide information about the blockchain process, the significance of using blockchain in healthcare services, the challenges, certain limitations of blockchain-based EHR and how they are currently being addressed. Based on the privacy and interoperability concerns, a systematic review is carried out to understand the different types of privacy-preserving approaches employed for EHRs and certain observations on the performance parameters considering the access-costs, storage-costs, retrieval time and security vulnerabilities. As there is no standard framework available to achieve EHR interoperability, the cross-chain and the semantic-based architectural styles are presented in this article as solutions to interoperability.

2 Methods

The study design is carried out by adopting the PRISMA guidelines (Fang et al., 2021). The main goal was to identify eligible articles on blockchain-based EHR and to summarize the current aspects, available design choices, and merits/demerits of adopting a blockchain-based approach and future directions. In this review process, the main intention was to understand the efforts and the ideas of researchers, so no quality assessment of various blockchain-based EHRs was performed. The following activities were defined and executed during the systematic review process.

2.1 Research questions

Following are research questions considered to address during this review.

***Table 1.** Research questions for literature review.*

Research questions	**Justifications**	**Relevant sections of this article that deal with the question**
What are the benefits, challenges, limitations of applying blockchain in the field of healthcare and different available standard blockchain architectural styles?	A basic study of blockchain is carried out- to understand the needs, benefits, process and types of blockchain, as well as the challenges and limitations of blockchain-based EHR and how they are currently being addressed.	Results are presented in sections 3 and 4.
What are the different privacy-preserving approaches available to achieve privacy of patient data?	EHRs are sensitive data, privacy is utmost important; thus, we present different types of privacy-preserving techniques employed for EHRs and summarize the observations made on the different privacy-preserving strategies of EHR and assess their performance.	Results are presented in Section 5.
How mature is blockchain technology for enabling EHR interoperability, and what are its challenges / limitations? Do any existing architectural styles achieve interoperability?	As EHR information is shared across different stakeholders, it should be interoperable. In this regard the challenges and limitations of EHR interoperability are discussed, and consideration of existing interoperability solutions with architectural styles and blockchain engines to achieve EHR interoperability is carried out.	Results are presented in Section 6.

2.2 Search strategy

Following is the search strings used: “blockchain”, AND (“electronic health records”) OR(“privacy and security“)OR(“interoperability”) OR(“medical records”) OR (“PHR”) OR (“EHR”) OR (“health records”). It was used to identify the suitable articles based from different academic publishers and repositories such as IEEE Xplore, Scopus, Springer Link, Web of Science, ACM, MEDLINE, Google Scholar and Science Direct.

2.3 Article selection

The following are the inclusion and exclusion steps carried out on the obtained articles to select appropriate research articles for the final review process. Electronic health records based on blockchain, patient-centric component, privacy techniques in the blockchain-based approaches and interoperability techniques are considered among inclusion criteria, while identical articles, survey articles, and articles with incomplete implementation information are excluded from the final selection. An overall stepwise selection process was performed. First, duplicate articles from different databases were excluded. Besides, article titles that were not relevant to the topic of discussion were excluded. Finally, article abstracts were reviewed and those not on blockchain-based Patient Health Record (PHR)/EHR and review articles were also excluded. Table 2 describes the inclusion and exclusion criteria.

Table 2. *Review inclusion and exclusion criteria.*

Topic of study	Inclusion criteria	Exclusion criteria
Privacy-preserving approaches used in EHR	The research work should refer to various privacy-preserving techniques utilized in EHR for data storage and patients data accessibility. Works mainly on blockchain-based approaches along with smart contracts for privacy-preserving EHR were incorporated.	Privacy-preserving techniques applied to non-medical cases were excluded.
EHR interoperability	The work must refer to EHR data standards or semantic-based approaches such as ontology, big data model approaches for EHR management. Websites/blogs describing mechanisms for interchanging of EHRs between different blockchain platforms.	Papers presenting semantic representation and standards other than for healthcare records and big data for non-medical applications are excluded.

2.4 Data abstraction

Some of the design parameters were selected to complete the data abstraction process, such as type of blockchain architecture, data storage, scalability solutions, smart contracts, privacy and security standards, interoperability solutions, PHR type, ability to read and write information and user interface are used. The limitations, future directions and areas of improvement were identified and presented under specific topics.

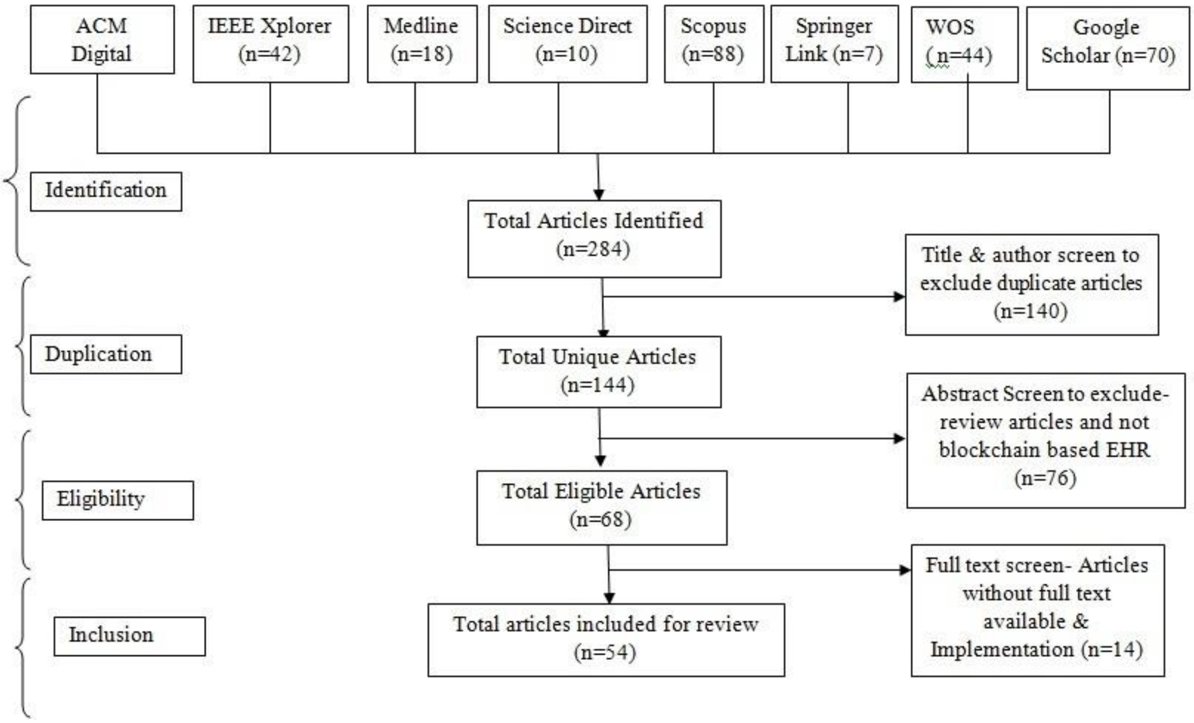
ACM Digital
IEEE Xplorer (n=42)
Medline (n=18)
Science Direct (n=10)
Scopus (n=88)
Springer Link (n=7)
WOS (n=44)
Google Scholar (n=70)
Identification
Total Articles Identified (n=284)
Title & author screen to exclude duplicate articles (n=140)
Duplication
Total Unique Articles (n=144)
Abstract Screen to exclude-review articles and not blockchain based EHR (n=76)
Eligibility
Total Eligible Articles (n=68)
Full text screen- Articles without full text available & Implementation (n=14)
Inclusion
Total articles included for review (n=54)

Figure 2. *Article filtering steps in systematic review process.*

3 Electronic Healthcare Records

3.1 Brief overview of current literature

This section starts with a brief overview of current literature on EHR and blockchain technology use. Azaria et al. (2016) proposed a framework called MedRec, a blockchain-based approach to achieving decentralization of health records. They utilized a public blockchain category that motivates scientists to mine new blocks in return for gaining access to anonymized clinical information. The authors claimed that their architecture increases the simplicity of healthcare records, security, and information privacy. The MedRec work was extended by Nchinda et al. (2019). They utilized blockchain to store consent contracts. In their work, suppliers could join the organization and grant patients and different elements access to their information bases utilizing their qualifications.

Mikula and Jacobsen (2018) utilized a unified and permission based blockchain to investigate auditability. Their assessment of the framework showed that the mining time to add a new block to blockchain was around 2-3 minutes, for a block size of around 3.8 MB. Whereas Haque et al. (2020) used two different blockchains to achieve security and data protection: one of them to store only EHRs and the other to store EHR solid files. Haque et al. (2020) also utilized a secure hashing algorithm called SHA-256 hash calculation to create a novel and indistinguishable 256-cycle or 32-byte hash for a specific clinical record. Since there is no trusted central authority to manage in a public blockchain-based approach arriving at a consensus between untrusted nodes is a significant issue. Raikwar et al. (2019) proposed an encryption approach for sharing patient health records among shared networks and utilizing smart contracts to manage access control and interoperability between hospitals.

For the consensus mechanism Zhang et al. (2021) proposed a blockchain-based framework and implemented a Practical Byzantine Fault Tolerance (PBFT), which is a consensus mechanism for exchanging information among patients and researchers. Compared to the previous consensus mechanism, the PBFT would consume less computation power and could be adopted for many other blockchain-based applications. The authors proposed a consensus calculation named Proof of Authenticity over the network for all clinical partners; thereby, clinics and healthcare centres are expected to perform the role of miners as well as valuators for adding a block to the distributed ledger.

The utilization of the blockchain-based approach for handling healthcare information is a significant research. The on-chain method increases the weight of calculation and capacity in the blockchain even if entire EHRs may be stored directly in the blockchain architecture. To tackle these issues, many related examinations and applications have embraced a cross-breed storage design. This is an off-chain storage system where only the reference information stored in a blockchain, and the actual copy of the information may be stored using an Interplanetary File System (IPFS) by Pilares et al. (2022).

3.2 Potential benefits of using blockchain in healthcare

A critical part of healthcare information is the EHR which contains private clinical analysis data of a patient. Aside from EHR, there are different kinds of medical care information (Mayer et al., 2019). These include:

a) PHR, which contains information such as the patients physiological health boundaries and sensitivity data.

b) drug/medication information which stores data for medical prescriptions; and

c) healthcare coverage information which includes data on the patients protection strategy, instalment data, and information on protection-related administrations.

Potential benefits of using blockchain in healthcare applications are discussed in Table 3.

Table 3. *List of potential benefits of using blockchain in healthcare.*

Decentralization	In the healthcare system stakeholders are distributed and require the system to be decentralized. Blockchain can provide the solutions by making data management system distributed where all the stakeholders can control the healthcare records without the need for a centralized authority (Puneeth and Parthasarathy, 2021).
Immutability	Immutability is another important feature of blockchain that mainly provides the security of health records stored in it, where data once written cannot be modified, corrupted or altered (Tanwar et al., 2020).
Smart contracts	Patients need to own their data and be in control of how their data are used. The configuration of the blockchain features, such as smart contracts and cryptographic protocols can help meet their requirements (Nchinda et al., 2019).
Robustness / Availability	With the concept of decentralization, replicated copies of healthcare information are available across multiple participating nodes. Availability of the data can be guaranteed, so the system is resilient against data losses or corruption (Zhang et al., 2021).
Transparency	Blockchain is open and transparent in nature; it helps create a trusted atmosphere among distributed healthcare applications.
Data verifiability	Without accessing plaintexts stored in blockchain, the integrity and legitimacy of those records can be confirmed using the hash value stored in each block as root information about the whole set of information or transactions stored in a block. This element is extremely helpful in the field of medical services.
Security	All the records in blockchain are encoded, time-stamped and arranged in a sequential order. The use of suitable cryptographic keys can achieve data security and privacy of patient details (Xia et al., 2017; Raikwar et al., 2019).

3.3 Difficulties and restrictions of blockchain-based EHR frameworks

In this subsection, a few technical difficulties of the blockchain technology are listed, such as throughput, latency, scalability, privacy and security, interoperability and usability.

Throughput: When the numbers of transactions and participating nodes in a network increases, more checks have to be carried out, leading to a network bottleneck. Therefore, throughput is a very important factor to be considered when working with healthcare ecosystems. Faster access to a required diagnosis could help doctors to save someone’s life.

Latency: The time taken to complete the process of validating a block in a blockchain varies depending on the type of consensus mechanism along with the type of blockchain architecture. Healthcare systems are dynamic and information should be accessed within a time frame.

Scalability: It is a critical issue particularly in connection to the volume of data involved in a healthcare system. Moreover it is not ideal, or even practicable in certain cases, to store high-volume biomedical information in the blockchain as this will undoubtedly cause performance degradation and also leads to an increase in latency (Yang and Yang, 2017; Lin et al., 2019; Yan et al., 2020).

Interoperability: It is the process of exchanging of information between two different entities. Applications created by various vendors or on different framework platforms will be unable to interoperate. For example, if two healthcare systems are developed, one using Ethereum and another using Hyperledger Fabric platform, it is troublesome to exchange/ transfer data between the two different platforms (Belchior et al., 2021).

Privacy and security: Issues with blockchain-based medical care providers' data privacy, for example, There is concern that, even using effective encryption techniques, it would still be feasible to find a patient's personal information on a public blockchain. The secret blockchain keys used for information encoding and decoding are also susceptible to potential trade-offs, which might result in unauthorised access to the stored healthcare data. (Sonkamble et al., 2021; Sorace et al., 2019; Watford et al., 2019).

A significant feature provided by blockchain called immutability, does not follow the general rules provided by the European Union’s General Data Protection Regulation (GDPR) "on the right to be forgotten", which specifies that the client has the option to demand total eradication of their information. Since data once written in a blockchain cannot be erased or changed, it could prove counterproductive when there is request to totally clear a patient’s clinical history.

Usability is about how to enable patients to administer their own information in the blockchain. Moreover patients, of different ages may not be willing or ready to take part in the administration of their EHR.

Some probable solutions to the above limitations to utilization of blockchain in healthcare applications have been proposed. For instance, as a corrective measure to the scalability issue, it is feasible to use an "off-chain," storage technique, where only the link/reference to the information is stored in the blockchain, whereas the actual data in encrypted form are stored using the IPFS (Pilares et al., 2022). This method of storage also resolves the GDPRs "right to be forgotten" issue, since in the off-chain approach, the original data are stored in IPFS, and can thus be erased forever. However, the reference to the information in the blockchain cannot be deleted. The use of permissioned blockchains such as private or consortium rather than public blockchains could be adopted. With the use of smart contracts, various standards can be characterized and modified to manage the process of storage and accessibility of patient data.

4 Blockchain Technology

4.1 Blockchain process

Every transaction on the blockchain is included in a block, which is then cryptographically encrypted using SHA-256, MD5, or other hashing algorithms. As a result, each block generates a distinct value known as a hash value. The information from the preceding block is combined with a newly produced hash value in the next block. A genesis block is the first block created and added to the blockchain, a block can be added to the blockchain network by any node. Figure 3 shows how blockchain works (Fang et al., 2021).

The blockchain network is a consensus based network in which each of the nodes present needs to settle on the exchange made dependent on consensus algorithm. A consensus calculation/ algorithm is a process by which different nodes present in a distributed network settle upon a choice. The consensus calculation/algorithm gives unwavering quality to an appropriated network. There are numerous consensus algorithms, such as Proof of Work (POW), Proof of Stake (POS), Byzantine Fault Tolerance (BFT) (Hashim et al., 2021).

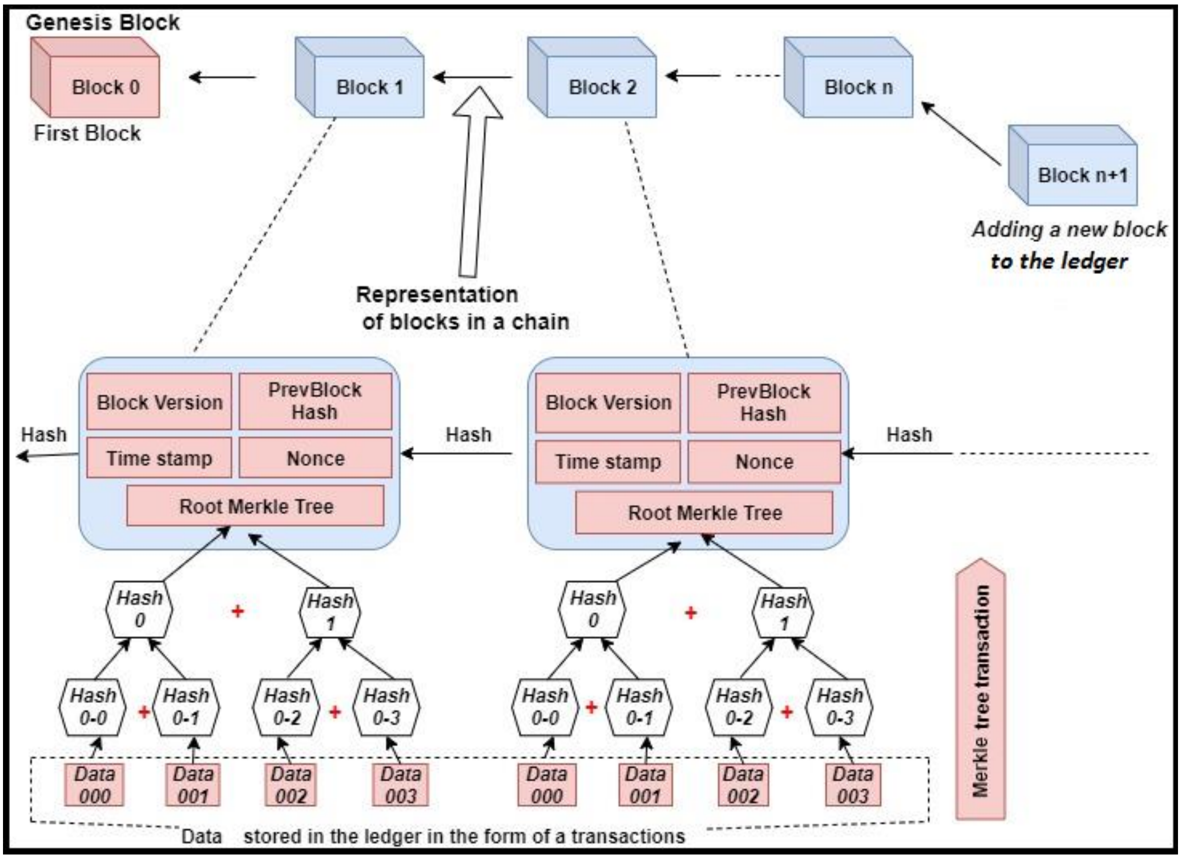

Figure 3. *Primary Blockchain Process.*

4.2 Types of blockchain

4.2.1 Public blockchain

A public blockchain is a kind of blockchain that is available to all. Any client can interface with a public blockchain, and no authorization is needed to join the organization. Any user associated with the public blockchain has the authorization to add a block to the blockchain network after completing a consensus process. A public blockchain can be exceptionally helpful in managing cryptocurrency (Fan et al., 2018).

4.2.2 Private blockchain

Unlike a public blockchain, in a private blockchain or permissioned blockchain, any client who wishes to join the organization needs to receive consent to be added to the organization. Where miners are predefined, no unapproved client is permitted to join the organization (Puneeth and Parthasarathy, 2021). Blockchain enables businesses to transact efficiently; Hyperledger is an open-source umbrella that offers tools for developing blockchain. Ripple is a blockchain-based digital payment network.

4.2.3 Consortium blockchain

The consortium blockchain architecture is also called the “federated” blockchain architecture, where one or more organizations govern the platform. It is neither a public platform nor a permissioned platform. It is a fully open, decentralized system and centrally controlled. A blockchain consortium of like-minded service providers can hold information to improve accountability, workflows and transparency. Quorum is based on Ethereum, R3 Corda or Hyperledger, which are some of the most popular blockchain development platforms (Qiao et al., 2020).

4.2.4 Hybrid blockchain

Hybrid blockchains lie close to private and public blockchains, contingent upon their design. A single corporation controls this blockchain, which combines public-private and public-permissioned blockchains to enable businesses to create private, permission-based systems alongside public, permissionless systems. IBM's hybrid blockchain serves as an illustration of integrating public and private blockchains (Yan et al., 2020).

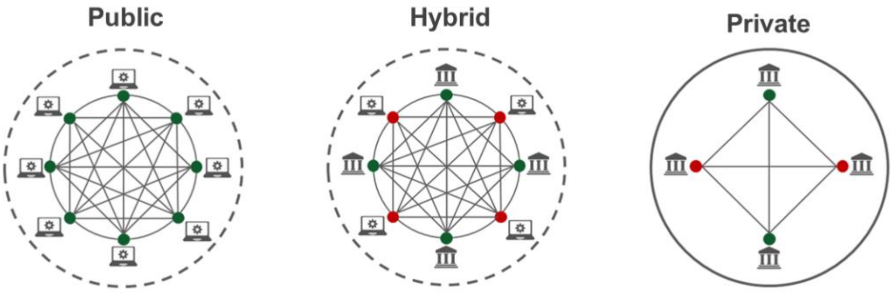

__Figure 4.__ Different types of blockchain. Source: Based on (Oodles, 2022).

Figure 4 represents the public, private and hybrid blockchain structures, where the participating nodes in the blockchain are represented with the dots, where a green dot represents a mining node and a red dot indicates normal or participating nodes in a blockchain.

4.3 Scalability

Scalability is one of the issues of blockchain which brings the consideration straightforwardly to possible arrangements (Garrido et al., 2021). The Solution to Scalability of Blockchain is discussed below.

a) **Sharding:** As a method of on-chain scaling, sharding is one of the common solutions for addressing the blockchain adaptation issue. In light of relevant data sets, sharding is a fantastic layer-1 scaling solution for blockchain networks. The process of "sharding" entails dividing information exchanges into smaller, discrete information groups. The organisation then processes the shards concurently. Data may be partitioned among several nodes with the use of sharding, which maintains data consistency. By using cross-shard correspondence rules, shards serve as the main chain's verification while maintaining their interconnectedness for the purpose of exchanging locations, general states, and balances. (Hashim et al., 2021).

b) **Nested blockchain:** It is essentially a decentralised network foundation that uses the primary blockchain to provide limits for a larger network of secondary blockchains. It also ensures that trades will be carried out through a network of optional chains that are connected to one another. One of the layer-2 configurations that show promise in addressing the blockchain versatility issue is nested blockchain. (Mattila et al., 2022).

c) **Consensus mechanisms:** As a result, prominent blockchain organisations like Bitcoin use the Proof of Work consensus model. Even while the Proof of Work consensus tool provides strong security, it is quite slow. This is why many blockchain networks see the Proof-of-Stake consensus mechanism as a potential solution to the blockchain's flexibility problems. The POS consensus mechanism does not need miners to resolve cryptographic computations by employing significant amounts of processing power. Contrary to popular belief, it ensures consensus through the selection of validators, which is determined by organisational stakes. By advancing decentralised security, the adoption of POS consensus might kindly assist in overcoming the constraint of Ethereum networks. (Sonkamble et al., 2021).

5 Privacy-Preserving Approaches Employed in EHRs

Nowadays, most of the healthcare-related documents are digitized. Data are generated from different origins in the healthcare area such as radiology images, monitoring sensors and other sources. Traditionally, the patient details are stored in several databases, where some of the information may be very sensitive. However, the use of blockchain in these areas helps achieve the privacy and security of the required information mainly due to features provided such as data traceability and immutability. Nevertheless, one important requirement, the privacy issue of EHR in the blockchain, is not completely resolved. There is still a need to resolve the issues connected with security while exchanging information (Fan et al., 2018; Guo et al., 2018; Loukides et al., 2014; Raikwar et al., 2019).

Identity privacy and transaction privacy are considered the main challenges to be handled efficiently in blockchains. Identity privacy is about maintaining the private identity of users such as patients and ensuring it is not relating to the transaction. Transaction privacy means to ensure that patient information is not obtained by any unauthorized users. To address this type of privacy, many techniques could be used such as k-anonymity or zero-knowledge proof (Lin et al., 2019), trusted execution environments, differential privacy, attribute based encryption method (Yan et al., 2020; Kim et al., 2020), identity-based encryption (Raikwar et al., 2019), elliptic curves cryptography (Shahnaz et al., 2019). Blockchain technology utilizes hashing and cryptographic techniques to achieve data security on data between nodes associated in a network, mainly SHA-256 or SHA-512 hashing algorithms.

Homomorphic encryption (Qu et al., 2020) can also be used to address the patient data privacy issue in a blockchain, where one can utilize, homomorphic encryption to store data over a blockchain with no significant changes in the properties of the blockchain. It also offers privacy protection and enables some form of computation over encrypted data without revealing the actual data. The Ethereum platform may be used to create blockchain-based applications for enhanced privacy and control over patient data since it supports homomorphic encryption for data stored in the blockchain.

Finally, as data security and privacy are crucial components of the healthcare system, using blockchain technology can assure accomplishing them. The selection of an appropriate privacy approach must be chosen very carefully because it might result in performance deterioration (Chenthara et al., 2020; Boumezbeur and Zarour, 2022). Different types of privacy-preserving approaches employed in EHR are presented and discussed in Table 4.

Table 4. *Represents the privacy preserving approaches employed for EHR.*

Privacy-preserving approaches		
Cryptography	It aims to apply encryption methods to sensitive information in EHR. Asymmetric and symmetric techniques are utilized to check the legitimacy and authority of the information.	Attribute level Privacy by design Patient controlled privacy
Disassociation	The process of disassociation is used to separate extremely sensitive traits from personality traits. This helps people with rare diseases keep their personalities hidden from potential adversaries.	De-linking sensitive attributers. Privacy by design
Anonymity	Sensitive or private information is obscured in the EHR by replacing it with random characters or summarising it with broad characteristics to avoid attracting attention.	K-anonymization algorithms, tools such as ARX-or Amnesia
Blockchain-based strategies	Blockchain upholds pseudo-obscurity of patients in EHR. Smart contracts used in the blockchain can assist in managing the access rights of users.	Role-based access management Smart contracts

Privacy-preserving approaches		
	Dividing the EHR into on-chain and off-chain data to manage the data efficiently and effectively.	Data storage partitioning
Cloud based approaches	As cloud suppliers offer administrations for clients, they use encryption procedures in the cloud to get information.	Encryption techniques privacy by design
Privacy levels	Each medical care specialist has pre-defined roles and access privileges which characterize what, how, and where it can be accessed.	User / role-based approaches Patient controlled privacy

The privacy preservation methods for EHR offer data security but influence factors such as performance and storage. The throughput is affected by some of the operations related to information retrieval, encryption/decryption and compliance checks (Sonkamble et al., 2021). We summarize the observations made on the different privacy-preserving strategies for EHR and also assess their performance in Table 5. They are the on-premise approach (Loukides et al., 2014; Fan et al., 2018; Guo et al., 2018; Xia et al., 2017), the cloud-based approach (Tu et al., 2010; Hamid et al., 2017; Li et al., 2013; Liu et al., 2015) and the blockchain-based approach (Akhter Md Hasib et al., 2022; Chelladurai and Pandian, 2022; Mantey et al., 2022; Mahajan et al., 2022).

Table 5. *Observation made on the different privacy preserving strategies of EHR.*

Observations on performance evaluation of privacy preservation approaches				
	Access costs	**Retrieval Time**	**Storage costs**	**Security vulnerability**
On-premise approach	Higher when additional security standards are leveraged on EHR frameworks such as encryption and decryption overheads.	Significantly shorter	Capacity costs are affected by on-premise centralized approach.	Denial of service (or DOS) attacks, data tampering, single point failure and performance bottlenecks are some of the vulnerabilities.
Cloud-based approach	Higher	Higher than on-premise approach	Storage costs may vary based on the service providers' accounting model.	Lack of trust by third-party service providers
Blockchain-based approach	Much higher than on-premise and cloud-based.	As smart contracts are used to validate healthcare data and manage user authentication, retrieval time is longer than two approaches.	Distributed replicated ledger is used, higher than two above approaches	Basic security aspects such as data privacy, data integrity and confidentiality can be addressed easily.

6 Interoperable Healthcare Data Sharing

6.1 EHRs interoperability: Role of blockchain

Blockchain is considered instrumental to attain interoperability of information, and the process can work without the need of a customary intermediary. In future, interoperability is likely to have become more persistent and better control of access and sharing of EHR can be achieved by utilizing blockchain (Chenthara et al., 2020). The features and approaches are discussed in Table 6.

Table 6. *EHR interoperability.*

No.	Features	Approaches
1	EHR accessibility	• The patient's clinical information can be mapped with the patient's public key. • Role-based access control and attribute-based access control can be achieved using customized smart contracts in the blockchain.
2	EHR aggregation	• Patients can consult different healthcare service providers; by using unique identification numbers information/history of details can be aggregated and communicated to the required entity.
3	Health data liquidity	• An open blockchain may be used to share sensitive patient data, ensuring liquidity and ready access to information as needed.
4	Patient identity	• Using unique ID such as Aadhaar-based (unique number for all residents in India) can be used to identify patient medical data.
5	Data immutability	• Clinical data should be safely exchanged in order to guarantee accessibility and preserve data integrity. • The fundamental characteristic of blockchain is immutability; once data has been recorded, it cannot be modified inside a block. If altered, the interconnections between the blocks are disconnected.

6.2 Issues due to absence of interoperability

There are a few issues caused by a shortfall in interoperability (Faheem et al., 2021):

- **Restricted information sharing**: The dominant EHR types on the market today limit the free progression of patient data across different service providers. The medical service framework causes extra expenses because of clinical test duplications that occur due to limited data accessibility.
- **Non-accessibility of collaborative patient data for understanding perspective:** The patient data with service providers are isolated from others which lead to data unavailability about the patient health history. There is no Application Programming Interface (API) that permits the different restrictive and frameworks to consistently impart information with one another.
- **Lack of significant information:** Due to the lack of accurate information and the EHR vendors' reluctance to upgrade their user interfaces, the benefits of information mining and information warehousing are severely constrained.

6.3 Interoperability solution: Cross-chain interoperability

Cross-chain interoperability is regarded as a mechanism by which one or more blockchains can communicate with each other across homogenous or heterogeneous platforms. In most of the published articles, EHR, are maintained and managed using a single blockchain framework approach. Moreover, EHRs can be shared across healthcare associations/organizations, using different frameworks. Thus, inter-organizational EHR interoperability approach demands that cross-chain interoperability be examined for information sharing (Sonkamble et al., 2021). Table 7 shows the architecture of cross-chain interoperability for EHR management system.

Table 7. *Cross-chain interoperability architecture*

No.	Type	Key features	Advantages	Limitations
1	Hash locking	• Hash trigger • A similar trigger activity will cause tasks across the two players.	• Non-interceded • Information privacy is ensured.	• Synchronous changes will be completed.
2	Relay or side-chain	• The record is replicated in an imperfect form.	• Non-interceded	• Security of EHR should be authorized across the two players.
3	Notary	• Trusted third party • Multiple outsiders can increase legitimacy.	• Interceded	• A non-intervened solution for EHR migrations cannot be created. • Privacy of EHR will be compromised.

6.4 Interoperability solution: Semantic interoperability

A standard representation followed in structural interoperability characterizes the syntax, format and organization of information. In semantic interoperability, systems should agree on a common interpretation of data. Subsequent to sharing information, the significance of the information must be protected and unaltered. There are two levels of semantic interoperability, i.e., full and partial semantic interoperability. In the partial interoperability process data are converted to an intermediate standard form that is understandable to both the sender and the receiver. In full semantic interoperability, the receiver accepts the health records in the sender's format, then converts and reproduces them based on the receiver's local standards. Some popular healthcare ontologies and EHR standards are reviewed and a list is represented in Table 8 (Lyniate, 2020; SNOMED, 2020; ICD, 2022; GO, 2022; OWL, 2022).

Table 8. *Healthcare ontologies and EHR standards.*

Healthcare ontologies	
OWL	Ontology representation as semantic web standards (generally applicable for knowledge representation)
GO	Generic information of species ranging from the molecular level to the organism level
SNOMED	Ontology based on general medical science
CARO	Facilitates interoperability between existing anatomy ontologies for different species
ICD	Used to classify diagnosis codes
EHR standards	
HL7	Facilitates clinical and administrative data sharing among different stake holders in a hospital

DICOM	Specifies the standard for medical data storage, interpretation and transmission
SNOMED-CT	Specifies the standard terms to be used in primary healthcare systems
CDA	Specifies EHR sharing in terms of documents
HL7-DS	Contains information in terms of image or coded data.
HISA	Architecture used to integrate healthcare information from different platforms

Notes: *OWL = Web Ontology Language; GO = Gene Ontology; SNOMED = Systematized Nomenclature of Medicine; CARO = Common Anatomy Reference Ontology; ICD = International Classification of Diseases; HL7 = Health Level 7; DICOM = Digital Imaging and Communications in Medicine; CDA = Clinical Document Architecture; HISA = Healthcare Information Systems Architecture.*

6.5 Limitations of interoperability for data sharing

Table 9 lists some of the challenges and barriers that might prevent blockchain-enabled patient-driven interoperability as well as solutions for overcoming these obstacles. (Belchior et al., 2021).

Table 9. *Limitation of Interoperability.*

No.	**Limitations**	**Remarks**
1	Incentives	• Investing in API frameworks to handle the competitive pressure from API-empowered frameworks while enabling non-empowered frameworks • A reward for a debt-to-credit agreement with full disclosure
2	Patient engagement	• Presentation of a patient-friendly application that allows patients to view their own records
3	Privacy and Security	• Introducing the blockchain consortium – authorized/permitted openness to reduce public transparency

7 Discussion

This review of the literature successfully identified both objective and subjective features of research that attempted to gain a comprehensive understanding of the ecosystem around EHRs in a blockchain. By responding to research inquiries, it found several common study aspects. In relation to EHR and blockchains, the challenges were emphasised along with unresolved problems, present information types, related principles, objectives, designs, and functionalities.

The main findings that are presented in this survey are related to the significance of realising EHR interoperability by means of the adoption of blockchain by healthcare service providers and the importance of open standards. In addition, different blockchain focus on addressing storage challenges (Mamun et al., 2022; Chelladurai and Pandian, 2022; Yang and Yang, 2017), such as better patient command over sensitive health information. Because of the sharing, accessibility, and integration of health information, these may be essential to improving healthcare management.

Following that, we discussed several EHR-related privacy-preserving strategies. Even if they provide data security, research needs to take certain aspects like storage and performance into account. The throughput of a blockchain process is impacted by several procedures relating to information retrieval, encryption/decryption, and compliance checks, in addition to the privacy mechanism. We compiled findings on the various privacy-preserving EHR approaches and evaluated their effectiveness. The data access times and storage costs are relatively high compared to the other existing approaches but considering the data privacy, security, data integrity and interoperability factors, the use of blockchain could be a significant approach for healthcare systems (Akhter Md Hasib et al., 2022; Chelladurai and Pandian, 2022; Mantey et al., 202; Mahajan et al., 2022; Watford et al., 2019).

7.1 Open research issues

The application of blockchain technology in the field of healthcare is an emerging field. More prototypes and proofs of concept are still to be developed by researchers to deepen the understanding of its applicability in the healthcare ecosystem. Methods, frameworks, models and architecture already proposed need to be verified thoroughly and evaluated to find out their pros and cons.

To facilitate the possibility of interoperability of patient data among different healthcare organizations or service providers, there is a need for open standards, so it is important for researchers to explore the standardization process and interoperability solutions. Also the scalability issue is a critical research problem in the field of blockchain-based healthcare systems, because of the huge volumes of data involved.

The storing of the huge volume of healthcare data in the blockchain is practically not possible, as it might lead to performance degradation. To improve the confidence of stakeholders in the use of blockchain technology, the challenges of patient data security, privacy, scalability and interoperability are considered to be the open research issues, yet more prototypes and efficient techniques are to be identified and applied to blockchain-based healthcare systems. Furthermore, the latency caused by the speed of processing transactions along with the time to load off-chain based information in a blockchain system need to be investigated.

8 Conclusion

This paper presented a systematic literature review conducted to understand the principal concepts of blockchain technology in managing data in the healthcare field. The main objective was to identify and consider the important issues, benefits, challenges of adopting blockchain in healthcare applications. The use of blockchain has extended beyond the financial sphere and shows a potential in the field of healthcare.

Examining the outcomes that were derived from the literature review, we infer that blockchain technology offers a promising solution to the common problems in the field of healthcare, such as EHR interoperability, privacy and security, auditability, and allowing patients to have control over their health information, which would help them decide and share their information based on needs. However, the use of a security scheme composed of suitable cryptographic techniques could be more appropriate to achieve higher privacy and security.

The results of our overview show that there is a need for more development in relation to semantic and cross-chain interoperability in frameworks that are currently employed by creating customised blockchain frameworks for interoperability. The most important research problem is to enable and provide a standardised mechanism for data exchange among various blockchain-based healthcare systems while protecting patient privacy. Future works and research may use this study as a foundation or source of inspiration.

Additional Information and Declarations

Conflict of Interests: The authors declare no conflict of interest.

Author Contributions: R.P.P.: Conceptualization, Methodology, Data curation, Investigation, Writing – Original draft preparation. G.P.: Supervision, Validation, Writing – Reviewing and Editing.

References

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*, e2366632. https://doi.org/10.1155/2022/2366632

Azaria, A. Ekblaw., T. Vieira., & Lippman, A. (2016). MedRec: Using Blockchain forMedical Data Access and Permission Management. In *2nd International Conference on Open and Big Data* (pp. 25-30). IEEE. https://doi.org/10.1109/OBD.2016.11

Belchior, R., Vasconcelos, A., Guerreiro, S., & Correia, M. (2021). A Survey on Blockchain Interoperability: Past, Present, and FutureTrends. *arXiv*. https://doi.org/10.48550/arXiv.2005.14282

Boumezbeur, I., & Zarour, K. (2022). Privacy Preservation and Access Control for Sharing Electronic Health Records Using Blockchain Technology. *Acta Informatica Pragensia*, *11*(1), 105–122. https://doi.org/10.18267/j.aip.176

Chelladurai, U., & Pandian, S. (2022). A novel blockchain based electronic health record automation system for healthcare. *Journal of Ambient Intelligence and Humanized Computing*, 13, 693–703. https://doi.org/10.1007/s12652-021-03163-3

Chenthara, S., Ahmed, K., Wang, H., Whittaker, F., & Chen, Z. (2020). Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology. *PLOS ONE*, *15*(12), e0243043. https://doi.org/10.1371/journal.pone.0243043

Cunha, M., Mendes, R., & Vilela, J. P. (2021). A survey of privacy-preserving mechanisms for heterogeneous data types. *Computer Science Review*, *41*, 100403. https://doi.org/10.1016/j.cosrev.2021.100403

Dubovitskaya, A., Shukla, R., Zambani, P. S., Schumacher, M., Aberer, K., Xu, Z., Idnani, N., Lachhani, R., Wang, F., Swaminathan, A., Jahangir, M., Baig, F., Chowdhry, K., Ryu, S., & Stoller, S. (2019). ACTION-EHR: Patient-Centric Blockchain-Based EHR Data Management for Cancer Care. *Journal of Medical Internet Research,* 22(8), e13598. https://doi.org/10.2196/13598

Faheem A. R., Maher O. Al-K., Waleed A. Z., Mohammad R. Al-M., Shadab A., & Ibrahim Al-S. (2021). Blockchain-Based Framework for Interoperable Electronic Health Record. *Annals of the Romanian Society for Cell Biology*, 25(3), 6486–6495.

Fan, K., Wang, S., Ren, Y., Li, H., & Yang, Y. (2018). MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain. *Journal of Medical Systems*, *42*(8), Article 136. https://doi.org/10.1007/s10916-018-0993-7

Fang, H. S. A., Tan, T. H., Tan, Y. F. C., & Tan, C. J. M. (2021). Blockchain Personal Health Records: Systematic Review. *Journal of Medical Internet Research*, *23*(4), e25094. https://doi.org/10.2196/25094

Garrido, A., Ramírez López, L. J., & Álvarez, N. B. (2021). A simulation-based AHP approach to analyze the scalability of EHR systems using blockchain technology in healthcare institutions. *Informatics in Medicine Unlocked*, *24*, 100576. https://doi.org/10.1016/j.imu.2021.100576

GO. (2022, Jan 02). *The Gene Ontology Resources*. https://geneontology.org/

Guo, R., Shi, H., Zhao, Q., & Zheng, D. (2018). Secure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain in Electronic Health Records Systems. *IEEE Access*, *6*, 11676–11686. https://doi.org/10.1109/access.2018.2801266

Hamid, H. A. A., Rahman, S. M. M., Hossain, M. S., Almogren, A., & Alamri, A. (2017). A Security Model for Preserving the Privacy of Medical Big Data in a Healthcare Cloud Using a Fog Computing Facility With Pairing-Based Cryptography. *IEEE Access*, *5*, 22313–22328. https://doi.org/10.1109/ACCESS.2017.2757844

Haque, R., Sarwar, H., Kabir, S. R., Forhat, R., Sadeq, M. J., Akhtaruzzaman, Md., & Haque, N. (2020). Blockchain-Based Information Security of Electronic Medical Records (EMR) in a Healthcare Communication System. In *Intelligent Computing and Innovation on Data Science*, (pp. 641–650). Springer. https://doi.org/10.1007/978-981-15-3284-9_69

Hashim, F., Shuaib, K., & Sallabi, F. (2021). MedShard: Electronic Health Record Sharing Using Blockchain Sharding. *Sustainability*, *13*(11), 5889. https://doi.org/10.3390/su13115889

Hathaliya, J. J., & Tanwar, S. (2020). An exhaustive survey on security and privacy issues in Healthcare 4.0. *Computer Communications*, *153*, 311–335. https://doi.org/10.1016/j.comcom.2020.02.018

ICD. (2022, Jan 02). *International Classification of Diseases, Version 10*. https://bioportal.bioontology.org/ontologies/ICD10

Kim, T.-H., Kumar, G., Saha, R., Rai, M. K., Buchanan, W. J., Thomas, R., & Alazab, M. (2020). A Privacy Preserving Distributed Ledger Framework for Global Human Resource Record Management: The Blockchain Aspect. *IEEE Access*, *8*, 96455–96467. https://doi.org/10.1109/ACCESS.2020.2995481

Li, M., Yu, S., Zheng, Y., Ren, K., & Lou, W. (2013). Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption. *IEEE Transactions on Parallel and Distributed Systems*, *24*(1), 131–143. https://doi.org/10.1109/tpds.2012.97

Liu, J., Huang, X., & Liu, J. K. (2015). Secure sharing of Personal Health Records in cloud computing: Ciphertext-Policy Attribute-Based Signcryption. *Future Generation Computer Systems*, *52*, 67–76. https://doi.org/10.1016/j.future.2014.10.014

Lin, Q., Wang, H., Pei, X., & Wang, J. (2019). Food Safety Traceability System Based on Blockchain and EPCIS. *IEEE Access*, *7*, 20698–20707. https://doi.org/10.1109/access.2019.2897792

Loukides, G., Liagouris, J., Gkoulalas-Divanis, A., & Terrovitis, M. (2014). Disassociation for electronic health record privacy. *Journal of Biomedical Informatics*, *50*, 46–61. https://doi.org/10.1016/j.jbi.2014.05.009

Lyniate. (2022, Jan 2022). *Rim Reference Information Model.* https://www.lyniate.com/knowledge-hub/rimreference-information-model/

Mahajan, H. B., Rashid, A. S., Junnarkar, A. A., Uke, N., Deshpande, S. D., Futane, P. R., Alkhayyat, A., & Alhayani, B. (2022). Integration of Healthcare 4.0 and blockchain into secure cloud-based electronic health records systems. *Applied Nanoscience,* in press. https://doi.org/10.1007/s13204-021-02164-0

Mamun, A. A., Azam, S., & Gritti, C. (2022). Blockchain-based Electronic Health Records Management: A Comprehensive Review and Future Research Direction. *IEEE Access*, 10, 5768–5789. https://doi.org/10.1109/access.2022.3141079

Mantey, E. A., Zhou, C., Srividhya, S. R., Jain, S. K., & Sundaravadivazhagan, B. (2022). Integrated Blockchain-Deep Learning Approach for Analyzing the Electronic Health Records Recommender System. *Frontiers in Public Health*, *10*. https://doi.org/10.3389/fpubh.2022.905265

Mattila, V., Rahman A., Ma, D. P., & Gauri, P. (2022). Enhancing Transaction Throughput in Public Blockchain Network Using Nested Chains. *International Journal of Social Sciences and Management Review*. 5. 257-263. https://doi.org/10.37602/IJSSMR.2022.5218

Mayer, A. H., da Costa, C. A., & Righi, R. da R. (2019). Electronic health records in a Blockchain: A systematic review. *Health Informatics Journal*, 26(2), 1273–1288. https://doi.org/10.1177/1460458219866350

Mikula, T., & Jacobsen, R. H. (2018). Identity and Access Management with Blockchain in Electronic Healthcare Records. In *21st Euromicro Conference on Digital System Design* (pp. 699-706). IEEE. http://doi.org/10.1109/DSD.2018.00008

Nchinda Ngek, E. S., Nsioge, R. M., Ngenge, M. B., & Kadia, B. M. (2019). An intriguing case of lichen simplex chronicus in an elderly sub-Saharan African with longstanding scabies and sensory neuropathy. *Pan African Medical Journal*, 34, Article 124. https://doi.org/10.11604/pamj.2019.34.124.19999

Oodle. (2022, Jan 15). *Types of Blockchain and their importance in the digital world*. https://blockchain.oodles.io/blog/types-of-blockchain-uses/

OWL. (2022, Jan 02). *Web Ontology Language*. https://www.w3.org/OWL/

Pilares, I. C. A., Azam, S., Akbulut, S., Jonkman, M., & Shanmugam, B. (2022). Addressing the Challenges of Electronic Health Records Using Blockchain and IPFS. *Sensors*, *22*(11), 4032. https://doi.org/10.3390/s22114032

Puneeth, R.P., & Parthasarathy, G. (2021). A Comprehensive Survey on Privacy-Security and Scalability Solutions for Blockchain Technology. In *Smart Intelligent Computing and Communication Technology* (pp. 173-178). IOS Press. https://doi.org/10.3233/APC210031

Qiao, R., Luo, X.-Y., Zhu, S.-F., Liu, A.-D., Yan, X.-Q., & Wang, Q.-X. (2020). Dynamic Autonomous Cross Consortium Chain Mechanism in e-Healthcare. *IEEE Journal of Biomedical and Health Informatics*, *24*(8), 2157–2168. https://doi.org/10.1109/jbhi.2019.2963437

Qu, W., Wu, L., Wang, W., Liu, Z., & Wang, H. (2020). A electronic voting protocol based on blockchain and homomorphic signcryption. *Concurrency and Computation: Practice and Experience,* 34(16), e5817. https://doi.org/10.1002/cpe.5817

Raikwar, M., Gligoroski, D., & Kralevska, K. (2019). SoK of Used Cryptography in Blockchain. *IEEE Access*, *7*, 148550–148575. https://doi.org/10.1109/access.2019.2946983

Rajput, A. R., Li, Q., & Ahvanooey, M. T. (2021). A Blockchain-Based Secret-Data Sharing Framework for Personal Health Records in Emergency Condition. *Healthcare*, *9*(2), 206. https://doi.org/10.3390/healthcare9020206

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

SNOMED. (2022, Jan 02). *SNOMED CT Standard Ontology Based on the Ontology for General Medical Science.* https://bioportal.bioontology.org/ontologies/SCTO

Sonkamble, R. G., Phansalkar, S. P., Potdar, V. M., & Bongale, A. M. (2021). Survey of Interoperability in Electronic Health Records Management and Proposed Blockchain Based Framework: MyBlockEHR. *IEEE Access*, *9*, 158367–158401. https://doi.org/10.1109/access.2021.3129284

Sorace, J., Wong, H.-H., DeLeire, T., Xu, D., Handler, S., Garcia, B., & MaCurdy, T. (2019). Quantifying The Competitiveness Of The Electronic Health Record Market And Its Implications For Interoperability. *International Journal of Medical Informatics*, 136, 104037. https://doi.org/10.1016/j.ijmedinf.2019.104037

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. https://doi.org/10.1016/j.jisa.2019.102407

Watford, S., Edwards, S., Angrish, M., Judson, R. S., & Paul Friedman, K. (2019). Progress in data interoperability to support computational toxicology and chemical safety evaluation. *Toxicology and Applied Pharmacology*, *380*, 114707. https://doi.org/10.1016/j.taap.2019.114707

Xia, Q., Sifah, E., Smahi, A., Amofa, S., & Zhang, X. (2017). BBDS: Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments. *Information*, *8*(2), Article 44. https://doi.org/10.3390/info8020044

Yan, X., Wu, Q., & Sun, Y. (2020). A Homomorphic Encryption and Privacy Protection Method Based on Blockchain and Edge Computing. *Wireless Communications and Mobile Computing*, *2020*, Article ID 8832341. https://doi.org/10.1155/2020/8832341

Yang, H., & Yang, B. (2017). A Blockchain-Based Approach to the Secure Sharing of Healthcare Data. In *Proceedings of the Norwegian Information Security Conference 2017* (pp. 100–111). NIKS.

Zhang, J., Li, Z., Tan, R., & Liu, C. (2021). Design and Application of Electronic Rehabilitation Medical Record (ERMR) Sharing Scheme Based on Blockchain Technology. *BioMed Research International*, *2021*, Article ID 3540830. https://doi.org/10.1155/2021/3540830

Zhuang, Y., Sheets, L. R., Chen, Y.-W., Shae, Z.-Y., Tsai, J. J. P., & Shyu, C.-R. (2020). A Patient-Centric Health Information Exchange Framework Using Blockchain Technology. *IEEE Journal of Biomedical and Health Informatics*, *24*(8), 2169–2176. https://doi.org/10.1109/jbhi.2020.2993072

Editorial record: The article has been peer-reviewed. First submission received on 17 March 2022. Revisions received on 12 April 2022, 16 June 2022, 13 July 2022 and 20 July 2022. Accepted for publication on 26 July 2022. The editors coordinating the peer-review of this manuscript were Mazin Abed Mohammed, Seifedine Kadry, and Oana Geman. The editor in charge of approving this manuscript for publication was Zdenek Smutny.

Special Issue: Deep Learning Blockchain-enabled Technology for Improved Healthcare Industrial Systems.

Acta Informatica Pragensia is published by Prague University of Economics and Business, Czech Republic.

ISSN: 1805-4951