IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 26, 2019, accepted January 7, 2020, date of publication January 28, 2020, date of current version February 4, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2969881

A Systematic Review of Blockchain in Healthcare: Frameworks, Prototypes, and Implementations

EMEKA CHUKWU[1] **AND LALIT GARG**[1,2]

[1]Department of Computer Information System (CIS), Faculty of Information Communication Technology (ICT), University of Malta, Msida 2080, Malta
[2]Laureate Online Education (Information Technology), University of Liverpool, Liverpool L69 3BX, U.K.

Corresponding author: Lalit Garg (lalit.garg@online.liverpool.ac.uk)

This work was supported by the University of Malta through student scholarship.

ABSTRACT Blockchain, a form of distributed ledger technology has attracted the interests of stakeholders across several sectors including healthcare. Its' potential in the multi-stakeholder operated sector like health has been responsible for several investments, studies, and implementations. Electronic Health Records (EHR) systems traditionally used for the exchange of health information amongst healthcare stakeholders have been criticised for centralising power, failures and attack-points with exchange data custodians. EHRs have struggled in the face of multi-stakeholder and system requirements while adhering to security, privacy, ethical and other regulatory constraints. Blockchain is promising amongst others to address the many EHR challenges, primarily trustless and secure exchange of health information amongst stakeholders. Many blockchain-in-healthcare frameworks have been proposed; some prototyped and/or implemented. This study leveraged the PRISMA framework to systematically search and evaluate the different models proposed; prototyped and/or implemented. The bibliometric and functional distribution of all 143 articles from this study were presented. This study evaluated 61 articles that discussed either prototypes or pilot or implementations. The technical and architectural analysis of these 61 articles for privacy, security, cost, and performance were detailed. Blockchain was found to solve the trust, security and privacy constraints of traditional EHRs often at significant performance, storage and cost trade-offs.

INDEX TERMS Bioinformatics, blockchain, DLT, distributed ledger technology, distributed computing, distributed databases, health information management, health information exchange, hospitals, pharmaceutical technology, telemedicine, digital health, eHealth, mHealth.

I. INTRODUCTION

A. HEALTHCARE

Healthcare systems around the world continue to face challenges that often lead to increasing costs [1] or poorer health outcomes (morbidity and mortality) [2]. Health sector is complex and made up of physicians from over 120 medical specialities and sub-specialities [3] including other practitioners, researchers and patients who face several challenges related to increased fragmentation of patient data. Disparate data-structures and workflows further compound this. Information security concerns sparked by data sharing regulations and 'fear of financial consequences associated with data sharing' amongst others have hindered efficient health information exchange [4]. Ability to exchange patient's health information amongst the various actors across and within the care continuum remain a major challenge [5]. This and more has led to sustained annual global interests in Health Information Exchange (HIE) as seen in the Google trend analysis in Figure 1. It shows the monthly minimum, average and maximum searches for 'Health Information Exchange' for the last two decades.

Electronic Medical Records (EMR) based systems have traditionally helped address health information digitisation and sharing within a health institution. Similarly, Personal Health Records (PHR) systems were also promoted to help manage patient data in the healthcare continuum. However, the nature of healthcare continuum has evolved. To leverage tools such as machine learning and other technologies for improved care, a complex many-to-many information sharing regime is inevitable. Health institutions will traditionally address this sharing need on a case-by-case basis through trust-agreements. In the current digital world, a trusted third-party is required to exchange information like patient

The associate editor coordinating the review of this manuscript and approving it for publication was Navanietha Krishnaraj Rathinam.

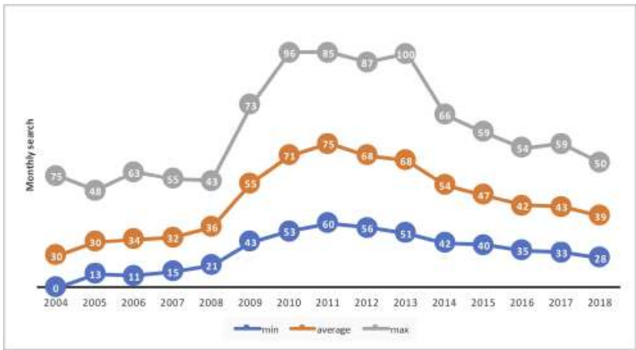

FIGURE 1. **Global Health Information Exchange (HIE) google trend analysis.**

data. Consequently, HIE network organisations have emerged and are being used to broker exchange agreements between hospitals, clinical domains, regulators, insurers and even the patient [6]. They promise to deliver the true Electronic Health Records (EHR) enabled integrated health systems. Available evidence still suggests the inability of these systems to adequately meet stakeholder needs adequately [7]. This current model has been criticised for lacking transparency, and having a central authority for ownership, failure, and attack [8]. Trust-deficit concerning security and privacy of entrusted patient information through deliberate or unwitting actions of these intermediaries is on the rise.

B. BLOCKCHAIN

Blockchain, a fusion of two old technologies (cryptography and peer-peer communication) [9] was popularised with the bitcoin white paper by Satoshi Nakamoto [10]. The resulting bitcoin blockchain originally conceptualised initially in response to the global financial crisis of 2008 has inspired widespread application of blockchain [11]. Proponents of blockchain as an alternative to the mostly centralised system of operation for several other sectors beyond finance often highlight speed, lower cost, security, fewer errors, fault tolerance and elimination of a central point of authority, attack or failure [11]. However, other challenges that limit its scalability have emerged [12].

Blockchain is a form of distributed-ledger-technology (DLT) which is a shared-ledger with a growing ordered list of records stored and persisted in a 'giant computer database'. This database is formed from several inter-connected devices (phones, computers or embedded systems) not restricted by geography [13]. It does not require network participants to trust one another because it has cryptographically enabled inbuilt trust mechanism [14]. Each entry in this ledger is called a block (composed of messages and transactions) linked and time-stamped through cryptographic hashes [15] and validated by network peers.

1) BLOCK STRUCTURE AND CONTENT

The structure and content of a typical block in public blockchain networks are as shown in Figure 2. The two main

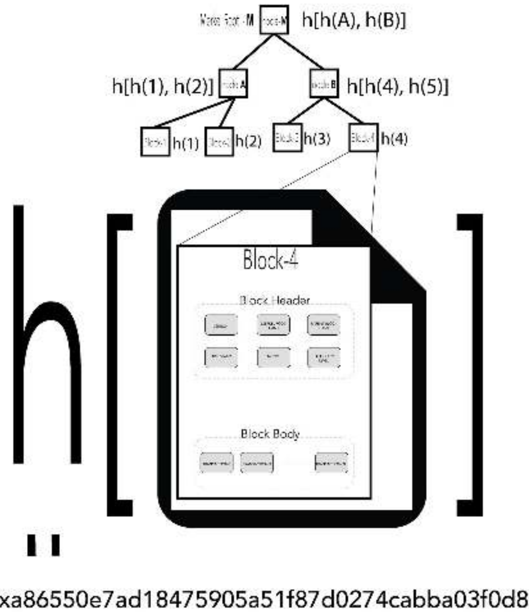

FIGURE 2. **The structure and content of typical blocks in a public blockchain.**

public blockchain networks Bitcoin and Ethereum use the Merkel tree binary hash structure [10]. A block on these blockchains is a hash value of information to be logged. Such information majorly contains a header and the message body. The header often contains the block version, Merkel root hash, parent hash, timestamp, nonce, and difficulty level. The block body contains a list of transactions packaged together as the particular blockchain allows. A hash is a string of alphanumeric value obtained by passing a piece of information (or file) through a hashing algorithm (e.g. SHA-2, SHA-256, etc.). Merkel tree is a popular technique for ensuring the integrity of a file or information in a distributed network against accidental corruption or intentional tempering. The technique uses a binary approach where a parent node contains the concatenation of hash values of siblings. The real power of Merkel tree approach lies in its ability for partial verification. The parent hash is the hash of the parent (predecessor) block in the Merkel tree, and the timestamp is the time the transaction happened. The nonce is a fixed bit length number that public blockchain miners are solving for values below. The difficulty level is a value adjusted periodically within each blockchain network.

Blockchain network participants benefit from the ability to execute transactions with untrusted third parties and log them on the blockchain network. Network members have a public and private key pair they use to send asymmetric cryptographic encrypted [15] message(s) or transaction through this untrusted network. Using a public key (or private key) to encrypt a message or transaction ensure that only the holder of the corresponding key pair can easily decrypt and read the message [16]. Validated messages are stored on the blockchain network and linked to predecessor block and corresponding message (or transaction) metadata hashed using

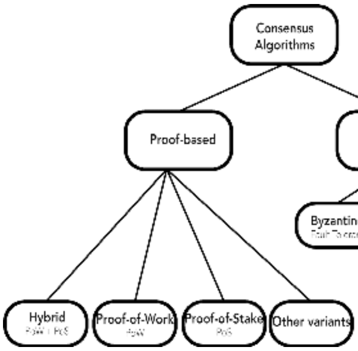

FIGURE 3. Blockchain consensus algorithm categorisations.

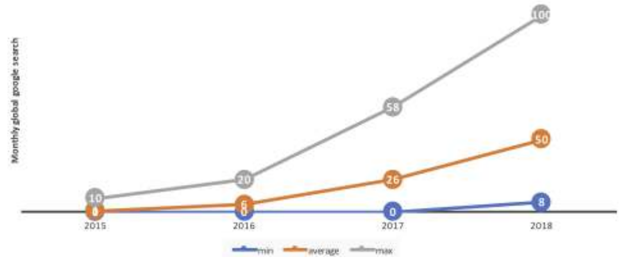

FIGURE 4. The global blockchain in healthcare Google trend analysis.

a one-way cryptography to ensure immutability as described above. The ‘hash’ value, a fixed length text that represents the transaction file will change with a slight change to the file. This way, block integrity is maintained.

2) CATEGORISATION, CONSENSUS AND CRYPTOCURRENCY

Blockchain networks can be classified by its type, how network members reach consensus and validate transactions or what platforms they run on [20]. When classified by type, a blockchain network can be public, private or consortium. A public blockchain is an open blockchain like Bitcoin [10] or Ethereum [19] that allows anyone to join, and the rules for participating including accompanying source code are public. A consortium blockchain on the other hand runs like a public blockchain but is only accessible to a closed group of approved network members [11]. On the contrary, a private blockchain has centralised ownership and management.

Similarly, a blockchain can also be classified based on how network members reach consensus on which transaction to validate and add to the blockchain. There are many different consensus algorithms, but they all fall under two broad categories: proof-based or vote-based as shown in Figure 3. Proof-of-Work, Proof-of-Stake, Proof-of-Authority, Proof-of-Activity and variants of these are all proof-based [20]. The proof-based algorithms are popular with a public blockchain. Similarly, there are ongoing researches and private proofs-of-concept and implementations of vote-based consensus algorithms. Details of each of these consensus algorithms and how they operate is beyond the scope of this work.

A token often referred to as cryptocurrency is sometimes required for a transaction on a blockchain network. These tokens are sometimes used to incentivise network members to contribute computing, connectivity and power resources necessary for network operation. On Bitcoin blockchain, this cryptocurrency is called ‘bitcoin’ and on Ethereum it is known as ‘ether’ and priced in gas. These cryptocurrencies often have equivalent fiat (traditional currency like US dollars) values. When a cryptocurrency is based on a jurisdictional fiat currency, they are often referred to as stable-coin.

3) SMART CONTRACTS AND CHAIN CODES

Smart contracts first introduced on Ethereum Mainnet (the main public blockchain of Ethereum) is a self executing code on the blockchain network [19]. It digitally facilitates the negotiation, verification, execution and enforcement of contracts without a third-party intermediary. Other variants have emerged including the Hyperledger chain codes [18]. Real world contracts or predefined rules can be modelled to get predictable outputs based on a discrete number of known inputs on blockchain networks. The bitcoin network does not use smart contracts or its equivalent, it limits its transaction by script size. Smart contracts on the other hand help eliminate transaction computation limit, it uses transaction gas fee on Ethereum blockchain acts as a rate limiter.

C. BLOCKCHAIN IN HEALTHCARE

Since the launch of bitcoin about a decade ago, several variants of blockchain has been introduced [23]. Blockchain is now being applied to digital assets beyond the financial transaction. Health sector application is one of the many sectors receiving attention and prospects. It is demonstrated in the sudden spike in global Google trends as shown in Figure 4.

1) STUDY RATIONALE

Given that traditional HIE and PHR-based exchanges have failed to meet their promise of shared integrated EHR, competing interests and many other factors continue to unearth the trust deficit inherent in traditional HIE intermediations. Privacy regulation and cases of data breaches have heightened these mistrust [6]. Stakeholders are as a result unwilling to cooperate or collaborate to the extents necessary for shared value. The consequence has been rising healthcare cost and dwindling health outcome. It may explain the sustained attention in HIE over the last two decades as illustrated by Google trends in Figure 1. If this trend provides a clear indication of current global interests, it then means that these challenges remain notwithstanding decade-long technological advances. We postulate that the trust deficit may be a key factor responsible for the lack of progress. Researchers are now turning to blockchain to help address some of these trust-linked challenges. This and many others have fuelled the new wave of interests in blockchain in healthcare. To further understand this research area and how it has progressed, this study was commissioned.

2) RESEARCH QUESTIONS (RQ)

The research questions answered by this study are:

- **RQ-1** *What is the current research state of the art of blockchain application in healthcare concerning*

TABLE 1. Comparing prior systematic reviews and our study.

Paper	Year	Bibliometric	Function	Security	Privacy	Performance	Architecture	Cost	Standards
Hölbl et al [20]	2018	Y	N	N	N	N	N	N	N
Agbo et al [21]	2019	Y	Y	Y	Y	N	N	N	Y
Meinert et al [24]	2018	Y	N	Y	Y	N	N	N	N
Jin et al [22]	2019	N	N	Y	Y	Y	N	Y	N
Drosatos et al [26]	2019	Y	Y	Y	N	N	N	N	N
Sujath et al [25]	2018	N	N	N	N	N	N	Y	N
Lua Erik [8]	2018	N	N	N	N	N	Y	N	Y
Our study	Planned	Y	Y	Y	Y	Y	Y	Y	Y

proposed systems (frameworks, concepts, and models), prototypes, and real-life implementations and/or pilots?

- **RQ-2** *How do they compare to traditional healthcare data management techniques?*
- **RQ-3** *What are the emerging trends?*

D. PRIOR REVIEWS

Our search for prior blockchain in healthcare reviews yielded seven (7) literature reviews all conducted in 2018 and 2019: [8], [20]–[22], [24]–[26]. These papers provided useful insight and background for this work and many valuable contributions to the body of knowledge.

[20] systematically reviewed and investigated the potential uses of blockchain in healthcare to highlight challenges and future research. Its review of the 33 papers did not cover any of the technical area under consideration in this paper. They also did not discuss the cost implication of blockchain application in healthcare.

Similarly, [21] systematically reviewed and investigated the use cases and challenges including trends of blockchain application in healthcare. They surveyed 65 papers and detailed bibliometric and functional findings. They also discussed the security and privacy considerations. This paper did not provide a technical analysis or the compliance frameworks in reviewed papers. They also did not look at the performance, architecture or costs of blockchain in healthcare. They discussed blockchain standards, but provided no detail of the relevant digital health standards used in reviewed papers.

Another survey by [24] looked at the efficiency of health records management, and assessed 71 articles. Though this paper also used a systematic approach, its focus was not a technical analysis. It investigated the strategies proposed to improve electronic health records using blockchain. It covered security and privacy compliance but did not discuss performance, architectures, costs or standards.

In the same light, [22] explored healthcare data sharing using blockchain. The review process was not systematic, but it analysed the security, privacy and cost implication of using blockchain. Critical concepts reviewed include identity management, access control, data encryption, encrypted keyword search, data storage and smart contract and data interoperability.

[26] systematically reviewed 47 papers to understand the problems and solutions of using blockchain for biomedical science. This review was however non-technical nor detailed.

The paper [25] systematically reviewed 14 papers looking at the people, process and technology and research gaps in the application of blockchain in healthcare. This paper only covered cost amongst the different metrics we are investigating.

The Thesis, [8] presented a non systematic analysis of the technical architecture and health standards, but did not address the other components in table 1.

Table 1 gives an analysis of select gap in prior reviews and how this study fills them. Analysis of these papers and other studies show that to our knowledge, no prior work addressed the research questions posed above. Also, there has not been a mapping of proposed models (or frameworks), prototypes and implementations of blockchain in healthcare. Only one paper reviewed the performance evaluation of the systems in reviewed studies, and this was based on security consideration. Similarly, only [8] discussed the architecture of reviewed papers, and it reviewed the health standard only, but not blockchain standard. Also, all previous reviews omitted vital search terms which could bias returned results and inadvertently exclude some articles. Filling these survey gaps is the main contribution of this paper. This paper investigates articles from three tripods: bibliometric, functional and technical. Also, the technical analysis of security, privacy, performance, architecture, costs and standards help bridge most identified gaps.

E. PAPER ORGANIZATION

The remaining sections of this paper are organised such that the research approach gives a detailed methodology for our systematic review, result presentation and analysis. The Preferred Reporting Items for Systematic and Meta-Analysis (PRISMA) chart of the methodology is shown in Figure 5. The study finding section details the bibliometric, functional and technical findings from reviewed articles. We used the discussions section to expand on and provide detailed analysis of the findings by each research question. Identified limitations to this study were outlined in the discussion section. The conclusion section was used to summarise the study while laying the foundation for future work.

II. RESEARCH APPROACH

A. SYSTEMATIC DATABASE SEARCH

Our choice of keywords for the search was determined by concatenating the two main words in the domains of interest,

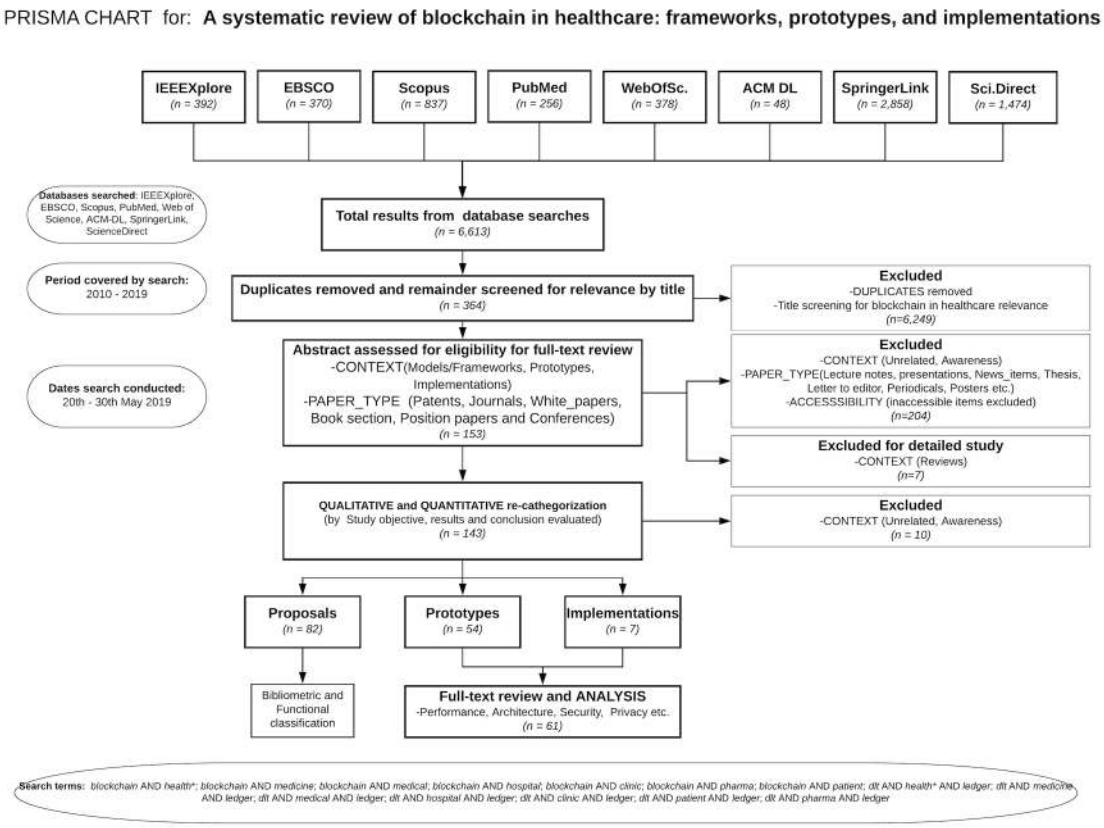

FIGURE 5. PRISMA CHART for the review process.

TABLE 2. Search terms and results by scholarly databases.

Search terms vs database	IEEE Xplore	EBSCO	Scopus	PubMed	Web of Science	ACM-DL	SpringerLink	Sci.Direct
blockchain AND health*	166	173	360	87	166	25	1116	485
blockchain AND medicine	17	12	40	40	20	2	295	161
blockchain AND medical	122	139	241	60	94	12	539	306
blockchain AND hospital	28	9	43	20	20	2	268	178
blockchain AND patient	55	37	140	47	75	3	394	227
blockchain AND pharma	1	0	4	0	1	0	45	21
blockchain AND clinic	3	0	6	2	1	4	67	41
dlt AND health* AND ledger	0	0	2	0	1	0	63	24
dlt AND medicine AND ledger	0	0	0	0	0	0	10	4
dlt AND medical AND ledger	0	0	0	0	0	0	25	10
dlt AND hospital AND ledger	0	0	0	0	0	0	10	8
dlt AND patient AND ledger	0	0	0	0	0	0	18	9
dlt AND pharma AND ledger	0	0	1	0	0	0	4	0
dlt AND clinic AND ledger	0	0	0	0	0	0	4	0
Total with duplicates	392	370	837	256	378	48	2858	1474

blockchain and *healthcare*. We then prepared a Research Information Template (RIT) where we disintegrated these words in our research into their parts. Each part was then reviewed for possible synonyms used by researchers as can be seen in the mind map as illustrated in Figure 6. The next step was to use the keyword pairs for the systematic search process as described below.

The alternative word used for blockchain is *'dlt'*, short for *distributed ledger technology*. However, *'dlt'* is an acronym with many other meanings particularly in medicine. To force context, the word *'ledger'* was included wherever 'dlt' was used as an alternative to blockchain. Similarly, the wildcard alternate *'health*'* was used to ensure there are no false negatives. Other terms widely used in healthcare publications were determined to include *'clinic'*, *'hospital'*, *'medicine'*, *'medical'*, *'patient'*, and *'pharma'*. Each of these was alternated for *'health*'* to yield the search criteria:

blockchain AND health*; blockchain AND medicine; blockchain AND medical; blockchain AND hospital; blockchain AND clinic; blockchain AND pharma;

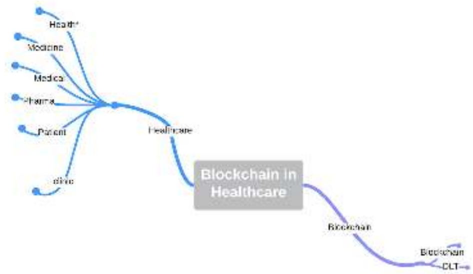

FIGURE 6. Keyword identification Research Information Template (RIT).

blockchain AND patient; dlt AND health* AND ledger; dlt AND medicine AND ledger; dlt AND medical AND ledger; dlt AND hospital AND ledger; dlt AND clinic AND ledger; dlt AND patient AND ledger; dlt AND pharma AND ledger

The systematic search was conducted on eight scholarly databases: IEEEXplore, EBSCO, Scopus, PubMed, Web of Knowledge, ACM digital library, SpringerLink and Science Direct. IEEEXplore was chosen because of its strategic importance to the digital health domain in general, and blockchain in healthcare in particular. EBSCO provided access to 26 databases including PsycINFO, MEDLINE, and Cochrane. Scopus, PubMed, Web of Knowledge, Springer, ACM, and Science Direct were all included in the search databases for completeness. The literature searches were conducted in May 2019. Each text string from the RIT was searched in the respective databases and results inputted into a synthesis matrix in Microsoft Excel document. We followed the PRISMA guideline as shown in Figure 5.

As the rise of blockchain started after the launch of bitcoin in 2009, early adoption focused on the use of blockchain in the financial sector. Application in other sectors including health and related published work was not commonplace before 2010. It justifies the date range covered by this review, which is between January 2010 and May 2019. Where the database permits, the entire metadata is selected for search terms, and where it is not possible, the best possible search option (keyword, title and abstract) are used. The distribution of search term results returned per database is as in Table 2.

A total of 6,613 results were returned from a search of all eight (8) databases. They were then screened by title for relevance to blockchain in healthcare and de-duplicated. After title screening and de-duplication, we categorised 364-published articles included as either *unrelated, awareness, reviews, concept/model/framework propositions, prototypes*, and *implementations or pilots*. Papers that propose a framework and discuss development of a laboratory prototype the framework are categorised as a prototype and not both (framework and prototype).

Those meeting the criteria for further review were selected if they discuss *concept/model/framework propositions, prototypes or implementations* and the rest were discarded.

After reviewing the abstracts, only publications identified from the abstract to be model-propositions, prototypes and implementation were included. Also, meeting abstracts, and newsletters were filtered out. Additionally, three non-English-language publications were excluded. Reviews category capture reviews, assessments, mapping or even systematic reviews. Both awareness and review papers, as mentioned above were excluded from this work.

TABLE 3. Abstract and full text review quality check questions.

s/n	Questions	Response
AQ1	Is publication relevant to blockchain in healthcare?	Yes/No
AQ2	Does research propose a new model, concept or framework or a modification of existing framework or does it describe a prototype or real-life implementation as a study objective?	Yes/No
AQ3	Is study published in a scholarly literature like journal, conference, white paper or book section?	Yes/No
AQ4	Is the discussion with a basic level of detail required to address the research question?	Yes/No

A total of 153 items were found within the three categories of interest. The study objectives, results and conclusion were then scanned in the context of the quality questions in table 3. Ten papers were further excluded and total number of papers available in all categories was 143 articles. All 143 articles including the proposal articles where then quantitatively categorised presenting their bibliometric and functional characteristics. Of these articles, there were 82 models, proposals or frameworks suggestion-only papers.

Similarly there were 54 prototype-papers that conducted workbench test either through a simulation software or by configuring the system in a laboratory environment. Majority of these prototype systems were prototyping existing proposed or prototyped systems. While a few where prototyping a new proposed system.

There were seven (7) pilots/implementations. Moreover, we categorised them as such if their testing process used human subject data, or are used in a production setting. A full text review was then conducted on each of the 61 papers in the prototypes and implementation categories.

Quality Metrics: To ensure the quality of the review process, questions AQ1, AQ2 and AQ3 in Table 3 served as quality check metrics for each of the review step. The title, abstract and full-text review qualities were checked against this metric.

III. STUDY FINDINGS

This section presents the findings necessary to address the research objectives. It details the bibliometric and functional findings of 143 articles. Also, technical analysis of 61 papers categorised as blockchain in healthcare prototypes and pilots or implementations were also presented here.

A. BIBLIOMETRIC DISTRIBUTION

The number of published literature articles proposing frameworks, concepts or models without either prototype or implementation accounted for 57 per cent (i.e. 82 of all 143) articles as shown in the chart in Figure 7. These propositions broadly included proposition for the adoption of blockchain in one or more healthcare domains, and proposition for improvements

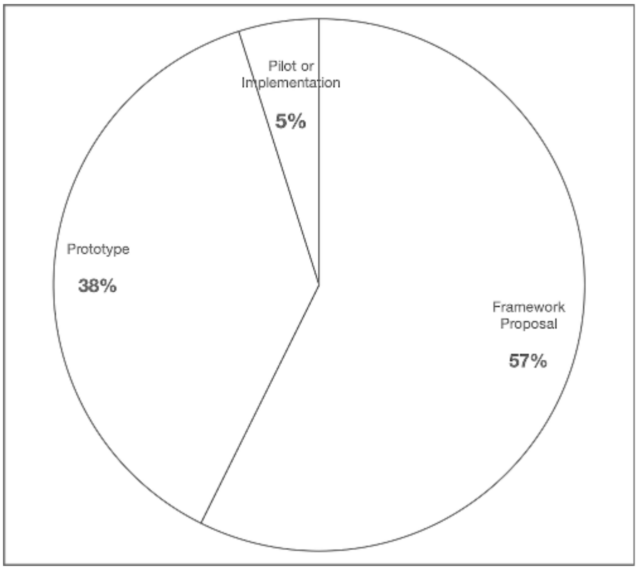

FIGURE 7. Article distribution of published blockchain in healthcare research.

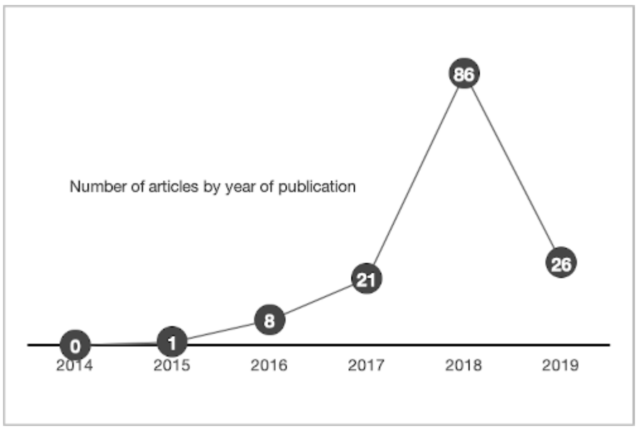

FIGURE 8. Distribution of the number of published articles by year of publication.

to existing blockchain ecosystem or a combination of these two categories. About a third (38 per cent) of reviewed studies discussed prototyping either a proposed model or prototyping existing models in an experimental or laboratory environment. Only about 5 per cent (i.e., 7 of all 143) of these papers discussed real-life implementation, pilot testing or evaluation of an implementation. Our study categorised articles into model propositions, prototypes, and implementations, see Table 4 for a full range of reviewed papers. Research into blockchain in the healthcare domain has increased rapidly from one (1) in 2015 and peaked at 86 (60 per cent) in 2018 as shown in Figure 8.

Reviewed papers were mostly journal-papers (n = 73) and conference-papers (n = 51), as shown in Figure 9. Also, there have been three US patents as of May 2019. A large proportion of papers were published in an Institute of Electrical Electronics Engineering (IEEE) affiliated journal or conference.

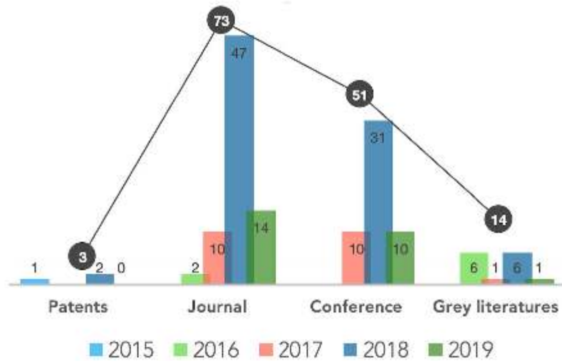

FIGURE 9. The trend of publication distribution by paper type.

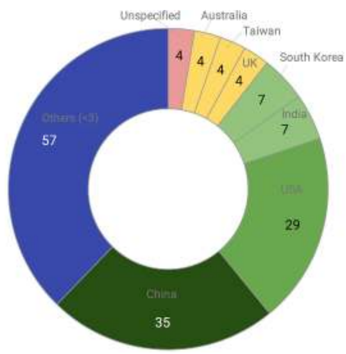

FIGURE 10. Geographic distribution of research in blockchain in healthcare.

Analysis by the country of the corresponding author's institutional affiliation as in Figure 10 shows that the leading countries in blockchain in healthcare research were China followed by the USA.

B. FUNCTIONAL DISTRIBUTION

Analysing the papers reviewed by their blockchain function, a similar trend as already discussed by Hölbl et al [20] emerged as in Figure 11. Reviewed articles' discussion dwells majorly on data sharing in the form of electronic medical records (EMR) or patient health records (PHR) or electronic health records (EHR). Others discussed access control with some focusing on identity management, master patient index and more. Auditability and non-repudiation of registered data was the focus of a few articles. Other reviewed papers discussed distributed computing, data storage, and data aggregation.

The papers were further categorised by health service delivery functions or application of blockchain in several healthcare domains. Papers featured service delivery applications for clinical trials, HIV, Insurance, Diabetes, Cancer, Blood management, Pharmaceutical and supply chain, financial inclusion and universal health coverage, Dermatology Radiology oncology, provider communication, DNA compression, Arrhythmia image classification, Haemoglobin test, Dental care and Dyslexia. One implementation discussed national level health system application. Table 4 provides details of these papers.

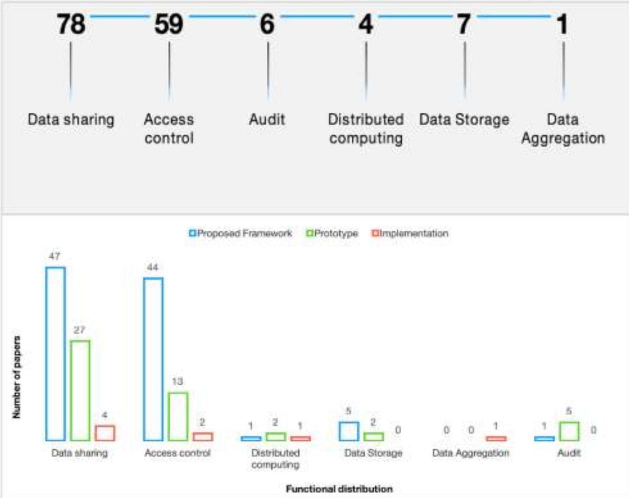

FIGURE 11. Functional distribution of articles.

TABLE 4. Detailed classification of reviewed papers by frameworks, prototypes and implementations.

Classification	Reference
Conceptual Models, Frameworks or Proposals	*Data sharing* [27]- [65] , [124] *Access Control* [29]- [34], [36]- [38], [40]- [42], [47], [49], [51]- [53], [55]- [60], [62]- [69], [114] , [115], [116], [118], [120], [121], [122], [123], [124], [150], [161] *Privacy* [126], [127], [128], [135], [136], [141] *Audit* [70], [114], [120] *Data storage* [117], [119], [120], [122], [123], [166] *Distributed Computing* [71], *Service delivery* - HIV [54], Clinical trial [28] [32] [60] [157] [165], Insurance [36] [41], Diabetes [55] [145], Cancer [64], Blood management [72], Pharmaceuticals [34] [146], Dermatology [44] LMIC [73], National Health System [74], Medical imaging [115] [147] [150], Health Education [121], Genetic data [152]
Prototypes and Experimentations	*Data sharing* [14], [75]- [98] *Access control* [14], [75], [76], [78], [80], [85], [87], [94], [95], [99], [91], [100], [101], [132], [140], [151], [161], [162], [158] *Privacy* [142], [143], [149], [157], [160], *Audit* [14], [75], [77], [80], [90], [102] *Distributed computing* [88], [103] *Data storage* [83], [104] *Service deliver* Software design [91] [105]] , Radiology Oncology [79] [81] [96], Cancer [79], Supply chain [82] [97], Patient centred care [77] [83] [86] [95], Provider communication [93], DNA compression [88], Arrhythmia image classification [99], Haemoglobin test (HbA1c) [102], Remote care [133]Dental care [136]
Implementations or Pilots	*Data sharing* [88], [97], [106], [137] *Access Control* [106], [163] *Distributed computing* [88] *Data aggregation and analysis* [107] *Service delivery* Dyslexia [107], National Health System [74] Supply chain management [97], [137]

C. TECHNICAL ANALYSIS

This section provides an in-depth analysis of the technical aspects of the 61 articles categorised as prototype and implementation. It was to guide practical next steps for implementing blockchain in healthcare. The architectures, storage schemes, standards, security, privacy, consensus mechanisms, performance, and cost discussed in these articles were analysed.

1) SYSTEM ARCHITECTURES

Broadly, three main types of architecture emerged based on our review of blockchain application in healthcare articles. The architecture of a prototyped or implemented blockchain network was found to be distinguished by its Certificates of Authority (CA). A Certificate Authority (CA) is the infrastructure that generates, stores, manages, distributes in addition to revoking these keys and related information. They three possible architectures that emerged were:

- *One-trusted-Certificate-Authority (One-CA) blockchain*,
- *Multiple-Certificate-Authorities (Multi-CA) blockchain*,
- *A Client-Self-Certificate-Authority blockchain*

Public key cryptographic technique is one way to to generate an asymmetric key for use on a blockchain network. As discussed earlier, this is typically a pair of keys, one designated as public and the other as private. These key pairs are used to sign and validate transactions on a blockchain network. These three groupings are as depicted in quadrants 2, 3 and 4 of Figure 12 conceptual architectures. The architecture in quadrant 1 depicts the current traditional EHR model that blockchain seeks to disrupt or enhance.

One architecture from articles that prototyped or implemented One-CA blockchain is part of a blockchain network, but use a trusted CA for asymmetric key generation. Articles that prototyped or implemented Multi-CA blockchain are part of a blockchain network, but use multiple nodes in the blockchain network as CA for asymmetric key generation. It can be one elected at a time or all acting in unison. Articles that prototyped or implemented Client-CA blockchain are part of a blockchain network, but each node generates its own asymmetric key locally and validates their key on the network.

The MedRec blockchain first published a white paper [92] in 2016 and prototyped on a private Ethereum network in 2017 [75]. This system follows the general architecture of a trusted-CA architecture where the custodians of the private blockchain are responsible for certificate issuing. The system is described as designed to allow vendors to use their existing systems.

Medblock [88] also uses a trusted CA architecture except that it proposes a Practical Byzantine Fault tolerant consensus algorithm. [101] also proposed and prototyped a trusted-CA architecture for identity and access management in Denmark.

[77] illustrates an architecture of a conceptual blockchain model for Health Information Exchange (HIE) amongst countries in the European Union. The model termed OpenNCP depicts a private blockchain network that logs transactions as they cross territorial borders. OpenNCP architecture represents quadrant 4 in our architecture where the nodes generate their key pairs. Only that in this case, this key pair is validated by a trusted internal CA.

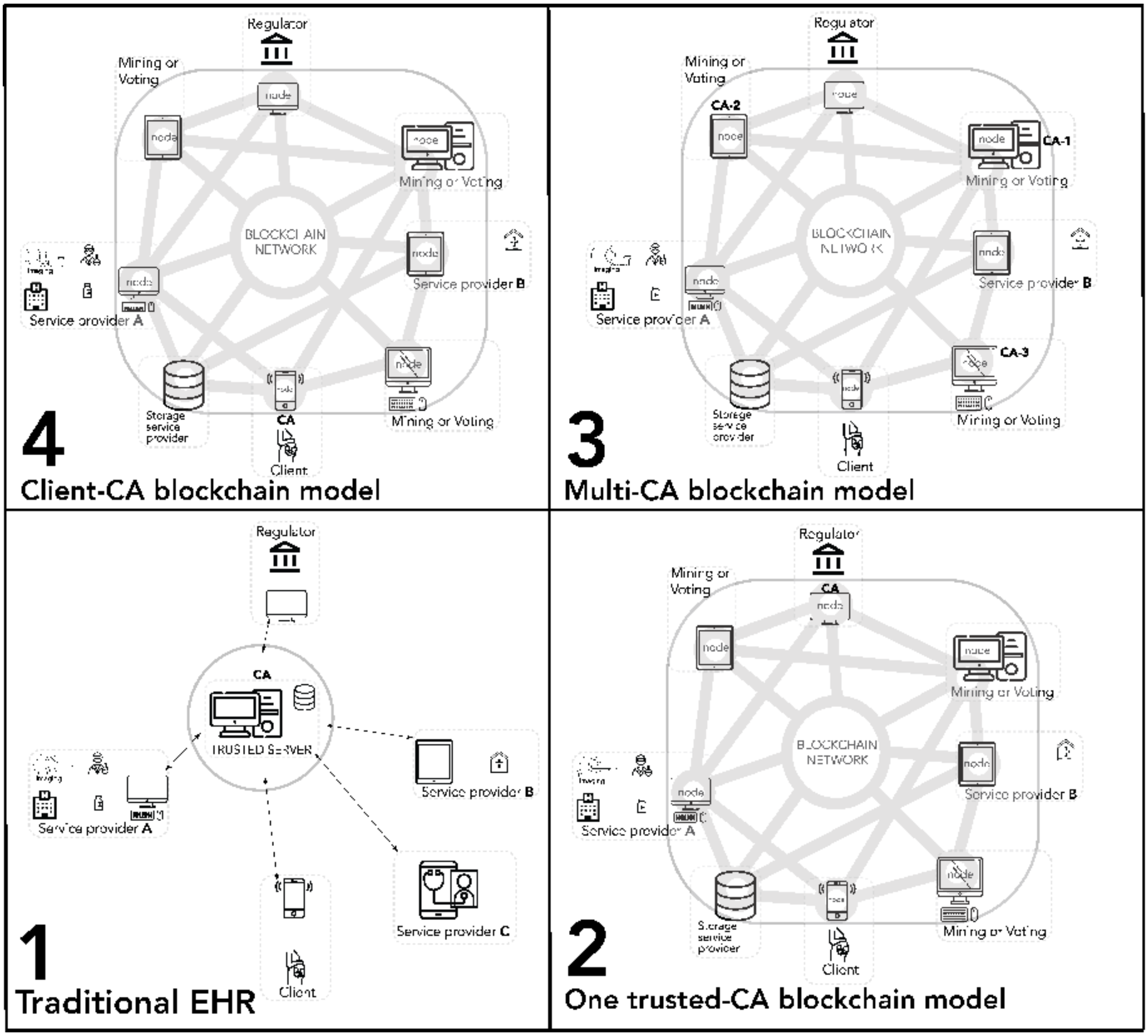

FIGURE 12. General blockchain architecture compared with traditional digital health architecture.

OmniPHR [95] proposed a patient-centric system based on a blockchain that gives the patient full control of their EMR while giving the provider a complete picture of a patient EMR hitherto scattered in multiple health data custodian institutions. The proposed system describes that data is encrypted and stored on the blockchain data blocks. The model considers every institution and individual including the patient and provider as nodes on the network. This model proposes the client-CA architecture of quadrant 4, where the client has full control of their EHR. It is also configurable to a Quadrant 2 architecture where the organisation can act as the Trusted CA. Information on if this is configurable as the multi-CA environment was not presented.

CB-SIFT [108] proposes the multi-CA architecture by outsourcing encrypted health information extraction overhead to cloud service providers on a blockchain network. CB-SIFT was found to perform better than bitcoin based on their evaluation.

[96] uses a membership service that acts as a CA to generate key pairs on the network. The paper did not provide further detail of the CA. [14] proposed GemOS blockchain broadly that can easily be any of the three architecture as the CA role technical detail was not provided. [82] similarly proposed Gcoin blockchain and prototyped same for logistics and supply chain. This system utilises the general architecture we presented in the second quadrant, where the one trusted CA issued the miner license and managed the root security of the blockchain.

Medshare [93] also use the Ethereum architecture, but to facilitate sharing of health data between cloud service providers connected on the same blockchain network. MedShare was evaluated, but provided no detail on how user

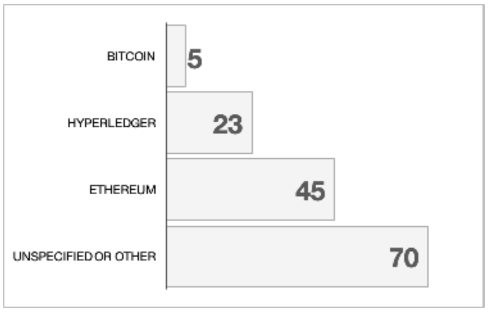

FIGURE 13. **Blockchain platforms by articles.**

authentication is generated. Hence we believe it is either a Trusted-CA architecture or a Multi-CA architecture.

BBDS [94] proposed a blockchain architecture that has a user, issuer, verifier, consensus nodes, and storage infrastructure. When compared to our conceptual architecture, users here are the client. The Issuer, verifier, and consensus nodes all are represented by the 'voting or mining' node on the conceptual architecture in Figure 12. In this paper, the Issuer acts as the CA, but the paper did not provide detail on if this was a single trusted CA or a combination of CAs in the blockchain network. Again, this system can easily be represented by quadrant 2 or 3 on our architecture.

[78] appear to extend our general blockchain architecture as it proposed a sensor interface that measures data about the patient and connects to a phone which then connects to the blockchain. We still consider this architecture to align with our general architecture as the Wireless body network sensors and the smart device can be viewed as the client in this case. Just like components and departments in a hospital can be viewed as the single hospital node that links and represents the institutions irrespective of other connected data sources.

2) BLOCKCHAIN PLATFORMS

More than half of the reviewed papers were silent on the blockchain platform used for either the proposition or prototype. Whereas most of the papers stating their platform of choice were those using the Ethereum platform, followed by Hyperledger fabric as shown in Figure 13. Papers using Bitcoin platform were mostly papers published in 2016. We have depicted the architecture of both blockchain file system in Figure 14.

Ethereum blockchain network is a public blockchain modelled after the Bitcoin blockchain. It still uses proof-of-work (PoW) for its consensus algorithm. It is also possible to run a private Ethereum blockchain. The structure of an Ethereum blockchain network can be decoupled into the presentation, Application Programming Interface (API), storage, and blockchain layers. The presentation layer is a web, mobile or desktop interface, and the API (currently a web3.js or web3.py framework) provides a connection to the Ethereum blockchain run by smart contracts (self-executing contracts). These smart contracts are often written in solidity programming language, but can also be written in

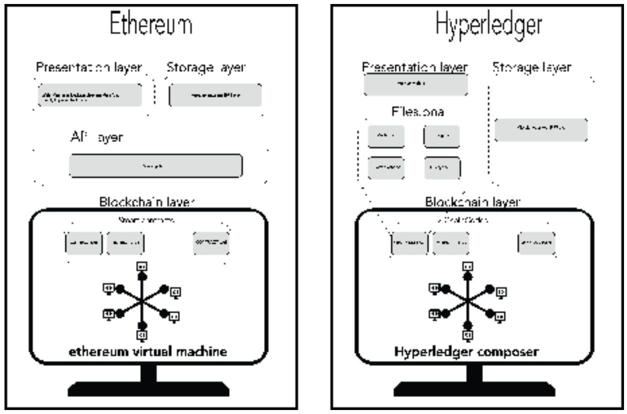

FIGURE 14. **Ethereum and Hyperledger blockchain architectures and file structures.**

other languages. The smart contracts are then converted to byte codes, a low level machine language once uploaded on the network. New consensus algorithms are being proposed like proof-of-stake for the Ethereum network. The MedRec blockchain [75], [92] deployed an unevaluated prototype with the following smart contracts: Registration Contract (RC), Patient-Provider-Relationship Contract(PPR), and Summary Contract (SC). The RC is used to register and map a patient's existing identification to their cryptographic address on the Ethereum network. The PPR on the other hand is used to configure and manage relationships between nodes on the network. The SC is then used to enable query of records by network participants. Medshare [93] utilised smart contract in general form for access management features, but provided no specific details. [78] utilises a minimum of two contracts running on a private Ethereum chain tested on Remix web platform. A main contract that calls other contracts that execute different business operations. [78] also prototyped the use of Ethereum blockchain for IoT Wireless body Area network and remote monitoring based on smart contracts. They compared the performance of their system with traditional EHR on HIPAA regulation privacy compliance metrics. [104] also prototyped using Ethereum to address the throughput challenge of bitcoin.

The Hyperledger fabric hosted by Linux Foundation has a similar architecture only that it has a business network archive (.bna) file. This file, made up of a model, logic, permissions, and query files aims to provide a complete system with all functionalities. Each of these files makes up the chain codes (the equivalent of the smart contracts in Ethereum). Composer is the primary development environment and most implementations are deployed through the docker container. Conversely, it also has the presentation, storage, and blockchain layers that mimic the Ethereum blockchain. The main difference between Hyperledger and Ethereum is that Hyperledger has only been implemented as Permissioned blockchain, while Ethereum has both Permissioned and Permissionless implementations. Current developments are focused on access and security management requirements of consortium blockchain rather than for public blockchain network where anyone can join. In our review, we found that [96] deployed Hyperledger and presented three scenarios for which to implement their Permissioned blockchain - Primary patient care, Data aggregate for research purpose, and shared health records. It was prototyped for radiology Oncology management. [76] also prototyped for the Hyperledger framework to demonstrate the tamperproof feature of blockchain. This paper also studied offline sync and fault-tolerance of the implemented system. Similarly, [79] equally implemented Hyperledger for radiology Oncology and cancer data sharing. It did not provide performance evaluation detail. [85] prototyped Hyperledger for access control functionality. [101] prototyped Hyperledger for access control and identity management.

A few others prototyped architectures that are neither Ethereum or nor Hyperledger follows the same general structure as described.

3) STORAGE SCHEMES

The data storage strategy for blockchain supported application is still linked to the scalability of blockchain networks. Clients on the public Ethereum network for instance implement using different databases like rocksdb and leveldb. Leveldb uses Google's key-value storage, and data storage on Ethereum blockchain is limited by gas price. Similarly, the data cap on the bitcoin network limits its scalability. This section is used to extract healthcare articles and their perspectives on managing healthcare data given the data storage constraints on blockchain networks, particularly the public ones. The patient can optionally store data off-site or on the blockchain network. The article [96], for instance used three categories of data for their prototype:

- *History and physical exams*,
- *Laboratory results*,
- *Radiation doses*

BlocHIE [83] uses two blockchains: EHR-chain and PHDchain to manage critical data and personal health data respectively. The paper explains that this helps combine off-chain storage with on-chain verification. The off-chain storage is maintained on the distributed database of the hospital using the EMR-chain. [87] also proposed an On-chain and Off-chain model to address the storage capacity and computation challenges. The roles in this proposed system are users, Authority agency and Administrator. The Authority agency and in this case the CA can be one or more. Similarly, the nodes are categorised as primary and backup. The primary node collects, groups and orders the transactions. The evaluation shows that varying number of attributes to be stored from 1 to 10 result in increased transaction time from 16seconds to 137seconds.

[104] proposed a data preservation scheme and tested the same using the Ethereum blockchain and analysed its performance. The Scheme will enable ensure primitiveness and verifiability of stored data while preserving the owner's privacy.

4) STANDARDS OR ONTOLOGIES ANALYSIS

This standards section discusses broadly two standards in reviewed articles: digital health standard and blockchain standard and how evaluated articles use or comply with these standards. Digital health standards are categorised for transportation, data structure and the language semantics. Only 40 papers of the 143 papers reviewed discussed any ontology or interoperability standard in their model, prototype or implementation. Health Level Seven (HL7's) Fast Healthcare Interoperability Resource (FHIR) ontology [27], [30], [51], [57], [64], [75], [80], [91], [92], [95], [102], [105], [159] dominated from reviewed papers.

[27] discussed a model that considers blockchain as a general-purpose data structure and proposes its application in healthcare using the FHIR standard. The choice of FHIR in this proposed design was two folds: It supports provenance and audit trail and it is an emerging standard that uses Representational State Transfer (REST) principles. The model uses proof of accurate data and proof of interoperability by ensuring incoming data meets structural and semantic constraints. The project achieved this using FHIR profiles as a computational conformance scheme.

Figure 15 shows the details of this distribution and others like older versions of HL7 [63], [65], [69], [75], [77], [80], [95], [123], Logical Observations Identifiers Names and Codes (LOINC) [30], [53], [65], [95], [165], World Health Organisation's (WHO's) International Classification of Diseases (ICD) [53], [65], [95], [130], International Organization for Standards (ISO) [95], Systematised Nomenclature of Medicine - Clinical Terms (SNOMED-CT) [59], [95], Digital Imaging and Communication in Medicine (DICOM) [65], [95], [114], Open Electronic Health Records (OpenEHR) [95], [106], [115]. OmniPHR [95] for instance uses a translator hosted as a super-peer (blockchain node) in the blockchain network. The super-peer is described as only triggered if the data passed is not in the openEHR format. When triggered, the translator translates the data from one of the other supported open standards to the OpenEHR format. The system uses two approaches to perform translation - 1) map open standards to OpenEHR standard. 2) use Natural Language Processing (NLP), Ontologies and use of Software agents to mediate heterogeneous standards.

Estonia national system uses XML based HL7 version 3 (extended) messaging standard [78]. There is a patient opt-out policy, and the system leverages the interconnection of existing 40 national information systems identification scheme and infrastructure linked together over the years.

Others mentioned once in reviewed papers are Integrating Healthcare Enterprise (IHE) [95], [114], [123], Institute of Electrical Electronics Engineers (IEEE) [65], XML Document Transform (xDT), CDMA [28], International Classification of Primary Care (ICPC) [53], CARRE [70], International Organization for Standards (ISO) Technical Committee 251 (TC251) [65], ISO13606 [106], European Committee for Standards (CEN) [95], Human Phenotype Ontology (HPO) [59], Online Mendelian

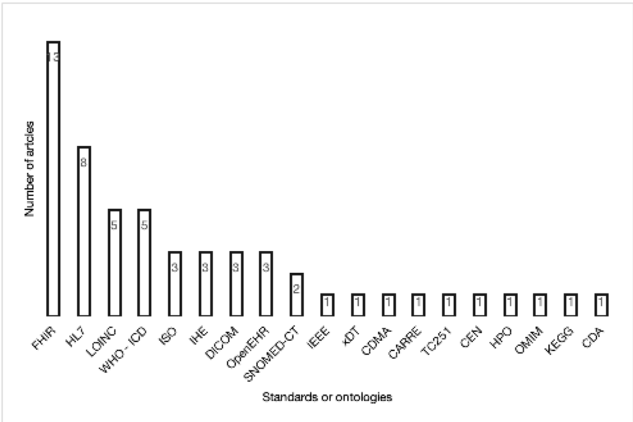

FIGURE 15. **Ontologies and standards used and their distribution.**

Inheritance of Man (OMIM) [59], Kyoto Encyclopaedia of Genes and Genomes (KEGG) [59], Clinical Document Architecture (CDA) [95], Systematised Nomenclature of Dentistry (SNODENT) [135].

None of the papers specifically focused on the blockchain standard, and this may also explain the reason why the performance evaluation metrics were wide and varied.

5) PRIVACY AND SECURITY ANALYSIS

This section looks at privacy and security, first from how they comply with existing regulation and second on how they address different security risks. A blockchain system like most Information Technology (IT) systems faces many different risks ranging from security of private keys, 51 per cent vulnerability, Byzantine fault tolerance, Double spending, criminal smart contracts, vulnerable smart contracts, under-priced and under-optimised smart contracts [109]. We reviewed the security of each prototype and implementation in the context of these criteria. Not every paper (we reviewed) provide enough detail for an objective analysis. Also, detailed security analysis is beyond the scope of this paper and is the subject of our future studies.

Only few reviewed papers discussed some form of compliance with established privacy and security regulations like Health Insurance Portability Accountability (HIPAA) [29], [37], [63]–[65], [75], [78], [80], [95], [102], [114] and European General Data Protection Regulation (GDPR) [38], [102]. [78] reported compliant with Protected Health Information (PIH) as defined by the HIPAA guideline. PHI is a set of datasets that if revealed either in isolation or in combination with other data can lead to the ability to identify the owner of the health information uniquely. Examples like name, phone number address etc. HIPAA provides a list and probably updates the list over time.

[93] verifies inconsistency in communication between cloud based health information sharing nodes on a blockchain network using cryptographic approaches and records such inconsistencies in a special database. OmniPHR [95] uses a configurable access control mechanism to give either the patient or the healthcare institution of choice total control such that they can manage permission themselves. The paper simulated the blockchain, but access management on the blockchain suggests it is a Permissioned blockchain. Information on what encryption algorithm used was not provided. [96] uses a set of metadata that a patient can set to enable read, write or share. Each data access is linked to the identity tag of the provider. The Hyperledger chain code manages all this. [98] implemented a proof-of-concept web portal and enrolled volunteers who were given a regenerated key which they could use to sign transactions on the web page. OpenNCP [77] an inter-jurisdiction health data exchange system has featured such as Audit management, patient identification, Data exchange and notification. The OpenNCP nodes by design regenerate keys and certificate every year and submit to the trusted internal CA. BMPLS [84] proposed and privacy and order-preserving encryption scheme for patient location data sharing with care provider. The scheme uses an SHA-256, OPE(2), and RSA-1024 encryption algorithms on a proof-of-work blockchain model for evaluation. [101] implemented an identity and access management using blockchain and evaluated to show that authentication and authorisation for all of Denmark's provider data (about 3.8MB) took 2-3 seconds. It was implemented using the Ethereum network. [91] proposed a keyless signature scheme for access control and management.

In Estonia, 99 per cent of patients have countrywide digital records access with an average of 300,000 patient queries and 100 per cent electronic healthcare billing annually [74], [111]. The blockchain that supports hospital databases runs a cross stakeholder decentralisation of three blockchain technologies. A Permissionless public and shared system based on Ethereum and Bitcoin, a Permissioned shared system based on Microsoft Coco, and a Permissioned private and shared system based on Hyperledger Keyless Signature Infrastructure (KSI) [112]. Guardtime manages the KSI on all the private, Permissioned, shared blockchain with three goals of regulatory compliance, integrity assurance, and compliance with dimensioning requirements. A technical evaluation of this project popularly called X-road is critical for a thorough understanding of this program to glean further technical details and understand its extent, health, and cost impacts.

6) BLOCKCHAIN TYPE AND CONSENSUS MECHANISM

Most of the studies used either consortium or private blockchain types in the design, prototype or implementation as shown in Figure 16. Most papers analysed did not discuss development strategy, yet a few mentioned their system as either open source or having an Open API or proprietary, and again most did not discuss this as shown in Figure 17. Only the following papers reviewed papers discussed one or more of the following consensus algorithms: Proof-of-Work [27], [31], [38], [40], [41], [44]–[46], [50], [70], [75], [77], [80], [84], [87], [92], [96], [98], [106], [108], [118], [122], [127], Proof-of-Stake [114], [115], [124], [125], Proof-of-Existence [28],

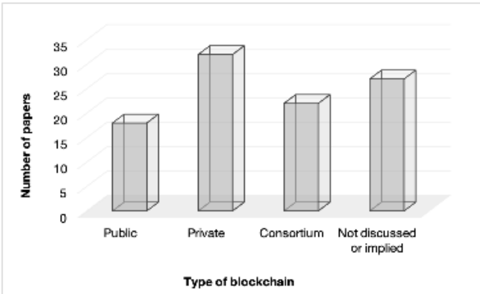

FIGURE 16. Distribution by types of blockchain used.

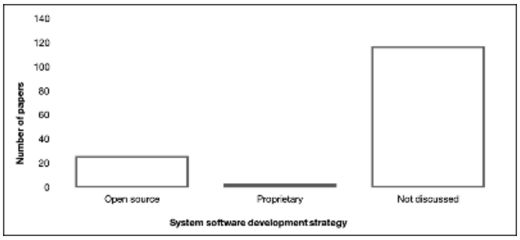

FIGURE 17. Distribution by the system development strategy.

Proof-of-Information [62], Delegated-Proof-of-Stake [34], [121], [166], Hybrid-Delegated-Proof-of-Stake [85], [90], Delegated-Proof-of-Work [103], Proof-of-Disease [59], Proof-of-Authority [143], and Proof-of-Familiarity [158].

7) PERFORMANCE ANALYSIS

The 61 Prototypes and Implementation papers were assessed for performance evaluation using established metrics by Hyperledger Performance and Scale Working Group [17].

About half (n = 31) papers classified as prototype or implementation papers discussed any form of performance or evaluation. Majority of papers discussing performance had various metrics for assessing their prototype or implementation performance. Each paper was reviewed according to observation points, transaction characteristics, number of tests, type of test, duration of the test, transaction latency, transaction throughput, read latency, read throughput, fault or network loads, challenges addressed, blockchain solution proposed, and hardware characteristics. None of the reviewed papers surveyed the read throughput characteristic of their evaluated implementation. Thus no article provided evaluation information across all metrics as listed in [17]. Some articles evaluated implementation using software simulation, others by experimentation on computer workbench set-ups.

Medshare [93] simulated its evaluation using JMeter with active requestors for data ranging from five (5) to 100 while time was varied to 2 minutes, 5 minutes, 10 minutes, 20 minutes, and 30 minutes. The latency of the evaluation was then recorded and compared with a similar system. OmniPHR [95] simulated its architecture evaluation using the OMNET++ and INET open source modelling and simulation frameworks. It simulated the design on 100 nodes of two groups of tests. It found that the CPU (2GHz 2 core) and RAM (8GB) were half utilised for between 100 and 3200 nodes. Details of latency and throughput are as in table 5. BlocHIE [83] was implemented using the python framework Django and performance measured and presented. This prototype also provided the mathematical proof of the fairness packaging algorithm.

Table 5 provides performance evaluation only for those papers which specified any of the evaluation metric information needed for the performance evaluation. In Table 5, 'N/A' denotes 'not available', implying this information was not provided in the reviewed papers. Seven (7) of the system simulated their performance evaluation, and there were 12 experimentations where actual devices where connected in a laboratory environment for the performance testing. Our study documented four pilot studies [88], [97], [106], [107] and an ongoing implementation [74].

8) COST ANALYSIS

The cost of a blockchain system remains a major bottleneck to its scalability. This section analyses the discussions by reviewed articles in relation to cost. [94] did not provide a prototype evaluation, but the detailed cost in space units required to store data adequately. [104] proposed, prototyped and evaluated a data preservation scheme and the preservation cost was estimated for text and media type files. As the size was varied from 10bytes to 500byte, the cost also varied from 0.1 to 1.6 US dollars almost evenly for both file types.

[150] evaluated the cost for the data of 50 random participants stored on a blockchain node on AWS cloud over a 9 days period. They estimated costs per transaction using the current wei-dollar conversion rates. Wei is the smallest denomination of ether, the cryptocurrency used on the Ethereum network. They found that each participant spent an average of $ 283.85 per transaction to store all their data on the Ethereum blockchain. The total transaction data from all 50 participants came to 259.2 kilo bytes.

IV. DISCUSSION AND LIMITATIONS

Here we discuss the implications of bibliometric, functional, and technical analysis, of proposed frameworks, prototypes and implementations. The discussions were to further address the research question of the current state of the art and emerging trends and emerging trends. The perceived limitation of this study is also discussed in this section.

A. DISCUSSIONS

The discussion grouped by the research questions interprets the findings from reviewed articles in the context of each research question.

RQ-1: *What is the current research state of the art of blockchain application in healthcare concerning proposed systems (frameworks, concepts, and models), prototypes, and real-life implementations and/or pilots?*

This study established the current state of the art in blockchain in healthcare. Papers proposing models without a prototype or implementation as stated earlier accounted for two-thirds of papers. It is expected for a relatively new

TABLE 5. Performance evaluation of reviewed papers using [17] metrics.

Paper	Observation	TestType	Test count	Test duration	Tx latency	Tx throughput	Rd latency	Hardware specs
[93]	5 -100 users	JMeter sim.	8 tests	54.4 -1286.73 secs	N/A	N/A	N/A	N/A
[95]	100 - 3200 nodes	OverSIM sim.	20 tests	3 hours	500ms average	N/A	N/A	2GHz,2-core, 8GB
[97]	IoT sensors	Pilot study	7576 points	1 month	N/A	N/A	N/A	N/A
[76]	4 Virtual Machines	Experimental	1 test	5 days	N/A	N/A	N/A	i5, 2.2GHz, 8GB
[83]	8 servers/clients	Experimental	56 Tx	N/A	N/A	46 Tx/s	N/A	N/A
[104]	1MB - 50MB file	Geth sim.	50 - 350 Tx	N/A	200ms - 500ms	30MB file	N/A	i5, 2.2GHz, 16GB, Mac
[84]	1 node	N/A	N/A	N/A	0-5 secs	N/A	N/A	i5, 2.5GHz, 8GB
[85]	N/A	N/A	5 - 100 con.	N/A	0-900ms	N/A	N/A	N/A
[87]	10 nodes	Experimental	1-10 nodes	N/A	23 - 205 secs	N/A	N/A	i7, 2.7GHz, 4GB
[106]	64-512 con.	Pilot study	40,000 adults	1week	184-556ms	26MB-278MB	N/A	N/A
[88]	N/A	N/A	25 samples	N/A	N/A	N/A	N/A	N/A
[100]	2 nodes	MIRCL cpabe sim.	10 runs	N/A	N/A	N/A	N/A	i5, 3.3GHz, 8GB
[89]	N/A	Virtual 3D Avatar	N/A	N/A	N/A	N/A	N/A	N/A
[108]	2-4 communities	Experimental	N/A	N/A	5-30mins	N/A	N/A	i5, 3.3GHz, 8GB
[101]	1 PC	Chrome sim.	4000 blocks	N/A	219ms	767kB	86ms	2.4GHz, 8GB, 1TB
[91]	1 PC	JMeter sim.	N/A	N/A	500ms	2048kB	N/A	N/A
[107]	N/A	Pilot study	15 persons	N/A	14 secs	N/A	N/A	N/A
[109]	N/A	N/A	Implementation	N/A	Ongoing	N/A	N/A	N/A
[132]	1 node	Java-pair cryp.Lib	N/A	N/A	TTP/MTP 1.5ms	N/A	N/A	i7,2GHz, 8GB, Win10
[133]	multiple	Remix	N/A	N/A	N/A	N/A	N/A	N/A
[137]	1 node	AWS cloud IoT	25tx	N/A	N/A	N/A	N/A	AWS EC2 instance
[138]	2 node	AWS cloud	500 participants	N/A	<=30sec	8kb - 128kb	N/A	ES2, UbuntuLT16.04
[139]	2 node	AWS cloud	10 patients	N/A	<=40ses	50kb - 300kb	N/A	ES2, UbuntuLT16.04
[140]	2 node	RaspberriPi	2 - 10 blocks	N/A	200ms - 2sec	8kb-128kb	N/A	RaspberriPi 3.3GHz
[143]	1 node	AWS cloud	N/A	N/A	5sec - 6sec	236bytes	N/A	ES2, UbuntuLT16.04
[148]	1 node	Remix	N/A	N/A	N/A	N/A	N/A	N/A
[149]	1 node	Experimental	N/A	N/A	7Mb/ms - 12Mb/ms	21kb-36kb	N/A	N/A
[150]	1 node	AWS cloud	50 users	9days	N/A	259.2kb	N/A	N/A
[153]	1 PC	N/A	N/A	N/A	N/A	N/A	N/A	ES2, UbuntuLT16.04
[157]	10 PCs	N/A	N/A	N/A	N/A	N/A	N/A	Win10, i7, 3.4GHz
[162]	4 PCs	Experiment	N/A	N/A	N/A	N/A	N/A	Xeon, ES2, Ubuntu

domain as this demonstrates active ongoing research. There were two significant categories of proposition papers - a proposition for application of existing blockchain design or platform to a new health service delivery domain and a propositions for using new functional use case that can be Identity management, Information sharing, audit, and access control. From the reviews, we postulated that all blockchain in healthcare application follow the same architecture with minor variation arising from how the Certificate Authority (CA) in the blockchain platform is constituted and managed. The signature or key pair generation, management and distribution role of the CA can be individually managed, a trusted-CA managed, or multi-CA managed. Other minor variations like some blockchain deployment using smart contract and others using chain code or some not using anywhere considered unimportant in categorising the architecture.

Similarly, a few types of research are ongoing on storage schemes and two significant categories emerged - on-chain storage and off-chain storage. The challenge is how to maintain a high level of anonymity of data as they are stored and exchange while guaranteeing performance. It has a direct implication on the cost of implementing or managing a blockchain in the healthcare system. Current evaluation of this cost indicates that it is unrealistically high and requires further research and innovation.

We analysed blockchain in healthcare articles for digital health standards adopted for data transportation, data structure and terminologies (semantics). Most of the papers only discuss digital health standards at superficial level. One paper discussed using NLP and ontology for data standards translation before exchange. The open standard FHIR as expected was the most widely discussed digital health standard. Most papers did not provide in-dept discussions on the applications of FHIR or other standards. Also, papers did not look at blockchain standards, and this is evident in the fact that performance evaluation result from articles varied widely.

Most articles focused on access control addressed privacy. Moreover, we assessed that complying with the relevant regulations like HIPAA and GDPR were possible, they only come at a performance cost. The security and trust profile of the different blockchain architectures are directly proportional to their CA type. A single trusted CA lean more to centralisation. An individual (patient or provider) managed CA on the other extreme lead to complicated data integrity and security system. Only a few systems discussed encryption algorithms used, either because the majority use the standard Ethereum or Hyperledger blockchain and did not provide further technical or mathematical detail of proposals or prototypes.

Issues around communication overhead, scalability, the time it takes to execute a transaction are key performance issues with current blockchain in healthcare systems. About half of the prototyped blockchain in healthcare papers did not include performance evaluation information. The few papers that did only include sparse information and were evaluated using different metrics. For instance, most papers discussed transaction latency and throughput, and there was limited information on read latency and read throughput. Also, the test environment is varied, observation points varied, and only one of the papers simulated effect of the fault and network outage on the reliability and ledger immutability. Most prototyped implementations used simulation software for their study evaluation. Majority of the reviewed papers used PoW as their consensus algorithm. It is not surprising as there are currently no implemented public alternative to PoW consensus algorithm.

RQ-2: *How do they compare to traditional healthcare data management techniques?*

Clients, health institutions and providers identification remain a major issue in the digital health space. Blockchain is one of the promising technologies to help address this challenge. This problem is more pronounced in developing countries and yet limited research was found from these domains. Not enough blockchain in healthcare proposals or pilots are considering digital health or other standard metrics. The current data management performance and costs are still below average given the current health care trends in data production, speed of processing and performance. Blockchain proved that it could solve the trust problem, but performance and cost remain a significant bottleneck. Many implementations also addressed privacy constraints including compliance with PHI requirement of HIPPA. They however are below average in performance.

RQ-3: *What are the emerging trends?*

We found the explosion of proposals and few prototypes and pilots. We are anticipating more implementation and proof-of-concept pilots. We also expect more comparison of blockchain proposals or implemented systems to traditional EMR systems. We believe the cost and performance issues will be addressed in near future research.

B. LIMITATIONS

A fundamental limitation of this study is that it focused on literary work and may have inadvertently excluded the many ongoing non-scholarly progress or advanced pilots or implementations that are yet to be published. An example is the Estonia national level implementation where published discussion of the implementation lacked details, that was only available from the project website and non-literary presentation online. Our architecture model is high-level and may not provide all the detail required for some readers.

V. CONCLUSION

This study sets out to answer the question on the current state of the art in blockchain in healthcare research and emerging trends. The bibliometric and functional distribution of 143 research articles in blockchain in healthcare were presented. Also presented is the technical analysis of 61 of these articles categorised as prototypes or implementations by architectures, storage schemes, standards and ontologies and privacy/security, performance and cost. We presented the distribution of blockchain platforms, types adopted by reviewed articles. This paper has demonstrated that though there is a surge of interest and research in blockchain in healthcare, most published studies are still conceptual, framework proposition, and experimental prototypes with minimal real-word implementation or pilots. This paper aggregates the current states of the art in blockchain in healthcare detailing the functional use cases. Data sharing, access control, audit, distributed computing, data storage, data aggregation where important functional use cases discussed by reviewed papers. Health domains with proposition or pilots include HIV aids, Cancer, Clinical trials, Insurance, Dyslexia, Haemoglobin tests, drug supply-chain, Arrhythmia Image classification, DNA compression, Radiology oncology and Care provider communication.

Our analysis shows that poor scalability, low general performance and high cost remain a real impediment to implementing a scalable blockchain in healthcare as in many other sectors. Area of future research should include an in-depth performance evaluation using standardised blockchain performance measurement metrics. Also, future research should also focus on the structure and semantics of exchanged data. This paper will prove invaluable to business, technical and non-technical health information exchange players who may be interested in a trend map of the current state of the art.

REFERENCES

[1] S. Mcclean, J. Gillespie, L. Garg, M. Barton, B. Scotney, and K. Kullerton, "Using phase-type models to cost stroke patient care across health, social and community services," *Eur. J. Oper. Res.*, vol. 236, no. 1, pp. 190–199, Jul. 2014.

[2] *WORLD HEALTH STATISTICS 2018: Monitoring Health for the SDGs*, WHO, Geneva, Switzerland, 2018.

[3] AAMC. (2019). *Careers in Medicine*. Accessed: Jan. 29, 2019. [Online]. Available: https://www.aamc.org/cim/specialty/exploreoptions/list/

[4] P. Zhang, D. C. Schmidt, J. White, and G. Lenz, "Blockchain technology use cases in healthcare," *Adv. Comput.*, vol. 111, pp. 1–41, Jan. 2018.

[5] M. Hosseini and B. E. Dixon, "Syntactic interoperability and the role of standards," in *Health Information Exchange: Navigating a Network of Health Information Systems*. Amsterdam, The Netherlands: Elsevier, 2016, p. 135.

[6] T. D. McFarlane, B. E. Dixon, and S. J. Grannis, "'Client registries: Identifying and linking patients," in *Health Information Exchange: Navigating and Managing a Network of Health Information Systems*, B. Dixon, Ed., 1st ed. Indianapolis, IN, USA: Elsevier, 2016, pp. 163–182.

[7] M. Tomlinson, M. J. Rotheram-Borus, L. Swartz, and A. C. Tsai, "Scaling up mHealth: Where is the evidence?" *PLoS Med.*, vol. 10, no. 2, Feb. 2013, Art. no. e1001382.

[8] E. Lau, "Decoding the hype blockchain in healthcare," M.S. thesis, Utrecht Univ., Utrecht, The Netherlands, Jun. 2018.

[9] J. Anderson, "Record audit logs through permissioned blockchain technology," Tech. Rep., 2018.

[10] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *J. Gen. Philosophy Sci.*, vol. 39, no. 1, pp. 53–67, 2008, doi: 10.1007/s10838-008-9062-0.

[11] D. Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money*.

[12] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, "Everything you wanted to know about the blockchain: Its promise, components, processes, and problems," *IEEE Consum. Electron. Mag.*, vol. 7, no. 4, pp. 6–14, Jul. 2018.

[13] M. Crosby, Nachiappan, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology beyond bitcoin," *Blockchain Technol.*, 2015.

[14] C. Burniske, E. Vaughn, J. Shelton, and A. Cahana, "How blockchain technology can enhance ehr operability," Gem | Ark Invest Res., Tech. Rep., 2016.

[15] B. Schneier, "Foundations," in *Applied Cryptography: Protocols, Algorithms and Source Code in C*, 2nd ed. 2006, pp. 1–5.

[16] B. Schneier, *Applied Cryptography: Protocols, Algorithm, and Source Code in C*, 2nd ed. 2006.

[17] *Hyperledger Blockchain Performance Metrics*, Hyperledger White Paper Work. Group, 2018.

[18] A. M. Turing, "Intelligent machinery, A heretical theory," *Philosophia Math.*, vol. 4, no. 3, pp. 256–260, Sep. 1996.

[19] V. Buterin, "A next generation smart contract and decentralized application platform," Ethereum, Ethereum White Paper, 2013.

[20] M. Hölbl, M. Kompara, and A. Kamisali, "'A systematic review of the use of blockchain in healthcare," Tech. Rep., Sep. 2018, pp. 1–22.

[21] C. Agbo, Q. Mahmoud, and J. Eklund, "Blockchain technology in healthcare: A systematic review," *Healthcare*, vol. 7, no. 2, p. 56, Apr. 2019.

[22] H. Jin, Y. Luo, P. Li, and J. Mathew, "A review of secure and privacy-preserving medical data sharing," *IEEE Access*, vol. 7, pp. 61656–61669, 2019.

[23] C. Saraf and S. Sabadra, "Blockchain platforms: A compendium," in *Proc. IEEE Int. Conf. Innov. Res. Develop. (ICIRD)*, May 2018, pp. 1–6.

[24] E. Meinert and C. F. Fcmi, "Implementing blockchains for efficient healthcare: A systematic review," Dept. Primary Care, Univ. Oxford, Oxford, U.K., Tech. Rep., 2018.

[25] S. Alla, L. Soltanisehat, U. Tatar, and O. Keskin, "Blockchain technology in electronic healthcare systems," in *Proc. IISE Annu. Conf. Expo*, May 2018, pp. 901–906.

[26] G. Drosatos and E. Kaldoudi, "Blockchain applications in the biomedical domain: A scoping review," *Comput. Struct. Biotechnol. J.*, vol. 17, pp. 229–240, Feb. 2019.

[27] K. Peterson, R. Deeduvanu, P. Kanjamala, and K. Boles, "A blockchain-based approach to health information exchange networks," in *Proc. NIST Workshop Blockchain Healthcare*, 2016, pp. 1–10.

[28] T. Nugent, D. Upton, and M. Cimpoesu, "Improving data transparency in clinical trials using blockchain smart contracts," *F1000Research*, vol. 5, p. 2541, Oct. 2016.

[29] G. Magyar, "Blockchain: Solving the privacy and research availability tradeoff for EHR data: A new disruptive technology in health data management," in *Proc. IEEE 30th Neumann Colloq. (NC)*, Nov. 2017, pp. 135–140.

[30] J. Brogan, I. Baskaran, and N. Ramachandran, "Authenticating health activity data using distributed ledger technologies," *Comput. Struct. Biotechnol. J.*, vol. 16, pp. 257–266, Jan. 2018.

[31] S. H. Lee and C. S. Yang, "Fingernail analysis management system using microscopy sensor and blockchain technology," *Int. J. Distrib. Sensor Netw.*, vol. 14, no. 3, Mar. 2018, Art. no. 155014771876704.

[32] F. Angeletti, I. Chatzigiannakis, and A. Vitaletti, "The role of blockchain and IoT in recruiting participants for digital clinical trials," in *Proc. 25th Int. Conf. Softw., Telecommun. Comput. Netw. (SoftCOM)*, Sep. 2017, pp. 1–5.

[33] A. Zhang and X. Lin, "Towards secure and privacy-preserving data sharing in e-Health systems via consortium blockchain," *J. Med. Syst.*, vol. 42, p. 140, Aug. 2018.

[34] P. Sylim, F. Liu, A. Marcelo, and P. Fontelo, "Blockchain technology for detecting falsified and substandard drugs in distribution: Pharmaceutical supply chain intervention," *JMIR Res. Protocols*, vol. 7, no. 9, Jul. 2018, Art. no. e10163.

[35] T. Dey, S. Jaiswal, S. Sunderkrishnan, and N. Katre, "HealthSense: A medical use case of Internet of Things and blockchain," in *Proc. Int. Conf. Intell. Sustain. Syst. (ICISS)*, Dec. 2017.

[36] H. Wang and Y. Song, "Secure cloud-based EHR system using attribute-based cryptosystem and blockchain," *J. Med. Syst.*, vol. 42, p. 152, Aug. 2018.

[37] X. Liang, S. Shetty, J. Zhao, D. Bowden, D. Li, and J. Liu, "Towards decentralized accountability and self-sovereignty in healthcare systems," in *Information and Communications Security* (Lecture Notes in Computer Science). Cham, Switzerland: Springer, 2018.

[38] X. Zheng, R. R. Mukkamala, R. Vatrapu, and J. Ordieres-Mere, "Blockchain-based personal health data sharing system using cloud storage," in *Proc. IEEE 20th Int. Conf. e-Health Netw., Appl. Services (Healthcom)*, Sep. 2018, pp. 1–6.

[39] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," in *Proc. IEEE 28th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Oct. 2017, pp. 1–5.

[40] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "Continuous patient monitoring with a patient centric agent: A block architecture," *IEEE Access*, vol. 6, pp. 32700–32726, 2018.

[41] L. Zhou, L. Wang, and Y. Sun, "MIStore: A blockchain-based medical insurance storage system," *J. Med. Syst.*, vol. 42, p. 149, Aug. 2018.

[42] S. Badr, I. Gomaa, and E. Abd-Elrahman, "Multi-tier blockchain framework for IoT-EHRs systems," *Procedia Comput. Sci.*, vol. 141, pp. 159–166, Jan. 2018.

[43] J. Chen, X. Ma, M. Du, and Z. Wang, "A blockchain application for medical information sharing," in *Proc. IEEE Int. Symp. Innov. Entrepreneurship (TEMS-ISIE)*, Mar. 2018, pp. 1–7.

[44] K. Mannaro, G. Baralla, A. Pinna, and S. Ibba, "A blockchain approach applied to a teledermatology platform in the sardinian region (Italy)," *Information*, vol. 9, no. 2, p. 44, Feb. 2018.

[45] S. Amofa, E. B. Sifah, K. O.-B. O. Agyekum, S. Abla, Q. Xia, J. C. Gee, and J. Gao, "A blockchain-based architecture framework for secure sharing of personal health data," in *Proc. IEEE 20th Int. Conf. e-Health Netw., Appl. Services (Healthcom)*, Sep. 2018, pp. 1–6.

[46] H. Jiang, H. Peng, and S. Dian, "A design of medical information sharing model based on blockchain technology," *IOP Conf. Ser., Mater. Sci. Eng.*, vol. 428, Oct. 2018, Art. no. 012006.

[47] Y. Du, J. Liu, Z. Guan, and H. Feng, "A medical information service platform based on distributed cloud and blockchain," in *Proc. IEEE Int. Conf. Smart Cloud (SmartCloud)*, Sep. 2018, pp. 34–39.

[48] C. Ananth, M. Karthikeyan, and N. Mohananthini, "A secured healthcare system using private blockchain technology," *J. Eng. Technol.*, vol. 6, no. 2, pp. 42–54, 2018.

[49] G. Srivastava, A. D. Dwivedi, and R. Singh, "Automated remote patient monitoring: Data sharing and privacy using blockchain," 2018, *arXiv:1811.03417*. https://arxiv.org/abs/1811.03417

[50] S. Rahmadika and K.-H. Rhee, "Blockchain technology for providing an architecture model of decentralized personal health information," *Int. J. Eng. Bus. Manage.*, vol. 10, Jan. 2018, Art. no. 184797901879058.

[51] M. Z. A. Bhuiyan, A. Zaman, T. Wang, G. Wang, H. Tao, and M. M. Hassan, "Blockchain and big data to transform the healthcare," in *Proc. Int. Conf. Data Process. Appl. (ICDPA)*, 2018, pp. 62–68.

[52] T. T. Thwin and S. Vasupongayya, "Blockchain based secret-data sharing model for personal health record system," in *Proc. 5th Int. Conf. Adv. Inform., Concept Theory Appl. (ICAICTA)*, Aug. 2018, pp. 196–201.

[53] S. Alexaki, G. Alexandris, V. Katos, and N. E. Petroulakis, "Blockchain-based electronic patient records for regulated circular healthcare jurisdictions," in *Proc. IEEE 23rd Int. Workshop Comput. Aided Modeling Design Commun. Links Netw. (CAMAD)*, Sep. 2018, pp. 1–6.

[54] J. Liu, "HIV digital vaccine strategy: An application of blockchain technology in preventing the spread of HIV," Tech. Rep., 2018.

[55] S. L. Cichosz, M. N. Stausholm, T. Kronborg, P. Vestergaard, and O. Hejlesen, "How to use blockchain for diabetes health care data and access management: An operational concept," *J. Diabetes Sci. Technol.*, vol. 13, no. 2, pp. 248–253, Mar. 2019.

[56] M. Hanley and H. Tewari, "Managing lifetime healthcare data on the blockchain," in *Proc. IEEE SmartWorld, Ubiquitous Intell. Comput., Adv. Trusted Comput., Scalable Comput. Commun., Cloud Big Data Comput., Internet People Smart City Innov. (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, Oct. 2018, pp. 246–251.

[57] P. B. Nichol and W. Dailey, "Micro-identities improve healthcare interoperability with blockchain: Deterministic methods for connecting patient data to uniform patient identifiers," ResearchGate, Berlin, Germany, Tech. Rep., 2016.

[58] A. Theodouli, S. Arakliotis, K. Moschou, K. Votis, and D. Tzovaras, "On the design of a blockchain-based system to facilitate healthcare data sharing," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun., 12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2018, pp. 1374–1379.

[59] A. K. Talukder, M. Chaitanya, D. Arnold, and K. Sakurai, "Proof of disease: A blockchain consensus protocol for accurate medical decisions and reducing the disease burden," in *Proc. IEEE SmartWorld, Ubiquitous Intell. Comput., Adv. Trusted Comput., Scalable Comput. Commun., Cloud Big Data Comput., Internet People Smart City Innov. (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, Oct. 2018, pp. 257–262.

[60] Z. Shae and J. J. Tsai, "On the design of a blockchain platform for clinical trial and precision medicine," in *Proc. IEEE 37th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jun. 2017, pp. 1972–1980.

[61] A. Al Omar, M. S. Rahman, A. Basu, and S. Kiyomoto, "MediBchain: A blockchain based privacy preserving platform for healthcare data," in *Security, Privacy, and Anonymity in Computation, Communication, and Storage* (Lecture Notes in Computer Science). Cham, Switzerland: Springer, 2017.

[62] T.-T. Kuo and L. Ohno-Machado, "ModelChain: Decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks," 2018, *arXiv:1802.01746*. [Online]. Available: https://arxiv.org/abs/1802.01746

[63] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," *Sustain. Cities Soc.*, vol. 39, pp. 283–297, May 2018.

[64] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, "FHIRChain: Applying blockchain to securely and scalably share clinical data," *Comput. Struct. Biotechnol. J.*, vol. 16, pp. 267–278, Jan. 2018.

[65] W. Liu, S. Zhu, T. Mundie, and U. Krieger, "Advanced block-chain architecture for e-health systems," in *Proc. IEEE 19th Int. Conf. e-Health Netw., Appl. Services (Healthcom)*, Oct. 2017, pp. 1–6.

[66] A. F. Hussein, N. Arunkumar, G. Ramirez-Gonzalez, E. Abdulhay, J. M. R. Tavares, and V. H. C. De Albuquerque, "A medical records managing and securing blockchain based system supported by a genetic algorithm and discrete wavelet transform," *Cognit. Syst. Res.*, vol. 52, pp. 1–11, Dec. 2018.

[67] R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems," *IEEE Access*, vol. 6, pp. 11676–11686, 2018.

[68] J. P. Dias, L. Reis, H. S. Ferreira, and A. Martins, "Blockchain for access control in e-Health scenarios," 2018, *arXiv:1805.12267*. [Online]. Available: https://arxiv.org/abs/1805.12267

[69] M. L. Gagnon and G. Stephen, "A pragmatic solution to a major interoperability problem: Using blockchain for the nationwide patient index," Tech. Rep., 2018.

[70] A.-S. Kleinaki, P. Mytis-Gkometh, G. Drosatos, P. S. Efraimidis, and E. Kaldoudi, "A blockchain-based notarization service for biomedical knowledge retrieval," *Comput. Struct. Biotechnol. J.*, vol. 16, pp. 288–297, Jan. 2018.

[71] Z. Shae and J. Tsai, "Transform blockchain into distributed parallel computing architecture for precision medicine," in *Proc. IEEE 38th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jul. 2018, pp. 1290–1299.

[72] S. Kim and D. Kim, "Design of an innovative blood cold chain management system using blockchain technologies," *ICIC Express Lett. B, Appl., Int. J. Res. Surv.*, vol. 9, no. 10, pp. 1067–1073, 2018.

[73] B. M. Till, A. W. Peters, S. Afshar, and J. Meara, "From blockchain technology to global health equity: Can cryptocurrencies finance universal health coverage?" *BMJ Global Health*, vol. 2, no. 4, Nov. 2017, Art. no. e000570.

[74] T. Heston, "A case study in blockchain health care innovation," *Int. J. Current Res.*, vol. 9, no. 11, pp. 60587–60588, 2017.

[75] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in *Proc. 2nd Int. Conf. Open Big Data (OBD)*, Aug. 2016, pp. 25–30.

[76] D. Ichikawa, M. Kashiyama, and T. Ueno, "Tamper-resistant mobile health using blockchain technology," *JMIR Mhealth Uhealth*, vol. 5, no. 7, p. e111, Jul. 2017.

[77] L. Castaldo and V. Cinque, "Blockchain-based logging for the cross-border exchange of ehealth data in Europe," in *Security in Computer and Information Sciences* (Communications in Computer and Information Science). Cham, Switzerland: Springer, 2018.

[78] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring," *J. Med. Syst.*, vol. 42, no. 7, p. 130, 2018.

[79] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, "How blockchain could empower eHealth: An application for radiation oncology," in *Data Management and Analytics for Medicine and Healthcare* (Lecture Notes in Computer Science). Cham, Switzerland: Springer, 2017.

[80] A. Ekblaw and A. Asaf, "'MedRec: Medical data management on the blockchain PubPub," PubPub, Tech. Rep., 2016.

[81] A. Allison, C. Anne, N. Diakun-Thibault, L. Forni, F. Landa, J. Mayo, and R. Vab Riezen, "Blockchain and health it: Algorithms, privacy and data," Tech. Rep.

[82] J.-H. Tseng, Y.-C. Liao, B. Chong, and S.-W. Liao, "Governance on the drug supply chain via gcoin blockchain," *Int. J. Environ. Res. Public Health*, vol. 15, no. 6, p. 1055, May 2018.

[83] S. Jiang, J. Cao, H. Wu, Y. Yang, M. Ma, and J. He, "BlocHIE: A blockchain-based platform for healthcare information exchange," in *Proc. IEEE Int. Conf. Smart Computing (SMARTCOMP)*, Jun. 2018, pp. 49–56.

[84] Y. Ji, J. Zhang, J. Ma, C. Yang, and X. Yao, "BMPLS: Blockchain-based multi-level privacy-preserving location sharing scheme for telecare medical information systems," *J. Med. Syst.*, vol. 42, p. 147, Aug. 2018.

[85] K. Fan, S. Wang, Y. Ren, H. Li, and Y. Yang, "MedBlock: Efficient and secure medical data sharing via blockchain," *J. Med. Syst.*, vol. 42, no. 8, p. 136, 2018.

[86] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control," *J. Med. Syst.*, vol. 40, p. 218, Oct. 2016.

[87] Y. Sun, R. Zhang, X. Wang, K. Gao, and L. Liu, "A decentralizing attribute-based signature for healthcare blockchain," in *Proc. 27th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Jul. 2018, pp. 1–9.

[88] S.-J. Lee, G.-Y. Cho, F. Ikeno, and T.-R. Lee, "BAQALC: Blockchain applied lossless efficient transmission of DNA sequencing data for next generation medical informatics," *Appl. Sci.*, vol. 8, no. 9, p. 1471, Aug. 2018.

[89] M. A. Rahman, M. S. Hossain, G. Loukas, E. Hassanain, S. S. Rahman, M. F. Alhamid, and M. Guizani, "Blockchain-based mobile edge computing framework for secure therapy applications," *IEEE Access*, vol. 6, pp. 72469–72478, 2018.

[90] J. Liu, X. Li, L. Ye, H. Zhang, X. Du, and M. Guizani, "BPDS: A blockchain based privacy-preserving data sharing for electronic medical records," 2018, *arXiv:1811.03223v1*. [Online]. Available: https://arxiv.org/abs/1811.03223v1

[91] G. Nagasubramanian, R. K. Sakthivel, R. Patan, A. H. Gandomi, M. Sankayya, and B. Balusamy, "Securing e-Health records using keyless signature infrastructure blockchain technology in the cloud," *Neural Comput. Appl.*, vol. 32, no. 3, pp. 639–647, Feb. 2020.

[92] A. Ekblaw, A. Azaria, J. D. Halamka, and A. Lippman, "A case study for blockchain in healthcare: 'MedRec' prototype for electronic health records and medical research data," in *Proc. IEEE Open Big Data Conf.*, 2016, p. 13.

[93] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain," *IEEE Access*, vol. 5, pp. 14757–14767, 2017.

[94] Q. Xia, E. Sifah, A. Smahi, S. Amofa, and X. Zhang, "BBDS: Blockchain-based data sharing for electronic medical records in cloud environments," *Information*, vol. 8, no. 2, p. 44, Apr. 2017.

[95] A. Roehrs, C. A. Da Costa, and R. Da Rosa Righi, "OmniPHR: A distributed architecture model to integrate personal health records," *J. Biomed. Inform.*, vol. 71, pp. 70–81, Jul. 2017.

[96] A. Dubovitskaya, Z. Xu, S. Ryu, and M. Schumacher, "Secure and trustable electronic medical records sharing using blockchain," in *Proc. AMIA Annu. Symp.*, 2018, p. 650.

[97] T. Bocek, B. B. Rodrigues, T. Strasser, and B. Stiller, "Blockchains everywhere—A use-case of blockchains in the pharma supply-chain," in *Proc. IFIP/IEEE Symp. Integr. Netw. Service Manage. (IM)*, May 2017, pp. 772–777.

[98] M. Benchoufi, R. Porcher, and P. Ravaud, "Blockchain protocols in clinical trials: Transparency and traceability of consent," *F1000Research*, vol. 6, p. 66, Jan. 2017.

[99] A. Juneja and M. Marefat, "Leveraging blockchain for retraining deep learning architecture in patient-specific arrhythmia classification," in *Proc. IEEE EMBS Int. Conf. Biomed. Health Inform. (BHI)*, Mar. 2018, pp. 393–397.

[100] X. Zhang and S. Poslad, "Blockchain support for flexible queries with granular access control to electronic medical records (EMR)," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May. 2018, pp. 1–6.
[101] T. Mikula and R. H. Jacobsen, "Identity and access management with blockchain in electronic healthcare records," in *Proc. 21st Eur. Conf. Digit. Syst. Design (DSD)*, Aug. 2018, pp. 699–706.
[102] A. Iyengar, A. Kundu, U. Sharma, and P. Zhang, "A trusted healthcare data analytics cloud platform," in *Proc. IEEE 38th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jul. 2018, pp. 1238–1249.
[103] S. Wang, J. Wang, X. Wang, T. Qiu, Y. Yuan, L. Ouyang, Y. Guo, and F.-Y. Wang, "Blockchain-powered parallel healthcare systems based on the ACP approach," *IEEE Trans. Comput. Soc. Syst.*, vol. 5, no. 4, pp. 942–950, Dec. 2018.
[104] H. Li, L. Zhu, M. Shen, F. Gao, X. Tao, and S. Liu, "Blockchain-based data preservation system for medical data," *J. Med. Syst.*, vol. 42, p. 141, Aug. 2018.
[105] P. Zhang, J. White, D. C. Schmidt, and G. Lenz, "Applying software patterns to address interoperability challenges in blockchain-based healthcare apps," Tech. Rep., 2017.
[106] A. Roehrs, C. A. Da Costa, R. Da Rosa Righi, V. F. Da Silva, J. R. Goldim, and D. C. Schmidt, "Analyzing the performance of a blockchain-based personal health record implementation," *J. Biomed. Inform.*, vol. 92, Apr. 2019, Art. no. 103140.
[107] M. A. Rahman, E. Hassanain, M. M. Rashid, S. J. Barnes, and M. S. Hossain, "Spatial blockchain-based secure mass screening framework for children with dyslexia," *IEEE Access*, vol. 6, pp. 61876–61885, 2018.
[108] X. Feng, J. Ma, T. Feng, Y. Miao, and X. Liu, "Consortium blockchain-based SIFT: Outsourcing encrypted feature extraction in the D2D network," *IEEE Access*, vol. 6, pp. 52248–52260, 2018.
[109] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Gener. Comput. Syst.*, to be published.
[110] D. Steffan Norberhuis, "MultiChain: A cybercurrency for cooperation," Delft Univ. Technol., Delft, The Netherlands, Tech. Rep., 2015.
[111] E-Estonia Webpage. (2019). *Healthcare*. Accessed: Jan. 31, 2019. [Online]. Available: https://e-estonia.com/solutions/healthcare/e-health-record/
[112] A. Novek, "Blockchain in estonian national health information system," Tech. Rep., 2018.
[113] H. Yang and B. Yang, "A blockchain-based approach to the secure sharing of healthcare data," in *Proc. Norwgian Inf. Secur. Conf.*, 2017, pp. 1–12.
[114] V. Patel, "A framework for secure and decentralized sharing of medical imaging data via blockchain consensus," *Health Inform. J*, vol. 25, no. 4, pp. 1398–1411, Dec. 2019.
[115] M. A. Uddin, A. Stranier, I. Gondal, and V. Balasubramanian, "A patient agent to manage blockchains for remote patient monitoring," *Stud. Health Technol. Inform.*, vol. 254, pp. 105–115, Apr. 2018.
[116] H. Kaur, M. A. Alam, R. Jameel, A. K. Mourya, and V. Chang, "A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment," *J. Med. Syst.*, vol. 42, no. 8, p. 156, 2018.
[117] H.-J. Cha, H.-K. Yang, and Y.-J. Song, "A study on access structure management of CP-ABTD based blockchain for medical information monitoring system," *Adv. Sci. Lett.*, vol. 24, no. 3, pp. 2026–2030, Mar. 2018.
[118] H. Han, M. Huang, Y. Zhang, and U. A. Bhatti, "An architecture of secure health information storage system based on blockchain technology," in *Cloud Computing and Security* (Lecture Notes in Computer Science). Cham, Switzerland: Springer, 2018.
[119] E. Gökalp, M. O. Gökalp, S. Çoban, and P. E. Eren, "'Analysing opportunities and challenges of integrated blockchain technologies in healthcare," in *Information Systems: Research, Development, Applications, Education* (Lecture Notes in Business Information Processing). Cham, Switzerland: Springer, 2018.
[120] E. Funk, J. Riddell, F. Ankel, and D. Cabrera, "Blockchain technology: A data framework to improve validity, trust, and accountability of information exchange in health professions education," *Acad. Med.*, vol. 93, no. 12, pp. 1791–1794, Dec. 2018.
[121] Y. Chen, S. Ding, Z. Xu, H. Zheng, and S. Yang, "Blockchain-based medical records secure storage and medical service framework," *J. Med. Syst.*, vol. 43, no. 1, p. 5, 2018.
[122] S.-W. Noh, Y. Park, C. Sur, S.-U. Shin, and K.-H. Rhee, "Blockchain-based user-centric records management system," *Int. J. Control Automat.*, vol. 10, no. 11, pp. 133–144, Nov. 2017.
[123] P. Mangesius, J. Bachmann, T. Healy, S. Saboor, and T. Schabetsberger, "Blockchains in IHE-based networks," *Stud. Health Technol. Inform.*, vol. 251, pp. 27–30, Jan. 2018.
[124] A. Mense and L. Athanasiadis, "Concept for sharing distributed personal health records with blockchains," *Stud. Health Technol. Inform.*, vol. 251, pp. 7–10, Jan. 2018.
[125] S. Chakraborty, S. Aich, and H.-C. Kim, "A secure healthcare system design framework using blockchain technology," in *Proc. 21st Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2019, pp. 260–264.
[126] K. Ito, K. Tago, and Q. Jin, "i-Blockchain: A blockchain-empowered individual-centric framework for privacy-preserved use of personal health data," in *Proc. 9th Int. Conf. Inf. Technol. Med. Educ. (ITME)*, Oct. 2018, pp. 829–833.
[127] J. Vora, A. Nayyar, S. Tanwar, S. Tyagi, N. Kumar, M. S. Obaidat, and J. J. P. C. Rodrigues, "BHEEM: A blockchain-based framework for securing electronic health records," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2018, pp. 1–6.
[128] K. Zheng, Y. Liu, C. Dai, Y. Duan, and X. Huang, "Model checking pBFT consensus mechanism in healthcare blockchain network," in *Proc. 9th Int. Conf. Inf. Technol. Med. Educ. (ITME)*, Oct. 2018, pp. 877–881.
[129] G. Yang and C. Li, "A design of blockchain-based architecture for the security of electronic health record (EHR) systems," in *Proc. IEEE Int. Conf. Cloud Comput. Technol. Sci. (CloudCom)*, Dec. 2018, pp. 261–265.
[130] I. Kotsiuba, A. Velvkzhanin, Y. Yanovich, I. S. Bandurova, Y. Dyachenko, and V. Zhygulin, "Decentralized e-Health architecture for boosting healthcare analytics," in *Proc. 2nd World Conf. Smart Trends Syst., Secur. Sustainability (WorldS)*, Oct. 2018, pp. 113–118.
[131] F. Tang, S. Ma, Y. Xiang, and C. Lin, "An efficient authentication scheme for blockchain-based electronic health records," *IEEE Access*, vol. 7, pp. 41678–41689, 2019.
[132] H. L. Pham, T. H. Tran, and Y. Nakashima, "A secure remote healthcare system for hospital using blockchain smart contract," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2018, pp. 1–6.
[133] J. Park, S. Park, K. Kim, and D. Lee, "CORUS: Blockchain-based trustworthy evaluation system for efficacy of healthcare remedies," in *Proc. IEEE Int. Conf. Cloud Comput. Technol. Sci. (CloudCom)*, Dec. 2018, pp. 181–184.
[134] V. Ramani, T. Kumar, A. Bracken, M. Liyanage, and M. Ylianttila, "Secure and efficient data accessibility in blockchain based healthcare systems," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2018, pp. 206–212.
[135] R. Wutthikarn and Y. G. Hui, "Prototype of blockchain in dental care service application based on hyperledger composer in hyperledger fabric framework," in *Proc. 22nd Int. Comput. Sci. Eng. Conf. (ICSEC)*, Nov. 2018, pp. 1–4.
[136] R. C. Celiz, Y. E. De La Cruz, and D. M. Sanchez, "Cloud model for purchase management in health sector of peru based on IoT and blockchain," in *Proc. IEEE 9th Annu. Inf. Technol., Electron. Mobile Commun. Conf. (IEMCON)*, Nov. 2018, pp. 328–334.
[137] Z. Xiao, Z. Li, Y. Liu, L. Feng, W. Zhang, T. Lertwuthikarn, and R. S. M. Goh, "EMRShare: A cross-organizational medical data sharing and management framework using permissioned blockchain," in *Proc. IEEE 24th Int. Conf. Parallel Distrib. Syst. (ICPADS)*, Dec. 2018, pp. 998–1003.
[138] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for secure EHRs sharing of mobile cloud based e-Health systems," *IEEE Access*, vol. 7, pp. 66792–66806, 2019.
[139] X. Zhang, S. Poslad, and Z. Ma, "Block-based access control for blockchain-based electronic medical records (EMRs) query in eHealth," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2018, pp. 1–7.
[140] E. Zaghloul, T. Li, and J. Ren, "Security and privacy of electronic health records: Decentralized and hierarchical data sharing using smart contracts," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Feb. 2019, pp. 375–379.
[141] R. N. Nortey, L. Yue, P. R. Agdedanu, and M. Adjeisah, "Privacy module for distributed electronic health records (EHRs) using the blockchain," in *Proc. IEEE 4th Int. Conf. Big Data Anal. (ICBDA)*, Mar. 2019, pp. 369–374.
[142] A. R. Rajput, Q. Li, M. Taleby Ahvanooey, and I. Masood, "EACMS: Emergency access control management system for personal health record based on blockchain," *IEEE Access*, vol. 7, pp. 84304–84317, 2019.

[143] N. Nchinda, A. Cameron, K. Retzepi, and A. Lippman, "MedRec: A network for personal information distribution," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Feb. 2019, pp. 637–641.

[144] K. Azbeg, O. Ouchetto, S. J. Andaloussi, L. Fetjah, and A. Sekkaki, "Blockchain and IoT for security and privacy: A platform for diabetes self-management," in *Proc. 4th Int. Conf. Cloud Comput. Technol. Appl. (Cloudtech)*, 2018, pp. 1–5.

[145] R. Kumar and R. Tripathi, "Traceability of counterfeit medicine supply chain through blockchain," in *Proc. 11th Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Jan. 2019, pp. 568–570.

[146] H. Tang, N. Tong, and J. Ouyang, "Medical images sharing system based on blockchain and smart contract of credit scores," in *Proc. 1st IEEE Int. Conf. Hot Inf.-Centric Netw. (HotICN)*, Aug. 2018, pp. 240–241.

[147] M. Alblooshi, K. Salah, and Y. Alhammadi, "Blockchain-based ownership management for medical IoT (MIoT) devices," in *Proc. Int. Conf. Innov. Inf. Technol. (IIT)*, Nov. 2018, pp. 151–156.

[148] T. H.-J. Kim and J. Lampkins, "BRICS: Blockchain-based resilient information control system," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2018, pp. 5363–5365.

[149] M. A. Rahman, M. S. Hossain, M. M. Rashid, S. J. Barnes, M. F. Alhamid, and M. Guizani, "A blockchain-based non-invasive cyber-physical occupational therapy framework: BCI perspective," *IEEE Access*, vol. 7, pp. 34874–34884, 2019.

[150] M. Franceschi, "ComeHere: Exploiting ethereum for secure sharing of health-care data," in *Proc. Eur. Conf. Parallel Process.*, 2019, pp. 585–596.

[151] S. Zhangy, "Genie: A secure, transparent sharing and services platform for genetic and health data," Nov. 2018, *arXiv:1811.01431*. [Online]. Available: https://arxiv.org/abs/1811.01431

[152] T. Quaini, A. Roehrs, C. A. Da Costa, and R. Da Rosa Righi, "UNiReC: An architecture proposal for integrating distributed electronic health records using blockchain," in *Proc. Int. Conf. WWW/Internet Appl. Comput.*, 2018, pp. 167–174.

[153] L. Nørfeldt, J. Bøtker, M. Edinger, N. Genina, and J. Rantanen, "Cryptopharmaceuticals: Increasing the safety of medication by a blockchain of pharmaceutical products," *J. Pharmaceutical Sci.*, vol. 108, no. 9, pp. 2838–2841, Sep. 2019.

[154] T. Motohashi, T. Hirano, K. Okumura, M. Kashiyama, D. Ichikawa, and T. Ueno, "Secure and scalable mhealth data management using blockchain combined with client hashchain: System design and validation," *J. Med. Internet Res.*, vol. 21, no. 5, Apr. 2019, Art. no. e13385.

[155] D. R. Wong, S. Bhattacharya, and A. J. Butte, "Prototype of running clinical trials in an untrustworthy environment using blockchain," *Nature Commun.*, vol. 10, no. 1, p. 917, Dec. 2019.

[156] L. Chen, W.-K. Lee, C.-C. Chang, K.-K.-R. Choo, and N. Zhang, "Blockchain based searchable encryption for electronic health record sharing," *Future Gener. Comput. Syst.*, vol. 95, pp. 420–429, Jun. 2019.

[157] S. Cao, G. Zhang, P. Liu, X. Zhang, and F. Neri, "Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain," *Inf. Sci.*, vol. 485, pp. 427–440, Jun. 2019.

[158] J. Yang, M. Onik, N.-Y. Lee, M. Ahmed, and C.-S. Kim, "Proof-of-familiarity: A privacy-preserved blockchain scheme for collaborative medical decision-making," *Appl. Sci.*, vol. 9, no. 7, p. 1370, Apr. 2019.

[159] T. Rupasinghe, F. Burstein, C. Rudolph, and S. Strange, "Towards a blockchain based fall prediction model for aged care," in *Proc. Australas. Comput. Sci. Week Multiconf. (ACSW)*, 2019, pp. 1–10.

[160] Z. Gao, L. Xu, G. Turner, B. Patel, N. Diallo, L. Chen, and W. Shi, "Blockchain-based identity management with mobile device," in *Proc. 1st Workshop Cryptocurrencies Blockchains Distrib. Syst. (CryBlock)*, 2018, pp. 66–70.

[161] H. Tian, J. He, and Y. Ding, "Medical data management on blockchain with privacy," *J. Med. Syst.*, vol. 43, no. 2, p. 26, Feb. 2019.

[162] A. Mohsin, A. Zaidan, B. Zaidan, O. Albahri, A. Albahri, M. Alsalem, and K. Mohammed, "Based blockchain-PSO-AES techniques in finger vein biometrics: A novel verification secure framework for patient authentication," *Comput. Standards Inter.*, vol. 66, Oct. 2019, Art. no. 103343.

[163] Y. Zhuang, L. Sheets, Z. Shae, J. J. P. Tsai, and C.-R. Shyu, "Applying blockchain technology for health information exchange and persistent monitoring for clinical trials," in *Proc. Annu. Symp. AMIA*, 2018, pp. 1167–1175.

[164] D. R. Ortega, C. M. Oikonomou, H. J. Ding, P. Rees-Lee, Alexandria, and G. J. Jensen, "ETDB-caltech: A blockchain-based distributed public database for electron tomography," *PLoS ONE*, vol. 14, no. 4, Apr. 2019, Art. no. e0215531.

[165] R. Kammergruber and J. Durner, "Laboratory information system and necessary improvements in function and programming," *LaboratoriumsMedizin*, vol. 42, no. 6, pp. 277–287, Dec. 2018.

[166] S. Wu and J. Du, "Electronic medical record security sharing model based on blockchain," in *Proc. 3rd Int. Conf. Cryptogr., Secur. Privacy (ICCSP)*, 2019, pp. 13–17.

[167] I. Mitchell and S. Hara, "BMAR—Blockchain for medication administration records," in *Blockchain and Clinical Trial*. Cham, Switzerland: Springer, 2019.

EMEKA CHUKWU received the B.Eng. degree in electrical electronics engineering from the Federal University of Technology, Owerri, Nigeria, in 2006, and the M.S. degree in information system management from the University of Liverpool, U.K., in 2014. He is currently pursuing the Ph.D. degree in computer information system with the University of Malta, Malta. His Ph.D. research is focused on the intelligent exchange of health information in resource-constrained environments using blockchain. His digital health and research experience span several organizations, including Research Triangle International, Worldbank, UNICEF, UNFPA, University of Washington, Pathfinder International, Health Strategy and Delivery Foundation, HealthEnabled, and KPMG Software, Malta. He project managed the collaborative drafting of Nigeria's National eHealth STRATEGY, from 2015 to 2020. He equally leads the collaborative drafting of Sierra Leone's National Digital Health strategy, from 2018 to 2023. He has worked in Nigeria, Sierra Leone, Cameroon, Kenya, and Malta.

LALIT GARG received the degree in electronics and communication engineering from Barkatullah University, Bhopal, India, in 1999, the master's degree in information technology from the ABV-Indian Institute of Information Technology and Management (IIITM), Gwalior, India, in 2001, and the Ph.D. degree from the University of Ulster, Coleraine, U.K., in 2010. He has worked as a Researcher at Nanyang Technological University, Singapore, and the University of Ulster, U.K. He is currently a Senior Lecturer in computer information systems with the University of Malta, Malta. He is also an Honorary Lecturer with the University of Liverpool, U.K. He has worked on many multimillion euros projects, such as RIGHT (Research Into Global Healthcare Tools) and MATCH (Multidisciplinary Assessment of Technology Centre for Healthcare) and presently handling EU funded projects of hundreds of thousands euros, such as Meditec (Training for Medical Education via Innovative e-Technology). He has supervised two DBA students (University of Liverpool, U.K.) and 180 Master of Science dissertations (University of Liverpool), and two Master of Science dissertation (University of Malta) and four Master of Engineering dissertations (Thapar University, India). Industrial organizations sponsored many of these. Also, supervising/co-supervising two Ph.D. students (University of Malta). He has published over 90 technical articles in refereed journals, conferences, and books. He has published over 100 technical articles in refereed high impact journals, conferences, and books and has more than 570 citations. His research interests are blockchain/DLT, missing data handling, machine learning, data mining, mathematical and stochastic modelling, operational research, and their applications, especially in the healthcare domain. His Ph.D. research was funded and awarded research studentship in healthcare modelling and nominated for the Operational Research Society Doctoral Prize "Most Distinguished Body of Research leading to the Award of a Doctorate in the field of OR." Several of his publications received the best paper awards.