International Journal of Medical Informatics 134 (2020) 104040

Contents lists available at ScienceDirect

International Journal of Medical Informatics

journal homepage: www.elsevier.com/locate/ijmedinf

Review article

Blockchain in healthcare and health sciences—A scoping review

Anton Hasselgren[a,*], Katina Kralevska[b], Danilo Gligoroski[b], Sindre A. Pedersen[c], Arild Faxvaag[a]

[a] Department of Neuromedicine and Movement Science, Faculty of Medicine and Health Sciences, NTNU-Norwegian University of Science and Technology, Trondheim, Norway

[b] Department of Information Security and Communication Technology, Faculty of Information Technology and Electrical Engineering, NTNU-Norwegian University of Science and Technology, Trondheim, Norway

[c] Library Section for Medicine and Health Sciences, NTNU University Library, NTNU-Norwegian University of Science and Technology, Trondheim, Norway

ARTICLE INFO

Keywords:
Blockchain
Health systems
Scoping review
Distributed ledger

ABSTRACT

Background: Blockchain can be described as an immutable ledger, logging data entries in a decentralized manner. This new technology has been suggested to disrupt a wide range of data-driven domains, including the health domain.

Objective: The purpose of this study was to systematically review, assess and synthesize peer-reviewed publications utilizing/proposing to utilize blockchain to improve processes and services in healthcare, health sciences and health education.

Method: A structured literature search on the topic was conducted in October 2018 relevant bibliographic databases.

Result: 39 publications fulfilled the inclusion criteria. The result indicates that Electronic Health Records and Personal Health Records are the most targeted areas using blockchain technology. Access control, interoperability, provenance and data integrity are all issues that are meant to be improved by blockchain technology in this field. Ethereum and Hyperledger fabric seem to be the most used platforms/frameworks in this domain.

Conclusion: This study shows that the endeavors of using blockchain technology in the health domain are increasing exponentially. There are areas within the health domain that potentially could be highly impacted by blockchain technology.

1. Introduction and rationale

The technology of blockchain, with inherited characteristics such as decentralization, transparency and anonymization, was introduced in the cryptocurrency Bitcoin in 2008 [1]. Bitcoin, with close to 400 million completed transactions (March 19, 2019) [2], represents a solid use-case that blockchain technology works. This has led to discussions and proposals that blockchain technology could be useful in a range of other data-driven domains, including healthcare [3].

According to IBM, 70 % of healthcare leaders predict that the greatest impact of blockchain within the health domain will be improvement of clinical trial management, regulatory compliance and providing a decentralized framework for sharing electronic health records (EHR) [4]. Moreover, the global blockchain technology market in the healthcare industry is expected to cross $500 million by 2022 [61]. Although blockchain technology is considered to have potential for real improvement of health information systems [3], the recent hype surrounding this technology similarly entails unrealistic proposals and ideas and current literature provides little overview of applications that have been developed, tested and/or deployed.

It is valuable to investigate if the current research meets the expectations to blockchain technology within healthcare, health sciences and health education (from hereinafter, referred to as “the health domain”). This study aims to systematically review, assess and synthesize published peer-reviewed studies where blockchain has been utilized (or proposed to be utilized) to improve processes and services within the health domain. In addition to examining the evidence, we also aim to provide an overview of what has been done, what is known, and the potential directions forward on this topic.

The remainder of this paper is organized as follows: Section **two** presents a background of blockchain technology with a description of its key elements and an overview of the problems in the health domain where blockchain potentially could add value. Section **three** outlines the systematic methodology of the study including search strategy, selection process, data extraction, data analysis and quality assessment of the included publications. The results are presented in section **four** with a bibliographic overview and descriptive analysis of the extracted data. Finally, section **five** presents a discussion of the research results in

* Corresponding author at: Norwegian University of Science and Technology, NTNU, 7491 Trondheim, Norway.
E-mail address: anton.hasselgren@ntnu.no (A. Hasselgren).

https://doi.org/10.1016/j.ijmedinf.2019.104040
Received 13 May 2019; Received in revised form 25 November 2019; Accepted 2 December 2019

the context of the aim and research questions, including strengths and limitations of this study.

2. Background

Blockchain can be described as an immutable ledger that logs data entries in a decentralized manner. It enables entities to interact without the presence of a central trusted third party. The blockchain maintains a continuously growing set of data entries, bundled together into blocks of data. These blocks are, upon acceptance to the blockchain linked to the previous and future blocks with cryptographic protocols [60]. In blockchain's original form, these data records/blocks are; readable by all, writable by all, and tamper-proof by all. This for instance allows decentralized transactions and data management. Due to these properties, blockchain has gained much attention for various applications. Additionally, blockchain allows for smart contracts; self-execution contracts that do not require any central authority. The blockchain Ethereum is at this date the largest facilitator of smart contracts on blockchain [5].

2.1. What is Blockchain

2.1.1. Key characteristics

A key attribute of blockchain is decentralization; no central authority controls the content added to the blockchain. Instead, the entries passed on to the blockchain are agreed upon in a peer-to-peer network using a various consensus protocols (see 2.1.4 Consensus mechanism). Another key characteristic of blockchain is persistency. It is practically impossible to delete entries after being accepted onto the blockchain due to the distributed ledger, stored across multiple nodes [6]. Furthermore, the possibility of anonymity (or pseudonymity) is an appealing characteristic utilized in many blockchains.

Blockchains make audit and traceability possible by linking a new block to the previous by including the hash of the latter, and in this way forming a chain of blocks. The transactions in the blocks are formed in a Merkle tree [7] where each leaf value (transaction) can be verified to the known root. This enables the tree structure to verify the integrity of the data by only storing the root of the tree on the blockchain. Fig. 1 provides a visualization of this basic structure.

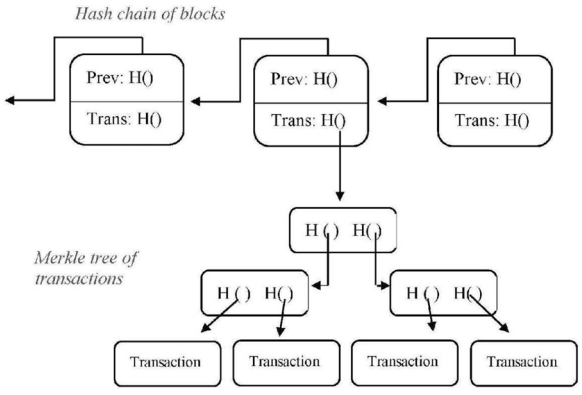

Fig. 1. Blockchain structure.

2.1.2. Type of blockchains

As illustrated in Table 1, there are mainly three types of blockchains: public (permissionless), consortium (public permissioned) and private [6]. They possess different characteristics regarding who can access, write and read the data on the blockchain. The data in a public chain can be viewed by all and anyone can join and contribute to both consensus (in theory) and changes to the core software [6]. The public blockchain is widely used in cryptocurrencies, and the two largest cryptocurrencies: Bitcoin [1] and Ethereum [5] (the main chain), are categorized as public permissionless chains. A consortium blockchain can be considered partially centralized, with only a limited number of selected groups of entities having access to view and participate in the consensus protocol. In a private blockchain, the network is distributed yet often centralized. Only selected nodes can participate in the network and they are often managed by one central authority [6]. The debate around the definition and the categorization of different types of blockchains presented here is ongoing. Currently, there is no broad consensus of which distributing qualities and consensus mechanisms are required to label a technology as "blockchain" [8].

2.1.3. Existing or new blockchains

There are currently existing blockchain frameworks and platforms that can be utilized for development of decentralized applications (dapps). Ethereum (decentralized platform) (5) and Hyperledger (framework) [9] are so far the most popular, and both allow developers to build new blockchain applications onto existing blockchains and to create new test-nets using their protocols.

2.1.4. Consensus mechanisms

A key component of blockchains is the way data entries are accepted onto the distributed ledger by a distributed consensus protocol validating the data entries. Several proposed and used consensus protocols exist, of which the three most commonly used are illustrated in Table 2 and presented in the following:

Table 2
Consensus mechanisms comparison [6].

Property	PoW	PoS	PBFT
Node management	Open	Open	Permissioned
Energy consumption	High	Medium	Low
Tolerated power of adversary	< 25% computing power	< 51% stake	< 33.3% faulty replicas
Example	Bitcoin [1]	Peercoin [13]	Hyperledger Fabric [12]

Proof-of-Work (PoW) is the consensus protocol most strongly associated with blockchain due to its integration in Bitcoin. When PoW protocol applies, so-called miners are competing in solving a computational hard puzzle. Using brute force, the miners try to find a hash of the proposed block with a value lower than a predetermined one. The miner who first computes this hash value validates the transactions (or other entries) within the block and gets an award (1). A major drawback of the PoW protocol is its energy demanding nature when applied

Table 1
Type of blockchains overview [6].

Property	Public blockchain	Consortium blockchain	Private blockchain
Consensus determination	All miners	Selected set of nodes	One organization
Read permission	Public	Public or restricted	Public or restricted
Immutability	Nearly impossible	Could be tampered	Could be tampered
Efficiency	Low	High	High
Centralized	No	Partial	Yes
Consensus process	Permissionless	Permissioned	Permissioned

on a large blockchain. This is illustrated by the fact that the current electricity consumed for Bitcoin mining is comparable to the electricity requirements of a smaller country [10].

With **Proof of Stake** (PoS), the selection of an approving node is determined by the stake each node has in the blockchain. For cryptocurrencies, the stake is represented by the balance one possesses of a given currency. This, however, might give an unfair advantage to the "richest" node. To account for this, several hybrid versions of PoS have been suggested where the stake is combined with some randomization to select the approving node. The second largest cryptocurrency Ethereum is planning to move from PoW to PoS [6].

Practical Byzantine Fault Tolerance (PBFT) is based on a Byzantine agreement protocol [11]. In PBFT, all nodes need to be known to the network, which limits the usage of this consensus protocol in a public blockchain. Three phases can be defined in the PBFT consensus process: pre-prepared, prepared and commit. Each node needs two thirds of the votes from all nodes to move through the three phases. PBFT is currently used in Hyperledger Fabric [12].

2.1.5. Smart contracts

Some blockchain infrastructures like Ethereum support smart contracts [5]. These are self-executing contractual agreements where pre-agreed upon provisions are formalized in source code. Since smart contracts are automatically enforced based on these pre-agreed provisions they work without any third party or intermediate. This function within a smart contract can be awoken in a blockchain transaction and the use of this functionality seems to be appealing to the health domain [5].

2.2. The potential of blockchain in the health domain

The healthcare sector is a problem-driven, data- and personnel-intensive domain where the ability to access, edit and trust the data emerging from its activities are critical for the operations of the sector as a whole. If we divide the operations within the healthcare sector into triage, health problem-solving, clinical decision-making, realization and assessment of knowledge-based care (Fig. 2), achieving the desired health outcomes hinges on engaging a multidisciplinary team of health personnel that apply the most appropriate knowledge, technologies and skills when dealing with the patient. When collaborating with educational institutions, the healthcare sector must provide access to patients and provide an arena for training so that students can develop and refine the necessary skills. In return, the educational institutions provide the sector with qualified personnel. When collaborating with institutions and companies with a research and engineering agenda, health institutions must assist in providing access to professionals, informants, test persons and samples. When participating in prospective clinical trials, health institutions must assist in developing, planning, conducting and reporting the experiments. In return, the research and engineering institutions provide the healthcare sector with updated knowledge, methods and tools. Hence, the activities of health institutions are tightly interwoven with institutions engaged in educating health personnel and in biomedical research and engineering (Fig. 2). The activities require effective interchange of consents, patient-related data and proofs, and reimbursements processes, which effectively means exchanging data across institutional borders. At the same time, health institutions are mandated to protect the highly sensitive data that patients choose to share with them.

To both maintain the patient's privacy and exchange data with other institutions in the healthcare ecosystem, access control, provenance, data integrity and interoperability are crucial. The traditional way of achieving **access control** commonly assumes trust between the owner of the data and the entities storing them. These entities are often servers fully entrusted for defining and enforcing access control policies [14]. **Interoperability** is the ability of different information systems, devices or applications to connect, in a coordinated manner, within and across organizational boundaries to access, exchange and cooperatively use

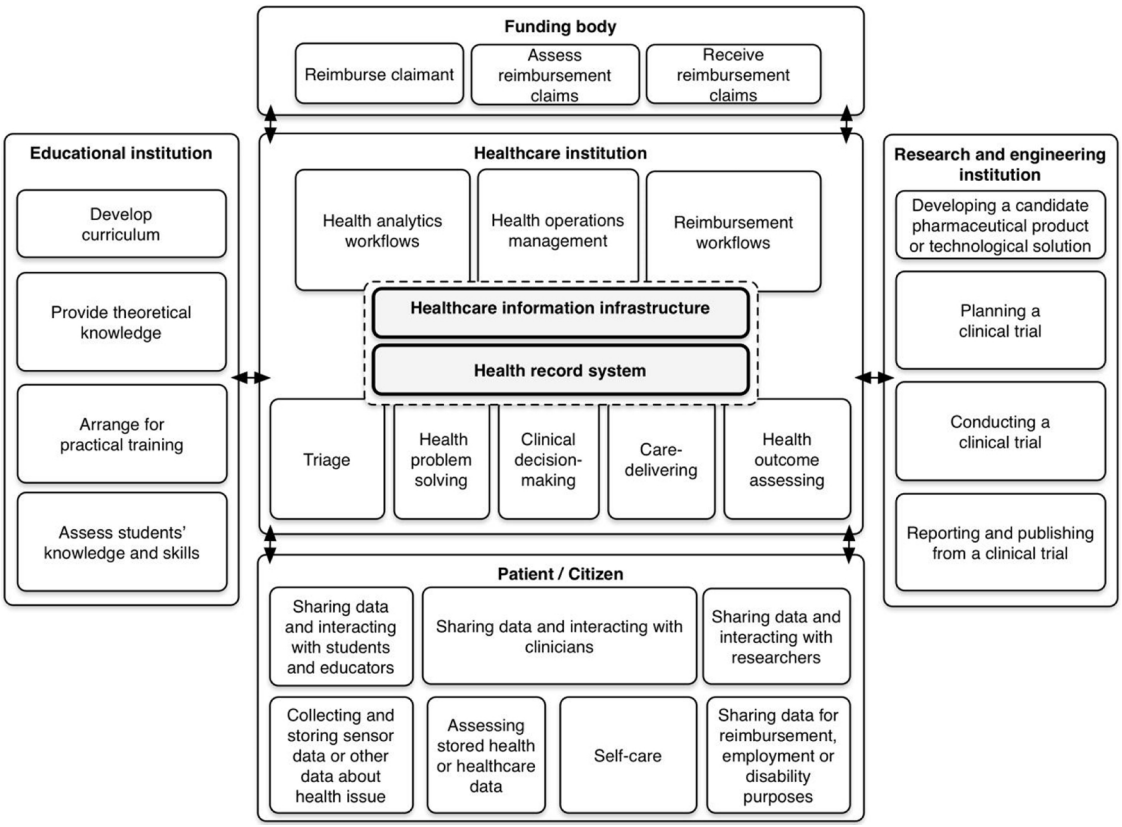

Fig. 2. Map of the health sector.

data amongst stakeholders, with the goal of optimizing the health of individuals and populations. **Data provenance** refers to the historical record of data and their origins. In the health domain data, provenance can, for example, be to deliver auditability and transparency in EHR, and to achieve trust in EHR software system. **Data integrity** as a general definition given by Courtney and Ware is the data quality definition which deals with the expected quality of the data [15]. This means that the degree to which the expected quality of the data is meet or exceeded determines the data integrity.

Healthcare institutions currently experience an increased demand of real-world data from industry and research organizations [16]. At the same time, unauthorized sharing, and highly publicized break-ins and robbery of sensitive data constantly erode the public trust in healthcare institutions. A third problem is malpractices within the healthcare ecosystem that exploits the very same trust (e.g. the problems with counterfeit drugs, procedures, skills and patients). Taken together, this is a situation that commands rethinking and consideration of alternative approaches. With some of its key attributes such as decentralization, distribution and data integrity, and without any necessary third party, blockchain technology has many appealing properties that could be utilized to improve and obtain a higher level of interoperability, information sharing, access control, provenance and data integrity among the mentioned stakeholders, thereby moving towards a new infrastructure for building and maintaining trust.

3. Method

3.1. Search strategy

A structured literature search on the topic was conducted in the following bibliographic databases with the aid of a medical research librarian [SAP]: MEDLINE, Embase, Cochrane Library, Scopus, Google Scholar, Compendex, Inspec, ACM and IEEE. The search strategy compromised searching for free-text terms for the concept “blockchain” within health topic databases. In the other databases, the concept “blockchain” was combined with the concept “health” using the Boolean operator AND. Within the concepts, word variants and related terms were covered and combined using the Boolean operator OR. Backward and forward search (snowballing method) [17] was applied for the included papers to further assure that all relevant sources were exhausted. This process applied on all included papers and considered complete when no new additional, relevant papers were found. The literature search was last updated 10th October 2018. All references from the databases were exported to EndNote (version x9.1) for duplicate removal and final screening. The search targeted published research in scholarly journals, conference proceedings and workshop reports that asses blockchain concepts within the health domain. For a complete overview over the applied search see Appendix A – Search strategy.

3.2. Selection process

Titles, abstracts and full articles were subsequently screened by reviewer 1 [AH] applying the inclusion and exclusion criteria (Appendix B – Protocol). Publications meeting the inclusive criteria, and those for which the first reviewer was in doubt, were reviewed a second time by three additional reviewers [AF, KK and DG]. In cases of disagreement, a discussion between all four reviewers determined inclusion or exclusion. Fig. 3 illustrates the process.

3.3. Data extraction

Data was extracted from the included papers in a pre-development matrix. The data extraction was mainly done by reviewer 1 [AH] and later re-examined by reviewers 2–4 [AF, KK and DG]. The extracted data was categorized and summarized in the matrix and later exported into tables and graphs. The data matrix was developed in Google Sheet for a convenient workflow within the research group and later exported to Microsoft Excel (version 16.16.5).

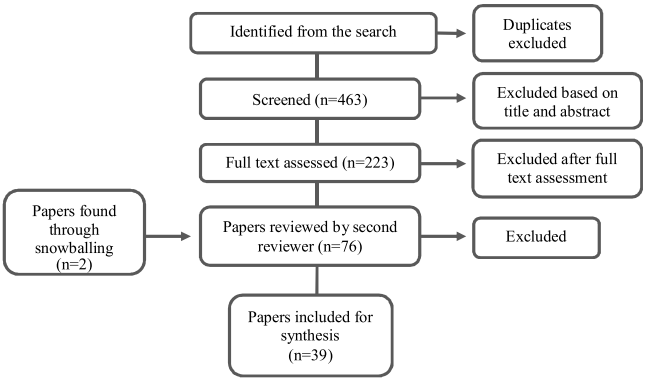

Fig. 3. Inclusion flowchart.

3.4. Data analysis

Relevant extracted quantified data was summarized. The data analysis was completed in Microsoft Excel (version 16.16.5). Where applicable, mean with standard deviation (SD) was calculated (expressed as ±). All numbers were rounded off to the closest integer. All categorical data are expressed as percentage if not stated otherwise.

3.5. Quality assessment

As an important part of the review process a meticulous quality assessment of included publications was conducted [17]. Since developed and validated tools for assessing the different methodologies of the included publications are lacking, development of a specific tool to serve the purpose was necessary. To this end, parts of the method presented by Hölbl et al. were used and modified as appropriate [18]. No papers were excluded in the quality assessment process. The papers received a score based on the criteria (Table 3). The score was given as follows: (NO or SCARCELY) = 0, (MODERATELY) = 1, (YES or ADEQUATELY) = 2. The process of quality assessment was done by reviewer 1 [AH] and later independently pre-reviewed by reviewers 2–4 [AF, KK and DG].

Table 3
Quality assessment tool adapted from Hölbl et al. [18].

Quality Assessment Query	Indicator (0–2)
Q2 Is the health domain problem described?	No-Moderately-YES
Q2 Are the research objectives clearly outlined?	No-Moderately-YES
Q3 Are the main contributions well described?	No-Moderately-YES
Q4 How appropriate is the problem-solution fit?	Scarcely-Moderately-Adequately
Q5 Are the proposed solutions feasible (scalable, economical, implementable)?	No-Moderately-YES

4. Results

The following section presents a summary of the extracted data from the included papers (n = 39).

4.1. Bibliographic overview

As shown in Table 4, the included publications seem to be evenly distributed between journal publications and conference proceedings. IEEE Access with five papers and The Journal of Medical Systems with six papers represented the journals with most included publications. All included papers presented a study design that could be categorized as a

Table 4
Bibliographic overview of the included studies.

Id, reference	Name of first author	Year of publication	Publication type	Publisher	Main contribution	Study design
1 [19]	Zhang, Peng	2018	Journal	Computational and Structural Biotechnology Journal	Structural design	Proof-of-Concept/Case-study
2 [20]	Shan, Jiang	2018	Conference proceeding	IEEE International conference on smart computing	Algorithm/Protocol	Proof-of-Concept
3 [21]	Kleinaki, Athina-Styliani	2018	Journal	Computational and Structural Biotechnology Journal	Structural design	Proof-of-Concept/Case-study
4 [22]	Peterson, Kevin	2016	Conference proceeding	Proc. NIST Workshop Blockchain Healthcare	Algorithm/Protocol	Proof-of-Concept
5 [23]	Ichikawa, Daisuke	2017	Journal	JMIR Mhealth and Uhealth	Structural design	Proof-of-Concept/Case-study
6 [24]	Patel, Vishal	2018	Journal	Health informatics journal	Structural design	Proof-of-Concept
7 [25]	Zhang, Jie	2016	Journal	IEEE Access	Security protocols	Proof-of-Concept
8 [26]	Roehrs, Alex	2017	Journal	Journal of biomedical informatics	Structural design	Proof-of-Concept
9 [27]	Liang, Xueping	2017	Conference proceeding	2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications	Structural design	Proof-of-Concept
10 [28]	Zhang, Aiqing	2018	Journal	Journal of medical systems	Algorithm/Protocol	Proof-of-Concept
11 [29]	Rahman, Abdur	2018	Journal	IEEE Access	Structural design	Proof-of-Concept
12 [30]	Gue, Rui	2017	Journal	IEEE Access	Algorithm/Protocol	Proof-of-Concept
13 [31]	Xia, Qi	2017	Journal	IEEE Access	Structural design	Proof-of-Concept
14 [32]	Zhou, Lijing	2018	Journal	Journal of medical systems	Algorithm/Protocol	Proof-of-Concept/Case-study
15 [33]	Azaria, Asaph	2016	Conference proceeding	International conference on open and big data	Structural design	Proof-of-Concept
16 [34]	Hussein, Ahmed,	2018	Journal	Cognitive Systems Research	Algorithm/Protocol	Proof-of-Concept
17 [35]	Zhao, Huawei	2017	Conference proceeding	2017 IEEE 13th International Symposium on Autonomous Decentralized System (ISADS)	Algorithm/Protocol	Proof-of-Concept/Case-study
18 [36]	Fan, Kai	2018	Journal	Journal of medical systems	Algorithm/Protocol	Proof-of-Concept
19 [37]	Mikula, Tomas	2018	Conference proceeding	2018 21 st Euromicro Conference on Digital System Design	Algorithm/Protocol	Proof-of-Concept/Case-study
20 [38]	Wang, Hao	2018	Journal	Journal of medical systems	Structural design/cryptographic primitive	Proof-of-Concept
21 [39]	Griggs, Kristen	2018	Journal	Journal of medical systems	Structural design	Proof-of-Concept
22 [40]	Dias, Joao Pedro	2018	Journal	arXiv	Structural design	Proof-of-Concept
23 [41]	Dagher, Gaby G	2018	Journal	Sustainable cities and society	Structural design/framework	Proof-of-Concept/Case-study
24 [42]	Chen, Jieying	2018	Conference proceeding	IEEE International Symposium on Innovation and Entrepreneurship	Structural design	Proof-of-Concept
25 [43]	Bocek, Thomas	2017	Conference proceeding	IFIP/IEEE Symposium on Integrated Network and Service Management	Structural design/framework	Proof-of-Concept/Case-study
26 [44]	Angeletti, Fabio	2017	Conference proceeding	25th International Conference on Software, Telecommunications and Computer Networks	Structural design	Proof-of-Concept
27 [45]	Theodouli, Anastasia	2018	Conference proceeding	17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications	Structural design	Proof-of-Concept
28 [46]	Nugent, Timothy	2016	Journal	F1000Research	Structural design	Proof-of-Concept
29 [47]	Momoshina, Polina	2018	Journal	Oncotarget	Structural design/framework	Proof-of-Concept
30 [48]	Liang, Xueping	2018	Conference proceeding	International Conference on Information and Communications Security	Algorithm/Protocol	Proof-of-Concept
31 [49]	Li, Hongyu	2018	Journal	Journal of medical systems	Algorithm/Protocol	Proof-of-Concept
32 [50]	Laskowski, Marek	2017	Conference proceeding	International Conference on Social Computing, Behavioral-Cultural Modeling and Prediction and Behavior	Structural design	Proof-of-Concept
33 [51]	Ji, Yaxian	2018	Journal	Journal of medical systems	Algorithm/Protocol	Proof-of-Concept/Case-study
34 (52)	Zhang, Xiaoshuai	2018	Conference proceeding	IEEE International Conference on Communications	Algorithm/cryptographic primitive	Proof-of-Concept
35 [53]	Xia, Qi	2017	Journal	Information	Structural design/framework	Proof-of-Concept
36 [54]	Uddin, Ashraf	2018	Journal	IEEE Access	Algorithm/Protocol	Proof-of-Concept/Case-study
37 [55]	Sun, You	2018	Conference proceeding	27th International Conference on Computer Communication and Networks	Algorithm/Protocol	Proof-of-Concept
38 [56]	Rahmadika, Sandi	2018	Journal	International Journal of Engineering Business Management	Algorithm/Protocol	Proof-of-Concept
39 [57]	Zhang, Peng	2017	Journal	arXiv	Structural design/framework	Proof-of-Concept/Case-study

Proof-of-Concept design. In addition, eleven of the included papers could be considered as a hybrid between a Proof-of-Concept and a Case-study design. The included papers were published during the following years; 2016 (n = 4), 2017 (n = 11) and 2018 (n = 23). Most studies were associated with Chinese research institutes or research groups (42 %) followed by institutes and groups in the USA (20 %). The papers had an average citation count of 21 ± 40 (up to March 2019).

The main contributions of the included publications were categorized as illustrated in Table 4. A large proportion proposed a structural design (54 %) as main contribution, followed by proposals including new algorithms or protocols (38 %) (Table 4).

4.1.1. Summary of proposed solutions

The included publications described several systems, processes and challenges in the health domain in which blockchain enhanced concepts were suggested as part of the solution. The most frequently targeted system was EHR, with 43 % of the publications addressing this topic. Other systems of focus were PHR (15 %) and clinical trial support systems (5 %). The processes within the target systems were mostly focused on sharing, storage, exchange and access of medical data. More than half of the publications (62 %) addressed some processes of sharing health data. Many of the PHRs were proposed as patient-controlled and not tethered to a particular health institution or system (Table 6).

4.1.2. Challenges which blockchain aims to improve

As illustrated in Table 5, blockchain was suggested as an improvement to **access control** in 35 % of the included publications. For

Table 5
Summary of proposed solutions impacted by blockchain technology.

Id, ref.	Health Information system	Process that is to be improved	Main challenge that is addressed
1 [19]	Electronic health records	Shared decision making	Interoperability, access control, data integrity
2 [20]	Electronic health records	Health data recording, storing and sharing	Access control, interoperability
3 [21]	Knowledge infrastructures	Aid decision-making by presenting knowledge	Data integrity, repudiation
4 [22]	Electronic health records	Sharing of healthcare information for clinical and research purposes	Access control, interoperability
5 [23]	Personal health records	M-health data recording, storing and sharing	Data integrity, data provenance
6 [24]	Picture archiving and communications systems	Exchange of medical images	Access control
7 [25]	IoT data management/Personal health data	Remote collection and storage of health data	Data integrity, access control
8 [26]	Personal health records	Sharing healthcare data between health institutions	Interoperability, data provenance
9 [27]	Personal health records	Automatic collection, storage and patient-controlled sharing of personal health data	Access control, interoperability
10 [28]	Personal health records	Sharing of health data for use by more than one healthcare institution	Access control, interoperability
11 [29]	Automated diagnostic service for patients	Collection and storage of data about symptoms of dyslexia for the purpose of automated diagnostics, decision-support and research.	Access control, data integrity, interoperability
12 [30]	Electronic health records	Sharing healthcare data between health institutions	Data integrity
13 [31]	Electronic health records	Sharing healthcare data between health institutions	Data integrity, access control
14 [32]	Administrative systems	Sharing healthcare information for administrative or economic purposes	Data integrity, data provenance
15 [33]	Electronic health records	Sharing healthcare data for clinical and research purposes. Recording and sharing of contracts/agreements.	Access control, interoperability, data integrity
16 [34]	Electronic health records	Sharing healthcare (health record) information for clinical, research and administrative [economic] purposes.	Access control, interoperability
17 [35]	Personal health records	Collecting and sharing [health-related] sensor data for clinical purposes.	Interoperability
18 [36]	Electronic health records	Sharing healthcare data for clinical and research purposes.	Access control, interoperability
19 [37]	Electronic health records/ Administrative system	Sharing healthcare data for administrative or economic purposes	Identity management, access control
20 [38]	Electronic health records	Patient data management and storage in a cloud environment	Access control, data integrity, data provenance
21 [39]	Population health management system	Collection and storage of sensor data for remote patient monitoring purposes	Data integrity, data provenance
22 [40]	Personal health data/Electronic health records	Managing access to personal health data and electronic health records	Access control, data integrity
23 [41]	Electronic health records	Patients' collection, archiving and sharing of healthcare data for clinical purposes	Access control, data integrity, interoperability
24 [42]	Electronic health records	Patients' collection, archiving and sharing of healthcare data for clinical purposes	Interoperability, access control
25 [43]	Pharma supply-chain	Monitoring the distribution of drugs in a pharmaceutical supply chain.	Data integrity, data provenance
26 [44]	Clinical Trial Support Systems	Recruitment of patients to clinical trials	Data integrity, data provenance
27 [45]	Electronic health records	Sharing healthcare data for clinical and research purposes	Interoperability, data provenance
28 [46]	Clinical Trial Support Systems	Sharing healthcare information for research purposes	Data integrity, data provenance
29 [47]	Research support systems	Establishing a patient-controlled marketplace for selling and buying of healthcare information for research purposes	Access control, interoperability
30 [48]	Personal health records	Patients' collection, archiving and sharing of healthcare data for clinical purposes	Access control, privacy, data integrity
31 [49]	Electronic health records	Health record storing	Data integrity, privacy
32 [50]	Infectious disease surveillance system	Public health management (monitoring the outbreak of infectious diseases)	Data integrity, data provenance
33 [51]	Telemedicine system	Finding the patient in the context of telemedicine services	Data integrity
34 [52]	Electronic health records	Retrieving information in the EHR	Access control, data integrity
35 [53]	Electronic health records	Sharing healthcare data for clinical and research purposes	Access control, security, interoperability
36 [54]	Personal health records	Patient-controlled collection and sharing of sensor data	Access control, data integrity
37 [55]	Electronic health records	Sharing healthcare data between health institutions	Data provenance
38 [56]	Electronic health records	Patient-controlled sharing of health data between healthcare providers	Access control, interoperability
39 [57]	Electronic health records	Exchange of healthcare data for clinical and research purposes	Access control, interoperability

Table 6
Healthcare information systems that are impacted by blockchain technology.

Information system category	Count	Proportion
Electronic health records	17	43 %
Personal health records	6	15 %
Clinical Trial Support Systems	2	5 %
Knowledge infrastructures	1	3 %
Picture archiving and communications systems	1	3 %
IoT data management/Personal health data	1	3 %
Automated diagnostic service for patients	1	3 %
Administrative systems	1	3 %
Electronic health records/Administrative system	1	3 %
Population health management system	1	3 %
Pharma supply-chain	1	3 %
Grand Total	**39**	

example, in the paper by Patel [24], access to the data (medical images) were provided by requesting and approving transactions of the data (stored off-chain) with private and public keys. Another approach was suggested by Peterson et al. [22], where access is granted by querying data on the blockchain and retrieving it with FHIR URLs once located. Hyperledger Fabric membership service was used by Liang et al. [27] for issuing enrollment certificate and transaction certificate for access control.

Blockchain solutions for the **interoperability** challenges were discussed in several papers (27 %) (Table 5). For example, interoperability was achieved by referencing FHIR resources (URLs) in some solutions [22,19]. Another approach was to provide a translator component as a gateway of the data blocks, translating formats using a different standard [26].

The ability to improve **provenance** was targeted in 12 % of the included publications (Table 5). In a blockchain concept for medical supply chains, data provenance was enhanced by the use of trusted IoT devices that execute smart contracts on the blockchain [43]. Other examples were found in the concepts addressing clinical trials, where data provenance issues are targeted by providing a tracking system of data used in the trials [44,46].

To increase **data integrity** a blockchain solution was proposed in 28 % of the included publications in this review (Table 5). Generally, the data integrity was maintained by the immutability property of the blockchain (2.1.1 – Key characteristics). Data integrity was enhanced by storing hashed medical data or hash pointer on chain [49,41,38]. Another approach for using blockchain to maintain data integrity was found within clinical trials where smart contracts and integration with trusted IoT devices are used [44,46].

4.2. Technical details of the proposed blockchain concepts

4.2.1. Type of blockchain

A consortium blockchain (38 %) was the preferred type among the included publications. Although several of the papers failed to define their approach (26 %), private- (10 %) and public blockchains (15 %) appears to be less used in the health domain (Fig. 4).

4.2.2. Blockchain platform/framework

Ethereum was utilized in eleven (28 %) of the 39 included publications, Hyperledger Fabric four times (10 %) and Exonum once (4 %) (Fig. 4). 14 studies (36 %) developed a new blockchain for their respective concepts. Eight (21 %) of the included studies failed to specify a platform or framework for their concept (Fig. 4).

4.2.3. Consensus algorithm

The summarized results indicate that a variety of consensus algorithms are used for blockchain concepts in the health domain (Table 7). The most frequent used consensus algorithm in the included

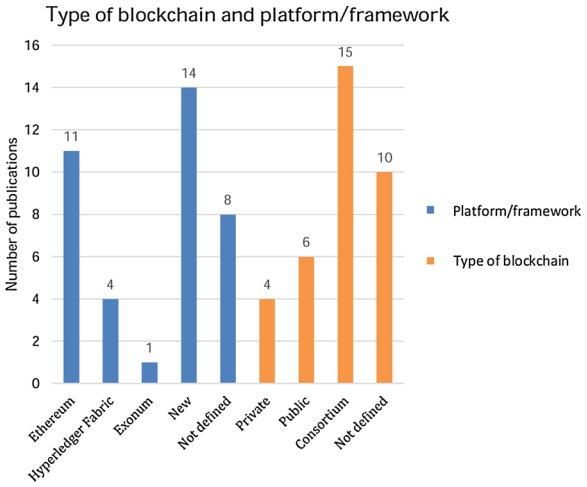

Fig. 4. Type of blockchain and platform/framework.

publications were PoW, accounting for 21 % of the cases. In addition, it is also noteworthy that not all concepts that are built using the Ethereum platform or Ethereum protocols used PoW. The second most frequent used consensus algorithm was PBTF (15 %). Several (41 %) of the publications failed to state which consensus protocol their concept intended to apply.

4.2.4. Smart contracts

In several of the proposed concepts, smart contracts were a feature: 38 % of the included studies used smart contracts for some functionality; the remaining studies did not define if smart contracts were a feature or not (Table 7).

Table 7
Usage of consensus algorithm and smart contracts.

Consensus algorithm	Count	Id
Proof of Work (PoW)	8	2, 3, 15, 22, 31–33, 38
Proof of Work (by pre-selected miner)	1	36
Practical Byzantine Fault Tolerance (PBFT)	6	5, 8, 14, 21, 24, 37
Proof of Stake (PoS)	1	6
Proof of Interoperability	1	4
Proof of Conformance	1	10
Permissioned Voting-based	2	19, 20
Ledger-based Byzantine Fault Tolerance	1	29
Hybrid (Delegated PoS + PBFT)	1	18
QuorumChain consensus	1	23
Not defined	16	1, 7, 8, 11–13, 16, 17, 25–28, 30, 34, 35, 39
Use of smart contracts		
Yes	15	1, 3, 4, 13, 15, 19, 21, 23, 25, 27, 28, 29, 31, 32, 39
Not defined	24	2, 5, 6–12, 14, 16–18, 20, 22, 24, 26, 30, 33-38

4.3. Quality assessment

Table 8 presents the results of the quality assessment. The maximum number of total points is ten and the minimum is zero. The average score for Q1 (1.0 ± 0.7), Q2 (0.9 ± 0.7) and Q3 (1.0 ± 0.5) appears to be lower than Q4 (1.6 ± 0.6) and Q5 (1.2 ± 0.6). The quality of the included publications varies with a standard deviation of 1.8 for the total mean score and a range of 1–9.

As shown in Fig. 5, the average quality increased in papers

Table 8
Quality assessment.

Id (ref)	Year	Q1 Feasibility	Q2 Problem description	Q3 Research objectives	Q4 Contribution description	Q5 Problem solution fit	Total score
4 [22]	2016	1	1	2	2	1	7
7 [25]	2016	2	1	0	2	0	5
15 [33]	2016	1	1	1	0	2	5
28 [46]	2016	0	0	1	0	0	1
5 [23]	2017	1	0	1	2	1	5
8 [26]	2017	1	2	0	2	1	6
9 [27]	2017	0	1	0	1	2	4
12 [30]	2017	2	0	1	2	1	6
13 [31]	2017	1	2	1	1	2	7
17 [35]	2017	0	0	1	2	1	4
25 [43]	2017	0	0	1	1	1	3
26 [44]	2017	1	0	1	1	1	4
32 [50]	2017	0	0	0	1	0	1
35 [53]	2017	1	1	1	1	2	6
39 [57]	2017	1	0	1	1	1	4
1 [19]	2018	1	2	1	2	2	8
2 [20]	2018	1	1	1	2	1	6
3 [21]	2018	2	1	1	2	2	8
6 [24]	2018	2	1	1	1	1	6
10 [28]	2018	1	2	1	2	1	7
11 [29]	2018	2	2	1	1	1	7
14 [32]	2018	2	2	1	2	1	8
16 [34]	2018	1	0	1	2	1	5
18 [36]	2018	1	1	1	2	2	7
19 [37]	2018	1	2	1	2	1	7
20 [38]	2018	1	0	1	2	1	5
21 [39]	2018	1	1	1	1	1	5
22 [40]	2018	1	0	1	2	1	5
23 [41]	2018	1	2	2	2	2	9
24 [42]	2018	2	1	1	0	1	5
27 [45]	2018	0	0	1	2	1	4
29 [47]	2018	2	1	2	2	2	9
30 [48]	2018	0	1	2	2	1	6
31 [49]	2018	1	0	1	2	1	5
33 [51]	2018	1	1	1	2	2	7
34 [52]	2018	0	1	1	2	1	5
36 [54]	2018	2	1	2	2	2	9
37 [55]	2018	0	1	1	2	2	6
38 [56]	2018	1	1	1	2	1	6
Mean (SD)		1.0 ± 0.7	0.9 ± 0.7	1.0 ± 0.5	1.6 ± 0.6	1.2 ± 0.6	5.7 ± 1.8

published in 2018 compared to 2016 and 2017. Fig. 5 indicates the quality trend of the included publications.

5. Discussion

In this scoping literature review, we have found that the research on the explorative use of blockchain in healthcare is an academic research topic in its infancy but that the number of research groups approaches and proposed solutions currently is growing exponentially. The quality of the papers is also on the rise (Fig. 5). Many researchers explore the use of Smart-contracts on the Ethereum platform, organized as a consortium blockchain. Most of the proposed solutions are implemented in Institution-controlled EHRs, in Personal health record systems (PHRs) or in the mHealth domain. Judged from the number of blockchain-related publications on Google Scholar, the inauguration and growth of blockchain in healthcare as an academic field is in line with those in other academic sectors.

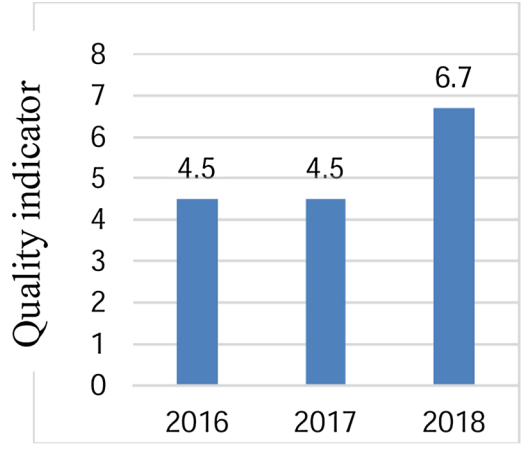

Fig. 5. Average quality score per year.

The utilization of smart-contracts partly explains why Ethereum is the mostly used platform for the proposed concepts (Fig. 4). A smart-contract function, which often has the purpose of reducing third party interaction, has the potential of making health informatic processes more efficient. However, none of the included papers contained evidence of such effect (More research and further exploration of the efficiencies of smart contracts compared to current solutions should be undertaken). In addition to Ethereum, Hyperledger was a popular platform/framework used in the included publications. This correlates well with the overall popularity of blockchain platforms. The reasons for this can be both the attributes that are offered by the respective platform, but also the number of developers available with knowledge on each platform as well as the strong overall market position of Ethereum and Hyperledger. Furthermore, a consortium blockchain appears to be the preferred design choice when it comes to type of blockchain. Since HIS deals with highly sensitive data [18], which usually entails that a limited number of entities should have access, a consortium blockchain may be more appropriate than a public permissionless and private to ensure that data are not accessible by those who have no view rights and also to comply with current health data regulations.

Most papers envisioned the use of blockchain in health record systems (EHRs and PHRs) (Table 6). Within these, the use of blockchain to build functionality for sharing of data within clinical teams and between clinicians and researchers were the most targeted use cases. With stronger emphasis on team-based care and continuity of care across institutional borders, and identity management and access control across different health systems, the processes of sharing becomes important [58]. Four publications [25,27,28,48] proposed to use blockchain for building a personal health record system that could bridge the gap between the patient and institution-specific EHRs. This is an alternative take on the use of health information to fix a broken healthcare system and improve the continuity of care [59] which builds on the patient in a more empowered and controlling role.

Five of the publications addressed the m-health domain and patient-controlled collection, storage and sharing of sensor data [23,27,35,39,32]. The collection and sharing of sensor data is relevant to all virtualized care scenarios (e.g. telecare, remote patient monitoring and population health), and technologies that can make sensor data more to be trusted upon are worthy of exploration. Although these five included publications do not provide enough collective evidence that blockchain may be superior to existing solutions, they provide an insight into an interesting use-case for several reasons; M-health is a rather new field and lacks a common data infrastructure and, to some degree, lacks common regulation around dealing with health data and getting the data accepted by the established health system. There is a reasonable assumption that m-health will increase at a rapid pace in the coming years and the need to verify and access m-health generated data by the health systems becomes crucial for the continued development of HIS and to insure that these data-driven systems stay up to date. The evidence collected in this review gives a clear indication that blockchain enhanced solutions for this area of the health system have a promising potential and needs to be explored further.

Three papers addressed the sharing of clinical data for use in non-clinical contexts [29,32,47]. Most of the use cases were related to biomedical research. Also, two publications explored the use of blockchain in clinical trial systems [44,46]. Hence, the use of blockchain to build better support for basic and translational biomedical research appear to be a well-recognized problem. As illustrated in Fig. 3, institutions that conduct biomedical research are an example of an institution that support and supply healthcare. Taken together, these constitute an ecosystem whose operations are tightly interwoven with those within the healthcare institutions proper. Most interactions involve the use of data that the patient has shared for purposes other than providing or assessing care. We found no publications on the use of blockchain in the context of interaction between patients and healthcare students in the context of healthcare education and training. Also, we found no publications on the use of blockchain for reimbursement purposes. We believe that the use of blockchain-based solutions also should be explored in these application areas. Furthermore, neither of the included publications described how their blockchain-based solution was compliant with GDPR, HIPAA or other national health data laws and regulations. This needs to be explored further to assess the implementation possibilities of blockchain technology within the health domain.

The strength of this publication is its stringent inclusion criteria and the quality assessment approach. This has enabled us to look beyond the mere publishing of thoughts and ideas and instead highlight what has actually been developed, tested and published in a peer-review setting.

The aim of this review was to summarize the peer-reviewed literature under the topic of blockchain in the health domain. Although this study provides a good overview of what has recently been investigated in an academic (peer-reviewed) setting, the review does not capture the whole picture of the development in the area. There are promising developments in the private sector in other areas of the health sector that are not covered in the included publications for this review; for example, genome management and medical credential systems.

Future research on the topic should consider adding more technical details to further enable feasibility assessment and decrease the gap between concepts and implementations, thus moving the technology forward in this area. In addition, further research should also address how blockchain-based solutions can be made to comply with current health data laws and standards. There is a need to explore which blockchain features and designs are suitable under these laws and standards, and which are not to further increase real-world implementation feasibility.

6. Conclusion

Research on the use of blockchain in healthcare is now established as an academic field, and the number and quality of publications are increasing rapidly. This trend is also noticeable in the global healthcare industrial sector, where the blockchain technology market is expected to cross $500 million by 2022. Due to the over-arching importance of maintaining trust while satisfying an ever-increasing demand for exchange of data within the healthcare ecosystem, healthcare institutions are in critical demand for new and improved trust-preserving solutions. The frontier of research, as portrayed in this review, show that blockchain-based solutions currently are being explored in a few EHR, PHR and Clinical trial system use cases. Several other health information system domains are under-explored as we found few if any publications on Knowledge infrastructures, Picture archiving and communications systems, Automated diagnostic service for patients, Administrative systems, Population health management system and Pharma supply-chains. The research agenda needs to be broadened to address these concrete areas, as well as to address the quest for blockchain-based solutions that preserve trust by mitigating threats from within as well from outside the healthcare sector.

Author contributions

All authors have made a substantial, direct, intellectual contribution to this study.

Summary points

What was already known on the topic?

- Blockchain technology has proven to work in cryptocurrencies like Bitcoin.
- The health sector has been one area outside of cryptocurrencies were blockchain technology have been proposed to add value.

What this study added to our knowledge?

- Blockchain-based solutions can improve and simplify the sharing of health record information from Electronic Health Record and Personal Health Record systems.
- Research on Blockchain-based solutions in healthcare is taking pace but it is still in its infancy, as many potential and promising areas remain under-researched and unexploited.

;1;

Declaration of Competing Interest

None.

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sector.

Appendix A. Supplementary data

Supplementary material related to this article can be found, in the online version, at doi:https://doi.org/10.1016/j.ijmedinf.2019.104040.

References

[1] S. Nakamoto, Bitcoin: a Peer-to-Peer Electronic Cash System, (2008).

[2] blockchain.com [cited 2019 09.03]. Available from: https://www.blockchain.com/charts/n-transactions-total.
[3] Blockchain technology in healthcare: the revolution starts here. e-health networking, applications and services (Healthcom), in: M. Mettler (Ed.), 2016 IEEE 18th International Conference on, IEEE, 2016.
[4] Health rallies for blockchains: Keeping patients at the center: IBM; 2016 [cited 19.03 2019]. Available from: https://www.ibm.com/downloads/cas/BBRQK3WY.
[5] Buterin VJwp, A Next-generation Smart Contract and Decentralized Application Platform, (2014).
[6] An overview of blockchain technology: architecture, consensus, and future trends, in: Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang (Eds.), Big Data (BigData Congress), 2017 IEEE International Congress on, IEEE, 2017.
[7] R.C. Merkle (Ed.), A Certified Digital Signature. Conference on the Theory and Application of Cryptology, Springer, 1989.
[8] M. Pilkington, 11 blockchain technology: principles and applications Research Handbook on Digital Transformations, (2016), p. 225.
[9] Architecture of the hyperledger blockchain fabric, in: C. Cachin (Ed.), Workshop on Distributed Cryptocurrencies and Consensus Ledgers, 2016.
[10] K.J. O'Dwyer, D. Malone, Bitcoin Mining and Its Energy Footprint, (2014).
[11] M. Castro, B. Liskov (Eds.), Practical Byzantine Fault Tolerance, OSDI, 1999.
[12] projects Tlf. Hyperledger [cited 19.03 2019]. Available from: https://www.hyperledger.org.
[13] S. King, N.S. Ppcoin, Peer-to-peer Crypto-currency With Proof-of-Stake, self-published paper, August (2012), p. 19.
[14] J.P. Anderson, Computer Security Technology Planning Study, ESD-TR-73-51 (1972).
[15] R. Courtney, W. Ware, Some informal comments about integrity and the integrity workshop, in: Z.G. Ruthberg, W.T. Polk (Eds.), Proc Of the Invitational Workshop on Data Integrity, National Institute of Standards and Technology, Special Publication, 1989.
[16] E. Coiera, Guide to Health Informatics, CRC press, 2015.
[17] Y. Levy, E. TJJIS, A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research, (2006), p. 9.
[18] M. Hölbl, M. Kompara, A. Kamišalić, L.J.S. Nemec Zlatolas, A Systematic Review of the Use of Blockchain in Healthcare, (2018), p. 470 10 (10).
[19] P. Zhang, J. White, D.C. Schmidt, G. Lenz, S.T. Rosenbloom, FHIRChain: applying blockchain to securely and scalably share clinical data, Comput. Struct. Biotechnol. J. 16 (2018) 267–278.
[20] BlocHIE: a BLOCkchain-based platform for healthcare information Exchange, in: J. Shan, C. Jiannong, W. Hanqing, Y. Yanni, M. Mingyu, H. Jianfei (Eds.), 2018 IEEE International Conference on Smart Computing (SMARTCOMP), 18-20 June 2018, Los Alamitos, CA, USA: IEEE Computer Society, 2018.
[21] A.S. Kleinaki, P. Mytis-Gkometh, G. Drosatos, P.S. Efraimidis, E. Kaldoudi, A blockchain-based notarization service for biomedical knowledge retrieval, Comput. Struct. Biotechnol. J. 16 (2018) 288–297.
[22] K. Peterson, R. Deeduvanu, P. Kanjamala, K. Boles, A Blockchain-Based Approach to Health Information Exchange Networks, (2017) 2017.
[23] D. Ichikawa, M. Kashiyama, T. Ueno, Tamper-resistant Mobile Health Using Blockchain Technology, ncbi.nlm.nih.gov (2017).
[24] V. Patel, A framework for secure and decentralized sharing of medical imaging data via blockchain consensus, Health Inf. J. (2018).
[25] J. Zhang, N. Xue, X. Huang, A secure system for pervasive social network-based healthcare, IEEE Access 4 (2016) 9239–9250.
[26] A. Roehrs, C.A. da Costa, R. da Rosa Righi, OmniPHR: a distributed architecture model to integrate personal health records, J. Biomed. Inform. 71 (2017) 70–81.
[27] X. Liang, J. Zhao, S. Shetty, J. Liu, D. Li (Eds.), Integrating Blockchain for Data Sharing and Collaboration in Mobile Healthcare Applications, Institute of Electrical and Electronics Engineers Inc, 2018.
[28] A. Zhang, X. Lin, Towards secure and privacy-preserving data sharing in e-Health systems via consortium blockchain, J. Med. Syst. 42 (8) (2018).
[29] M.A. Rahman, M.S. Hossain, E. Hassanain, M. Rashid, S. Barnes, Spatial blockchain-based secure mass screening framework for children with dyslexia, IEEE Access (2018) 1-.
[30] R. Guo, H. Shi, Q. Zhao, D. Zheng, Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems, IEEE Access 6 (2018) 11676–11686.
[31] Q. Xia, E.B. Sifah, K.O. Asamoah, J. Gao, X. Du, M. Guizani, MeDShare: trust-less medical data sharing among cloud service providers via blockchain, IEEE Access 5 (2017) 14757–14767.
[32] L. Zhou, L. Wang, S.Y. MIStore, A blockchain-based medical insurance storage system, J. Med. Syst. 42 (8) (2018).
[33] MedRec: using blockchain for medical data access and permission management, in: A. Azaria, A. Ekblaw, T. Vieira, A. Lippman (Eds.), 2016 2nd International Conference on Open and Big Data (OBD), 22-24 Aug 2016, Los Alamitos, CA, USA: IEEE Computer Society, 2016.
[34] A.F. Hussein, N. ArunKumar, G. Ramirez-Gonzalez, E. Abdulhay, T. JMRS, V.H.C. de Albuquerque, A medical records managing and securing blockchain based system supported by a Genetic Algorithm and Discrete Wavelet Transform, Cogn. Syst. Res. 52 (2018) 1–11.
[35] H. Zhao, Y. Zhang, Y. Peng, R. Xu (Eds.), Lightweight Backup and Efficient Recovery Scheme for Health Blockchain Keys, Institute of Electrical and Electronics Engineers Inc, 2017.
[36] K. Fan, S. Wang, Y. Ren, H. Li, Y. Yang, MedBlock: efficient and secure medical data sharing via blockchain, J. Med. Syst. 42 (8) (2018).
[37] T. Mikula, R.H. Jacobsen, Identity and access management with blockchain in electronic healthcare records, 2018 21st Euromicro Conference on Digital System Design (DSD) (2018) 2018 29-31 Aug.
[38] Y.S. Hao Wang, Secure Cloud-Based EHR System Using Attribute-Based Cryptosystem and Blockchain, (2018).
[39] K.N. Griggs, O. Ossipova, C.P. Kohlios, A.N. Baccarini, E.A. Howson, T. Hayajneh, Healthcare blockchain system using smart contracts for secure automated remote patient monitoring, J. Med. Syst. 42 (7) (2018).
[40] J. Dias, L. Reis, H. Ferreira, Â. Martins, Blockchain for Access Control in e-Health Scenarios, arXiv preprint arXiv:180512267 (2018).
[41] G.G. Dagher, J. Mohler, M. Milojkovic, P.B. Marella, Ancile: privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology, Sustain. Cities Soc. 39 (2018) 283–297.
[42] A blockchain application for medical information sharing, in: J. Chen, X. Ma, M. Du, Z. Wang (Eds.), 2018 IEEE International Symposium on Innovation and Entrepreneurship (TEMS-ISIE), 2018 30 March-1 April 2018.
[43] T. Bocek, B.B. Rodrigues, T. Strasser, B. Stiller (Eds.), Blockchains Everywhere – A Use-Case of Blockchains in the Pharma Supply-Chain, Institute of Electrical and Electronics Engineers Inc, 2017.
[44] F. Angeletti, I. Chatzigiannakis, A. Vitaletti, Privacy preserving data management in recruiting participants for digital clinical trials, Proceedings of the First International Workshop on Human-Centered Sensing, Networking, and Systems; Delft, Netherlands, ACM, 2017, pp. 7–12 3144733.
[45] S.A. Anastasia Theodouli, K. Moschou, K. Votis, D. Tzovaras, On the Design of a Blockchain-Based System to Facilitate Healthcare Data Sharing, (2018).
[46] T. Nugent, D. Upton, M. Cimpoesu, Improving data transparency in clinical trials using blockchain smart contracts, F1000 Res. (2016) 5.
[47] P. Mamoshina, L. Ojomoko, Y. Yanovich, A. Ostrovski, A. Botezatu, P. Prikhodko, et al., Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare, Oncotarget 9 (5) (2018) 5665–5690.
[48] X. Liang, S. Shetty, J. Zhao, D. Bowden, D. Li, J. Liu, S. Qing, D. Liu, C. Mitchell, L. Chen (Eds.), Towards Decentralized Accountability and Self-Sovereignty in Healthcare Systems, Springer Verlag, 2018, pp. 387–398.
[49] H. Li, L. Zhu, M. Shen, F. Gao, X. Tao, S. Liu, Blockchain-based data preservation system for medical data, J. Med. Syst. 42 (8) (2018).
[50] M. Laskowski, N. Osgood, D. Lee, R. Thomson, Y.R. Lin (Eds.), A Blockchain-Enabled Participatory Decision Support Framework, Springer Verlag, 2017, pp. 329–334.
[51] Y. Ji, J. Zhang, J. Ma, C. Yang, Y.X. BMPLS, Blockchain-based multi-level privacy-preserving location sharing scheme for telecare medical information systems, J. Med. Syst. 42 (8) (2018).
[52] X. Zhang, S. Poslad (Eds.), Blockchain Support for Flexible Queries With Granular Access Control to Electronic Medical Records (EMR), Institute of Electrical and Electronics Engineers Inc, 2018.
[53] Q. Xia, E.B. Sifah, A. Smahi, S. Amofa, X. Zhang, BBDS: Blockchain-based data sharing for electronic medical records in cloud environments, Inf. (Switzerland) 8 (2) (2017).
[54] M.A. Uddin, A. Stranieri, I. Gondal, V. Balasubramanian, Continuous patient monitoring with a patient centric agent: a block architecture, IEEE Access 6 (2018) 32700–32726.
[55] A decentralizing attribute-based signature for healthcare blockchain, in: Y. Sun, R. Zhang, X. Wang, K. Gao, L. Liu (Eds.), 2018 27th International Conference on Computer Communication and Networks (ICCCN), 2018 30 July-2 Aug. 2018.
[56] S. Rahmadika, K. Rhee, Blockchain technology for providing an architecture model of decentralized personal health information, Int. J. Eng. Bus. Manage. (2018).
[57] P. Zhang, J. White, D. Schmidt, G. Lenz, Applying Software Patterns to Address - Interoperability in Blockchain-based Healthcare Apps, arXiv preprint arXiv:170603700 (2017).
[58] W. Wilkowska, M. Ziefle, Privacy and data security in E-health: requirements from the user's perspective, Health Inf. J. 18 (3) (2012) 191–201.
[59] T.W. Bice, S.B. Boxerman, A quantitative measure of continuity of care, Med. Care 15 (4) (1977) 347–349.
[60] M. Raikwar, D. Gligoroski, K. Kralevska, SoK of used cryptography in blockchain, IEEE Access 7 (2019) 148550–148575.
[61] Frost & Sullivan, Global Blockchain Technology Market in the Healthcare Industry 2018–2022, (2019) 4847375.