Blockchains in health information systems: A literature review on use cases and status of implementation of blockchains for electronic health records

Timo Sternat, Reinhard Bernsteiner*, Christian Ploder and Thomas Dilger
Management Communication & IT, MCI The Entrepreneurial School, Innsbruck, Austria

Abstract.
BACKGROUND: The careful management of health data is crucial due to its immense value and high sensitivity. Blockchain technologies can manage data in a trustworthy way.

OBJECTIVE: The central aim is to identify the current state of blockchain technologies applied to Electronic Health Records (EHR) to identify common structures and functionalities. This common ground could be the starting point for defining clear global standards.

METHODS: A systematic literature review is used.

RESULTS: The benefits of enhancing the digitalization and cross-institutional accessibility of health data are undoubted. Four main application areas of blockchain for the EHR can be identified: storing, sharing, audit logging, and managing the identity of data accessors. Since on-chain transactions are slow and inefficient, most research promotes a hybrid approach for handling transactions as a combination of off-chain and on-chain approaches.

CONCLUSIONS: Several approaches, frameworks, and models exist for applying blockchain technologies in the context of EHR. The research revealed that a) only a few concepts are already implemented, b) the existing system implementations are based on different backgrounds and technology stacks, and c) a lack of comprehensive and global standards and norms. All these factors are barriers to a broader usage of blockchain-based EHRs.

Keywords: Blockchain, electronic health record, health information systems, off-chain data management, societal human systems, public-private health data management, systematic literature review

Timo Sternat completed his studies in Management, Communication & IT at the Management Center Innsbruck. During his studies, he worked as a Product Manager for medical universal archives and networking systems for hospitals at global supplier of Health Information Systems. He also played a significant role in the advancement of medical robots controlled through head movements in the field of microsurgery in the European market. This allowed him to gather insights from the surgical field and directly incorporate them into product development. Currently, he is involved in integrating an AI platform at a medical PACS provider.

*Corresponding author: Reinhard Bernsteiner, MCI, The Entrepreneurial School, Universitaetsstrasse 15, A-6020 Innsbruck, Austria. Tel.: +43 6764037941; E-mail: reinhard.bernsteiner@mci.edu.

Reinhard C. Bernsteiner is professor in the Academic Department "Management, Communication & IT" at MCI, Management Center Innsbruck. He is adjunct faculty member of the Department of Information Systems & Quantitative Analysis, College of Information Science & Technology at the University of Nebraska at Omaha. He holds degrees in Business Administration and Computer Science from Kepler University, Austria. His main Research Fields are Data and Information Engineering and Information Management with a focus on Big Data and Analytics. His aim is to combine the business and technical perspective on Data as a basis for innovative business models and knowledge management.

Christian Ploder: After his studies of Information Systems at the University of Innsbruck, Christian Ploder moved to the private sector in 2009 after completing his Ph.D. in information systems. As head of international IT and ERP projects in the medical device and pharmaceutical industry, he gained valuable experience in the fields of systems planning, process/project management, and leadership. Finally, his attachment to teaching and research has brought him back home to Tyrol and his current challenge at the Management Center Innsbruck as Professor for ERP Systems and Operational Excellence.

Thomas Dilger teaches and leads various research projects on different aspects of IT governance, corporate budgeting, compliance (GDPR), Web 3.0 and corporate finance. Besides his current position as Senior Lecturer, he teaches at several other universities, e.g. University of Omaha Nebraska | Executive Master of Science in Information. He specializes in the intersection of management, controlling and IT, particularly in regulated environments that have a direct impact on the financial and IT landscape of modern organizations.

1. Introduction

Many information systems exist in healthcare, usually designed and developed for particular requirements defined by single organizations and institutions. Patients trust Healthcare Information Systems (HIS) to manage health data and deliver optimal patient care effectively. However, the current state of HIS reveals a lack of interoperability that varies depending on countries, regions, providers, or stakeholders [1]. As a Healthcare Information System (HIS) component, Electronic Health Records (EHR) strive to facilitate the seamless sharing of health data across institutions. The objective is to create a comprehensive patient record encompassing all pertinent health information to ensure effective and efficient patient care. The EHR achieves this objective by offering an infrastructure that enables the management and exchange of health data between institutions, IT systems, stakeholders, and the patient [2].

An EHR adheres to interoperability standards to establish connectivity with other systems while housing sensitive patient information. As a result, it necessitates the implementation of the most suitable technology to ensure adequate protection. Numerous emerging technologies have been developed to safeguard health data's privacy, integrity, and confidentiality [3].

Blockchain has emerged as a potential solution to address these requirements. Blockchains have gained significant attention in the financial sector with the rise of cryptocurrencies like Bitcoin and Ethereum. The financial industry also shares similar demands for privacy and security regarding data management. Various organizations and researchers are looking for a possible solution for combining EHR with blockchain technologies in the healthcare sector [4]. Data leaks and successful attacks on HIS demonstrate the need for comprehensive protection of patient data in all data management activities [5].

The benefits and potential applications of blockchain technology for standardizing and streamlining the exchange of EHR are being actively discussed by hospitals, private companies, and international health and political organizations, such as the European Union (EU).

However, medical records often lack comprehensiveness, featuring incomplete and inconsistent data due to fragmentation in the healthcare landscape [6, 7]. A global standardized solution for the digital storage of all historical patient health data, called EHR, is still missing. According to [8], every patient in the US has almost 20 different health records. 150 exabytes of health data are stored yearly [9] but in various standards, rules, and regulations.

Standards that are globally implemented might support Social Development Goal 3, which is about "Goal 3: "Ensure healthy lives and promote well-being for all at all ages", which is goal 3 of the Sustainable Development Goals defined by the United Nations [10]. There is evidence that HIS supports this goal [10–14].

To address the research gap, it is crucial and pertinent to provide an overview of the current state of

blockchain technologies applied to EHR to identify common structures and functionalities.

The gap introduced, and the central aim of this research lead to the following research question: "Which blockchain use cases exist for Electronic Health Records as part of Health Information Systems, and what is the current implementation status according to relevant literature?"

From a methodological perspective, a systematic literature review should provide the basis for answering the research question.

The main contribution of this research is to identify a common ground for blockchain-based implementations of EHR. This common ground could be the starting point to define clear global standards for system compatibility in terms of data exchange, data structures, and core functions of an EHR. The paper contains contributions to health management and the scientific community and provides policy recommendations. Due to the increasing number of publications and the growing complexity of the topic over time, it is essential to methodically filter, synthesize, evaluate, and integrate the results of the research subject, evaluate and present them.

The paper is structured as follows: The most relevant terms and concepts are briefly presented after this introduction. The following section describes the methodological approach used to answer the research question. Section 5 offers the status quo of blockchain technologies in HIS and the current ideas about the European Health Data Space. The paper ends with a discussion, limitations, and a conclusion with an outlook for future research streams.

2. Central concepts and terms

This section gives an overview of central concepts and terms relevant to this work.

2.1. Blockchain

Bitcoins are the starting point of blockchain technologies. Bitcoin is a new payment network and the first decentralized currency. The cryptocurrency Bitcoin, based on blockchain, was introduced in 2008 by Satoshi Nakamoto, a pseudonym for either a person or a group of people [15].

Wang et al. state that blockchain is an Internet-based technology creating a decentralized peer-to-peer ledger through which transactions in the form of a sequence of data blocks (chain) are intercon-

nected in a timely order [16]. This way, a protected data structure is formed and prevents the tampering of blocks in the chain. Distributed Ledger Technology is an approach to sharing and recording data across different data stores called ledgers [17]. Fosso Wamba et al. analyzed 141 articles to overview various definitions of blockchain [18].

When examining various explanations of blockchain, numerous authors emphasize its characteristics of decentralization and access to information within a transparent network. This entails a peer-to-peer network that lacks a central authority but grants approval rights to all participants. Such a setup fosters an environment of democratic consensus and decentralized trust [19]. The access rights guarantee that every participant obtains a complete copy of the entire blockchain. Other authors draw attention to the cryptographic context, using a digital signature to sign and verify a transaction.

2.2. Electronic health (eHealth)

For many years, the healthcare sector has witnessed the growing significance of digital transformation. Despite this progress, communication between geographically separated health service providers remains inadequate in providing comprehensive patient care [20]. The availability of information, regardless of time and location, can enhance operational efficiency and lead to cost savings within the healthcare system as a beneficial consequence [21]. The same is true for electronic knowledge sharing among the healthcare staff.

Pagliari et al. point out the importance of referring to the functional scope of eHealth. Based on their work, they compiled 36 definitions [22]. They derived a general definition of eHealth: "eHealth is an emerging field of medical informatics, referring to the organization and delivery of health services and information using the Internet and related technologies. In a broader sense, the term characterizes not only a technical development but also a new way of working, an attitude, and a commitment to networked, global thinking to improve health care locally, regionally, and worldwide by using information and communication technology." [22].

2.3. Health information systems

As in any other domain, information systems play a crucial role in today's eHealth sector. The flood of daily collected data about patients, physicians,

nurses, pharmacists, emergency staff, and many other involved parties must be stored. The processes in health services, including surgeries, emergency and rescue operations, patient care, visitors to the general practitioner, examinations and diagnostics, health service billing, imaging, and lab analyses, are to be documented well to facilitate the best possible patient treatment [23]. Harmonizing central and decentralized systems is indispensable in an increasingly digitalized health environment.

2.4. Electronic health record

A central part of an HIS is the EHR, which represents a lifelong, time- and location-independent collection of all health-related data of a patient [24]. A central characteristic is that the entire record is in the hands of the person concerned. Patients can view all their medical-related documents, regardless of which institution created them. It is important to stress that patients own their health data. They can decide which health service provider they allow access to their documents and which institutions they deny access to.

In some cases, patients can even upload health data. One example is the evaluation result of smart fitness equipment, which a patient can upload to the EHR to complement the overall picture of his health status [25]. The EHR infrastructure bundles standardized eHealth components necessary to enable patient data management and secure health data exchange, including user authentication, access management, logging, and data storage. The EHR infrastructure provides standardized interfaces and an adaptor set to integrate IT systems, which may not yet support standardized interfaces [26].

2.5. Security and privacy of health data

Healthcare data are highly personal and must be treated very sensitively. Therefore, it needs security and the utmost care due to legal requirements on different levels [27]. The European Program for Critical Infrastructure Protection (EPCIP) is one example of safety requirements on the infrastructure level [28, 29]. For hackers, the value of stolen health data seems to be high [30, 31]. Those might sell data to third parties, such as insurance organizations interested in patients' medical history, to identify if an individual might have any conditions that could make them uninsurable in the future. The reputational and financial loss of having sensitive data leaked can be severe and potentially ruin companies and institutions, harming

the patient [32]. The consequences are immense, but ensuring the necessary security proves to be a complicated task. According to Esposito et al., ensuring the security of EHR ecosystems and the underlying systems and components that form the ecosystem is crucial yet challenging due to the interplay and complexity between the systems and components [33]. Therefore, securing this EHR ecosystem has been an active research area for companies and organizations related to healthcare [3].

The EU's General Data Protection Regulation (GDPR) is highly relevant for health data privacy and security. The GDPR has regulated data protection uniformly throughout EU member states for the first time. The European Commission and Council of the European Union introduced the regulation in 2016. At the end of the transitional period, it became a law for all EU member states in 2018 [34]. The GDPR is binding for all public and non-public data processing legal bodies with a branch in the EU, selling goods within the EU, or processing data in the EU. This means that even non-EU companies acting in the EU are in the GDPR scope and thus must comply with the regulations.

The "Healthcare Insurance Portability and Accountability Act" (HIPAA) represents essential rules and regulations and protects all health data in the United States since 1996. Within the scope of this act, data and privacy regulations preserve the availability, confidentiality, and integrity of Protected Health Information (PHI) [35].

The 21st Century Cures Act mandates the Office of the National Coordinator for Health Information Technology (ONC) to establish a framework for the interoperable exchange of electronic health information. Section 4003 of the Act instructs the ONC to "develop or support a trusted exchange framework, including a common agreement among health information networks nationally." [36]

This legislation aims to grant patients greater control over their EHR. The Cures Act and the HIPAA Privacy Rule share the common goal of safeguarding patient rights, though they achieve this through different approaches. A key element of the HIPAA Privacy Rule is the right of access provision, which requires providers to allow patients to inspect, access, and copy their medical records. The Cures Act further empowers patients by enabling them to access, exchange, and use their electronic health information as they see fit. This bipartisan legislation was crafted to enhance both patient and provider choice and access [37]. Therefore, GDPR and HIPAA form

the central legal fundament for health data privacy and protection in the respective regions.

3. Blockchain technologies in EHR

It has become apparent that applying blockchain technology in healthcare brings many advantages and challenges. Compared to cryptocurrencies, HISs are more complex due to the many stakeholders with specific requirements. In general, the patient is the center of healthcare services as the source of data generation in an HIS. The theDataMap (see Fig. 1) was created by researchers at Harvard University [38]. This map aims to identify and elucidate the individuals and entities engaged in handling a patient's data and the movement of that data among them. The authors present this map as evidence of the many actors involved in collecting, storing, transferring, and analyzing health data. Moreover, this model illustrates the information flow between these actors, providing insights into their relationships. These actors encompass humans and organizations, including human and non-human participants.

According to relevant research, blockchain opens up an opportunity to track the location of health data and exchange data to improve personal treatment outcomes, medical research, and clinical trials. Bringing eHealth to a new level through blockchain addresses two issues simultaneously: an enhancement of interoperability and adequate privacy handling of data [39–43].

Blockchain technology is the basis on which EHR can ensure security and privacy, enabling patients to control their data. Data security is crucial in the electronic processing of patient data, its digital transmission, and retrieval via various devices and platforms. Security is one of the critical arguments for implementing blockchain in the EHR context. First, research outlines blockchain can ensure data security against loss, falsification, or unauthorized access through blockchain technologies [44–47]. In GDPR terminology, blockchain guarantees health data availability, integrity, and confidentiality, the main three pillars of ensuring privacy.

Since transactions in a blockchain are slow due to the consensus mechanism of nodes, scalability, and transaction cost are the two main problems hindering blockchain technology's wide usage [48, 49]. To tackle this issue, data managed in the blockchain network (on-chain) are combined with data managed outside the blockchain (off-chain). Off-chain storage means that data is not stored directly on the blockchain but locally, e.g., in a relational database. The data inside the blockchain accesses off-chain data, for example, through metadata and hash keys. The metadata indicates where the off-chain information is located, and the key allows the on-chain data to access it. Off-chain storage is a common approach for controlling access and identities of accessors.

This integrated model aims to minimize the code executed by on-chain transactions, shifting the responsibility of connecting off-chain operations with the blockchain [50]. As a result, transaction costs are reduced, including more transactions in each block. Consequently, the waiting time for a transaction to be included in a block could be shorter. This approach offers several benefits, including lower transaction costs and latency, increased transaction throughput, and improved privacy due to fewer on-chain executions of transactions.

Different approaches exist for combining on-chain and off-chain data management [51–54].

4. Methodological approach

The methodological approach followed in this paper is oriented toward a systematic literature review. A systematic literature review is entirely based on evident (secondary) scientific literature and follows predefined steps. It is "a replicable, scientific and transparent process, in other words, a detailed technology that aims to minimize bias through exhaustive literature searches of published and unpublished studies and by providing an audit trail of the reviewer's decisions, procedures and conclusions." [55]

According to Fettke, a systematic literature review follows a classical scheme of five phases: In the problem formulation phase, the review question is formulated and specified. A literature search serves to identify the literature suitable for the research question [56]. This literature is checked for relevance during the literature evaluation and then analyzed and interpreted. The review usually ends with the presentation of the results [56].

4.1. Problem formulation

The central aim is to identify which blockchain use cases exist for Electronic Health Records as part of Health Information Systems and their current implementation status.
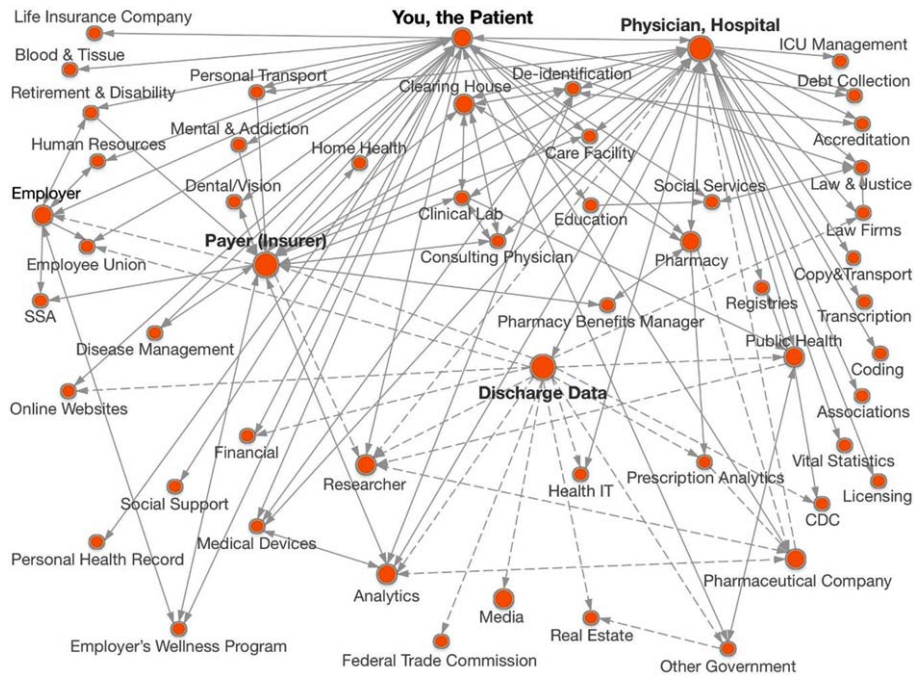
Fig. 1. The data map.

Table 1
Keywords for literature search

Search term	Combined with	Search term	Combined with	Search term
Bitcoin	+	Clinical	+	Application
Blockchain		Information		Approach
Ethereum		Systems		Architecture
Hyperledger		eHealth		Benefits
		EHR		Challenges
		Electronic Health		Frameworks
		Record		Implementation
		Health data		Model
		Health		Pitfalls
		Information		Programs
		Systems		Project
		Health Record		Regulation
		Hospital		Status quo
		Information		Storage
		Systems		System
		Electronic		Transaction
		Medical Record		Use cases

4.2. Literature search

Firstly, potentially relevant literature was identified using search terms in different databases.

Table 1 illustrates combinations of search terms to provide a basic framework for search queries. It is important to note that this search catalog is only a fundamental overview of the search criteria. Articles, studies, and reviews were included in this review if they were in English and either peer-reviewed or published in academic literature, ensuring adherence to established quality criteria. Systematic reviews were

Table 2
Overview of used scientific databases.

General databases	Technical databases	Medical databases
SpringerLink	IEEE Xplore	PubMed
Science Direct		JMIR
Emerald		

incorporated to leverage the extensive information already gathered, thereby enhancing the validation of our review. There was no limit concerning the publication date of an article. Using scientific databases facilitated the literature search according to the subject area covered. Table 2 categorizes the databases used in three sections.

Secondly, the remaining literature was screened for relevance to address the research question. The screening process started with the most recent publications. The search was extended to highly relevant articles by reviewing referenced sources in the identified body of literature.

4.3. Literature evaluation

After screening the proposed literature, irrelevant information was excluded. A further overview of relevant topics was collected by reading the abstracts and searching keywords in the text to see what topics were addressed. The data extraction took place after the selection of studies for the scope of this review. After first skimming and scanning for an overview, an in-depth reading of all selected literature was necessary to extract all relevant information from the text.

4.4. Literature analysis and interpretation

Next follows a qualitative synthesizing of the literature content and analysis of common explanations, definitions, descriptions, models, elaborations, and differences. This step also includes an interpretation of the research question.

4.5. Presentation of the results

As the last step, the findings are presented. An overview of the status quo of the combination of EHR and blockchain technology is provided. Trends, fundamental implementation standards, as well as similarities are discussed. With a focus on the research question, this literature review provides an overview of the current technology and substantial reasoning for its current implementation status.

5. Status quo of blockchain technologies in EHR

This section overviews different approaches to using blockchain technologies as part of an HER. First, typical use cases derived from literature are presented, followed by exemplary system implementations.

5.1. Use cases

According to the literature, fields of blockchain application for the EHR are manifold. A shared characteristic among these approaches is the interconnectedness of patient data encompassing medical history, diagnostics, and treatment through cooperative sharing within an immutable and trustworthy blockchain. Additionally, blockchain technology can effectively integrate other medical domains, including research and development, billing, and insurance [42, 57–59].

By leveraging blockchain technology, it becomes possible to provide the research community access to anonymized patient data. This enables the development of health-related use cases by applying big data analytics [60, 61].

Simultaneously, the outcomes of therapies and medications can be relayed to healthcare providers and the pharmaceutical industry, as Ullah et al. highlighted. Physicians and hospitals can seamlessly share their findings and treatment approaches with pharmacies, therapists, and post-treatment care facilities [62]. Laboratory results can be digitally integrated before, during, and after treatment, ensuring prompt availability to all relevant stakeholders [63]. Another notable application area is telemedicine, wherein doctors are consulted online through electronic devices [64]. Blockchain-enabled telemedicine plays a significant role in various aspects of healthcare, ranging from initial visits for minor cases to the engagement of specialists in medical history, diagnosis, and treatment, as well as follow-up care and physiotherapy. Moreover, in the ongoing COVID-19 pandemic, blockchain-powered telemedicine has emerged as a vital tool.

Dai et al. claim that blockchain can improve the analysis and transmission of patient health data, which they call the "Internet of Medical Things".

Even rehabilitation on distance and quarantine might benefit from blockchain implementation since it facilitates treatment recommendations between different health professionals and patients [65]. A commonly known improvement for an optimal patient path is the seamless, timely, complete, and consistent exchange of patient data via blockchain, which is only possible in the form of an EHR. During the literature review, four main blockchain application clusters for EHR could be identified. Those are the storage, sharing, and audit logging of health data and identity management. For a better understanding, the four applications are described in Table 3.

These four application areas are often intertwined. Most scientific papers explain a solution for a specific feature but do not clarify one-fits-all emerging technology. Others illustrate blockchain architectures within or outside the hospital for implementing different layers of blockchain to existing clinical infrastructure. Several frameworks suggest a hybrid approach by combining on-chain and off-chain data management.

5.2. Current status and challenges of implementations

Most literature about blockchain and EHR discusses frameworks, models, and concepts, but only a minor part includes actionable suggestions on implementation or a final prototype [66]. This suggests that the implementation is still at an early stage and that some unsolved challenges exist despite the advantages research and industry agree on. According to the scientific studies examined, these are primarily

a. concerns in terms of security, privacy, and data protection [67, 68].
b. computational power [69], e.g. for smart contracting or data management using blockchains.
c. high implementation and operational costs e.g. cost of operation, cost of sharing data, cost of following regulatory guidelines, and cost of maintenance [70–73]. It must be noted that EHR have the potential to reduce cost compared to traditional, non-IT-based systems [74].
d. potential resistance to blockchain due to overall negative experience with cryptocurrency [75].
e. lack of technological understanding [76].
f. lack of best practices or legal requirements, such as GDPR [76] GDPR might hinder a blockchain implementation for eHealth in the EU points out that data privacy and security requirements

are challenging to realize [77] within a supranational concept for the exchange of highly susceptible health data [78].

However, it seems interesting to glance at researchers' current propositions. The following systems are presented explicitly due to their specific characteristics and importance for other EHR systems.

Hypderledger Fabric, started by Linux Foundation, seems to be the open-source software for building a permissioned blockchain network in healthcare. Decentralized networks such as Bitcoin and Ethereum operate on a permissionless basis, enabling any node to join without the need for prior authorization. In these networks, every node can participate in the consensus mechanism. These permissionless blockchains are known for their transparency and decentralization. On the contrary, permissioned blockchains necessitate invitations for node participation. They are commonly employed in private business environments and customized for specific use cases. Power is concentrated within a limited group of validators who are crucial in making network decisions. While transparency may be restricted, permissioned blockchains often exhibit enhanced network upgrade time and scalability [79, 80].

The platform provides a public-private key infrastructure, equipping each participant (node) with a cryptographic certificate. Hyperledger Fabric uses lightweight consensus algorithms instead of the Proof of Work mechanism, using a modular toolkit for adopting fast and secure. This makes Hyperledger Fabric a powerful platform for implementing blockchains efficiently [8]. Based on the literature review, many start-ups build on this architecture for implementation.

Roehrs, da Costa, et al. implemented a blockchain prototype for EHR storage and accessing called OmniPHR prototype [81]. The model is built on a distributed peer-to-peer network structure using Hyperledger Fabric. The EHR is stored in "data blocks in the format of archetypes, which is a relational DBMS" [81] in the cloud. The project relies on openEHR, an uprising open-source health data standard specifically for EHR, as part of a complex archetype environment for more modern, easier health data exchange. Patients and health service providers access the EHR via a client module. The EHR is stored within a private blockchain network, secured via encryption (hashes), and chained to the

Table 3
Clusters of application areas of blockchains for HER

Application	Explanation	Addressed by which authors and under which topic
Storing health data	With its distributed network and consensus mechanism, the blockchain allows for secure decentralized storing option for the massive volume of sensitive EHR.	Storing large data: [91–93] Storing data securely: [32, 94–97]
Sharing health data	The health providers, especially the patients themselves, can easily access health data from any facility in a blockchain-based system. This ensures control for the patient and fast passing on of data for optimal care.	Prove of access authentication, e.g through smart contracting: [8, 81, 98–103] Interoperable sharing: [104–110] Data encryption: [111–116]
Audit logging of health data	The blockchain provides a record of all audit logs of access of any changes to an EHR, which can be very useful for later issues with the health data content, and to monitor who entered a patient's EHR and when.	[117–121]
Managing the identity of health data accessors	Following the requirement of health data privacy, blockchain permits access to EHR only to identified authorized entities by identification mechanisms.	[122–127]

previous and subsequent transactions. Access permissions are granted via smart contracting, which ensures that health data is kept private and secure. [81] Conducted availability tests with 10,000 to 40,000 simultaneous network requests. The results proved that EHRs are available at 98%. However, DICOM images can cause storage issues, even in the cloud, due to the enormous file size.

MediChain is built on Hyperledger Fabric and puts the patient in the system's center. MediChainTM is a permissioned blockchain solution for data storage and access for Big (health) Data and is scalable and extensible. It uses the permissioned Hyperledger Fabric and is both scalable and extensible. MediChain comprises three characteristics: It stores health data off-chain, manages access permissions through smart contracting emitted by the patient or service provider, and is easy to use due to an intuitive mobile or web app interface. The idea is that patients take over control of their data. Depending on the role (patient, practi-

tioner, or caregiver), the user receives a blockchain ID, labeled as data owner or requester. In addition to data storage and retrieval, appointment requests, contacting physicians, andanaging health care plans are possible over MediChain [8].

One of the most mentioned blockchain EHR systems in literature is **MedRec**. MedRec provides a hybrid solution for EHR, as most implementation examples do. The blockchain itself does not store the EHR, but its metadata and only accesses off-chain data of health facilities. Med Rec is a network rather than a service. Integration of the various stakeholders is an essential feature of this system.

Overall, most concepts and frameworks only exist theoretically. Still, some successfully implemented examples were found that prove the usefulness of blockchain technology in improving the storage, sharing, and management of EHR. Private companies and governments or supranational institutions, such as the EU, share the common goal of adapting

patient health data management to the present claim for a digitalized collaborative world.

The Estonian e-Health System is an advanced and comprehensive digital healthcare infrastructure implemented in Estonia. It is considered one of the most successful and innovative examples of a national EHR system globally. In 2016, the Estonian e-Health Foundation initiated a pilot program to launch the blockchain-based national eHealth project. This program aimed to safeguard patient data cybersecurity and effectively manage national health databases using blockchain technology. The project's primary focus was to secure activity log records associated with processing personal health information, ensuring the confidentiality and integrity of medical data at the national level. With just over 1.3 million people, Estonia integrated the blockchain-managed registry into its e-health ecosystem. This registry now functions as a decentralized monitoring system, overseeing and documenting any access or modifications made to a patient's medical data by external parties. It continuously updates and safeguards datasets while maintaining comprehensive logs for potential audits [82, 83].

Since medical data are often stored in different EHR systems, health data must be transferred between different, partly incompatible systems [84]. To combat this problem, cross-chain collaboration systems have been developed to ensure a secure and trustworthy transfer of health data between various EHRs. **MediLinker** is an example of this kind of service. One such service is MediLinker, a healthcare application designed to resolve issues of fragmented health information, patient ID management, and automating health records and credentials. MediLinker empowers patients with full access and control over their personal data, allowing them to create digital versions of their identity credentials and authorize their use by healthcare providers [85]. A comprehensive survey on patient tokenization to link data from multiple EHRs can be found in [86].

5.3. European health data space

An initiative on a larger scale is the European Health Data Space (EHDS), which was proposed in March 2022 and is still in its early stages. The EHDS refers to an EU initiative to create a secure and interconnected ecosystem for health data exchange and collaboration. It seeks to enable seamless and secure sharing of health data across borders and among various stakeholders within the EU,

including healthcare providers, researchers, policymakers, and patients. The EHDS intends to facilitate the exchange of health data to promote better healthcare outcomes, advance medical research, and support policy decision-making. The initiative aims to overcome existing barriers and improve interoperability between different healthcare systems and data sources across the EU by harnessing the potential of digital technologies and standardized data formats.

The main pillars are [87–90]:

Interoperability: Promoting common standards and technical specifications ensures seamless and secure health data exchange across different systems and stakeholders.

Data governance: Establishing a data governance and protection framework to safeguard health data's privacy and security. This includes adhering to the EU's GDPR and other relevant regulations.

Access and portability: Enabling individuals to have greater control over their health data and facilitating their access to their health information while supporting data portability between healthcare providers and across borders

Research and innovation: Promoting research collaborations by facilitating access to health data for scientific and innovation purposes while ensuring appropriate privacy and ethical safeguards.

Citizen empowerment: Fostering citizens' engagement and empowerment by providing access to reliable health information, digital tools, and services to support their healthcare decisions and promote personalized care.

The EHDS aims to strengthen the European healthcare ecosystem, improve healthcare delivery, accelerate medical research, and contribute to evidence-based policymaking. It aspires to facilitate the secure and responsible use of health data to unlock its full potential for the benefit of individuals, healthcare professionals, and society. Based on the intentions and pillars of the system, it can be assumed that blockchain technologies will play a role in its implementation.

6. Discussion

Based on a systematic literature review, some common aspects and differences in blockchain-based EHR approaches should be highlighted throughout the examined studies, legal papers, journal articles, conference proceedings, reports, etc. Based on the literature review results, this chapter serves to

answer the underlying research question of this paper: "Which blockchain use cases exist for Electronic Health Records as part of Health Information Systems, and what is the current implementation status according to relevant literature?"

The presented implementation examples give an overview of current attempts to introduce blockchain technology for EHR systems and what concepts have made it to the market. Blockchain implementation for EHR systems can be clustered into four groups, as presented in Table 4.

The findings can be split up into three fields: practical, technical, and regulatory challenges.

6.1. Practical challenges

Even though some blockchain-based EHRs have already shown success, some concepts and ideas of EHRs that do not have a concrete implementation plan are presented. Some suggestions outline the potential for EHR without a concrete implementation plan. For some frameworks, prototypes already exist to prove the concept. The research revealed that most proposals suggest a build-up layer on existing healthcare systems frameworks like Hyperledger Fabric.

Little literature suggests a general approach for implementation, whereas the majority describes one specific concept or model in detail. A one-fits-all solution for applying blockchain technologies for EHR is not proposed due to different standards, infrastructure, health systems, and health data handling rules. Before standard base functions can be designed, all stakeholders must be invited to collect detailed requirements. This is a prerequisite for the acceptance of any system.

The considerable effort and cost for implementation, as well as the potential savings, must be considered.

6.2. Technical challenges

Since medical records contain highly sensitive data, ensuring that data is only accessible to authorized individuals while maintaining privacy is challenging.

Storing large volumes of medical records on the blockchain is impractical due to its size. Solutions like off-chain storage with on-chain references need to be designed. Most authors propose a hybrid approach combining on-chain and off-chain data management. Several options for this hybrid data management are available.

Traditional blockchains, like Bitcoin and Ethereum, have limited transaction throughput. The high volume of transactions in healthcare requires a scalable solution. Blockchain transactions can take time to be confirmed, which may not be acceptable for real-time medical applications requiring immediate access to records. Most systems use the Proof of Stake algorithm.

Facilitating seamless data exchange between healthcare providers and systems using blockchain implementations requires robust interoperability protocols. While data can be encrypted, managing keys and ensuring that encryption standards are up-to-date and effective is complex. Ensuring blockchain systems comply with existing healthcare data standards and integrate with legacy systems is difficult.

6.3. Regulatory challenges

Regulations for blockchain EHRs vary by country and region, but they generally focus on ensuring privacy, security, and interoperability. Clarifying and managing data ownership and control rights in a decentralized network can be complex.

Within the European Union, the GDPR regulates the processing of personal data, including health data. Blockchain solutions must ensure data protection principles and data sovereignty.

In the United States, two acts are central to implementing and providing EHR systems. HIPAA ensures the privacy and security of health information and requires entities to implement safeguards to protect health information. The Cures Act promotes interoperability and patient access to health records.

Regulatory bodies and standards organizations are continually evolving their guidelines to keep up with the advancements in blockchain technology and its applications in healthcare. It is crucial for entities utilizing blockchain for EHRs to stay informed and compliant with these regulations to ensure this technology's safe and effective use

6.4. Limitations

Finally, it is essential to consider the study's limitations critically. First, as in every literature review, the examined literature reflects only a part of all blockchain research concerning EHR. Thus, the results are only an excerpt of the current status quo. Furthermore, some implemented concepts might not be addressed in scientific literature since it was found that more information on blockchain

Table 4
Description of the four clusters of blockchain application in HER

Application	Explanation
Storing health data	With its distributed network and consensus mechanism, the blockchain allows for a secure decentralized storing option for the massive volume of sensitive EHR.
Sharing health data	Health providers, especially patients, can easily access health data from any facility in a blockchain-based system. This ensures control for the patient and fast passing on of data for optimal care.
Audit logging of health data	The blockchain provides a record of all audit logs of access of any changes to an EHR, which can be very useful for later issues with the health data content, and to monitor who entered a patient's EHR and when.
Managing the identity of health data accessors	Following the requirement of health data privacy, blockchain permits access to EHR only to identified authorized entities by identification mechanisms.

trends is available in the media, which was not in the scope of this review. Since unreliable resources were excluded from the analysis, some use cases that deserve discussion are likely not addressed.

Even though no particular focus on a region or continent is set, most studies were about European or US approaches to blockchain implementation for EHR. This seems especially striking since many of the respective sources come from other countries, especially Asian countries. This bias on some world regions more than others brings with it that the status quo of blockchain for EHR in this paper might not reflect the situation in all countries equally. Further research is needed to examine global differences in this topic. Due to the authors' professional experiences in healthcare, it also needs to be mentioned that they cannot entirely avoid personal bias. However, the focus on blockchain as a new field of knowledge and the keyword-based literature review helped mitigate any potential bias.

7. Conclusion

While the literature has identified numerous use cases for blockchain in Electronic Health Records (EHR), additional application possibilities will likely emerge. Companies can leverage these findings to gain crucial insights into securing and providing access to medical data for all relevant authorities along the patient journey. Managing this kind of human system requires special attention to both sides: the interest of patients as data owners and, finally, society in improving the public health system. Successful blockchain implementation in healthcare institutions could significantly advance patient care's functional effectiveness, efficiency, and productivity.

However, achieving this would necessitate international collaboration and a regulatory framework to ensure global EHR standards. Like Sweden or Estonia's approach, a global blockchain EHR consortium would be ideal for promoting interoperability and digitizing secured EHR across stakeholders.

The importance of a standardized EHR solution is undeniable. However, institutions like the EU still critically discuss blockchain due to challenges such as implementation costs and the need for a universally suitable consensus mechanism. The key challenge lies in achieving granular-level interoperability of blockchain technology for EHR, as the secure data exchange between individuals and parties with legitimate interests using state-of-the-art technologies. Despite the promising application of blockchain in EHR, there is a considerable journey ahead to establish an international blockchain healthcare solution. Many countries, including Germany, still lack an EHR for patients, relying on various records and files. Nevertheless, ongoing research reflects positive strides toward standardizing and securing our most sensitive data.

Most existing literature predominantly delves into the technical aspects of blockchain-based EHRs. For these systems to succeed, all relevant stakeholders must commit to and utilize them, ensuring the integration of HIS and EHR platforms is successful and viable. Broad acceptance becomes a critical success factor given stakeholders' diverse interests and requirements. Additionally, integrating advanced data analytics and artificial intelligence emerges as crucial aspects in the realm of eHealth systems.

This research contributes to the scientific community and healthcare management on information technologies used in EHR systems by providing an

overview of blockchain implementations and their common functional areas. The results show that different HER systems are based on various standards. Furthermore, the distribution of data on-chain and off-chain storage is handled in different ways. All this leads to several incomplete EHR systems, which can be considered a barrier to broad usage in the health sector. A global working group should be initiated to define standards and norms for better interoperability of EHR systems as a societal human system. Finally, these standards and norms should be formally implemented as policies based on a legal foundation. Those measures can potentially promote number three of the Sustainable Development Goals.

Acknowledgments

Author contributions

For every author, his or her contribution to the manuscript needs to be provided using the following categories: CONCEPTION: Sternat, Timo; Bernsteiner, Reinhard; Ploder, Christian and Dilger, Thomas

METHODOLOGY: Sternat, Timo; Bernsteiner, Reinhard; Ploder, Christian and Dilger, Thomas

DATA COLLECTION: Sternat, Timo and Bernsteiner, Reinhard

INTERPRETATION OR ANALYSIS OF DATA: Sternat, Timo

PREPARATION OF THE MANUSCRIPT: Sternat, Timo and Bernsteiner, Reinhard

REVISION FOR IMPORTANT INTELLECTUAL CONTENT: Sternat, Timo and Bernsteiner, Reinhard; Ploder, Christian and Dilger, Thomas

SUPERVISION: Bernsteiner, Reinhard.

References

[1] Kobusinge G. Putting Interoperability on Health-information-systems' Implementation Agenda. In: Bui T, editor. Putting Interoperability on Health-information-systems' Implementation Agenda; 2020. Hawaii International Conference on System Sciences.

[2] Winter A, Haux R, Ammenwerth E, Brigl B, Hellrung N, Jahn F. Health Information Systems. London: Springer London 2011.

[3] Puppala M, He T, Yu X, Chen S, Ogunti R, Wong STC. Data security and privacy management in healthcare applications and clinical data warehouse environment. In: Data security and privacy management in healthcare applications and clinical data warehouse environment; 2016. IEEE; 5-8.

[4] Dubovitskaya A, Xu Z, Ryu S, Schumacher M, Wang F. Secure and trustable electronic medical records sharing using blockchain. In: Secure and trustable electronic medical records sharing using blockchain; 2017; 650.

[5] An S, Xiao C, Stewart WF, Sun J. Longitudinal Adversarial Attack on Electronic Health Records Data. In: Liu L, White R, editors. Longitudinal Adversarial Attack on Electronic Health Records Data; 2019. New York, NY, USA: ACM; 2558-64.

[6] Moon S, Carlson LA, Moser ED, Agnikula K, Bhavani S, Smith CY, Rocca WA, Gazzuola Rocca L, Bielinski SJ, Liu H, Larson NB. Identifying Information Gaps in Electronic Health Records by Using Natural Language Processing: Gynecologic Surgery History Identification. J Med Internet Res 2022;24(1):e29015 [https://doi.org/10.2196/29015] [PMID: 35089141]

[7] Shabo A. Electronic Health Record. In: Liu L, Özsu MT, editors. Encyclopedia of Database Systems. New York, NY: Springer New York 2017; 1-6.

[8] Rouhani S, Butterworth L, Simmons AD, Humphery DG, Deters R. MediChain TM : A Secure Decentralized Medical Data Asset Management System. In: MediChain TM : A Secure Decentralized Medical Data Asset Management System; 2018. IEEE; 1533-8.

[9] CORDIS - EU research results. My Health My Data: MHMD; 2019. Available from: URL: http://www.myhealthmydata.eu/why-mhmd/.

[10] UN General Assembly. Transforming Our World: The 2030 Agenda for Sustainable Development, 21 October 2015, A/RES/70/1 2015.

[11] Chirchir LK, Aruasa WK, Chebon SK. Technical factors influencing electronic health records adoption by nurses at Moi Teaching and Referral Hospital, Kenya. African Journal of Science, Technology, Innovation and Development 2021;13(5):551-8 [https://doi.org/10.1080/20421338.2020.1777676]

[12] Shapiro LM, Kamal RN. Implementation of Electronic Health Records During Global Outreach: A Necessary Next Step in Measuring and Improving Quality of Care. J Hand Surg Am 2022;47(3):279-83 [https://doi.org/10.1016/j.jhsa.2021.09.016] [PMID: 34756514]

[13] Hagel C, Paton C, Mbevi G, English M. Data for tracking SDGs: Challenges in capturing neonatal data from hospitals in Kenya. BMJ Glob Health 2020;5(3):e002108 [https://doi.org/10.1136/bmjgh-2019-002108] [PMID: 32337080]

[14] Suthar AB, Khalifa A, Joos O, Manders EJ, Abdul-Quader A, Amoyaw Frank, Aoua C, Aynalem G, Barradas D, Bello G, Bonilla L, Cheyip M, Dalhatu IT, Klerk M, Dee J, Hedje J, Jahun I, Jantaramanee S, Kamocha S, Lerebours L, Lobognon LR, Lote N, Lubala L. National health information systems for achieving the Sustainable Development Goals. BMJ Open 2019;9(5):e027689 [https://doi.org/10.1136/bmjopen-2018-027689] [PMID: 31101699]

[15] Zhou Y, Luo X, Zhou M. Cryptocurrency transaction network embedding from static and dynamic perspectives: An overview. IEEE/CAA Journal of Automatica Sinica. 2023;10(5):1105-21.

[16] Wang X, Zha X, Ni W, Liu RP, Guo YJ, Niu X, Zheng K. Survey on blockchain for Internet of Things. Computer Communications. 2019;136:10-29 [https://doi.org/10.1016/j.comcom.2019.01.006]

[17] Park Y-H, Kim Y, Lee S-O, Ko K. Secure Outsourced Blockchain-Based Medical Data Sharing System Using Proxy Re-Encryption. Applied Sciences. 2021;11(20):9422 [https://doi.org/10.3390/app11209422]

[18] Fosso Wamba S, Kala Kamdjoug JR, Epie Bawack R, Keogh JG. Bitcoin, Blockchain and Fintech: A systematic review and case studies in the supply chain. Production Planning & Control. 2020;31(2-3):115-42 [https://doi.org/10.1080/09537287.2019.1631460]

[19] Witzig P, Salomon V. Cutting out the middleman: A case study of blockchain technology induced reconfigurations in the Swiss financial services industry. In: Kraus D, Obrist T, Hari O, editors. Blockchains, Smart Contracts, Decentralised Autonomous Organisations and the Law. Edward Elgar Publishing 2019.

[20] Lapão LV. The Future of Healthcare: The Impact of Digitalization on Healthcare Services Performance. In: Pereira Neto A, Flynn MB, editors. The Internet and Health in Brazil. Cham: Springer International Publishing 2019;435-49.

[21] Lokshina I, Lanting C. A Qualitative Evaluation of IoT-Driven eHealth: Knowledge Management, Business Models and Opportunities, Deployment and Evolution. In: Kryvinska N, Greguš M, editors. Data-Centric Business and Applications. Cham: Springer International Publishing 2019; 23-52.

[22] Pagliari C, Sloan D, Gregor P, Sullivan F, Detmer D, Kahan JP, Oortwijn W, MacGillivray S. What is eHealth (4): A scoping exercise to map the field. J Med Internet Res 2005;7(1):e9 [https://doi.org/10.2196/jmir.7.1.e9] [PMID: 15829481]

[23] Haux R. Health information systems - past, present, future. Int J Med Inform 2006;75(3-4):268-81 [https://doi.org/10.1016/j.ijmedinf.2005.08.002] [PMID: 16169771]

[24] Grasso GM, Cuzzocrea A, Nucita A. A Patient-Centric Distributed Architecture for Electronic Health Record Systems. In: A Patient-Centric Distributed Architecture for Electronic Health Record Systems; 2014. IEEE; 83-90.

[25] Sujansky W, Kunz D. A standard-based model for the sharing of patient-generated health information with electronic health records. Pers Ubiquit Comput 2015;19(1):9-25 [https://doi.org/10.1007/s00779-014-0806-z]

[26] Arsad FS, Syed Soffian SS, Megat Kamaruddin, Puteri Sofia Nadira, Nordin NR, Baharudin MH, Baharudin Ummi M, Hassan MR, Mohamed N Azmawati, Ahmad N. The Impact of eHealth Applications In Healthcare Intervention: A Systematic Review. Journal of Health Research. 2022;37(3):6.

[27] Babu ES, Yadav BVRN, Nikhath AK, Nayak SR, Alnumay W. MediBlocks: Secure exchanging of electronic health records (EHRs) using trust-based blockchain network with privacy concerns. Cluster Comput. 2023;26(4):2217-44 [https://doi.org/10.1007/s10586-022-03652-w]

[28] Pursiainen C, Kytömaa E. From European critical infrastructure protection to the resilience of European critical entities: What does it mean? Sustainable and Resilient Infrastructure 2023;8(sup1):85-101 [https://doi.org/10.1080/23789689.2022.2128562]

[29] Yang Z, Barroca B, Weppe A, Bony-Dandrieux A, Laffréchine K, Daclin N, November V, Omrane K, Kamissoko D, Benaben F, Dolidon H, Tixier J, Chapurlat V. Indicator-based resilience assessment for critical infrastructures - A review. Safety Science 2023;160:106049 [https://doi.org/10.1016/j.ssci.2022.106049]

[30] He Y, Zamani E, Yevseyeva I, Luo C. Artificial Intelligence-Based Ethical Hacking for Health Information Systems: Simulation Study. J Med Internet Res 2023;25:e41748 [https://doi.org/10.2196/41748] [PMID: 37097723]

[31] Raghupathi W, Raghupathi V, Saharia A. Analyzing Health Data Breaches: A Visual Analytics Approach. AppliedMath 2023;3(1):175-99 [https://doi.org/10.3390/appliedmath3010011]

[32] Al Omar A, Rahman MS, Basu A, Kiyomoto S. MediBchain: A Blockchain Based Privacy Preserving Platform for Healthcare Data. In: Wang G, Atiquzzaman M, Yan Z, Choo K-KR, editors. Security, Privacy, and Anonymity in Computation, Communication, and Storage. Cham: Springer International Publishing 2017;534-43.

[33] Esposito C, Santis A de, Tortora G, Chang H, Choo K-KR. Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? IEEE Cloud Comput. 2018;5(1):31-7 [https://doi.org/10.1109/MCC.2018.011791712]

[34] Hach I, Meseli F. Nicht-Interventionelle Studien am Kommunalen Grosskrankenhaus und die Umsetzung der Datenschutzgrundverordnung (DSGVO). Gesundheitswesen 2022;84(1):75-9 [https://doi.org/10.1055/a-1192-5114] [PMID: 32693417]

[35] Oh SH, Kang M, Lee Y. Protected Health Information Recognition by Fine-Tuning a Pre-training Transformer Model. Healthc Inform Res 2022;28(1):16-24 [https://doi.org/10.4258/hir.2022.28.1.16] [PMID: 35172087]

[36] Savage L. Playing with FHIR: The Path to Ensuring We Bring the Power of Supercomputing to How We Understand Healthcare in Medicine. In: Douville S, Marx EW, editors. Advanced Health Technology: Managing Risk While Tackling Barriers to Rapid Acceleration. New York, NY: Routledge 2023;291-304.

[37] Arvisais-Anhalt S, Lau M, Lehmann CU, Holmgren AJ, Medford, RJ, Ramirez CM, Chen, CN. The 21st Century Cures Act and Multiuser Electronic Health Record Access: Potential Pitfalls of Information Release. J Med Internet Res 2022;24(2):e34085 [https://doi.org/10.2196/34085] [PMID: 35175207]

[38] Harvard University. The Data Map [cited 2023 July 13] Available from: URL: https://thedatamap.org.

[39] Gordon WJ, Catalini C. Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability. Comput Struct Biotechnol J 2018;16:224-30 [https://doi.org/10.1016/j.csbj.2018.06.003] [PMID: 30069284]

[40] Zhang P, Walker MA, White J, Schmidt DC, Lenz G. Metrics for assessing blockchain-based healthcare decentralized apps. In: Metrics for assessing blockchain-based healthcare decentralized apps; 2017. IEEE; 1-4.

[41] Kevin J. Peterson, Rammohan Deeduvanu, Pradip Kanjamala, Kelly Boles Mayo. A Blockchain-Based Approach to Health Information Exchange Networks. In: Proc. NIST Workshop Blockchain Healthcare.

[42] Girardi F, Gennaro G de, Colizzi L, Convertini N. Improving the Healthcare Effectiveness: The Possible Role of EHR, IoMT and Blockchain. Electronics 2020;9(6):884 [https://doi.org/10.3390/electronics9060884]

[43] Zhuang Y, Chen Y-W, Shae Z-Y, Shyu C-R. Generalizable Layered Blockchain Architecture for Health Care Applications: Development, Case Studies, and Evaluation. J Med Internet Res 2020;22(7):e19029 [https://doi.org/10.2196/19029] [PMID: 32716300]

[44] Dinh TTA, Liu R, Zhang M, Chen G, Ooi BC, Wang J. Untangling Blockchain: A Data Processing View of Blockchain Systems. IEEE Trans. Knowl. Data Eng. 2018;30(7):1366-85 [https://doi.org/10.1109/TKDE.2017.2781227]

[45] Liu L, White R, editors. The World Wide Web Conference. New York, NY, USA: ACM; 2019.

[46] Saxena D, Verma JK. Blockchain for public health: Technology, applications, and a case study. In: Computational Intelligence and Its Applications in Healthcare. Elsevier 2020;53-61.

[47] Shi S, He D, Li L, Kumar N, Khan MK, Choo K-KR. Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. Comput Secur 2020;97:101966 [https://doi.org/10.1016/j.cose.2020.101966] [PMID: 32834254]

[48] Kim S, Kwon Y, Cho S. A Survey of Scalability Solutions on Blockchain. In: A Survey of Scalability Solutions on Blockchain; 2018. IEEE; 1204-7.

[49] Zhou Q, Huang H, Zheng Z, Bian J. Solutions to Scalability of Blockchain: A Survey. IEEE Access 2020;8:16440-55 [https://doi.org/10.1109/ACCESS.2020.2967218]

[50] Gudgeon L, Moreno-Sanchez P, Roos S, McCorry P, Gervais A. SoK: Layer-Two Blockchain Protocols. In: Bonneau J, Heninger N, editors. Financial Cryptography and Data Security. Cham: Springer International Publishing 2020; 201-26.

[51] Salve A de, Franceschi L, Lisi A, Mori P, Ricci L. L2DART: A Trust Management System Integrating Blockchain and Off-Chain Computation. ACM Trans. Internet Technol. 2023;23(1):1-30 [https://doi.org/10.1145/3561386]

[52] Campanile L, Iacono M, Marulli F, Mastroianni M. Designing a GDPR compliant blockchain-based IoV distributed information tracking system. Information Processing & Management 2021;58(3):102511 [https://doi.org/10.1016/j.ipm.2021.102511]

[53] Miyachi K, Mackey TK. hOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design. Information Processing & Management 2021;58(3):102535 [https://doi.org/10.1016/j.ipm.2021.102535]

[54] Jayabalan J, Jeyanthi N. Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy. Journal of Parallel and Distributed Computing 2022;164:152-67 [https://doi.org/10.1016/j.jpdc.2022.03.009]

[55] Tranfield D, Denyer D, Smart P. Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review. Br J Management 2003;14(3):207-22 [https://doi.org/10.1111/1467-8551.00375]

[56] Fettke P. State-of-the-Art des State-of-the-Art. Wirtsch. Inform. 2006;48(4):257–66 [https://doi.org/10.1007/s11576-006-0057-3]

[57] Akkaoui R, Hei X, Cheng W. EdgeMediChain: A Hybrid Edge Blockchain-Based Framework for Health Data Exchange. IEEE Access 2020;8:113467-86 [https://doi.org/10.1109/ACCESS.2020.3003575]

[58] Murugan A, Chechare T, Muruganantham B, Kumar SG. Healthcare information exchange using blockchain technology. IJECE 2020;10(1):421 [https://doi.org/10.11591/ijece.v10i1.pp421-426]

[59] Patil RM, Kulkarni R. Universal Storage and Analytical Framework of Health Records using Blockchain Data from Wearable Data Devices. In: Universal Storage and Analytical Framework of Health Records using Blockchain Data from Wearable Data Devices; 2020. IEEE; 311-7.

[60] Dwivedi AD, Srivastava G, Dhar S, Singh R. A Decentralized Privacy-Preserving Healthcare Blockchain for IoT. Sensors (Basel) 2019;19(2):326 [https://doi.org/10.3390/s19020326] [PMID: 30650612]

[61] Hasselgren A, Kralevska K, Gligoroski D, Pedersen SA, Faxvaag A. Blockchain in healthcare and health sciences- A scoping review. Int J Med Inform 2020;134:104040 [https://doi.org/10.1016/j.ijmedinf.2019.104040] [PMID: 31865055]

[62] Ullah HS, Aslam S, Arjomand N. Blockchain in Healthcare and Medicine: A Contemporary Research of Applications, Challenges, and Future Perspectives; 2020 Mar 30.

[63] Dubovitskaya A, Novotny P, Xu Z, Wang F. Applications of Blockchain Technology for Data-Sharing in Oncology: Results from a Systematic Literature Review. Oncology 2020;98(6):403-11 [https://doi.org/10.1159/000504325] [PMID: 31794967]

[64] Ichikawa D, Kashiyama M, Ueno T. Tamper-Resistant Mobile Health Using Blockchain Technology. JMIR Mhealth Uhealth 2017;5(7):e111 [https://doi.org/10.2196/mhealth.7938] [PMID: 28747296]

[65] Dai H-N, Imran M, Haider N. Blockchain-Enabled Internet of Medical Things to Combat COVID-19. IEEE Internet Things M. 2020;3(3):52-7 [https://doi.org/10.1109/IOTM.0001.2000087]

[66] Chukwu E, Garg L. A Systematic Review of Blockchain in Healthcare: Frameworks, Prototypes, and Implementations. IEEE Access 2020;8:21196-214 [https://doi.org/10.1109/ACCESS.2020.2969881]

[67] Saxena S, Arya N, Bharti SK, Dwivedi V. A Lightweight and Efficient Scheme for e-Health Care System using

Blockchain Technology. In: A Lightweight and Efficient Scheme for e-Health Care System using Blockchain Technology; 2023. IEEE; 1-5.

[68] Lin C-P, Wu Z-Y, Liu C-H. Privacy Protection Scheme for Personal Health Record System Using Blockchain Based on Homomorphic Encryption. In: Privacy Protection Scheme for Personal Health Record System Using Blockchain Based on Homomorphic Encryption; 2023. IEEE; 212-5.

[69] Hannan A. A Blockchain Technology to Secure Electronic Health Records in Healthcare System. London Journal of Research In Computer Science and Technology 2023;23(1):1-13.

[70] Aste T, Tasca P, Di Matteo T. Blockchain Technologies: The Foreseeable Impact on Society and Industry. Computer 2017;50(9):18-28 [https://doi.org/10.1109/MC.2017.3571064]

[71] Mamun Q. RETRACTED: Blockchain technology in the future of healthcare. Smart Health 2022;23:100223 [https://doi.org/10.1016/j.smhl.2021.100223]

[72] Deloitte. Blockchain to blockchains in life sciences and health care: What broader integration is making possible today; 2018 [cited 2024 June 25] Available from: URL: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/life-sciences-health-care/us-lshc-tech-trends2-blockchain.pdf.

[73] Clohessy T, Treiblmaier H, Acton T, Rogers N. Antecedents of blockchain adoption: An integrative framework. Strategic Change 2020;29(5):501-15 [https://doi.org/10.1002/jsc.2360]

[74] Alzahrani S, Daim T, Choo K-KR. Assessment of the Blockchain Technology Adoption for the Management of the Electronic Health Record Systems. IEEE Trans. Eng. Manage. 2023;70(8):2846-63 [https://doi.org/10.1109/TEM.2022.3158185]

[75] Cunningham JA, Ainsworth JD. Enabling Patient Control of Personal Electronic Health Records Through Distributed Ledger Technology. Studies in health technology and informatics 2017;245:45-8.

[76] Durneva P, Cousins K, Chen M. The Current State of Research, Challenges, and Future Research Directions of Blockchain Technology in Patient Care: Systematic Review. J Med Internet Res 2020;22(7):e18619 [https://doi.org/10.2196/18619] [PMID: 32706668]

[77] Koumpounis S, Perry M. Blockchain-based electronic health record system with patient-centred data access control. In: Blockchain-based electronic health record system with patient-centred data access control; 2023. IEEE; 17-24.

[78] Finck M. Blockchains and Data Protection in the European Union. SSRN Journal 2017 [https://doi.org/10.2139/ssrn.3080322]

[79] Gans J. Permissioned Versus Permissionless. In: Gans J, editor. The Economics of Blockchain Consensus. Cham: Springer International Publishing 2023; 51-67.

[80] Díaz Á, Kaschel H. Scalable Electronic Health Record Management System Using a Dual-Channel Blockchain Hyperledger Fabric. Systems 2023;11(7):346 [https://doi.org/10.3390/systems11070346]

[81] Roehrs A, Da Costa CA, Da Rosa Righi R, Da Silva VF, Goldim JR, Schmidt DC. Analyzing the perfor-

mance of a blockchain-based personal health record implementation. J Biomed Inform 2019;92:103140 [https://doi.org/10.1016/j.jbi.2019.103140] [PMID: 30844481]

[82] Kassen M. Blockchain and e-government innovation: Automation of public information processes. Information Systems 2022;103:101862 [https://doi.org/10.1016/j.is.2021.101862]

[83] Malik A, Bhushan B, Parihar V, Karim L, Cengiz K. Blockchain-Powered Smart E-Healthcare System: Benefits, Use Cases, and Future Research Directions. In: Ahad MA, Casalino G, Bhushan B, editors. Enabling Technologies for Effective Planning and Management in Sustainable Smart Cities. Cham: Springer International Publishing 2023; 203-28.

[84] Hu M, Sheng F. Blockchain-enabled cross-chain collaboration model for elderly health information from a whole process perspective. Front Public Health 2023;11:1081539 [https://doi.org/10.3389/fpubh.2023.1081539] [PMID: 36969615]

[85] Bautista JR, Harrell DT, Hanson L, Oliveira E, Abdul-Moheeth M, Meyer ET, Khurshid A. MediLinker: A blockchain-based decentralized health information management platform for patient-centric healthcare. Front Big Data 2023;6:146023 [https://doi.org/10.3389/fdata.2023.1146023] [PMID: 37426689]

[86] Zhuang Y, Shyu C-R, Hong S, Li P, Zhang L. Self-sovereign identity empowered non-fungible patient tokenization for health information exchange using blockchain technology. Comput Biol Med 2023;157:106778 [https://doi.org/10.1016/j.compbiomed.2023.106778] [PMID: 36934533]

[87] Hussein R, Scherdel L, Nicolet F, Martin-Sanchez F. Towards the European Health Data Space (EHDS) ecosystem: A survey research on future health data scenarios. Int J Med Inform 2023;170:104949 [https://doi.org/10.1016/j.ijmedinf.2022.104949] [PMID: 36521422]

[88] Bradjašević E. Implementation of the Regulation on the European Health Data Space (EHDS) in Croatia. In: Hägglund M, editor. Caring Is Sharing – Exploiting the Value in Data for Health and Innovation: Proceedings of MIE 2023. 1st ed. Amsterdam: IOS Press Incorporated 2023.

[89] Marelli L, Stevens M, Sharon T, van Hoyweghen I, Boeckhout M, Colussi I, Degelsegger-Máarquez A, El-Sayed S, Hoeyer K, van Kessel R, Zając DK, Matei M, Roda S, Prainsack B, Schlünder I, Shabani M, Southerington T. The European health data space: Too big to succeed? Health Policy 2023;135:104861 [https://doi.org/10.1016/j.healthpol.2023.104861] [PMID: 37399677]

[90] Chemini N, Hioual O, Hemam SM. Semantic Interoperability in Electronic Health Record System Based on Blockchain Technology: A Survey. In: Semantic Interoperability in Electronic Health Record System Based on Blockchain Technology: A Survey; 2023. IEEE; 1-8.

[91] Zheng X, Mukkamala RR, Vatrapu R, Ordieres-Mere J. Blockchain-based Personal Health Data Sharing Sys-

tem Using Cloud Storage. In: Blockchain-based Personal Health Data Sharing System Using Cloud Storage; 2018–1-6.

[92] MTBC. MTBC Takes Electronic Health Records to the Next Level with Blockchain Technology; 2018 [cited 2020 September 7] Available from: URL: https://www.globenewswire.com/news-release/2018/06/27/1530349/0/en/MTBC-Takes-Electronic-Health-Records-to-the-Next-Level-with-Blockchain-Technology.html.

[93] Liu J, Li X, Ye L, Zhang H, Du X, Guizani M. BPDS: A Blockchain Based Privacy-Preserving Data Sharing for Electronic Medical Records. In: BPDS: A Blockchain Based Privacy-Preserving Data Sharing for Electronic Medical Records; 2018. Piscataway, NJ: IEEE; 1-6.

[94] Zhao H, Zhang Y, Peng Y, Xu R. Lightweight Backup and Efficient Recovery Scheme for Health Blockchain Keys. In: Lightweight Backup and Efficient Recovery Scheme for Health Blockchain Keys; 2017. Piscataway, NJ: IEEE; 229-34.

[95] Kim M, Yu S, Lee J, Park Y, Park Y. Design of Secure Protocol for Cloud-Assisted Electronic Health Record System Using Blockchain. Sensors (Basel) 2020;20(10):2913 [https://doi.org/10.3390/s20102913] [PMID: 32455635]

[96] Heston TF. A Case Study in Blockchain Health Care Innovation. International Journal of Current Research 2017;9(11):60587-8.

[97] Guo R, Shi H, Zhao Q, Zheng D. Secure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain in Electronic Health Records Systems. IEEE Access 2018;6:11676-86 [https://doi.org/10.1109/ACCESS.2018.2801266]

[98] Nguyen DC, Pathirana PN, Ding M, Seneviratne A. Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems. IEEE Access 2019;7:66792-806 [https://doi.org/10.1109/ACCESS.2019.2917555]

[99] Rifi N, Rachkidi E, Agoulmine N, Taher NC. Towards using blockchain technology for eHealth data access management. In: Towards using blockchain technology for eHealth data access management; 2017. Piscataway, NJ: IEEE; 1-4.

[100] Tariq F, Khan ZA, Sultana T, Rehman M, Shahzad Q, Javaid N. Leveraging Fine-Grained Access Control in Blockchain-Based Healthcare System. In: Barolli, Ditzinger, editors. Advanced Information Networking and Applications. 1st ed. [S.l.]: Springer International Publishing 2020; 106-15.

[101] Sadeghi R. JK, Prybutok VR, Sauser B. Theoretical and practical applications of blockchain in healthcare information management. Information & Management 2022;59(6):103649 [https://doi.org/10.1016/j.im.2022.103649]

[102] Al-Sumaidaee G, Alkhudary R, Zilic Z, Swidan A. Performance analysis of a private blockchain network built on Hyperledger Fabric for healthcare. Information Processing & Management 2023;60(2):103160 [https://doi.org/10.1016/j.ipm.2022.103160]

[103] Esmaeilzadeh P. Benefits and concerns associated with blockchain-based health information exchange (HIE): A qualitative study from physicians' perspectives. BMC Med Inform Decis Mak 2022;22(1):80 [https://doi.org/10.1186/s12911-022-01815-8] [PMID: 35346176]

[104] Kim MG, Lee AR, Kwon HJ, Kim JW, Kim IK. Sharing Medical Questionnaries based on blockchain. In: Zheng H, editor. Sharing Medical Questionnaries based on blockchain; 2018. [Piscataway, NJ]: IEEE; 2767-9.

[105] Zhang P, White J, Schmidt DC, Lenz G, Rosenbloom ST. FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data. Comput Struct Biotechnol J 2018;16:267-78 [https://doi.org/10.1016/j.csbj.2018.07.004] [PMID: 30108685]

[106] Jabbar R, Fetais N, Krichen M, Barkaoui K. Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity. In: Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity; 2020. IEEE; 310-7.

[107] Villarreal ERD, Garcia-Alonso J, Moguel E, Alegria JAH. Blockchain for Healthcare Management Systems: A Survey on Interoperability and Security. IEEE Access 2023;11:5629-52 [https://doi.org/10.1109/ACCESS.2023.3236505]

[108] Hajian A, Prybutok VR, Chang H-C. An empirical study for blockchain-based information sharing systems in electronic health records: A mediation perspective. Computers in Human Behavior 2023;138:107471 [https://doi.org/10.1016/j.chb.2022.107471]

[109] Amanat A, Rizwan M, Maple C, Zikria YB, Almadhor AS, Kim SW. Blockchain and cloud computing-based secure electronic healthcare records storage and sharing. Front Public Health 2022;10:938707 [https://doi.org/10.3389/fpubh.2022.938707] [PMID: 35928494]

[110] Shashi M. Leveraging Blockchain-Based Electronic Health Record Systems in Healthcare 4.0. IJITEE 2022;12(1):1-5 [https://doi.org/10.35940/ijitee.A9359.1212122]

[111] Seol K, Kim Y-G, Lee E, Seo Y-D, Baik D-K. Privacy-Preserving Attribute-Based Access Control Model for XML-Based Electronic Health Record System. IEEE Access 2018;6:9114-28 [https://doi.org/10.1109/ACCESS.2018.2800288]

[112] Alkhushyni SM, Alzaleq DM, Gadjou Kengne NL. Blockchain Technology applied to Electronic Health Records. In: Yuan W, Shi Y, Miller L, Lee G, Hu G, Goto T, editors. Blockchain Technology applied to Electronic Health Records; 2019. EPiC Series in Computing; 34-42.

[113] Wang S, Zhang Y, Zhang Y. A Blockchain-Based Framework for Data Sharing With Fine-Grained Access Control in Decentralized Storage Systems. IEEE Access 2018;6:38437-50 [https://doi.org/10.1109/ACCESS.2018.2851611]

[114] Dubovitskaya A, Xu Z, Ryu S, Schumacher M, Wang F. Secure and Trustable Electronic Medical Records Sharing using Blockchain. AMIA Annu Symp Proc 2017;2017:650-9 [PMID: 29854130]

[115] Dubovitskaya A, Baig F, Xu Z, Shukla R, Zambani PS, Swaminathan A, Jahangir MM, Chowdhry K, Lachhani R, Idnani N, Schumacher M, Aberer K, Stoller SD, Ryu S, Wang F. ACTION-EHR: Patient-Centric Blockchain-

Based Electronic Health Record Data Management for Cancer Care. J Med Internet Res 2020;22(8):e13598 [https://doi.org/10.2196/13598] [PMID: 32821064]

[116]   Sharma V, Gupta A, Hasan NU, Shabaz M, Ofori I. Blockchain in Secure Healthcare Systems: State of the Art, Limitations, and Future Directions. Security and Communication Networks 2022;2022:1-15 [https://doi.org/10.1155/2022/9697545]

[117]   Benchoufi M, Ravaud P. Blockchain technology for improving clinical research quality. Trials 2017;18(1):335 [https://doi.org/10.1186/s13063-017-2035-z] [PMID: 28724395]

[118]   Castaldo L, Cinque V. Blockchain-Based Logging for the Cross-Border Exchange of eHealth Data in Europe. In: Gelenbe E, Campegiani P, Czachórski T, Sokratis KK, Ioannis K, Luigi R, Dimitrios T, editors. Security in Computer and Information Sciences. Cham: Springer International Publishing 2018; 46-56.

[119]   Xia Q, Sifah EB, Asamoah KO, Gao J, Du X, Guizani M. MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain. IEEE Access 2017;5:14757-67 https://doi.org/10.1109/ACCESS.2017.2730843

[120]   Kushch S, Ranise S, Sciarretta G. Blockchain Tree for eHealth. In: Blockchain Tree for eHealth; 2019. IEEE; 1-5.

[121]   Angraal S, Krumholz HM, Schulz WL. Blockchain Technology: Applications in Healthcare. Circulation: Cardiovascular Quality and Outcomes 2017;10(9):130-9.

[122]   Kuo T-T, Kim H-E, Ohno-Machado L. Blockchain distributed ledger technologies for biomedical and health care applications. J Am Med Inform Assoc 2017;24(6):1211-20 [https://doi.org/10.1093/jamia/ocx068] [PMID: 29016974]

[123]   Houtan B, Hafid AS, Makrakis D. A Survey on Blockchain-Based Self-Sovereign Patient Identity in Healthcare. IEEE Access 2020;8:90478-94 [https://doi.org/10.1109/ACCESS.2020.2994090]

[124]   Hardjono T, Pentland A. Verifiable Anonymous Identities and Access Control in Permissioned Blockchains; 2019 Mar 11.

[125]   Guo H, Li W, Nejad M, Shen C-C. Access Control for Electronic Health Records with Hybrid Blockchain-Edge Architecture. In: Access Control for Electronic Health Records with Hybrid Blockchain-Edge Architecture; 2019. Los Alamitos, California, Washington, Tokyo: IEEE Computer Society, Conference Publishing Services; 44-51.

[126]   Fan K, Wang S, Ren Y, Li H, Yang Y. MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain. J Med Syst 2018;42(8):136 [https://doi.org/10.1007/s10916-018-0993-7] [PMID: 29931655]

[127]   Mikula T, Jacobsen RH. Identity and Access Management with Blockchain in Electronic Healthcare Records. In: Novotný M, Konofaos N, Skavhaug A, editors. Identity and Access Management with Blockchain in Electronic Healthcare Records; 2018. Piscataway, NJ: IEEE; 699-706.