



Blockchain technology applications in the health domain: a multivocal literature review

Merve Vildan Baysal^{1,2} · Özden Özcan-Top¹ · Aysu Betin-Can¹

Accepted: 10 August 2022 / Published online: 30 August 2022

© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022

Abstract

Blockchain technology has been changing the nature of several businesses, from supply chain management to electronic record management systems and copyright management to healthcare applications. It provides a resilient and secure platform for modifications due to its distributed and shared nature and cryptographic functions. Each new technology, however, comes with its challenges alongside its opportunities. Previously, we performed a systematic literature review (SLR) to explore how blockchain technology potentially benefits health domain applications. The previous SLR included 27 formal literature papers from 2016 to 2020. Noticing that blockchain technology is rapidly growing, we extended the previous SLR with a multivocal literature review (MLR) approach to present the state of the art in this study. We focused on understanding to what degree blockchain could answer the challenges inherited in the health domain and whether blockchain technology may bring new challenges to health applications. The MLR consists of 78 sources of formal literature and 23 sources of gray literature from 2016 to 2021. As a result of this study, we specified 17 health domain challenges that can be categorized into four groups: (i) meeting regulatory requirements and public health surveillance, (ii) ensuring security and privacy, (iii) ensuring interoperability, and (iv) preventing waste of resources. The analysis shows that blockchain makes significant contributions to the solutions of these challenges. However, 10 new pitfalls come with adopting the technology in the health domain: the inability to delete sensitive data once it is added to a chain, limited ability to keep large-scale data in a blockchain, and performance issues. The data we extracted during the MLR is available in a publicly accessible online repository.

Keywords Blockchain · Health domain challenges · Software development · Multivocal literature review · Formal literature · Gray literature

✉ Özden Özcan-Top
ozdenoz@metu.edu.tr

Extended author information available on the last page of the article

1 Introduction

Blockchains, most recognized as the technology behind cryptocurrencies [1], have found a wide application area, including supply chain management [1], electronic copyrights [2], digital voting [3], used car trading [4], and real estate management [5]. Technically, blockchains are tamper-resistant and tamper-evident distributed databases. They enable transparency and traceability of data transactions and thus ensure a trusted data management system for users [1].

Our research revealed that blockchain applications are widely adopted in the health domain. For instance, the Dentacoin application [6] uses a blockchain network to associate dental clinics and patients for various services. MediBloc [7] and SRCoin [8] utilize blockchain technology to process and manage health data for healthcare professionals, patients, and researchers in a secure way. Medishares [9] provides a blockchain platform that serves as a decentralized marketplace for insurance management. It enables participants to create insurance in smart contracts; thus, anyone in the insurance circle can securely access insurance-related data. The AI Doctor platform [10] is a decentralized artificial intelligence virtual doctor application. In this application, users who provide their health data are rewarded with AIDOC tokens on the blockchain platform. Later on, the AIDOC tokens can be used as credentials for health insurance at preferential rates. Patients' data stored on the platform can also be used by various organizations such as pharmaceuticals, medical institutions, and AI companies for drug development and clinical research. MedicalChain [11, 12] is another blockchain-based application running at various hospitals across the UK which enables patients to control their medical data. It provides a platform that enables users to give conditional data access to stakeholders such as doctors, laboratories, hospitals, pharmacists, and health insurers. Patientory [13] is a HIPAA [14] compliant platform that allows patients, clinicians, and healthcare organizations to securely access and transfer sensitive health information while providing actionable insights to improve health outcomes.

According to the 2020 OECD policy brief, adopting blockchain on a national scale is rare; however, there are government initiatives toward deploying blockchain in the health domain [15]. In 2016, the Estonian government commenced a project to use blockchain technology to find new and innovative ways to secure the health records of its 1.3 million residents. Estonia has become the first country to use blockchain in the health domain on a national scale [2]. Malta is the other country that deploys blockchain in the health domain at the national scale. A blockchain application called Dwarna manages the "dynamic consent" of citizens on biospecimens for research studies [16].

Compared with blockchain applications developed for non-safety critical domains, the health domain software applications need to be audited and verified by regulatory bodies and be ensured that they fulfill the regulatory standards.

Different regulations may be applied depending on the region in which healthcare applications are marketed. The Food and Drug Administration (FDA) [17] and the Medical Device Directives [18] regulate the healthcare applications

marketed in the USA and the European Union, respectively. Currently, no policy or guideline is published to regulate blockchain usage in the healthcare system/software development by regulatory bodies to the best of our knowledge. However, recently, the FDA unveiled the *Technology Modernization Action Plan* [19], claiming that blockchain technology is on their radar for addressing health domain-related challenges. Additionally, IBM, Walmart, and Merck have been selected for an FDA pilot program that will use blockchain technology to improve the security of drug supply chains [20]. These latest developments indicate that regulatory bodies will remain focused on blockchain research in the health domain.

The use of blockchain in healthcare solutions has gained significant momentum in recent years. Various blockchain-oriented applications and research have been released by practitioners and researchers. We believe that this is an appropriate time to explore the recent advancements and provide a synthesis of what practitioners and researchers think about the potential usage areas of blockchain in the health domain and the extent to which blockchain technology provides a solution to the field. We also aim to lead future research directions by exploring the new challenges that blockchain introduces to the domain.

With these purposes, we present a multivocal literature review (MLR) of blockchain adoption in the health domain in this study. MLR approach provides a methodology to systematically review both formal literature and gray literature. Luxembourg states that “*gray literature is produced on all levels of government, academics, business and industry in print and electronic formats, but which is not controlled by commercial publishers, i.e., where publishing is not the primary activity of the producing body*” [21, 22]. Thus, both theoretical and practitioner (e.g., developers, designers, and quality engineers) viewpoints could be reflected in the study with the MLR approach.

In this study, we aim to answer the following research questions:

- RQ1: What are the blockchain application areas in the health domain and what is the motivation behind it?
- RQ2: What are the challenges of developing health software?
- RQ3: To what extent does blockchain technology contribute resolving existing software development challenges in the health domain?
- RQ4: Does blockchain introduce new challenges to software development in the health domain?
- RQ5: What are existing solution suggestions to the blockchain-related challenges in the health domain?

In 2021, we conducted a systematic literature review (SLR) [23] with the same purposes. The SLR included 27 formal literature resources from 2016 to 2020. On the other hand, the MLR consists of 78 formal literature and 23 Gy literature resources. Among 78 formal literature studies, only 25 exist in the previous SLR we performed. This increase indicates how rapidly the blockchain health applications domain is growing. The number of new papers that passed the quality assessment criteria and were added to the paper pool has tripled in a single year.

There are other review studies focusing on potential application areas of blockchain in the health domain [24–39], but they do not cover and discuss the challenges faced by practitioners and associated solutions in depth.

This MLR study contributes to the literature with a comprehensive review and analysis of the.

state-of-the-art blockchain research from the health domain perspective. It acknowledges all current application areas of blockchain technology in the health domain. It also explores existing health domain challenges in a detailed way. Although most of these challenges are not new (e.g., being unable to specify falsified drugs and prevent modification of clinical trial data), the COVID-19 pandemic signified their impacts on people's lives and the environment.

In the post-pandemic world, companies are exploring ways to run their businesses more effectively and make their businesses resilient against minor, major, and unexpected events. Blockchain, one of the emerging technologies, could support businesses in being resilient.

Therefore, from the managerial perspective, this study shows the potential usage areas of blockchain in the health domain and supports strategic planning and decision-making processes. Policymakers could also use this extensive study to understand the existing blockchain adoption challenges and make better plans to address problems. Finally, this MLR study sheds light on significant challenges from a theoretical perspective and leads future research.

The rest of the paper is structured as follows: Sect. 2 provides a background on blockchain technology and health domain software. Section 3 explains our research methodology while performing the MLR. Section 4 presents results and discussion. Finally, in Sect. 5, we draw conclusions and present suggestions for further work.

2 Background

2.1 2.1 Blockchain technology overview

National Institute of Standards and Technology (NIST) defines *blockchain* as a tamper-resistant and tamper-evident digital ledger implemented in a distributed manner, generally without a central authority [1]. Data can only be added to a blockchain after several approvals, and once added, it cannot be deleted or modified without the approval of network participants.

The basis of blockchain technology emerged in the late 1980s and early 1990s. Leslie Lamport developed the Paxos protocol in 1989 [40], which provides a consensus model to reach an agreement on an unreliable network. Haber and Stornetta proposed a method for the secure timestamping of digital documents in 1990 [41]. This method enables signing documents digitally so that none of the signed documents are changed [41]. Satoshi Nakamoto published an electronic cash system in 2008. The study includes the concepts of consensus models among distrusted participants and digital signatures [42]. In 2009, the Bitcoin cryptocurrency blockchain network was established [1]. Several different cryptocurrencies followed Bitcoin, such as Ethereum [43].

Blockchain networks are categorized according to network participants' "permission" requirements [1]. If a participant can publish a new block to the network without getting permission from any authority, it is called a "*permissionless*" blockchain network. Publishing blocks in a permissionless network requires consensus of the majority of the participants. The network is called "*permissioned*" when only certain participants are allowed to publish blocks. In permissioned blockchain networks, data blocks must be approved by authorized nodes in a network.

Blocks are the records that comprise blockchain networks. Each block has its own hash, data, and the preceding block's hash. This hash is a unique value created from block data by a cryptographic hash function [1]. Block data includes a list of transactions and ledger events within that block. If a single data is changed in a block, the associated hash also changes. Therefore, attempts to modify data can be detected easily [1]. Figure 1 was adapted from [1] and shows the generic chain of blocks.

The interactions among participants of the blockchain are represented by *transactions*. These transactions are validated by *nodes*, each of which is an individual system within a blockchain network. "*Full nodes*" store the entire blockchain and validate the transactions, whereas "*lightweight nodes*" do not store a full copy of data and usually pass it to the full nodes to be processed [1].

Consensus models provide agreement among non-trusted parties by ensuring the validity and authenticity of blocks without a central authority [1]. Network participants agree that a transaction is valid through consensus models.

Asymmetric-key cryptography is used in blockchain technology to create a trusting relationship between network participants. Asymmetric-key cryptography [1] offers a method for verifying transaction integrity and authenticity. *Cryptographic hash* is used to compare large datasets and verify that data has not been tampered with by creating a unique small fingerprint for all data [3, 4]

A *smart contract*, a concept first proposed in 1994 by Nick Szabo [5], is a piece of code on the blockchain network [1] that emerges to minimize the need for trusted intermediaries. If a series of pre-defined conditions are fulfilled, a smart contract executes itself, and the execution results are recorded in the blockchain. Smart contracts are deployed on blockchain networks using cryptographically signed transactions; therefore, they are tamper-resistant as well [1].

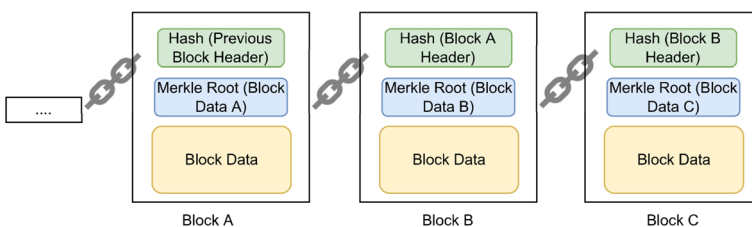


Fig. 1 Chain of Blocks based on Ref [1]

Participants in certain blockchain networks utilize *wallets*, specific software for public and private key management and calculating digital assets [1].

As the health domain is a multi-stakeholder structure, blockchain applications in this domain often require interoperability. The NIST defines *blockchain interoperability* as “a composition of distinguishable blockchain systems, each representing a unique distributed data ledger, where atomic transaction execution may span multiple heterogeneous blockchain systems, and where data recorded in one blockchain are reachable, verifiable, and referable by another possibly foreign transaction in a semantically compatible manner.” As this definition implies, information assets will be exchanged and used between different ledgers, and this exchange needs to be verifiable. Although the NIST defines *interoperability* as the communication between heterogeneous blockchain systems, Belchior et al.’s [44] definition covers homogeneous blockchain systems as well. In both cases, transactions require a trusted third party to ensure the correctness of underlying protocols [44]. It should be noted that complete interoperability may not be achieved due to reliability issues among different blockchain networks [45]. During a transaction that spans multiple ledgers, a source blockchain issues transactions against a target blockchain, and an exchange occurs between the source node and the target node. Decentralization is achieved when participants elect a source node from the source blockchain and a target node from the target blockchain [44].

2.2 Health Domain Software Overview

Health domain software must comply with the regulatory requirements defined by international standards and health regulatory agencies. Figure 2, adapted from Heidenreich [46], categorizes health domain software in terms of the regulatory compliance requirements.

As shown in Fig. 2, health domain software is categorized into health software and medical software. Medical software covers both the software embedded in medical devices and software that serve as a medical device (SaMD). On the other hand, health software includes SaMDs and other health software applications. Medical device software (MDS) processes, analyzes, or creates

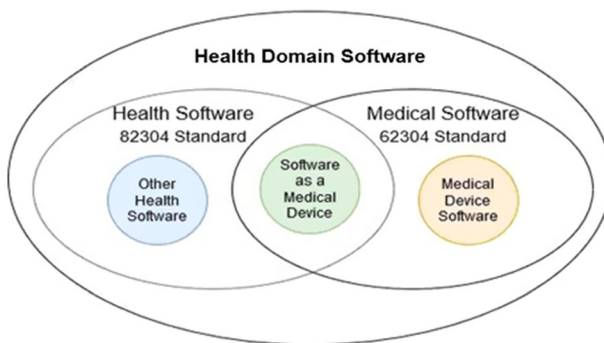


Fig. 2 Health Domain Software Categories and Standards—adapted from Ref [46]

medical data [47]. Various devices, including EKG monitors, insulin pumps, and medical imaging devices, are run with the medical device software applications. Software as a medical device (SaMD) is used for medical purposes and is not necessarily a part of hardware [48]. SaMDs may be used on desktop computers, tablets, smartphones, and smartwatches to aid healthcare professionals and patients in treatment planning, medical image viewing, heart-rate monitoring, and drug dosage calculations. Other health software, on the other hand, is stand-alone health applications that are executed on hardware [46], which can be exemplified as healthcare data management and clinical software applications.

These different types of software are subject to various regulations. While health software applications have to comply with the ISO/IEC 82,304 standard [49], medical software applications require compliance with the IEC 62,304 standard [50]. The ISO/IEC 82,304:2016 Health Software standard defines the processes and practices for guiding healthcare software development. Furthermore, it refers to the safety and security of health software that runs on general-purpose IT platforms, such as smartphones and tablets. IEC 62,304:2006 specifies the requirements to be followed while developing medical device software.

Besides the aforementioned two primary standards, the following standards are applied in the health domain:

- ISO 14971:2009 [51]: the international risk management standard for the production of medical device
- IEC 80,002–1:2009 [52]: the standard guiding the application of the ISO 14971 standard for medical device software
- IEC 80,002–3:2014 [53]: the process reference model for medical devices that defines software life cycle processes based on IEC 62,304:2006

While ISO 14971:2009 is an international risk management standard for medical device production, IEC 80,002–1:2009 guides the application of the ISO 14971 standard for medical device software. IEC 80,002–3:2014 is a process reference model for medical devices that defines software life cycle processes based on IEC 62,304:2006.

Software applications must be audited by different regulatory agencies depending on the region in which the application is marketed. The Food and Drug Administration (FDA) [17] in the USA and the Medical Device Directives [18] in the European Union are responsible for conducting the regulatory audits. Above, a detailed explanation is given for the standards valid in the EU. The FDA also provides clear guidelines such as developing clinical decision support software [54], software as a medical device [55], wireless medical devices [56], and medical device software [57].

As mentioned above, several standards and guidelines exist on various components of the health domain system and software development. Blockchain technology is on the radar of the FDA [19, 20].

3 Research methodology

Considering the purpose of our study, both contextual information and evidence from the industrial community [58] would be significant. We specified that many sources indicate high practitioner interest in the topic. Multivocal literature review (MLR) suits our purposes very well, as it is used for addressing research questions by using both formal literature (FL) and gray literature (GL) sources [21]. We systematically applied Garousi et al.’s *MLR* guideline [21] to perform the MLR process in this study. We used a Google Drive spreadsheet to collectively extract and analyze the raw data. The source pool and extracted data are publicly available at [59].

The overview of the MLR process is given in Fig. 3.

The definition of the “white,” “gray,” and “black” literature differs among studies. For instance, books are a part of the gray literature, according to [60]. On the other hand, they are considered part of the white literature, according to [61]. Compiling these studies ([60] and [61]), we agreed on the spectrum classification given in Table 1. To classify the sources based on their types in the gray literature, we used an existing model from Garousi et al.’s guideline [58]. We revised the examples of the second-tier category, i.e., preprints, e-prints, technical reports, lectures, and datasets.

3.1 Planning the MLR

We decided to carry out this MLR by observing the substantial increase in research in this area after conducting the SLR in 2020. We explored the existing literature review studies before proceeding with the research. At this stage, we also revisited the research questions given in Sect. 1. Below, we briefly discuss to what degree our research questions were covered in the previous SLR studies on

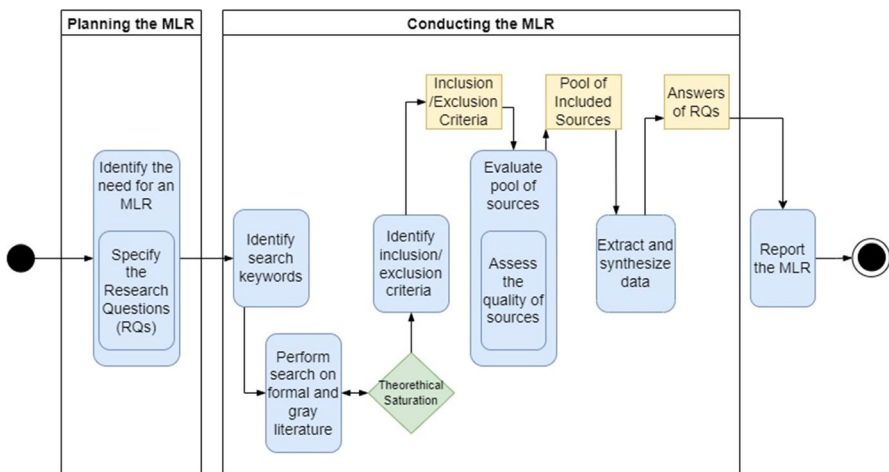


Fig. 3 The Phases and Steps of the MLR process we applied

Table 1 Spectrum of the “white,” “gray,” and “black” literature

White (Formal) Literature	Published journal papers, Conference proceedings, Books
Gray Literature	<p>First Tier (High outlet control/High credibility): Magazines, Government reports, White papers</p> <p>Second Tier (Moderate outlet control/Moderate credibility): Annual reports, News articles, Presentations, Audio–Video, Preprints, e-Prints, Technical reports, Lectures, Datasets, Q/A sites (such as Stackoverflow), Wiki articles</p> <p>Third Tier (Low outlet control/Low credibility): Blogs, e-mails, tweets</p>
Black Literature	Ideas, Concepts, Thoughts

developing healthcare applications using blockchain technology. The papers that do not follow a systematic literature review approach were excluded.

We list the previous SLR studies along with their publication dates, the number of the papers included in each of these studies, and the years covered in Table 2. We also added the columns for our research questions stated in Sect. 1 to highlight the similarities and differences of these SLRs with our study.

We specified that while the vast majority of the SLR studies in Table 2 addressed the potential application areas of blockchain in the health domain (RQ1), none of them explored the motivation for adopting blockchain in this field in detail. Thirteen SLR studies [24, 25, 28, 30–35, 38, 39, 62, 63] explore the inherited challenges in health software development that blockchain addresses (RQ2). In addition, these 13 studies discussed the role of blockchain technology in resolving these inherited software development challenges. However, they do not include technical details or explanations for solving these challenges.

Eleven studies [24–29, 32, 33, 36, 39, 62, 63] explored the challenges of developing health applications using blockchain technology (RQ4). Among these 11 studies, only Agbo et al. [26] and Al Mamun et al. [39] provided information on possible answers to these blockchain-related problems (RQ5).

Flangovan et al. [37] focus on the application areas of blockchain in the health domain and the reasons for its use. Adere [38] analyzes trends and highlights the potential benefits of blockchain deployment in IoT and healthcare. Al Mamun et al. [39] show the distribution of blockchain types and platforms adopted by the reviewed articles. Jadhav and Deshmukh [62] highlight the challenges faced and the potential benefits of blockchain technology in the healthcare supply chain. Attaran [63] identifies blockchain application areas for pharmaceuticals, challenges, and opportunities for implementing blockchain technology in healthcare. These studies mainly provide an overview of the use of blockchain in the health domain. On the other hand, our MLR study contains detailed information on constraints and solution proposals with information from various sources.

Different from the studies mentioned above, our research includes:

Table 2 Systematic literature review studies on blockchain in the health domain

Ref	Publication date	# of Papers included	# of Gray literature sources included	Years covered	RQ1	RQ2	RQ3	RQ4	RQ5
[24]	2019	Not given in the paper	No	2016–2017	Partially Yes	Yes	Partially Yes	Yes	No
[25]	2019	39	No	2016–2019	Partially Yes	Yes	Partially Yes	Yes	No
[26]	2019	65	No	2016–2018	Partially Yes	No	No	Yes	Yes
[27]	2018	33	No	2015–2018	Partially Yes	No	No	No	No
[28]	2019	44	No	2016–2019	Yes	Yes	Yes	Yes	No
[29]	2019	38	No	2016–2018	Yes	No	No	Partially Yes	No
[30]	2020	6	No	2016–2019	Partially Yes	Yes	Partially Yes	No	No
[31]	2020	42	No	2016–2019	Yes	Yes	Partially Yes	No	No
[32]	2020	37	No	2017–2020	Yes	Yes	Yes	Yes	No
[33]	2021	21	No	2016–2020	Yes	Partially Yes	Partially Yes	Yes	No
[34]	2021	70	No	2016–2020	Yes	Yes	Partially Yes	No	No
[35]	2021	10	No	2021	Yes	Partially Yes	Partially Yes	No	No
[36]	2021	49	9	2016–2020	No	No	No	Yes	No
[37]	2022	22	No	2016–2019	Yes	No	Partially Yes	No	No
[38]	2022	73	No	Not given in the paper	Partially Yes	Partially Yes	Partially Yes	No	No
[39]	2022	99	No	2016–2020	No	Partially Yes	Yes	Yes	Partially Yes
[62]	2022	61	No	2019–2021	Partially Yes	Yes	Yes	Yes	No
[63]	2022	Not given in the paper	No	2018–2020	Yes	Yes	Yes	Yes	No

(i) the most recent studies in the literature searched until October 2021 (78 formal pieces of literature).

(ii) gray literature sources (selected and extracted using a systematic approach) considering the experiences of practitioners in the implementation of blockchain. The MLR includes a wide variety of gray literature resources such as videos, white papers, Web pages, Q/A sites, and formal literature.

(iii) This is the first MLR performed systematically in blockchain health domain. Fang et al. [36] included gray literature in the systematic literature review; however, the study includes fewer sources with less variety (white papers, reports). It focuses on the current trends of the blockchain, key design decisions, current limitations encountered, and future directions. However, the study only discusses these topics in the personal health records field. In this MLR, we explore the use of blockchain in the health domain from a broader perspective covering medical supply chain management, clinical trials, precision medicine, remote patient monitoring, IoT use with blockchain, electronic health records, public health surveillance, and health insurance.

3.2 Conducting the MLR

In this section, we provide information on the stages of evaluation process, selection of formal literature and gray literature sources, and data extraction process.

3.2.1 Formal literature

Evaluation process and selection of the publications. We performed the search using the search string given in Table 3 on the IEEE Xplore and ACM libraries, Google Scholar, PubMed databases, and Research Rabbit tool. The initial search was completed on October 15, 2021.

To present a broader scope, we used the following inclusion criteria:

(i) the papers that share practitioner/researcher experiences;
 (ii) the papers that present blockchain solutions in the health domain;
 (iii) the papers that describe software development challenges encountered in the health domain;

(iv) the papers that meet the quality criteria presented in Table 3;

(v) the papers that are written in English and accessible.

We excluded secondary studies to eliminate the duplication of the findings.

The initial search yielded 4076 results. The first evaluation was performed based on the titles and abstracts of the publications. After the 1st evaluation, the paper pool was reduced to 178 papers. The second evaluation was conducted by reading the papers thoroughly. After that, we expanded the paper pool by performing snowballing on these publications and including papers related to the subject. The search process

Table 3 Search string used for formal and gray literature

(blockchain OR block chain) AND (healthcare OR health OR medical OR medicine OR e-health OR e-health OR EHR OR EMR)

Table 4 Results of evaluation process

Online library	Initial research	First evaluation result	Second evaluation result
Google Scholar	2.400	47	124
IEEE Xplore	443	21	11
ACM Digital library	754	11	4
Pubmed	279	6	6
ResearchRabbit	200	37	22
Snowballing		56	23
Total	4076	178	78

Table 5 Quality assessment questions

ID	Quality assessment query	Quality indicator (0–2)
Q1	Are the authors' intentions with the research made clear?	0—No 1—Partially 2—Yes
Q2	Does the study contain conclusions, implications for practice and future research?	0—No 1—Partially 2—Yes
Q3	Does the study give a realistic and credible impression?	0—No 1—Partially 2—Yes
Q4	Are the challenges or solutions adequately defined in detail?	0—No 1—Partially 2—Yes

was stopped when the results reached theoretical saturation, which meant that no new concepts emerged. As a result, 78 formal pieces of literature were added to the review process.

Table 4 shows the number of publications found in online libraries and the outputs of each evaluation process.

Quality assessment. To determine the quality of the papers in the formal literature, we used the following assessment criteria. Q1, Q2, and Q3 in Table 5 belong to Höst and Runeson's quality checklist [64], and we defined Q4.

All authors of this paper took place in the quality assessment process. For the 178 papers that passed the first evaluation, we used three-level indicators to address the quality assessment questions:

- (i) Level 0 when the criterion was addressed very poorly or not at all.
- (ii) Level 1 when the criterion was addressed partially.
- (iii) Level 2 when the publication successfully fulfilled the criterion.

The studies with a four-star rating or higher were included in the review.

Data extraction. All authors used a collective spreadsheet to extract the data from the papers and review the data. We retrieve bibliometric data (i.e., publication type and year, number of citations) and the information required to answer the research questions.

Table 6 Results of evaluation process

GL database	Initial research	First evaluation result	Second evaluation result
Google	160*	66	5
YouTube	382	65	14
Stackoverflow	30	6	1
Snowballing		5	3
Total	572	141	23

* The query we performed on the Google search engine yielded around 92.2 million results. We reviewed 160 sources in detail (i.e., the first 16 pages), as irrelevant results appear beginning the 17th page

Table 7 Quality assessment questions

Q.ID	Quality assessment query	Quality indicator (0–2)
Q1	Does the source have a clearly stated aim?	0—No 1—Partially 2—Yes
Q2	Does the item have a clearly stated date?	0—No 1—Partially 2—Yes
Q3	Does the study give a realistic and credible impression?	0—No 1—Partially 2—Yes
Q4	Are the challenges or solutions defined in detail?	0—No 1—Partially 2—Yes

3.2.2 Gray literature

Evaluation process and selection of the sources We performed the search on a general Web search engine (i.e., Google), a specialized database (i.e., YouTube), and a social question–answer website (i.e., Stackoverflow) using search string given in Table 3.

The searches, which were performed between August 23, 2021, and October 1, 2021, yielded 572 results in total. We applied the following inclusion criteria to present a better scoped research:

- (i) The sources that share experiences of practitioners;
- (ii) The sources presenting blockchain solutions in the health domain;
- (iii) The sources describing encountered challenges in software development in the health domain;
- (iv) The sources that conform to specified quality criteria given in Table 4;
- (v) The sources that belong to first- or second-tier outlet types;
- (vi) The number of views higher than 1000 (valid only for videos);
- (vii) Written in English and accessible sources.

The initial source elimination was performed based on the source titles. In the second evaluation, we examined the full content of the source based on the inclusion criteria given above. As a result, 23 sources from gray literature were included in the review process. We finalized the search process when the findings reached theoretical saturation, which means no new concepts emerged [64].

The number of sources found and the results of each evaluation are given in Table 6.

Quality assessment. We applied the following criteria to assess the quality of the sources in the gray literature given in Table 7. We retrieved Q1 and Q2 from Garousi et al.'s quality checklist [58] and Q3 from Höst and Runeson's quality checklist [64] and added Q4 to these questions.

All three authors of this paper were involved in the quality assessment process. We answered the quality assessment questions for 141 sources that passed the first evaluation according to the three-level indicator presented in Sect. 3.2.1.

Data extraction. As mentioned in the formal literature section, we used a spreadsheet to collectively manage the data extraction process. We downloaded the videos to a local computer to extract audio data and transform them into text using the pyTranscriber application [65]. We have added the bibliometric data of the sources and all the information needed to answer the research questions in this document.

4 Results and discussion

In this section, first, we provide the bibliometric overview of the sources included in the MLR and continue with the discussion of research questions.

In the final MLR source pool, there are 78 formal literature and 23 Gy literature sources. Out of the 78 papers, 53 were published in journals and 25 were published in conference proceedings. Figure 4 shows the publication years of the papers included and the publication dates of gray literature sources. Although Satoshi Nakamoto introduced blockchain in 2008, no publications on its use in the health domain were found until 2016. The number of publications raised gradually in 2018, 2019, and 2020, as shown in the following graph. The numbers appear to be decreasing in 2021. As the year had not yet been over when the last search was conducted on October 1, 2021, we anticipate that interest in this field will continue to grow.

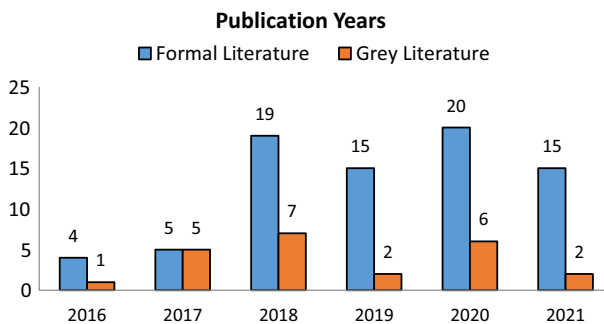


Fig. 4 The Publication Years of the Sources Included

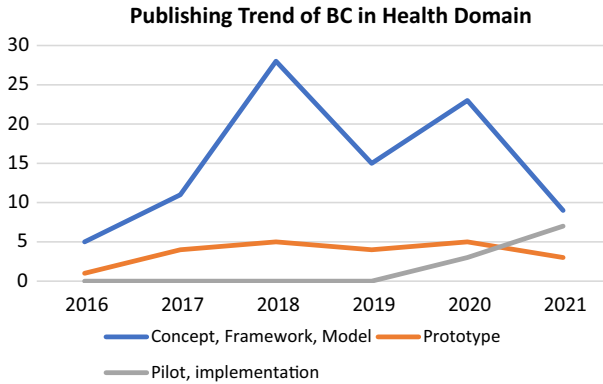


Fig. 5 Evolution of Publications in Blockchain Technology in the Health Domain

Figure 5 shows the publishing trend of blockchain technology in the health domain from 2016 to 2021. The number of studies on the topic shows an upward trend after 2017 and a downward trend after 2020. When we analyzed the publication types, we saw that early studies focused more on the concept, framework, and model development, and piloting implementation studies gained a rapid momentum as of 2019.

Figure 6 shows the frequencies of the most published venues of formal literature studies. There are two venues with the highest number in terms of frequency: *Journal of Medical Systems* and *IEEE Access*. *Journal of Medical Internet Research* venue follows them with three studies. *International Journal of Environmental Research and Public Health*, *International Conference on Open and Big Data*, *IEEE Globecom Workshops (GC Wkshps)*, *Blockchain in Healthcare Today*, *Sensors*, and *AMIA Annual Symposium Proceedings* venues follow them with two FL studies.

In Fig. 7a, b, we present the distribution of formal (white) literature sources' citation numbers and YouTube video view numbers to show the interest in the field.

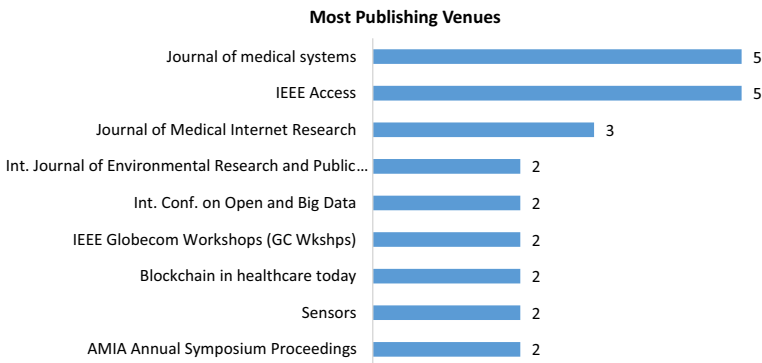


Fig. 6 The Frequencies of most Published Formal Literature Venues

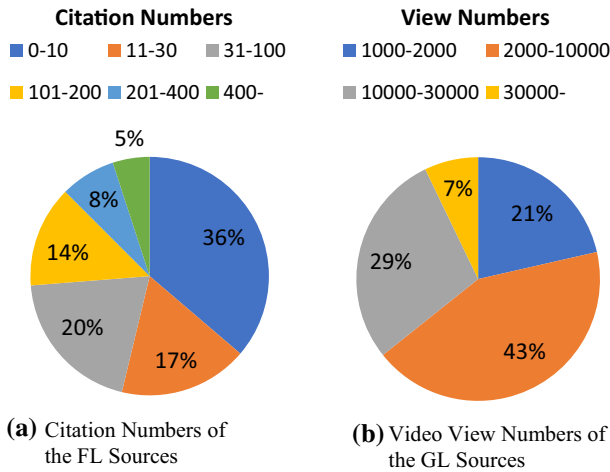


Fig. 7 a Citation Numbers of the FL Sources,

It was specified that 770 new papers were published in the domain within just one year. As mentioned in Sect. 1, the number of the new papers added to the MLR study has tripled in a single year. Thirty-six percentage of the publications have low citation numbers (less than ten citations per publication), mainly because these papers have been published in recent years (in 2020 and 2021). Considering that the latest publication date is 2016, the citation numbers of the remaining papers in the paper pool are pretty high. Eighty percentage of the YouTube videos included in the MLR source pool also have high viewing numbers above 2000.

In the next part, we present the results of the MLR, i.e., the answers to the research questions based on the analyzed formal and gray literature sources.

4.1 RQ1. What are the blockchain application areas in the health domain, and what is the motivation behind it?

Table 8 highlights the primary blockchain application areas in the health domain, the rationale for adopting this technology in these areas, and examples of blockchain-oriented solutions presented in our resource pool. The use of blockchain technology for electronic health and medical record management is mentioned in most publications and GL sources (47 FL and 16 GL sources). The second most prevalent application area is Remote Patient Monitoring/Internet of Medical Things, with 12 formal literature sources (namely papers). Other application areas are medicine supply chain management (7 FL and 4 GL sources), clinical trials (7 FL), precision medicine (3 FL), blockchain in strengthening public health surveillance (1 FL and 1 GL sources), and health insurance (1 FL and 1 GL sources).

We present the summary of this information in Fig. 8, including the application areas and the number of resources in those areas.

Table 8 Blockchain technology in the health domain

Application areas	Motivation behind adopting blockchain in the relevant area	Examples of blockchain-oriented solutions
Medicine supply chain management	<p>Difficulty of identifying unauthorized medicines</p> <p>Difficulty of specifying falsified medicines that misrepresent their content or source</p>	<p>Sylim et al. present a blockchain-based pharmacosurveillance system in [68]. Tseng et al. [78] and Takyar [69] developed blockchain applications to manage the entire pharmaceutical supply chain life cycle. The originChain application created by Lu and Xu [163] aims to secure medicine data availability to service providers and automate regulatory compliance checks in the pharmaceutical supply chain</p> <p>Uddin developed the Medledger application, which securely and efficiently executes drug supply chain transactions in a private permissioned distributed network of different pharmaceutical stakeholders [66]. Haq and Esuka [70] and Musamih et al. [127] developed blockchain applications for the pharmaceutical industry to track the drugs in manufacturing in a decentralized manner until they are delivered to patients. Omar et al. [128] presented a blockchain solution using smart contracts to automate the Group Purchasing Organizations (GPOs) contract process. GPOs are large groups that healthcare providers usually reach out to improve procurement efficiency and collective pricing power in supply chain systems</p> <p>Besides the researchers above, IBM [75] has launched a blockchain network called Rapid Supplier Connect to enable government agencies and healthcare organizations to identify alternative supplies and equipment vendors to overcome supply chain shortages experienced in the COVID-19 pandemic. Maury [71] and IBM [72] also presented two blockchain solutions for fraud prevention in medicine supply chains</p>

Table 8 (continued)

Application areas	Motivation behind adopting blockchain in the relevant area	Examples of blockchain-oriented solutions
Clinical trials	<p>Risk of clinical trial data manipulation</p> <p>The need for providing data transparency in clinical trials for scientific reliability of the findings</p> <p>The need for sharing and ensuring traceability of clinical trial data</p> <p>The need for structuring clinical trial data which is usually kept in silo forms</p>	<p>Nugent et al. [76], Choudhury et al. [79], and Wong et al. [82] created smart contracts on a permissioned blockchain network to enable data transparency, eliminate data manipulation, and ensure scientific reliability in clinical trials. Shae et al. [175] developed a four-layered system architecture for creating blockchain-based applications for clinical trials, precision medicine, and supporting medical decision-making</p> <p>Zhuang et al. [96] developed a blockchain framework with patient recruitment and patient engagement features. The framework also includes persistent monitoring modules to detect anomalies in patients' records in real time and minimize the risk of record manipulation. Omar et al. [80] developed a blockchain-based framework for clinical trials data management using Ethereum smart contracts, which employs InterPlanetary Filesystem (IPFS) as the file storage system to automate processes and information exchange among clinical trials stakeholders. Jung et al. [81] developed a blockchain-based healthcare solution named Decentralized Clinical Study Consent Management (D-CSCM). It contains features to create and manage consent documents, store them decentralized, and log all views and changes of the database entries on a chain</p>
Precision medicine	<p>The need for ensuring privacy and security of data in diagnosing, treating and preventing diseases by considering the variabilities in genes, environment and lifestyle of individuals</p>	<p>Juneja and Marefat [84] introduced a system that uses deep learning to classify arrhythmias and smart contracts to keep access in control. Lee and Yang [176] created a nail analysis system that combines microscopy sensors and blockchain to predict reliably the diagnosis of fingerprint diseases</p> <p>Gong and Zhao [122] proposed a blockchain-based healthcare system that generates scientific knowledge such as the characteristics of gastric cancer or the cause of diabetes from personal health data by applying big data analysis techniques, knowledge discovery, and knowledge refining</p>

Table 8 (continued)

Application areas	Motivation behind adopting blockchain in the relevant area	Examples of blockchain-oriented solutions
Remote patient monitoring/internet of medical things	The need for a secure system in collecting and sharing data in a real time manner via IoT technology (e.g., body scanners, wearable devices, and heart monitors)	<p data-bbox="248 202 395 890">Griggs et al. [86] used customized threshold values stored in smart contracts to analyze patient data gathered via IoT healthcare devices. Saravanan et al. [116] created a smart contract-based IoT system for diabetes patients. Jita and Preterse [87] proposed an architectural design for a homecare system development that incorporates smart devices for monitoring patient vitals and blockchain for data storage</p> <p data-bbox="415 167 538 890">Liang et al. [88], Pawar et al. [137], and Taralunga et al. [97] developed a blockchain-based user-centric health data-sharing solution. Dey et al. [98], Pham et al. [130], Bhawiyuga et al. [150], and Kumar et al. [99] developed four different blockchain-based IoT solutions that employ biosensors to measure patients' medical conditions and save the data in a blockchain</p> <p data-bbox="558 167 656 890">Uddin et al. [135] provided an architecture for developing a continuous patient monitoring system. Data streaming from body area sensors needs to be securely stored. An agent manages end-to-end data streams, and the blockchain stores data in a distributed manner</p> <p data-bbox="676 185 749 890">Hathaliya et al. [123] proposed a decentralized AI and blockchain network for monitoring patients in real time, and remotely. Blockchain and Machine Learning technologies were integrated for the early prediction of diseases in this network</p>

Table 8 (continued)

Application areas	Motivation behind adopting blockchain in the relevant area	Examples of blockchain-oriented solutions
Electronic health/medical record management	<p>The need for systems to be secure against attacks due to the sensitivity of patient data in electronic health records (EHR)</p> <p>The need for patient data to be up to date and available when needed</p>	<p>[85, 115, 117, 126, 132, 145, 177] provide EHR solutions for effective and secure storage of patients' medical data using blockchain. Due to their decentralized structure and cryptographic functions, blockchains prevent hackers from breaching or corrupting data, and keeping data up-to-date</p> <p>[89–92, 94, 95, 100–112, 118, 119, 124, 125, 131, 136, 138–140, 143, 144, 146, 147, 151–153, 156, 159, 162, 165, 178] from formal literature and [2, 11, 12, 73, 74, 154]</p> <p>[15, 120, 129, 133, 134, 141, 142, 148, 149, 157, 158] from gray literature propose blockchain-based EHR sharing solutions. In these solutions, the accountability and transparency of transactions are maintained during the data-sharing process, and user-centric health data-sharing solutions are obtained using blockchain technology</p> <p>Coelha [121] and Sharma [160] proposed optimized, blockchain-based monitoring and reporting systems for disease surveillance that enable data transparency and enhance the accessibility of validated data. These blockchain-based solutions protect the society from future health risks</p>
Blockchain in empowering public health surveillance	<p>The need for the disease monitoring systems, especially for infectious diseases, to aggregate data coming from a large network of agents. The need to validate data received and make it available to health officials to help manage their response to public health demands</p>	

Table 8 (continued)

Application areas	Motivation behind adopting blockchain in the relevant area	Examples of blockchain-oriented solutions
Health Insurance	The need for the health insurance management systems to securely and efficiently exchange information between multiple entities used in decision making	<p>Panda et al. [155] presented a decentralized authentication system based on the insurance claim blockchain (ICBChain) system that ensures patients' privacy and the exchange of sensitive healthcare information between multiple entities in a secure way</p> <p>Synaptic Health Alliance [161] conducted a pilot project and provided a blockchain solution to gather up-to-date demographic information about physicians and other providers</p>

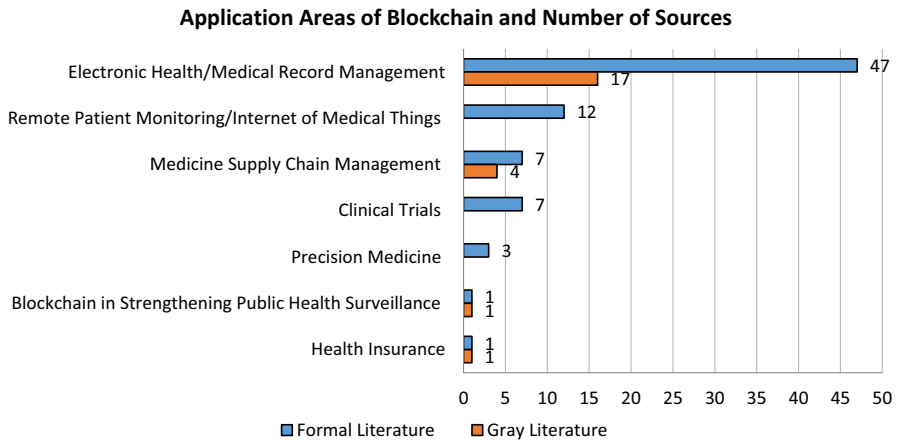


Fig. 8 The Application Areas of Blockchain and the Number of Sourcesb. Video View Numbers of the GL Sources

4.2 RQ2. What are the challenges of developing health software? RQ3. To what extent does blockchain technology contribute resolving these software development challenges in the health domain?

We have grouped the challenges and associated solution suggestions of the MLR sources under four main headings: 1) meeting regulatory requirements and public health surveillance, 2) security and protection of privacy, 3) ensuring interoperability, and 4) preventing waste of resources.

4.3 (1) Meeting regulatory requirements and public health surveillance

Challenge 1.1 Falsified drugs are one of the most serious threats to the pharmaceutical industry [66] 53 55 57 58 128 130. The World Health Organization (WHO) highlights that one in ten medicines produced in developing countries is substandard or falsified and has serious adverse effects on human lives [67]. To prevent the distribution of falsified medicines, regulatory agencies require to monitor the product supply chain before and during distribution [68, 69].

Solution 1.1. It is possible to detect data anomalies, unauthorized data insertions, and missing raw materials, identify authorized medication vendors/manufacturers, and store medical information by using blockchain technology and smart contract-based structures after data is inserted. Blockchain technology, which confirms and authenticates transactions, allows not only the system members but also drugs to be tracked throughout the medical supply chain [68–74].

The primary structure used in blockchain for this problem is smart contracts. Smart contracts provide traceability by tracking information on the blockchain in the form of transparent, immutable, and timestamped blocks by recording medicines, their active ingredients, and distribution data [66, 73, 74]. An account could be allocated to FDA and is notified by a smart contract when a transaction (i.e., the

production, transportation, or receipt of medicine) occurs in a supply chain. The FDA account, as an oracle, could verify all transactions. When all other accounts attempt to upload a file, they automatically publish a session key encrypted with the FDA public key. Sylim et al. suggest that when unregistered products are entered into the medical supply chain, discrepancies in specific data points (e.g., dosage, ingredients) could be detected [68].

Additionally, a permissioned blockchain could be used to enable only trusted parties to join the network and to push data to the blockchain [70]. These mechanisms aim to prevent data manipulation at the entry of data into the chain to some degree. However, blockchain cannot handle if data is manipulated at the source. For instance, if a permissioned network participant manipulates the content of drugs and records the manipulated data into the chain, the blockchain cannot notice the manipulation. However, this manipulation can be tracked down to the source once detected elsewhere.

Challenge 1.2. During the COVID-19 pandemic, healthcare industry leaders point out that reviewing suppliers can be time-consuming. Given the ongoing demand for materials, healthcare organizations need to make quick decisions to locate and verify new vendors [75].

Solution 1.2 These days, IBM leverages blockchain technology to help address medical supply chain shortages due to the COVID-19 pandemic. The company has launched a blockchain network called, Rapid Supplier Connect to help government agencies and healthcare organizations identify alternative supplies and equipment vendors more quickly. By creating their supply chains and adding non-traditional suppliers to their networks, they had a sufficient stock of equipment and materials. The blockchain network also helps identify existing supplies and excess unused inventory, allowing hospitals to make them available to others and route supplies where they are most needed [75].

Challenge 1.3. All clinical trials must make their methodology and findings available to regulatory agencies; however, more than half of the trials fail to do so [76]. Furthermore, a recent study [77] found that clinical trials are highly vulnerable to data manipulation. Subject registration, trial registration data, and clinical measures might be subject to manipulation [76].

Solution 1.3. The clinical trial life cycle includes trial registration, recruitment of subjects, regulatory approval, data entry, compliance with the trial protocol, amendments to a clinical trial protocol, patient monitoring for giving or withdrawing their informed consent, and reporting of adverse events stages. Blockchain prevents backward data manipulation during the clinical trial life cycle if data is added to the blockchain at every stage when the data is created instead of bulk data entry at the end of a trial [76]. Although blockchain does not guarantee correct data entry, a staged data entry process would reduce data manipulation risk. Smart contracts could be used to promote transparency in reporting clinical trial data by capturing data that might be intended to be manipulated [76, 78–81].

Additionally, smart contracts mandate a stage-by-stage data entry during the clinical trial process. This way, during a clinical trial, the intermediary stages

can be traced, and the results can be disclosed to regulatory agencies without any missing data.

Challenge 1.4. Clinical researchers or clinicians may be fraudulent or careless and record misleading or incorrect data into case report forms (CRFs), including all data of patients participating in a clinical trial [82]. A common healthcare fraud involves perpetrators who provide false or exaggerated diagnosis data for patients so that fraudulent insurance claims can be submitted for extra payment [11]. According to the FBI report: “The total cost of insurance fraud is estimated to be more than \$40 billion per year.” in the USA [83].

Solution 1.4. One method to solve this issue is to encourage clinical researchers and clinicians to provide raw data to the blockchain as early as possible. Incorrect data entry cannot be prevented by using blockchain; however, adding raw data early into the chain would eliminate data tampering to adapt to new situations. Later on, statistical analyses can be applied to verify the data [82] to detect discrepancies that signal data manipulation at the source.

Challenge 1.5. The Health Insurance Portability and Accountability Act (HIPAA) establishes standards for healthcare-related electronic transactions [14]. The HIPAA Privacy Rule requires protecting the privacy of health information. Therefore, patient information should be stored anonymously to prevent the identification of patients [84, 85].

Solution 1.5. Blockchain offers a partial solution with pseudo-anonymity where the user is anonymous, but their account identifiers are not [86]. The pseudo-anonym structure allows patients to hide their identities with alphanumeric addresses and yet to authenticate their identity when needed [73, 85, 87–92]. Pseudo-anonymity is still considered personal data [93]. Although privacy cannot be fully ensured with pseudo-anonymized data, it constitutes a partial solution for data privacy. Smart contracts enable regulation of the access control policy and achieve HIPAA compliance [94].

4.4 (2) Ensuring security and privacy

Health data is a tempting target for criminals due to its potential economic value [11, 15, 70, 71, 86, 92, 95]. Therefore, health data storage and transmission processes must be performed in a reliable and secure way [85, 87, 94, 96–106].

[15, 89, 91, 107–112]. According to the Trustwave report: “a healthcare data record may be valued at up to \$250 per record on the black market compared to \$5.40 for the next highest value record (a payment card)” [113]. The number patient records compromised in 2020 exceeded 40 million according to the incidents reported to the USA government [114]. Criminals may attack the healthcare system and threaten confidentiality, integrity, and availability of patients’ personal health information.

Challenge 2.1. Intruders may tamper with or delete patients’ data, thereby benefiting insurance companies or hiding medical malpractices (e.g., delayed diagnosis and misdiagnosis) [111, 115]. Intruders may also tamper with the

cold-chain shipping data in medicine supply chains when the essential information is stored in centralized databases [69].

Solution 2.1.a. In blockchain, all data and transactions are digitally signed which enables prevention of unauthorized access to network [70, 85, 89, 98, 99, 101, 104, 116–121]. It employs asymmetric cryptography to authenticate users and safeguard data, thus enabling confidentiality among the participants of a system [116, 122–125].

Solution 2.1.b. Each block in a chain keeps permanent logs of data transmissions [79, 84, 85, 87, 102, 103]. As data are timestamped in a blockchain, data manipulations can be recognized [121, 126]. Blockchain technology ensures transaction security; however, it does not offer a specific advantage in preventing data theft. Using zero trust principles in a blockchain could enhance the overall security. While blockchain ensures transaction security, zero trust policies, including data encryption, would improve access management and user authentication [95].

Solution 2.1.c Nodes have full access to ledgers; however, users are only allowed to perform activities based on their role and can only access the files they own or have permission to view [91, 95, 127]. Smart contracts can be used to assign the network users to different roles with associated functions and privileges [102, 128, 129] and generate immutable logs of transactions [15, 97, 110, 124, 130, 131].

Solution 2.1.d. A wrapper layer integration mechanism can be used between the cloud-based EHR management systems and public blockchain networks to develop tamper-proof health record management systems [115].

Solution 2.1.e. Because of the sensitivity of health data, permissioned blockchains (e.g., Hyperledger Fabric) could be used to enhance privacy [2, 11, 72, 73, 79, 97, 111, 125, 131–133]. In a permissioned network, participants are included in a system in a controlled manner. Thus, confidentiality in a network is met [131].

Challenge 2.2. When health records are stored in centralized databases, it becomes a necessity to rely on single authorities that may not effectively protect the data against internal and external attacks [11, 73, 125, 134]. For example, in disease surveillance, authorities and independent agents must record sensitive information in centralized information systems. But, centralized data control systems are subject to single point of failure problem and do not provide data transparency [121].

Solution 2.2. Blockchain's decentralized nature enables elimination of single point of failures. If a node fails or is compromised in a chain, the failure does not cause the entire system to stop. Therefore, it has a more robust structure and resilient to cyber-attacks [74, 79, 81, 85, 89, 90, 92, 95, 98, 107, 121, 122, 127, 131, 135, 136]. Patients' health data are stored on the servers of various healthcare providers in blockchain-based applications; thus, a single failure does not affect all locations to stop working simultaneously [74, 118]. It can be said that BC-based systems are robust against data loss or data corruption [73, 121] and eliminate the need to rely on central authorities [74, 95, 126, 134].

Challenge 2.3. Healthcare system users (e.g., patients) should have control over on their own data due to its sensitivity [70, 85, 89, 101, 110, 112, 118, 123, 135, 137–142]. Data ownership management is a major challenge for healthcare systems currently [136]. Cernian et al. mention that there is no platform to monitor patient traceability throughout the entire healthcare chain [143]. The risk of intermediaries

or intruders accessing the patients' reports without their consent remains valid. Such information may be exploited by insurance vendors and other third parties [144]. Patients should be the ones to decide with whom their health data will be shared, neither third parties nor institutions.

Solution 2.3. Blockchain technology allows patients to take ownership of their health data and share data without violating patient rights. Patients could retain control over every transaction in a blockchain-based system by accessing their health data using an asymmetric encryption algorithm. Only the trusted parties authorized by patients may access the data [2, 11, 73, 74, 85, 87, 91, 96, 101, 107, 118, 124, 130, 134, 135, 137, 141, 142, 144–148]. As an example [11], when a patient wants to grant access to a doctor to view their health data, the patient encrypts their health data with a symmetric key in an external database. This symmetric key is sent to the doctor using the asymmetric key encryption. The doctor uses their private key to access the symmetric key of the patient and decrypts the health data using this symmetric key [11]. This secure sharing among doctors and patients eliminates the intermediary parties [106]. When the patient wants to revoke the access grant to their health data, the data is encrypted with a new symmetric key. Patients could also track how many times their records have been accessed by using smart contracts [74, 112] and whether a change was made on their records, and the owner of the change [124]. Thus, blockchain-based health applications enable the storage and sharing of health data in a patient-centric manner.

Challenge 2.4. Patients' health data may not always be recorded electronically in healthcare systems. This issue affects the quality of health care. There is a need to establish a patient-reporting mechanism to improve the quality of care [94, 129, 149].

Solution 2.4. Blockchain gives patients the right to report their health records on ledgers [94]. This functionality creates opportunities to use health records for medical research with permission [118].

Challenge 2.5. IoT devices used for remote patient monitoring are especially vulnerable to cyber-attacks and data theft [130, 136, 150]. Hackers can take complete control of wearable IoT devices and misuse them. For instance, Johnson & Johnson had previously warned patients about the vulnerability of one of the insulin pumps that the hackers could exploit to overdose the patients [136]. In blockchain and IoT integrated systems, IoT devices may subject cyber-attacks.

Solution 2.5. Blockchain cannot be a solution to prevent the attacks or temper resistant to these attacks. However, audit trails in blockchain allow tracking who made the changes and when the changes were made [151]. Cryptographic hash functions create immutable audit trails and guarantee that the most recent version of the record is always used [148]. When a patient's report residing in the blockchain network needs to be updated, a new report is generated with the reference of the original report and uploaded to the blockchain. This reference enables the updated reports to be identified [121].

4.5 (3) Ensuring interoperability

Challenge 3.1. Regulations on data transfer among healthcare providers are not well defined. In addition, interoperability of systems is another issue when effective and coordinated data sharing is concerned [66, 74, 101, 119, 139, 152–154]. Therefore, there is a need to develop a secure and efficient data-sharing mechanism for highly sensitive health information among the stakeholders of healthcare systems [155].

Solution 3.1.a. When a nationwide blockchain application covering all the health stakeholders is deployed, there is no need to transfer data among health providers. As blockchain enables the patients to control their health data, patients could give access rights to health providers directly. As a result, it is possible to avoid undefined procedures and interoperability issues in sharing data among healthcare providers [151].

Solution 3.1.b. When a single ledger is developed to include all stakeholders in a healthcare system, there is no need to manually transfer added or modified patient data from one system to another [11, 134]. Agreements among patients, government, providers, and insurance companies can be stored via smart contracts. Thus, interoperability would not be a concern. Additionally, data format requirements can be defined on blockchain to record all information correctly. In this way, the problem of preventing data sharing due to inadequate information can be reduced or eliminated [154].

Challenge 3.2. Patient mobility requires cross-border exchange of patient data, which causes difficulties in complying with different countries' privacy and data protection standards [156].

Solution 3.2. Different data privacy, security, and sharing policies need to be addressed in designing blockchains and smart contracts considering the patient mobility fact [138, 156]. In addition, we suggest developing a structure that allows each country participating in the network to implement specific policies for the protection and control of health-related data.

Challenge 3.3. Patel states that infrastructures used for cross-site medical imaging data transfers require relying on third-party intermediaries [90]. However, ensuring the trust among the relevant stakeholders is highly difficult.

Solution 3.3. A blockchain application dedicated to corresponding stakeholders could be a solution for cross-domain image sharing. Blockchain framework eliminates the third-party access to protect health information [90].

4.6 (4) Preventing waste of health resources

Challenge 4.1. In clinical research, manual processing may be required to capture, manage, and report data [79, 80], as the patient data is collected as bio-samples, questionnaires, and laboratory results. The clinical research forms and questionnaires are usually paper based. Such a manual intervention for data management and maintenance increases the cost of clinical studies. Backup and the data recovery time for such systems are also high [79, 80, 89]. In addition, clinical trial data have to be stored confidentially and securely for audits and potential future studies [136].

Solution 4.1. Blockchain-based data management frameworks may reduce the administrative burden and the time and effort to ensure data integrity and confidentiality in clinical trials [79]. In blockchain health systems, medical data is recorded continuously. Additionally, since previous clinical studies' trial data are encrypted and stored in the blockchain in a distributed manner, they remain unchanged and would be available for future studies [136].

Challenge 4.2 Patients often experience burden in remembering their medication history or carrying physical copies of their medication records [152]. Patient reports, tests, and medical treatments generated by various doctors are managed independently [11, 12, 99, 142, 144, 157]. Many health institutions, doctors, and laboratories have their own database and manages their own information [99], without the intervention of patients. This situation affects the prevention and treatment of diseases for the population due to misinformation about a patient, potential information loss, or data leakage, which may imply an immediate risk to individuals and increase public health costs [124]. For instance, doctors might prescribe a medicine to patients that they are allergic to, as they cannot access the patients' medical history [158]. On the other hand, patients may be unaware of their medical reports, as they are not provided with complete documentation [117, 144].

Solutions 4.2. Electronic health records that are securely published on blockchain-based health applications with patients' consents would address the problem given in Challenge 4.2. Using a decentralized ledger system, health professionals could update and query medication histories of patients after getting patients' approval [152]. Thus, doctors and other healthcare providers can reach patients' health data [148, 157] and perform transactions such as adding scans and laboratory results [12].

Challenge 4.3. The patients' consent is essential for using their medical records for various purposes. However, most people give consent using paper forms, and they do not have control over it. Healthcare organizations are also having difficulties in dealing with the patients' consent. Patients give consent and may want to withdraw it later. There is a need to allow healthcare organizations to manage patients' consent [159].

Solution 4.3. Individuals'/Patients' consent could be stored in blockchain and shared by the participating parties in an immutable way [159]. This is a way to provide individuals to have control over their data. Rather than one-time-only consent models, this dynamic structure allows individuals to override their consent terms in time as a new block [16].

Challenge 4.4. A patient's medical history or patient's informed consent must be available at the required time [81, 110]. In current systems, maintaining a medical history to meet this criterion is costly [99], time-consuming, and labor-intensive.

Solution 4.4. The health records stored on the blockchain network are permanent and are replicated across multiple nodes [121]. This ensures that all patient data is available at the required moment and required place [160].

Challenge 4.5. Regulations require insurance companies to maintain directories that contain up-to-date demographic information about doctors and other healthcare providers. Maintaining its index for each insurer is time-consuming and expensive.

Claim and payment processing may be delayed if the information in these directories is inaccurate. Roughly \$2.1 billion is spent annually to track and maintain provider data across the healthcare system in the USA. A review completed by the Centers for Medicare and Medicaid Services (CMS) found that 52% of listed provider directory locations had at least one inaccuracy [161].

Solution 4.5. Administrative costs and data quality can be improved by sharing healthcare provider data and sharing changes of different parties on a blockchain. This feature enables identifying data inaccuracies within healthcare provider data [161].

In Table 9, we provide the FL and GL sources that highlight the blockchain-related solutions given above.

4.7 RQ4. Does blockchain introduce new challenges to software development in the health domain? RQ5. What are existing solution suggestions to the blockchain-related challenges in the health domain?

We compiled the blockchain-related problems and solutions below.

Challenge 1. Data cannot be altered or deleted after storing it in a blockchain [74]. However, according to health data protection laws, data is required to be deleted when a patient requests it [127, 138, 159] or to be changed (e.g., if a manufacturer enters incorrect information about a medicine) [127].

Solution 1. Storing the actual health data in an external storage and its hash value in the blockchain could be a solution to this problem [15, 84, 102, 131, 138, 141, 147]. The details of this topic are discussed more in-depth in Solution 9 as part of this paper. By not having the data itself on the blockchain, we could delete the data when requested by its owner. Hash values whose data has been deleted would remain in the blockchain.

Challenge 2. Heterogeneous data (e.g., X-rays, images and ECG signal data) are heavily used in the health domain [162], and size of health data can be pretty large [66, 146]. Along with the increase in data size, we need to deal with storage issues [124, 163] and mining costs [107].

Solution 2. Storing the original large-scale data in an external storage and keeping its hash in a blockchain would resolve dealing with large-sized data [84, 102, 131, 138, 141, 147] without compromising the tamper-resistant nature of blockchain. The hashes of large data embedded in a digitally signed transaction are added to blockchain by consensus. When the hash for the data in the external storage matches the hash in the blockchain, the origin and timestamp of the data can be verified. Furthermore, when the data in the external storage changes, the hash of the data also changes, and thus, data manipulations could be detected.

However, there is a deletion risk of external data when the data is stored off-chain. The rollup technology could be an alternative to this solution. Rollups move the computation off-chain but retain some data per transaction on-chain. It also provides a solution to the storage problem as the amount of data published on the chain is the minimum amount required to validate the rollups transaction [164] locally.

Table 9 Titles of blockchain powered solutions and the sources

Blockchain-powered solutions	Formal literature sources	Gray literature sources
Traceability and enabling authorized monitoring	[68, 70, 131, 151]	[69, 71–75, 161]
Smart contracts for automatically executing and controlling actions	[66, 76, 78–81, 91, 94, 95, 102, 127, 128, 138, 156, 159]	[73, 74, 129, 154]
Tamper resistance, keeping logs of transactions permanent/unchanged	[76, 79, 84, 85, 87, 89, 102, 103, 115, 126, 130, 136]	[73, 121]
Transparency and immutability contributing to the security and privacy of health data	[89, 95, 97, 99, 110, 124, 127, 131, 144]	[12, 74, 121, 134, 148, 157]
Consensus protocols eliminating the possibility of entering incorrect information	[136]	[121]
Pseudo-anonymity	[85–92]	[73]
Decentralized network structure making the system robust and resilient to intruders	[79, 81, 85, 89, 90, 92, 95, 98, 107, 118, 122, 127, 131, 135, 136, 152, 160]	[11, 74, 121, 134]
Ensuring authentication and security by using digital signatures	[70, 85, 89, 98, 99, 101, 104, 105, 116–119, 122–125]	[120, 121, 148]
Permissioned blockchains contributing to privacy of health data	[70, 79, 97, 109, 111, 125, 131, 132]	[2, 11, 72, 73, 133]
Patient reporting and health data control mechanisms	[85, 87, 91, 94, 96, 101, 107, 112, 118, 124, 130, 135, 137, 143–147, 151]	[2, 11, 73, 74, 134, 141, 142, 148]
Eliminating auditing role of central authority and intermediaries	[90, 95, 106, 126]	[74, 134]

Challenge 3. Blockchain poses performance [91, 101, 117, 127, 130, 133, 146] and scalability challenges [66, 92, 110]. As a performance issue, the read latency increases with the growth of ledgers [94, 122]. Public blockchains suffer from scalability issues due to ledger replication in all network participants and consensus mechanisms [165] and the need for significant computing power and storage space required on each node [92]. As each node repeats the same process for mining the next block, it is impossible to perform parallel executions in a blockchain, which reduces system efficiency, and therefore may cause bandwidth and response time problems.

Solution 3.a. Architectural design decisions such as using consensus models impact blockchain system performance [127]. The choice of consensus algorithms affects both scalability and computing performance. For example, Practical Byzantine Fault Tolerance (PBFT) consensus algorithm is not that scalable but offers superior performance than Proof of Work (PoW) consensus algorithm [91, 92]. Instead of the Proof of Work (PoW), the Delegated Proof of Stake (DPOS) algorithm could be employed in medical blockchain to avoid high energy costs, as DPOS does not require competition over discovering the blocks and is, therefore, more efficient [89]. Another design decision is to make the blockchain public, consortium or fully private [166]. Consortium blockchain networks with trusted nodes may be preferred if high performance is expected from an application. They have much higher execution and processing efficiency (35,000 transactions per second) and higher computing power than public blockchain solutions [66].

Solution 3.b. Dividing the network into small groups, called shards, could be used to address scalability issues [165]. Hyperledger Fabric supports multiple channels, each maintaining a separate ledger and smart contract [79]. Transactions can be processed in parallel while running consensus within each shard with a subset of blockchain nodes. Although this technique could help solve scalability issues, the communication overhead between shards can degrade network performance. Minimization of cross-shard communication is possible by creating complete shards based on “the need to participate” nodes per patient [165]. We should also note that currently there is active research ongoing on sharding features in Ethereum as of July 2022 [127, 167].

Solution 3.c. The efficiency of the blockchain is highly dependent on the coding of smart contracts. A smart contract which is coded properly (e.g., reduced external data storage access) could be executed in a quick and efficient manner [127].

Solution 3.d. Standardizing the data to be stored and exchanged on a blockchain could be a solution to achieve better performance and efficiency. Ledgers could align and define data’s type, size, and format. Restricting access to the blockchain network also helps standardize the data [66].

Challenge 4. Data providers may not have a culture of handing over the control of the data [151]. Furthermore, not everyone is capable of managing their personal health data. Studies conducted by the Connected Health Cities Programme and Wellcome Trust Fund have shown that most citizens are not interested in managing their data [147]. On the other hand, a vast majority of the population is unfamiliar with blockchain technology. If patients lose their private keys, the associated resources become inaccessible to these patients and this issue requires recovery

solutions outside of blockchain to re-establish ownership of the patient [90]. To fully obtain the potential benefits of blockchain in the health domain, all parties involved in a health system need to be part of blockchain-based solutions [82, 99]. Some stakeholders may be reluctant to join the network for fear of losing their competitive advantage [66].

Solution 4. Solutions to these problems have not yet been proposed.

Challenge 5. Blockchain development imposes certain constraints on the development processes. **Challenge 5.1** A smart contract code cannot be changed once it is added to a network. When a change request is received, a new contract needs to be deployed (upgrading) [168, 169].

Solution 5.1 While this issue reminds us running a waterfall-like plan-driven development process for smart contract development, it does not guarantee error-free features. However, this problem can be addressed by establishing new software design principles to assist the development of high-quality smart contracts.

Challenge 5.2 Smart contracts need to be tested in a production environment as part of the development process. Testing smart contract in the production environment in the public blockchain includes an execution fee (called gas price in Ethereum). This fee varies depending on the operations performed by the smart contract. Calculating the cost of executing a smart contract on a blockchain network may be challenging, particularly for large-scale projects with complex coding [170].

Solution 5.2 There is no solution addressing this problem in our resource pool. Smart contract testing is free in test networks. Before deploying smart contracts to production environment, testing practices need to be applied in the test network to reduce the costs.

Challenge 5.3. Gas costs are proportional to the number of stored data and operations (i.e., memory and storage access) in smart contracts. Storage access needs increase gas cost dramatically [127].

Solution 5.3. There are tools (e.g., Remix IDE) that could estimate execution and transaction costs and helps adjust these costs [127]. Additionally, this problem may be solved by establishing cost-efficient smart contract programming practices and a software development life cycle specific to blockchain-based applications to manage the development process better.

Challenge 6. There is a trade-off between transparency and confidentiality. Blockchain is intended to increase trust and enable transparency by sharing health data. Access control imposes limits on data sharing and provides a level of confidentiality [105].

Solution 6. When developing a blockchain platform, access control should only be on the identifiable data, yet a level of transparency should be allowed on the blockchain for other data types/categories [105].

Challenge 7. Blockchain keeps log of all the activities taken place in the chain. Data is stored in every block of the blockchain; so, there is no chance of losing data, but there is a possibility of creating redundant data [162].

Solution 7. The blockchain technology would require upgrades to solve the redundant data creation problem [162]. Additionally, InterPlanetary Filesystem (IPFS) is a distributed, peer-to-peer storage network which inherently allows

deduplication [80]. Therefore, IPFS could be used together with blockchain to leverage deduplication feature of IPFS [171].

Challenge 8. Blockchain networks work in their unique way, leading to interoperability issues where different blockchains cannot communicate [127].

Solution 8. This problem can be avoided if a unified blockchain-based solution is used between healthcare centers. However, it will be very difficult to make them interoperable if healthcare centers decide to use different blockchain-based solutions in varying platforms [127].

Challenge 9. Many countries have strong regulations for storing or transmitting medical data [131]. Therefore, storing and transmitting personal data in a transparent medium are not allowed.

Solution 9. Rather than storing the actual data, its hash value could be stored or could be transmitted in a blockchain [15, 84, 102, 131, 133, 138, 141, 147]. Whether hashed data being considered as personal data is an ongoing debate. If it is considered as personal data, hash sharing becomes another challenge. In this regard, it is important that regulatory guidance is issued on this subject [93]. Kim et al. also mention that medical data is only kept by certified bodies in some countries including South Korea and member states of the European Union. As a solution to this problem, they suggest keeping the hash of the data in a blockchain and leaving the storage of the data only to certified medical bodies, in separate databases [131]. On the other hand, hash itself may not be secure enough, as the hash can be linked with patients, and is subject to brute force attack [172]. In such circumstances, a keyed-hash may be a better alternative, as it uses a secret key as an additional input to hashing [173].

Challenge 10. In blockchain solutions, it may be difficult to define the legal boundaries in blockchain technology components, which complicates the role of health authorities. For instance, when a new drug-related transaction is executed on a blockchain network, health authorities need to define legal obligations for the stakeholders involved in the transaction. Although there is still no definitive provision in the current laws and regulations for blockchain technology in healthcare [66], blockchain networks need to comply with the existing regulatory requirements, such as the U.S. Drug Supply Chain Security Act (DSCA) and General Data Protection Regulation (GDPR) [66].

Solution 10. Blockchain frameworks need to be developed to comply with existing regulatory frameworks. Hyperledger Fabric can be given as an example which was designed compliant with HIPAA and GDPR [174]. Additionally, the policymakers need to consider addressing issues such as block ownership and access permissions on blockchain networks.

5 Conclusion and future work

In this study, we performed a multivocal literature review to identify blockchain application areas and the motivation behind adopting blockchain in the health domain. We extracted data from both formal and gray literature sources to identify

the problem and solution suggestions on this topic. On the problem side, we focused on both the challenges of developing software and adopting blockchain technology in the health domain. On the solution side, we specified blockchain technology's contribution in resolving inherited health application development challenges and the solutions occur due to adopting blockchain technology into health software development.

We found that blockchain technology in the health domain is applied in the following fields: electronic health and medical record management, Internet of medical things/remote patient monitoring, medicine supply chain management, clinical trials, precision medicine, empowering public health surveillance, and health insurance.

Blockchain has a significant potential in contributing to the inherent health domain challenges such as ensuring regulatory requirements and ensuring public health surveillance, dealing with security, privacy, interoperability issues, and preventing waste of health resources. Blockchain technology contributes to resolving these challenges by enabling regulatory bodies to monitor medical supply chains and preventing data manipulation. The technology increases transparency in transactions, gives patients control of their health data and the right to report personal health records, and enables pseudo-anonymity by eliminating the auditing role of central authority and intermediaries.

While providing solutions to the inherent health domain challenges, blockchain introduces new challenges as well: issues of data protection, data size, performance, confidentiality, personal data management, development process, creation of redundant data, and ensuring interoperability among different blockchain parties.

We summarize solution suggestions to these challenges as follows: addressing data protection and size problems by storing health data in external storages and its hash in the blockchain; increasing performance with architectural design decisions, consensus protocol decisions, and cost-effective smart contract coding; meeting confidentiality by using permissioned blockchain type and allowing pre-selected participants to join the network; addressing development process issues by using tools for estimation of gas cost, developing new software design principles, and by creating a new software development life cycle to meet specific constraints of blockchain-based applications; and addressing interoperability among different blockchains by using unified blockchain-based solutions among healthcare centers.

The FL and GL sources' analysis reveals that both source types highlight similar challenges and solutions. Compared with the SLR we performed in 2020 [23], we found new blockchain application areas, challenges, and solution suggestions with the MLR. We summarize the differences of the results of these studies in Table 10.

Blockchain technology introduces specific constraints to development processes in the health domain. While developing a blockchain application in the health domain, we recommend addressing the blockchain-related challenges and solution suggestions we have presented in this MLR.

Table 10 Comparison of the SLR [23] and the MLR

	SLR	New Information found with the MLR
Blockchain application areas	Electronic health and medical record management, Internet of Medical Things, medicine supply chain management, clinical trials, precision medicine	Empowering public health surveillance, health insurance
Inherent health domain challenges	Ensuring regulatory requirements, dealing with security, privacy, and interoperability issues	Ensuring public health surveillance, preventing waste of resources
Blockchain-powered solutions to the inherent health domain challenges	Enabling regulatory bodies to monitor medical supply chains, and preventing data manipulation. The technology increases transparency in transactions and gives patients control of their health data	Pseudo-anonymity, eliminating auditing role of central authority and intermediaries, enabling patient-reporting mechanism
New challenges introduced by blockchain to the health software development	Issues of data protection, data size, performance, personal data management, development process	Issues of confidentiality, creation of redundant data, interoperability between different blockchain parties
Solution suggestions to the blockchain-related challenges	Addressing data protection and size problems by storing health data in external storages and its hash in the blockchain; increasing performance with architectural design decisions, developing new software design principles, and by creating a new software development life cycle to meet specific requirements of blockchain-based applications	Addressing data protection and size problems by consensus protocol decisions, and proper smart contract coding; ensuring confidentiality by using private blockchain type and allowing pre-selected participants to join the network; addressing development process issues by using tools for estimation of gas cost; resolving redundant data problem by regular upgrade of blockchain technology; addressing interoperability between different blockchains by using unified blockchain-based solutions among healthcare centers

5.1 Future work

We can state that there is still room for improvements in adoption of the blockchain in the health domain. The results of this study which present both theoretical and practical perspectives could be used for identifying potential research topics and issues to consider before adoption. Below, we list these potential research topics on blockchain adoption in the health domain:

- Policymakers, blockchain researchers, and developers need to work together in developing regulatory guidelines for addressing the rules for the collaboration of network participants, data privacy, what data to share, data deletion on patient demand, and ensuring interoperability between various ledgers in blockchain networks.
- Different data privacy, security, and sharing policies need to be addressed in designing blockchains and smart contracts considering the patient mobility across nations.
- Use of blockchain technology in the health domain has the potential to generate massive amounts of sensitive personal health data. Blockchain technology could be used together with artificial intelligence to meaningfully process the data collected in blockchain.
- In large-scale blockchain adoption, data grows exponentially, and this causes performance issues in data retrieval. Effective and efficient data retrieval processes suitable for such blockchain applications need to be developed.
- Integration of blockchain technology with currently running healthcare systems (e.g., electronic health record management systems) could be explored.
- Data in the blockchain is transparent, which causes data privacy infringement. In the health domain, sensitive patient data is stored transparently. Additional privacy mechanisms such as keyed hash need to be developed.
- Current development life cycle models are not fully compatible with the development process of blockchain-based applications due to the structural characteristics of blockchain, such as contract immutability, necessity of testing in production environments, and test execution fees. Therefore, it is necessary to develop a new blockchain development life cycle model considering its structural characteristics and guiding an efficient and sustainable blockchain development environment.
- Malta, Estonia, and South Korea are countries adopting blockchain at national scale in the health domain. These successful implementations at governmental levels may be inspirations for other countries.
- We also suggest regularly continuing the MLR studies to reflect current state of the art both from the researcher and practitioner perspectives.

Data availability The datasets generated and analyzed during this study are publicly available in the Google Drive repository at the following link: <https://docs.google.com/spreadsheets/d/1BgiSc5I19pnk85ItWVdyegTZq9z0oH5M/edit?usp=sharing&ouid=103349517467780229403&rtppof=true&sd=true>

Declarations

Conflict of interest All authors state that this study is not funded by any sources of funding, and there are no financial or non-financial conflicts of interest with the names referred in the manuscript.

References

1. Yaga D, Mell P, Roby N, Scarfone K (2019) Blockchain technology overview. National Institute of Standards and Technology Internal Report, NIST.IR.8202. <https://doi.org/10.6028/NIST.IR.8202>
2. T. Einaste, "Blockchain and healthcare: the Estonian experience." <https://e-estonia.com/blockchain-healthcare-estonian-experience/> Accessed 5 Sep 2021
3. Jeong S, Ahn B (2022) A study of application platform for smart contract visualization based blockchain. *J Supercomput* 78(1):343–360
4. Yoo SG, Ahn B (2021) A study for efficiency improvement of used car trading based on a public blockchain. *J Supercomput* 77(9):10621–10635
5. Jeong S, Ahn B (2021) Implementation of real estate contract system using zero knowledge proof algorithm based blockchain. *J Supercomput* 77(10):11881–11893
6. "Dentacoin ecosystem," 2020. <https://dentacoin.com> Accessed 28 Aug 2021
7. "MediBloc," 2020. <https://medibloc.org/en> Accessed 30 Aug 2021
8. "SRcoin," 2020. <https://www.srcoin.info> Accessed 30 Aug 2021
9. Coinopsy, "MediShares (MDS)," 2021. <https://www.coinopsy.com/medishares-mds/> Accessed 30 Aug 2021
10. G. Hohenheim, "AIDOC, blog on a blockchain company in AI & Healthcare," 2018. <https://medium.com/@grhohenheim/aidoc-blog-on-a-blockchain-company-in-ai-healthcare-b6020488cc4> Accessed 1 Sep 2021
11. Medicalchain, "Medicalchain Whitepaper," 2018. [Online]. Available: <https://medicalchain.com/Medicalchain-Whitepaper-EN.pdf>. Accessed 1 Sep 2021
12. Medicalchain, "Medicalchain Explainer Video - Blockchain Technology for Electronic Health Records." <https://www.youtube.com/watch?v=CsxjlsBYmrl>. Accessed 1 Sep 2021
13. "Patientory," 2021. <https://patientory.com/> Accessed 2 Sep 2021
14. "The health insurance portability and accountability act (HIPAA)." <https://www.hhs.gov/hipaa/for-professionals/privacy/index.html> Accessed 02 Jan 2022
15. Lindman J et al. (2020) "The uncertain promise of blockchain for government", OECD working papers on public governance, No. 43, OECD Publishing, Paris, <https://doi.org/10.1787/d031cd67-en> Accessed 28 May 2022
16. Mamo N, Martin GM, Desira M, Ellul B, Ebejer JP (2020) Dwarna: a blockchain solution for dynamic consent in biobanking. *Eur J Hum Genet* 28(5):609–626
17. "The food and drug administration (FDA)." <https://www.fda.gov/home> Accessed 5 Jan 2022
18. "The medical device directives," European commission. https://ec.europa.eu/growth/sectors/medical-devices/current-directives_en Accessed 5 Jan 2022
19. FDA, "FDA 's technology modernization action plan (TMAP)," 2019. <https://www.fda.gov/media/130883/download> Accessed 5 Jan 2022
20. Reuters, "IBM , Walmart , Merck in blockchain collaboration with FDA." <https://www.reuters.com/article/us-fda-blockchain/ibm-walmart-merck-in-blockchain-collaboration-with-fda-idUSKCN1TEISA> Accessed 5 Jan 2022
21. Barbara Kitchenham O, Brereton P, Budgen D, Turner M, Bailey J, Linkman S (2009) Systematic literature reviews in software engineering – a systematic literature review. *Inform Softw Technol* 51(1):7–15. <https://doi.org/10.1016/j.infsof.2008.09.009>
22. Schöpfel J, Farace DJ (2009) Gray literature, In: *Encyclopedia of library and information sciences*, Third Edition pp 2029–2039 (CRC Press)

23. Baysal MV, Özcan-Top Ö, Can AB (2021) Implications of Blockchain technology in the health domain. In: Arabnia HR, Deligiannidis L, Tinetti FG, Tran Q-N (eds) *Advances in software engineering, education, and e-Learning: Proceedings from FECS'20, FCS'20, SERP'20, and EEE'20*. Springer International Publishing, Cham, pp 641–656. https://doi.org/10.1007/978-3-030-70873-3_45
24. McGhin T, Choo KKR, Liu CZ, He D (2019) Blockchain in healthcare applications: research challenges and opportunities. *J Netw Comput Appl* 135:62–75. <https://doi.org/10.1016/j.jnca.2019.02.027>
25. Yaqoob S et al (2019) Use of blockchain in healthcare: a systematic literature review. *Int J Adv Comput Sci Appl* 10(5):644–653. <https://doi.org/10.14569/ijacsa.2019.0100581>
26. Agbo C, Mahmoud Q, Eklund J (2019) Blockchain technology in healthcare: a systematic review. *Healthcare* 7(2):56. <https://doi.org/10.3390/healthcare7020056>
27. Hölbl M, Kompara M, Kamišalić A, Zlatolas LN (2018) A systematic review of the use of blockchain in healthcare. *Symmetry* 10(10):470. <https://doi.org/10.3390/sym10100470>
28. Hussien HM, Yasin SM, Udzir SNI, Zaidan AA, Zaidan BB (2019) A systematic review for enabling of develop a blockchain technology in healthcare application: taxonomy, substantially analysis, motivations, challenges, recommendations and future direction. *J Med Syst*. <https://doi.org/10.1007/s10916-019-1445-8>
29. Mayer AH, da Costa CA, Righi RDR (2020) Electronic health records in a Blockchain: a systematic review. *Health Inform J* 26(2):1273–1288
30. Santoso DB, Fuad A, Herwanto GB, Maula AW (2020) Blockchain technology implementation on medical records data management: a review of recent studies. *Jurnal Riset Kesehatan* 9(2):107–112. <https://doi.org/10.31983/jrk.v9i2.5742>
31. Tandon A, Amandeep Dhir AKM, Islam N, Mäntymäki M (2020) Blockchain in healthcare: a systematic literature review, synthesizing framework and future research agenda. *Comput Ind* 122:103290. <https://doi.org/10.1016/j.compind.2020.103290>
32. Abu-elezz I, Hassan A, Nazeemudeen A, Househ M, Abd-alrazaq A (2020) The benefits and threats of blockchain technology in healthcare: a scoping review. *Int J Med Inform* 142:104246. <https://doi.org/10.1016/j.jmedinf.2020.104246>
33. I. Dauda, B. Nuhu, J. Abubakar, and D. Maliki, 2021 “Blockchain technology in healthcare systems : applications, methodology, problems, and current trends,” 9 1 p 431–443
34. Aithal PS, Aithal A, Dias E (2021) Blockchain technology - current status and future research opportunities in various areas of healthcare industry. *Int J Health Sci Pharm* 5(1):130–150. <https://doi.org/10.47992/ijhsp.2581.6411.0070>
35. Fang HSA (2021) Commercially successful blockchain healthcare projects: a scoping review. *Blockchain Healthcare Today* 1:1–8. <https://doi.org/10.30953/bhty.v4.166>
36. Fang HSA, Tan TH, Tan YFC, Tan CJM (2021) Blockchain personal health records: systematic review. *J Med Internet Res* 23(4):e25094
37. Elangovan D, Long CS, Bakrin FS, Tan CS, Goh KW, Yeoh SF, Ming LC (2022) The use of blockchain technology in the health care sector: systematic review. *JMIR Med Inform* 10(1):e17278
38. Adere EM (2022) Blockchain in healthcare and IoT: a systematic literature review. *Array* 14:100139. <https://doi.org/10.1016/j.array.2022.100139>
39. Mamun AA, 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>
40. Lamport L (1998) The part-time parliament. *ACM Trans Inform Syst* 16(2):133–169. <https://doi.org/10.1145/279227.279229>
41. Stuart Haber W, Stornetta S (1991) How to time-stamp a digital document. In: Menezes AJ, Vanstone SA (eds) *Advances in Cryptology-CRYPTO' 90*. Springer, Berlin, Heidelberg, pp 437–455. https://doi.org/10.1007/3-540-38424-3_32
42. Kornmesser S (2008) Theoretizität im logischen empirismus und im strukturalismus – erläutert am fallbeispiel des neurobiologischen konstruktivismus. *J Gen Philos Sci* 39(1):53–67. <https://doi.org/10.1007/s10838-008-9062-0>
43. Ethereum Web site, <https://ethereum.org/en/> Accessed 4 July 2022
44. Belchior R, Vasconcelos A, Guerreiro S, Correia M (2021) A survey on blockchain interoperability: past, present, and future trends. *ACM Comput Surv (CSUR)* 54(8):1–41
45. Lafourcade P, Lombard-Platet M (2020) About blockchain interoperability. *Inf Process Lett* 161:105976

46. G. Heidenreich, (2014) "Scope of IEC health software standards", In: TOPRA annual medical devices symposium.
47. J. Jensen and I. Sandoval-watt, (2020) "Software in medical devices", https://www.advamed.org/sites/default/files/resource/software_in_medical_devices_-_module_1.pdf Accessed 5 Dec 2020
48. International medical device regulatory forum, "IMDRF software as a medical device (SaMD)," 2013. [Online]. Available: <http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-131209-samd-key-definitions-140901.pdf>.
49. "IEC 82304-1:2016 Health software — Part 1: General requirements for product safety," 2016. <https://www.iso.org/standard/59543.html>.
50. "IEC 62304:2006 Medical device software — Software life cycle processes," 2006. <https://www.iso.org/standard/38421.html>.
51. "ISO 14971:2019 Medical devices — Application of risk management to medical devices," 2019.
52. "IEC/TR 80002-1:2009 Medical device software — Part 1: Guidance on the application of ISO 14971 to medical device software," 2009.
53. "IEC/TR 80002-3:2014 Medical device software — Part 3: Process reference model of medical device software life cycle processes (IEC 62304)," 2014. <https://www.iso.org/standard/65624.html>.
54. Mankowitz S (2018) 2.1 Clinical decision support. In: Mankowitz S (ed) Clinical informatics board review and self assessment. Springer International Publishing, Cham, pp 41–69. https://doi.org/10.1007/978-3-319-63766-2_3
55. US food and drug administration, 2017 "Software as a medical device (SAMd): clinical evaluation," <https://doi.org/10.1109/ISIT.2012.6284109>.
56. FDA, "wireless medical devices," 2014. <http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/ConnectedHealth/WirelessMedicalDevices/default.htm> Accessed 6 Dec 2020
57. U.S. food and drug administration, "General principles of software validation; final guidance for industry and FDA staff," 2002. [Online]. Available: <http://www.fda.gov/downloads/RegulatoryInformation/Guidances/ucm126955.pdf>
58. Garousi V, Felderer M, Mäntylä MV (2019) Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. *Inform Softw Technol* 106:101–121. <https://doi.org/10.1016/j.infsof.2018.09.006>
59. Baysal, M. V., Özcan-Top, Ö., Betin-Can, A. Multivocal Literature review: online repository, 2022 <https://docs.google.com/spreadsheets/d/1BgSc5II9pnk85ltWVdyegTZq9z0oH5M/edit?usp=sharing&oid=103349517467780229403&rtpof=true&sd=true>
60. Adams RJ, Smart P, Huff AS (2017) Shades of grey: guidelines for working with the grey literature in systematic reviews for management and organizational studies. *Int J Manag Rev* 19(4):432–454. <https://doi.org/10.1111/ijmr.12102>
61. "Finding the hard to finds - HLWIKI," 2012. <https://studylib.net/doc/7663974/finding-the-hard-to-finds---hlwiki-canada>
62. Jadhav J, Deshmukh J A review study of the blockchain-based healthcare supply chain, Available at SSRN 4088924 (Preprint).
63. Attaran M (2022) Blockchain technology in healthcare: challenges and opportunities. *Int J Healthcare Manage* 15(1):70–83
64. M.Höst and P.Runeson, 2007 "Checklists for software engineering case study research," In: Proceedings - 1st international symposium on empirical software engineering and measurement, ESEM 2007, pp 482–484
65. Raryelcostasouza, "pyTranscriber application," 2020. <https://github.com/raryelcostasouza/pyTranscriber/releases> Accessed 20 Oct 2021
66. Uddin M (2021) Blockchain medledger: hyperledger fabric enabled drug traceability system for counterfeit drugs in pharmaceutical industry. *Int J Pharm* 597:120235. <https://doi.org/10.1016/j.ijpharm.2021.120235>
67. World health organisation (WHO) (2017) "1 in 10 medical products in developing countries is substandard or falsified," Who, <http://www.who.int/mediacentre/news/releases/2017/substandard-falsified-products/en/> Accessed 27 Dec 2021
68. Sylim P, Liu F, Marcelo A, Fontelo P (2018) Blockchain technology for detecting falsified and substandard drugs in distribution: pharmaceutical supply chain intervention. *JMIR Res Protoc* 7(9):1–12. <https://doi.org/10.2196/10163>
69. A. Takyar, "Blockchain in pharma supply chain-reducing counterfeit drugs," 2021. <https://www.leewayhertz.com/blockchain-in-pharma-supply-chain/>. Accessed 10 Dec 2020

70. Haq I, Muselemu O (2018) Blockchain technology in pharmaceutical industry to prevent counterfeit drugs. *Int J Comput Appl* 180(25):8–12. <https://doi.org/10.5120/ijca2018916579>
71. R. Mauri, “Blockchain for fraud prevention: Industry use cases,” *IBM Blockchain Blog*, 2017. <https://www.ibm.com/blogs/blockchain/2017/07/blockchain-for-fraud-prevention-industry-use-cases/>. Accessed 10 Dec 2020
72. IBM, “Using blockchain to prevent counterfeit drugs in Kenya.” <https://www.youtube.com/watch?v=11Z4-XYoZAE>. Accessed 26 Oct 2021
73. Telusko, (2021) “Blockchain in healthcare | use case.” <https://www.youtube.com/watch?v=dvFOMm6mBao> Accessed 12 Nov 2021
74. Webmedy (2021) “Advantages of blockchain technology for healthcare.” https://www.youtube.com/watch?v=r5Eqdm9v2_E Accessed 22 Nov 2021
75. H. Landi, “IBM rolls out blockchain network to address supply-chain issues caused by COVID-19,” 2020. <https://www.fiercehealthcare.com/tech/ibm-rolls-out-blockchain-network-to-match-healthcare-organizations-non-traditional-suppliers>. Accessed 05 Dec 2020
76. Nugent T, Upton D, Cimpoesu M (2016) Improving data transparency in clinical trials using blockchain smart contracts. *F1000Research* 5:2541. <https://doi.org/10.12688/f1000research.9756.1>
77. “COMPARE Tracking Switched Outcomes in Clinical Trials.” <https://compare-trials.org/results> Accessed 28 Dec 2021
78. Tseng J-H, Liao Y-C, Chong B, Liao S-W (2018) Governance on the drug supply chain via gcoin blockchain. *Int J Environ Res Public Health* 15(6):1055. <https://doi.org/10.3390/ijerph15061055>
79. O. Choudhury, N. Fairiza, I. Sylla, and A. Das, “A Blockchain (2019) Framework for managing and monitoring data in multi-site clinical trials,” In: *IEEE international conference on healthcare informatics (ICHI)*, pp 1–9
80. Omar IA, Jayaraman R, Salah K, Simsekler MCE, Yaqoob I, Ellahham S (2020) Ensuring protocol compliance and data transparency in clinical trials using blockchain smart contracts. *BMC Med Res Methodol* 20(1):1–17. <https://doi.org/10.1186/s12874-020-01109-5>
81. Jung HH, Pfister FMJ (2020) Blockchain-enabled clinical study consent management. *Technol Innov Manag Rev* 10(2):14–24. <https://doi.org/10.22215/timreview/1325>
82. Wong DR, Bhattacharya S, Butte AJ (2019) Prototype of running clinical trials in an untrustworthy environment using blockchain. *Nat Commun* 10(1):1–8. <https://doi.org/10.1038/s41467-019-08874-y>
83. FBI, “Insurance fraud.” <https://www.fbi.gov/stats-services/publications/insurance-fraud> Accessed 28 Dec 2021
84. A. Juneja and M. Marefat, (2018) “Leveraging blockchain for retraining deep learning architecture in patient-specific arrhythmia classification,” In: *Proceedings 2018 IEEE EMBS international conference on biomedical and health informatics, BHI 2018*, vol. 2018-Janua, pp 393–397
85. D. Ivan, (2016) “Moving Toward a Blockchain-based Method for the Secure Storage of Patient Records,” In: *Proceedings NIST workshop on blockchain & healthcare*, pp 11, [Online], Available: https://www.healthit.gov/sites/default/files/9-16-drew_ivan_20160804_blockchain_for_healthcare_final.pdf
86. Griggs KN, Ossipova O, Kohlios CP, Baccarini AN, Howson EA, Hayajneh T (2018) Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *J Med Syst* 42(7):1–7. <https://doi.org/10.1007/s10916-018-0982-x>
87. H. Jita and V. Pieterse, (2018) “A framework to apply the internet of things for medical care in a home environment,” In: *Proceedings ACM international conference proceeding series*, pp 45–54
88. X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li (2018) “Integrating blockchain for data sharing and collaboration in mobile healthcare applications,” In: *Proceedings IEEE international symposium on personal, indoor and mobile radio communications, PIMRC*, vol. 2017, pp 1–5
89. Chen Y, Ding S, Xu Z, Zheng H, Yang S, Chen Y (2017) Blockchain-based medical records secure storage and medical service framework. *J Med Syst* 43(1):2019
90. Patel V (2019) A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. *Health Inform J* 25(4):1398–1411. <https://doi.org/10.1177/1460458218769699>
91. A. Muniat, P. R. Ullah, and S. Mushsharat, (2021) “An automated approach towards smart healthcare with blockchain and smart contracts,” In: *Proceedings international conference on computing, communication, and intelligent systems*, pp 250–255

92. Pandey P, Litoriya R (2020) Implementing healthcare services on a large scale: challenges and remedies based on blockchain technology. *Health Policy Technol* 9(1):69–78. <https://doi.org/10.1016/j.hlpt.2020.01.004>
93. Finck M (2018) Blockchains and data protection in the European Union. *Eur Data Prot L Rev* 4:17
94. Xiao Y, Xu B, Jiang W, Wu Y (2021) The healthchain blockchain for electronic health records: development study. *J Med Internet Res* 23(1):1–13. <https://doi.org/10.2196/13556>
95. Sultana M, Hossain A, Laila F, Taher KA, Islam MN (2020) Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology. *BMC Med Inform Decis Mak* 20(1):1–10
96. Y. Zhuang et al., “Development of a blockchain framework for virtual clinical trials,” pp 1412–1420
97. Taralunga DD, Florea BC (2021) A blockchain-enabled framework for mHealth systems. *Sensors* 21(8):1–24. <https://doi.org/10.3390/s21082828>
98. T. Dey, S. Jaiswal, S. Sunderkrishnan, and N. Katre (2018) “HealthSense: a medical use case of internet of things and blockchain,” In: Proceedings of the international conference on intelligent sustainable systems, ICISS 2017, no. Iciss, pp 486–491
99. Kumar A, Krishnamurthi R, Nayyar A, Sharma K, Grover V, Hossain E (2020) A novel smart healthcare design, simulation, and implementation using healthcare 4.0 processes. *IEEE Access* 8:118433–118471. <https://doi.org/10.1109/ACCESS.2020.3004790>
100. 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):44. <https://doi.org/10.3390/info8020044>
101. A. Ekblaw, A. Azaria, J. D. Halamka, and A. Lippman, (2016) “A case study for blockchain in healthcare,” In: Proceedings of IEEE open & big data conference, vol. 13, p. 13, [Online]. Available: https://www.healthit.gov/sites/default/files/5-56-onc_blockchainchallenge_mitwhitepaper.pdf
102. A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman (2016) “MedRec: Using blockchain for medical data access and permission management,” In: Proceedings - 2016 2nd international conference on open and big data, OBD 2016, pp 25–30
103. Xia QI, Sifah EB, Asamoah KO, Gao J, Du X, Guizani M (2017) MeDShare : trust-less medical data sharing among. *IEEE Access* 5:1–10. <https://doi.org/10.1109/ACCESS.2017.2730843>
104. Lee H, Kung H, Udayasankaran JG (2020) An architecture and management platform for blockchain-based personal health record exchange : development and usability study. *J Med Internet Res* 22:1–15. <https://doi.org/10.2196/16748>
105. Antwi M, Adnane A, Ahmad F, Hussain R, ur RehmanKerrache MHCA (2021) The case of hyperledger fabric as a blockchain solution for healthcare applications. *Blockchain Res Appl* 2(1):100012. <https://doi.org/10.1016/j.bcr.2021.100012>
106. Sun B, Lv Z, Li Q (2021) Obstetrics nursing and medical health system based on blockchain technology. *J Healthcare Eng* 2021:1–11. <https://doi.org/10.1155/2021/6631457>
107. Gharat A, Aher P, Chaudhari P, Alte B (2021) A framework for secure storage and sharing of electronic health records using blockchain technology. *ITM Web Conf* 40:03037. <https://doi.org/10.1051/itmconf/20214003037>
108. Cyran MA (2018) Blockchain as a foundation for sharing healthcare data. *Blockchain Healthcare Today*. <https://doi.org/10.30953/bhty.v1.13>
109. R. Kumar, N. Marchang, R. Tripathi (2020) “Distributed off-chain storage of patient diagnostic reports in healthcare system using IPFS and Blockchain,” In: 2020 International conference on communication systems & networks (COMSNETS), pp 1–5
110. Zhuang Y, Sheets LR, Chen YW, Shae ZY, Tsai JJP, Shyu CR (2020) A patient-centric health information exchange framework using blockchain technology. *IEEE J Biomed Health Inform* 24(8):2169–2176. <https://doi.org/10.1109/JBHI.2020.2993072>
111. Chentharas S, Ahmed K, Wang H, Whittaker F (2020) A novel blockchain based smart contract system for referral in healthcare: healthchain. In: Huang Z, Siuly S, Wang H, Zhou R, Zhang Y (eds) *Health information science: 9th international conference, HIS 2020, Amsterdam, The Netherlands, October 20–23, 2020, Proceedings*. Springer International Publishing, Cham, pp 91–102. https://doi.org/10.1007/978-3-030-61951-0_9
112. Zhuang Y, Chen Y, Shae Z, Shyu C, Hall PN (2020) Generalizable layered blockchain architecture for health care applications : development, case studies, and evaluation. *J Med Internet Res* 22:1–13. <https://doi.org/10.2196/19029>

113. T. Taylor, "Hackers , breaches , and the value of healthcare data," 2021. <https://www.securelink.com/blog/healthcare-data-new-prize-hackers/> Accessed 2 Jan 2022
114. Healthcare IT News Staff, "The biggest healthcare data breaches of 2021," Healthcare IT News, 2021. <https://www.healthcareitnews.com/news/biggest-healthcare-data-breaches-2021> Accessed 2 Jan 2022
115. I. Khalil, (2019) "A novel architecture for tamper proof electronic health record management system using blockchain wrapper," In: Proceedings of the 2019 ACM international symposium on blockchain and secure critical infrastructure, pp 97–105
116. M. Saravanan, R. Shubha, A. M. Marks, and V. Iyer (2018) "SMEAD: A secured mobile enabled assisting device for diabetics monitoring," In: Proceedings 11th IEEE international conference on advanced networks and telecommunications systems, ANTS 2017, pp 1–6
117. J. Vora et al., (2019) "BHEEM: A blockchain-based framework for securing electronic health records," In: 2018 IEEE globecom work. GC Wkshps 2018-Proceedings, pp 1–6
118. H. Wu and L. Wang (2019) "A patient-centric interoperable framework for health information exchange via Blockchain," pp 0–4
119. Cichosz SL, Stausholm MN, Kronborg T, Vestergaard P, Hejlesen O (2019) How to use blockchain for diabetes health care data and access management: an operational concept. *J Diabetes Sci Technol* 13(2):248–253. <https://doi.org/10.1177/1932296818790281>
120. Healthureum (2021) "Healthureum HHEM - introducing blockchain into healthcare." <https://www.youtube.com/watch?v=pX0uWV1utbg> Accessed 17 Dec 2021
121. F. C. Coelho (2021) "Optimizing disease surveillance by reporting on the blockchain," pp. 1–10, 2018, [Online]. Available: <http://dx.doi.org/https://doi.org/10.1101/278473> Accessed 20 Dec 2021
122. Gong J, Zhao L (2020) Blockchain application in healthcare service mode based on health data bank. *Front Eng Manage* 7(4):605–614. <https://doi.org/10.1007/s42524-020-0138-9>
123. J. Hathaliya, P. Sharma, S. Tanwar, and R. Gupta (2019) "Blockchain-based remote patient monitoring in healthcare 4.0," In: Proceedings 2019 IEEE 9th international conference on advanced computing, pp 87–91
124. Gutiérrez O, Romero G, Pérez L, Salazar A, Charris M, Wightman P (2020) Healthyblock: blockchain-based IT architecture for electronic medical records resilient to connectivity failures. *Int J Environ Res Public Health* 17(19):7132. <https://doi.org/10.3390/ijerph17197132>
125. Chentharas 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>
126. Wang H, Song Y (2018) "Securlockce cloud-based EHR system using attribute-based cryptosystem and bhain. *J Med Syst* 42(8):1–9
127. Musamih A et al (2021) A blockchain-based approach for drug traceability in healthcare supply chain. *IEEE Access* 9:9728–9743. <https://doi.org/10.1109/ACCESS.2021.3049920>
128. Omar IA, Jayaraman R, Debe MS, Salah K, Yaqoob I, Omar M (2021) Automating procurement contracts in the healthcare supply chain using blockchain smart contracts. *IEEE Access* 9:37397–37409. <https://doi.org/10.1109/ACCESS.2021.3062471>
129. Coinsider, "Can blockchain " fix " healthcare ? (Solve . Care Deep Dive)." https://www.youtube.com/watch?v=sJDSF18M_5g
130. H. L. Pham, T. H. Tran, and Y. Nakashima, (2019) "A secure remote healthcare system for hospital using blockchain smart contract," In: Proceedings 2018 IEEE globecom workshops, GC Wkshps 2018-Proceedings, pp 1–6
131. Kim TM et al (2021) Dynamichain: development of medical blockchain ecosystem based on dynamic consent system. *Appl Sci* 11(4):1–20. <https://doi.org/10.3390/app11041612>
132. Usman M, Qamar U (2020) Secure electronic medical records storage and sharing using blockchain technology. *Procedia Comput Sci* 174:321–327. <https://doi.org/10.1016/j.procs.2020.06.093>
133. Stackoverflow (2021) "Permissions within a blockchain ?," <https://stackoverflow.com/questions/46308820/permissions-within-a-blockchain> Accessed 23 Nov 2021
134. Interbit (2021) "" Blockchain in healthcare " from BTL CTO hugh halford Thompson." <https://www.youtube.com/watch?v=yT0aM6D-TTk> Accessed 12 Dec 2021
135. Uddin MA, Stranieri A, Gondal I, Balasubramanian V (2018) Continuous patient monitoring with a patient centric agent: a block architecture. *IEEE Access* 6:32700–32726. <https://doi.org/10.1109/ACCESS.2018.2846779>
136. Tripathi G, Ahad MA, Paiva S (2020) S2HS- A blockchain based approach for smart healthcare system. *Healthcare* 8(1):100391. <https://doi.org/10.1016/j.hjdsi.2019.100391>


137. Pawar P, Parolia N, Shinde S, Edoh TO, Singh M (2021) eHealthChain—a blockchain-based personal health information management system. *Ann Telecommun.* <https://doi.org/10.1007/s12243-021-00868-6>
138. Esposito C, De Santis A, Tortora G, Chang H, Choo KKR (2018) Blockchain: A panacea for healthcare cloud-based data security and privacy? *IEEE Cloud Comput* 5(1):31–37. <https://doi.org/10.1109/MCC.2018.011791712>
139. Fan K, Wang S, Ren Y, Li H, Yang Y (2018) MedBlock: efficient and secure medical data sharing via blockchain. *J Med Syst* 42(8):1–11. <https://doi.org/10.1007/s10916-018-0993-7>
140. Chouhan AS, Qaseem MS, Basheer QMA, Mehdi MA (2021) Blockchain based EHR system architecture and the need of blockchain in healthcare. *Mater Today Proc.* <https://doi.org/10.1016/j.matpr.2021.06.114>
141. H. Foundation (2021) “ACTION-EHR : Patient-centric blockchain-based healthcare data management for alevtina dubovitskaya.” <https://www.youtube.com/watch?v=mH5jUNaiejs>. Accessed 2 Dec 2021
142. M. Mccarthy (2021) “Harvard blockchain health care use cases MIT’ s Shada AlSalama PhD.” <https://www.youtube.com/watch?v=lc0SIx1zvP0> Accessed 8 Dec 2021
143. Cernian A, Tiganoaia B, Sacala IS, Pavel A, Iftemi A (2020) Patientdatachain: a blockchain-based approach to integrate personal health records. *Sensors* 20(22):1–24. <https://doi.org/10.3390/s20226538>
144. Rathee G, Sharma A (2020) A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology. *Multimed Tools Appl* 79(15):9711–9733
145. M. T. de Oliveira et al., (2019) “Towards a Blockchain-Based Secure Electronic Medical Record for Healthcare Applications.” In: *Proceedings IEEE international conference on communications*, vol. 2019 <https://doi.org/10.1109/icc.2019.8761307>
146. A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, (2017) “Secure and trustable electronic medical records sharing using blockchain,” In: *Annual symposium proceedings. AMIA symposium*, , vol. 2017, pp 650–659
147. Leeming G, Cunningham J, Ainsworth J (2019) A ledger of me: personalizing healthcare using blockchain technology. *Front Med* 6:1–10. <https://doi.org/10.3389/fmed.2019.00171>
148. e-estonia (2021) “An overview of e-health services in estonia [Video].” <https://www.youtube.com/watch?v=H4QLzQGM3k> Accessed 2 Dec 2021
149. T. Crypto, “Solve care - healthcare on blockchain.” <https://www.youtube.com/watch?v=IYGJ9q5cMcc> Accessed 17 Dec 2021
150. A. Bhawiyuga, A. Wardhana, K. Amron, and A. P. Kirana, “Platform for integrating internet of things based smart healthcare system and blockchain network.” In: *Proceedings 6th NAFOSTED conference on information and computer science*, pp 55–60, 2019
151. Kshetri N (2018) Blockchain and electronic healthcare records. *IEEE Comput* 51(12):59–63
152. Zolfaghari AH, Nasiri M, Sharifian R (2019) Comment on: DMMS: a decentralized blockchain ledger for the management of medication histories. *Blockchain Healthcare Today.* <https://doi.org/10.30953/bhty.v2.98>
153. Abdeen MAR, Ali T, Khan Y, Yagoub MCE (2019) Fusing identity management, HL7 and blockchain into a global healthcare record sharing architecture. *Int J Adv Comput Sci Appl* 10(6):630–636. <https://doi.org/10.14569/ijacsa.2019.0100681>
154. I. Blockchain (2021) “How blockchain can streamline healthcare.” <https://www.youtube.com/watch?v=h3aZ8mrlR-0> Accessed 16 Nov 2021
155. Panda SS, Jena D, Das P (2021) A blockchain-based distributed authentication system for healthcare. *Int J Healthcare Inform Syst Inform* 16(4):1–14. <https://doi.org/10.4018/ijhisi.20211001.0a12>
156. Castaldo L, Cinque V (2018) Blockchain-based logging for the cross-border exchange of ehealth data in Europe. In: Gelenbe E, Campegiani P, Czachórski T, Katsikas SK, Komnios I, Romano L, Tzovaras D (eds) *Security in computer and information sciences: first international ISICIS security workshop 2018, Euro-CYBERSEC 2018, London, UK, February 26-27, 2018, revised selected papers.* Springer International Publishing, Cham, pp 46–56. https://doi.org/10.1007/978-3-319-95189-8_5
157. BlocksEDU, “Blockchain for electronic health records ?” <https://www.youtube.com/watch?v=FVQOOF5GCFs>
158. AMSYS (2021) “AMCHART patient driven electronic health record on the blockchain.” <https://www.youtube.com/watch?v=KpmRnPc1eIk> Accessed 18 Dec 2021

159. Tith D et al (2020) Patient consent management by a purpose-based consent model for electronic health record based on blockchain technology. *Healthcare Inform Res* 26(4):265–273. <https://doi.org/10.4258/hir.2020.26.4.265>
160. S. Sharma (2019) “PubHeal-A decentralized platform on health surveillance of people,” In: Proceedings 2019 IEEE pune section international conference, pp 1–6
161. Synaptic health alliance (2021) “Our pilot project,” 2021. <https://www.synaptichealthalliance.com/project> Accessed 23 Dec 2021
162. Kaur H, Alam MA, Jameel R, Mourya AK, Chang V (2018) A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment. *J Med Syst* 42(8):1–14. <https://doi.org/10.1007/s10916-018-1007-5>
163. Lu Q, Xu X (2017) Adaptable blockchain- based systems: a case study for product traceability. *IEEE Softw* 34(6):21–27
164. An Incomplete Guide to Rollups. <https://vitalik.ca/general/2021/01/05/rollup.html> Accessed 16 May 2022
165. Hashim F, Shuaib K, Sallabi F (2021) Medshard: electronic health record sharing using blockchain sharding. *Sustainability* 13(11):1–21. <https://doi.org/10.3390/su13115889>
166. X. Xu et al., (2017) “A taxonomy of blockchain-based systems for architecture design,” In: IEEE international conference on software architecture, pp 243–252
167. Shard Chains. <https://ethereum.org/en/upgrades/shard-chains/> Accessed 16 May 2022
168. Sillaber C, Waltl B (2017) Life cycle of smart contracts in blockchain ecosystems. *Datenschutz und Datensicherheit - DuD* 41(8):497–500. <https://doi.org/10.1007/s11623-017-0819-7>
169. R. Koul (2018) “Blockchain oriented software testing - challenges and approaches,” In: Proceedings 2018 3rd international conference for convergence in technology, pp 1–6
170. Miraz MH, Ali M (2020) Blockchain enabled smart contract based applications: deficiencies with the software development life cycle models. *Baltica J* 33(1):101–116
171. Zheng Q, Li Y, Chen P, Dong X (2018), An innovative IPFS-based storage model for blockchain, In: 2018 IEEE/WIC/ACM international conference on web intelligence (WI) pp 704–708 IEEE
172. European commission (2014) Article 29 Data protection working party. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf Accessed 28 May 2022
173. European parliamentary research service (2019). Blockchain and the general data protection regulation - can distributed ledgers be squared with European data protection law?. [https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU\(2019\)634445_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf) Accessed 28 May 2022
174. Hyperledger Web site, <https://www.hyperledger.org/blog/2019/12/02/hyperledger-for-healthcare-how-fabric-drives-the-next-generation-pharma-supply-chain> Accessed 31 May 2022
175. Z. Shae and J. J. P. Tsai, 2017 “On the design of a blockchain platform for clinical trial and precision medicine,” In: Proceedings - International conference on distributed computing systems, pp 1972–1980
176. Lee SH, Yang CS (2018) Fingernail analysis management system using microscopy sensor and blockchain technology. *Int J Distrib Sens Netw* 14(3):155014771876704. <https://doi.org/10.1177/1550147718767044>
177. Pandey P, Litoriya R (2020) Securing and authenticating healthcare records through blockchain technology. *Cryptologia* 44(4):341–356. <https://doi.org/10.1080/01611194.2019.1706060>
178. Kim HJ et al (2021) Smart decentralization of personal health records with physician apps and helper agents on blockchain: Platform design and implementation study. *JMIR Med Inform* 9(6):1–14. <https://doi.org/10.2196/26230>

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.

Authors and Affiliations

Merve Vildan Baysal^{1,2} · Özden Özcan-Top¹  · Aysu Betin-Can¹

Merve Vildan Baysal
vildan.baysal@metu.edu.tr

Aysu Betin-Can
betincan@metu.edu.tr

¹ Graduate School of Informatics, Middle East Technical University, Ankara, Türkiye

² The Scientific and Technological Research Council of Turkey (TÜBİTAK), Ankara, Türkiye