IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 24, 2021, accepted January 2, 2022, date of publication January 7, 2022, date of current version January 18, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3141079

Blockchain-Based Electronic Health Records Management: A Comprehensive Review and Future Research Direction

ABDULLAH AL MAMUN[1], SAMI AZAM[2], (Member, IEEE), AND CLEMENTINE GRITTI[3]
[1]School of Engineering and Computer Science, Victoria University of Wellington, Wellington 6012, New Zealand
[2]College of Engineering, IT and Environment, Charles Darwin University, Casuarina, NT 0810, Australia
[3]Computer Science and Software Engineering, University of Canterbury, Christchurch 8041, New Zealand

Corresponding author: Sami Azam (sami.azam@cdu.edu.au)

ABSTRACT Electronic Health Records (EHRs) are electronically-stored health information in a digital format. EHRs are typically shared among healthcare stakeholders and face power failure, data misuse, lack of privacy, security, and audit trail. On the other hand, blockchain is the revolutionary invention of the twentieth century that offers a distributed and decentralized setting to communicate among nodes in a list of networks without a central authority. It can address the limitations of EHRs management and provide a safer, secured, and decentralized environment for exchanging EHRs data. Three categories of blockchain-based potential solutions have been proposed by researchers to handle EHRs: conceptual, prototype, and implemented. This study focused on a Systematic Literature Review (SLR) to find and analyze articles submitted either conceptual or implemented to manage EHRs using blockchain. The study examined 99 papers that were collected from various publication categories. The deep technical analysis focused on evaluating articles based on privacy, security, scalability, accessibility, cost, consensus algorithms, and the type of blockchain used. The SLR found that blockchain technology promises to provide decentralization, security, and privacy that traditional EHRs often lack. Moreover, results obtained from the detailed studies would provide potential researchers with the type of blockchain for future research. Finally, future research directions, in the end, would direct enthusiasm to combine new blockchain-based systems to manage EHRs properly.

INDEX TERMS EHR, blockchain, P2P, DLT, encryption, interoperability, distributed ledger technology, distributed computing, eHealth.

ABBREVIATION

EHR	Electronic Health Record.
DLT	Distributed Ledger Technology.
P2P	Peer to Peer.
TTP	Trusted Third Party.
DApps	Decentralized Applications.
CA	Certificate Authority.
HL7	Health Level Seven.
FHIR	Fast Health Interoperability Resources.
NeHA	National eHealth Authority.
vMR	virtual Medical Record.
HIPAA	Health Insurance Portability and Accountability Act.
AI	Artificial Intelligence.
ML	Machine Learning.
IoMT	Internet of Medical Things.
M2M	Machine to Machine.
ABE	Attribute-based Encryption.
AES	Advanced Encryption Standard.

The associate editor coordinating the review of this manuscript and approving it for publication was Sathish Kumar.

I. INTRODUCTION

Blockchain has been a buzzword in Information and Communication Technology industry in recent years. The rise of this new technology has greater potentials to solve data privacy, security, and integrity issues. The word blockchain came in the front line after the publication of the Bitcoin white paper by Satoshi Nakamoto in 2008 [1]. The fundamental mechanism behind Bitcoin is to make financial transactions possible without the intervention of a trusted third party. The technology is mainly considered a distributed Peer to Peer

(P2P) network where digital data may publicly or privately be allocated to all users on the web in a secure and verifiable way. In traditional financial transactions, both sender and receiver need to depend on a Trusted Third Party (TTP), e.g., bank. It involves a few security issues and operational difficulties. For instance, a TTP gets access to a user's financial data, which indicates the lack of user privacy. Moreover, the time involved in a TTP transaction is lengthy as there are many steps in between the operation. Furthermore, users need to pay the TTP for their service. Bitcoin solves the above limitations and makes the TTP vanish for a successful transaction between two users.

The practical Bitcoin cryptocurrency came into the market in 2009. However, since the code for Bitcoin was open source, other programmers could edit and improve Bitcoin. The blockchain technology has evolved in different phases.[1]

- *Blockchain 1.0:* The use of Distributed Ledger Technology (DLT) contributed to the first and most noticeable use of the technology: cryptocurrencies. Blockchain 1.0 is the first cryptocurrency that uses a transparent mechanism to monitor bitcoin transactions on a shared ledger.
- *Blockchain 2.0:* Doing transactions through some legally binding policies, also called Smart Contracts, which are generated from a set of small computer programs, is considered blockchain 2.0. The most prominent blockchain in phase 2.0 is Ethereum.
- *Blockchain 3.0:* The next incarnation in this technology is blockchain 3.0, which focuses on Decentralized Applications (DApps) by avoiding centralized infrastructure. Unlike traditional apps, DApps store and communicate through decentralized storage and decentralized server. The aim of blockchain 3.0 was to popularize blockchain among conventional sectors, government, health, and education.
- *Blockchain 4.0:* It provides solutions and methods that can meet several business demands of Industry 4.0, which involves automation, resource planning, and integration of various execution programs. It requires enhanced trust and privacy which can be met by blockchain.

Many surveys have been published on the application of blockchain in various areas. Among these papers, many were systematic reviews on the application of blockchain in healthcare sectors [2]–[6]. Researchers discussed blockchain technology's limitations, possible applications, and future directions in healthcare, government, supply chain, and many other fields. We have proposed a comprehensive SLR on the application of blockchain to manage EHRs.

A. MOTIVATION AND CONTRIBUTION

Owing to the pandemic situation of COVID-19, an enormous amount of digital healthcare data is 7being generated and stored online worldwide through the Internet of Things (IoT) devices by healthcare providers [7]. Tons of healthcare data would be highly beneficial for healthcare providers if analyzed. These data can help us in fighting the virus through medical assistance, early notification, and recommendation [8]. However, it has become a big challenge for researchers to store and analyze health data because most are incomplete and imperfect. Therefore verification and validation of such data are crucial for reporting, and recommendation [9]. Blockchain technology has great potentials to tackle the pandemic crisis. It can help build a decentralized data tracking system that can be retrieved when necessary.

In addition, this big healthcare data, especially EHRs, is vulnerable to privacy and security breaches. Starting from the COVID-19 outbreak, healthcare providers and academic organizations faced several complex cyberattacks [10]. The International Criminal Police Organization (INTERPOL) published a report about cyber-attacks related to COVID-19 in April 2020.[2] Healthcare industries have been severely affected alongside others by these attacks. On 6 May 2020, INTERPOL released an awareness campaign where various cyber-attacks during pandemic were listed.[3] Therefore, it is crucial to take the necessary steps to tackle these threats.

Many researchers proposed to use blockchain technology to overcome the above issues [11]–[14]. However, blockchain is still in the developing phase, which means the solutions offered with this technology are still not handy to root users. There is still a lot of contributions needed from researchers in this field.

By considering the above scenario, this paper aims to identify the potentiality of blockchain to manage EHRs and show the challenges and future scopes. This systematic review only explores research that offers conceptual solutions, experimental results, prototypes, and blockchain implementations for managing EHRs.

The rest of the paper is outlined as follows. In Section 2, the background technologies are discussed. Research methodology, research questions, and discussion are detailed in Section 3. Then, thoughts on directions for future work are presented in Section 4. Section 5 concluded the paper.

II. BACKGROUND

We discuss blockchain technology, in brief, to help readers understand the rest of the paper. A blockchain can be considered a public ledger that can be shared among peers in a network. Cryptocurrencies like Bitcoin first adopted the blockchain. However, gradually it becomes useful for data storage. We discuss the essential characteristics and types in

[1] Blockchain evolution: from 1.0 to 4.0", https://unibrightio.medium.com/blockchain-evolution-from-1-0-to-4-0-3fbdbccfc666, Accessed 20 May 2021.

[2] INTERPOL's COVID-19 Global Threat Assessment https://www.interpol.int/en/News-and-Events/News/2020/Preventing-crime-and-protecting-police-INTERPOL-s-COVID-19-global-threat-assessment, Accessed 25 May 2021.

[3] INTERPOL launches awareness campaign on COVID-19 cyberthreats, https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-launches-awareness-campaign-on-COVID-19-cyberthreats, Accessed 25 May 2021.

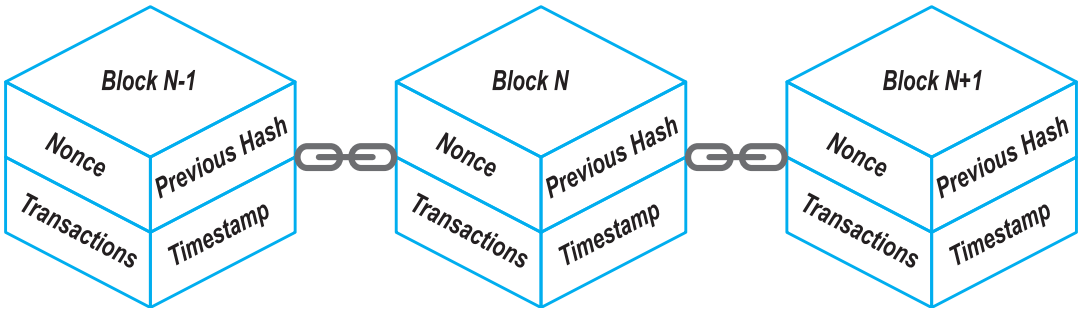

FIGURE 1. A standard structure of a blockchain.

the following subsections to best understand the survey and blockchain concept.

A. BLOCKCHAIN FRAMEWORKS

Blockchain technology is an association of two technologies, cryptography, and P2P. A blockchain is a series of timestamped blocks connected through a cryptographic hash. Typically each block contains transaction records verified by the peers, called miners. The chain is increased continuously, and each new block is added to the end. However, each new block contains a reference, basically a cryptographic hash (e.g., SHA-256), of the previous block's header. The creation of each block ensures anonymity, transparency, and immutability [15]. The whole operation of blockchain is held in a P2P network. The basic structure of a blockchain is shown in Fig. 1. Each block except the genesis block (first block of the network) has the hash value of data from the previous hash. Besides, each block has a difficulty value called Nonce, a Timestamp, and other attributes (e.g., the list of transactions).

1) P2P NETWORK

A P2P network works more or less like a BitTorrent network,[4] where a peer, commonly known as a node, not only deploys the system for its benefit but also contributes to the whole system with its resources like storage, bandwidth, and processing power. Depending on the blockchain network type (discussed in a later section), the network node is restricted to fewer people or open for all. The bright side for nodes in the blockchain is that their identity is kept safe, as only the user's public key is shown to the other peers of the network. Nodes also work as miners, who validate a transaction to be added to the chain.

2) ROLE OF MINERS

Blockchain follows the structure of a linked list, where a new block is added and connected to the previous block in the list. However, to be added to the blockchain, a block must first be verified by a miner. Mining here doesn't mean checking the transaction's eligibility; it means doing some extra work after that, also called Proof-of-Work (PoW). All miners in the network compete in computing the targeted nonce value. The nonce, short for ''number used once,'' is a random or pseudo-random number used for authentication protocols and makes sure that old communications never happen again [16]. To produce a hash value below a target difficulty level, the Nonce refers to a number (32-bit unsigned integer) generated by PoW operation on mining nodes. The difficulty level is set to be solved within the given time limit; Bitcoin takes around ten minutes to add a new block. As soon as a miner reaches a value less than the given target, he becomes eligible to get some rewards. However, as long as the nonce value is higher than the target value, the block won't be eligible to be added to the blockchain.

B. TYPES OF BLOCKCHAIN

This section contains a description of different types of blockchain. Depending on the network size, application, and kind of consensus algorithms (seen below), blockchain has various kinds. Commonly, three types of blockchain exist in the market, mentioned below.

- Public
- Private
- Consortium (Hybrid)

1) PUBLIC BLOCKCHAIN

Anyone can join the network in a public blockchain and access the block data. It uses public DLT, where anyone with internet connectivity can join to become an authorized miner to mine a block. However, the users' identity address is generated using a pseudo-anonymous hash value even in the public blockchain network. Anyone can only know that someone with that address exists but does not know exactly who. After joining the network, a user can check transactions and mine a block to be added to the network. This kind of public blockchain normally offers financial incentives to the successful miner for helping to solve PoW. Example of this type of blockchain includes Bitcoin [1], Ethereum (public) [17], and Litecoin [18]. Public blockchains impose some interaction costs (i.e., transaction fees), so whenever someone wants to upload or download a document such as EHRs, they will be charged for it. Besides, public blockchain

[4]Bittorent Network, https://www.bittorrent.com/btt/btt-docs/BitTorrent_(BTT)_White_Paper_v0.8.7_Feb_2019.pdf, Accessed 11 May 2021.

is designed in a way that any anonymous user can join the chain anytime, and it is slow in adding blocks, which is not ideal for EHRs management. Hence, this type of blockchain is not recommended for managing EHRs.

2) PRIVATE BLOCKCHAIN

Private blockchain has several similarities with a public one in terms of operation and algorithms. However, it differs in purpose. In simple terms, a private blockchain is a restrictive or permissioned blockchain. It is operated based on some access control rules in a closed network, which is distributed yet centralized. This type of blockchain is usually used within an organization or company where one or more nodes control which node can perform transactions, act as miners or perform smart contracts. The security, accessibility, permissions, and authorization are controlled by a TTP organization. This type of blockchain is used normally for supply chain management, electronic voting, digital asset management, and data preservation. Hyperledger Fabric [19] and Ripple [20] are excellent examples of private blockchains. Nobody can join a private blockchain network without an invitation from authorized personnel. In addition, it consumes less power than the public blockchain, and it is faster in adding blocks to the chain. As a result, a private blockchain is suggested to manage EHRs.

3) CONSORTIUM BLOCKCHAIN

The consortium blockchain can be best understood by comparing it with public and private blockchains, as the term itself sometimes sounds confusing. We can define this type as partly centralized and partly decentralized. Firstly, it is not used by a single organization; rather, it is expanded in several organizations. On the other hand, it is only accessible to groups of previously registered nodes, so one cannot directly access the network without first being a registered member. A single organization in a consortium blockchain cannot make any illegal activity, as, without the consent of other organizations, one cannot perform any operation. The whole concept of consortium blockchain came in to help enterprises collaborate to improve their business. The example of consortium blockchain are Hyperledger Fabric [19], Quorum [21], and Corda [22].

C. CONSENSUS ALGORITHMS FOR BLOCKCHAIN

The consensus algorithm is a decision-making process in a group of nodes in the blockchain which needs to be followed by the rest of the nodes. To understand this in detail, let us consider the following example. Suppose there are 20 people in a business meeting to decide on an upcoming project. Everyone can suggest their own opinion regarding the project, but the thought that benefits most people will get a higher preference. Similarly, if we consider a cryptocurrency, e.g., Bitcoin, the miners need to solve mathematical puzzles to meet PoW consensus and get some rewards in the form of Bitcoin. In most blockchains, consensus algorithms are the vote of majority participants. The primary purpose of a consensus algorithm is to allow nodes to communicate among them and provide valid transactions to be added to the blockchain. Some of the standard consensus algorithms are discussed below:

1) PoW (PROOF-OF-WORK)

PoW [1] is the first, currently most popular, and highly robust consensus algorithm. A miner must find a hash value that is less than the difficulty target and then share it with other miners before the block is added to the blockchain. However, PoW has certain limitations. The algorithm is resource hungry, and as the blockchain grows more prominent with time, the algorithm needs lots of computational power [1].

2) PoS (PROOF-OF-STAKE)

PoS [23] is the substitute for PoW as it deals with the main drawback of PoW, i.e., consumption of lots of CPU power. Unlike PoW, where any node can mine a transaction, in PoS, a miner is chosen based on its wealth, also called stake. Generally, a pseudorandom selection process is used to select the node allocation. In PoS, there is no incentive for mining; alternatively, the chosen miner collects the transaction fee [24]. Blockchains that use PoS are NEO[5] and Polkadot [25].

3) DPoS (DELEGATED PROOF-OF-STAKE)

In DPoS [26], tokens or stakeholders don't work to validate blocks. Instead, they elect delegates to validate blocks. The selection process works so that the stakeholders are always in control, as they lose a lot if the network doesn't function properly. Stakeholders can vote to remove a delegate and add another if they find any anomaly in block creation. Delegates can work together to validate a block and get the transaction reward accordingly [27]. Bitshre [28], Steem [26], Tezos[6] are some examples of blockchain projects that use DPoS.

4) PoA (PROOF-OF-AUTHORITY)

PoA[7] is an amalgamation of PoW and PoS. It values the reputation of the identity of a stakeholder. Hence, a stakeholder is not directly supported with a stake but their reputation. Therefore, the building blocks in the blockchain are secured by authentic and trustworthy participants. Decred [29] is an example using this algorithm.

5) PoV (PROOF OF VOTE)

The PoV [30] algorithm is a bit different from all other consensus algorithms. In a group of enterprises, they need to mutually share business data, to create transaction blocks in the blockchain. As a result, they elect a third-party team to work for them. The team will forward the block to each company under the network for verification through voting,

[5]Neo White Paper, https://docs.neo.org/docs/en-us/basic/whitepaper.html, Accessed 15 May 2021.

[6]Tezos Whitepaper, https://tezos.com/whitepaper.pdf, Accessed 26 May 2021.

[7]POA Network Whitepaper, https://github.com/poanetwork/wiki/wiki/POA-Network-Whitepaper, Accessed 12 May 2021.

which ensures the decentralized property of blockchain. The work of the hired team is supersized from time to time by the owners of enterprises. This algorithm was developed to be used in consortium blockchains [30].

6) PBFT (PRACTICAL BYZANTINE FAULT TOLERANCE)

PBFT [31] is the first proposed consensus algorithm to handle Byzantine fault tolerance, where a distributed network can achieve even if some node is malicious. It can be highly effective where non-deterministic chain-codes are executed [30]. Stellar [32], Hyperledger Fabric [19], and Ripple [20] are examples of PBFT.

7) PoI (PROOF-OF-IMPORTANCE)

In PoI[8] the miner is decided not based on the amount of work nor the amount of stake he carries, but he is chosen depending on the productivity. The reward is not given to users with a high balance but brings the number of transactions into the account. Each user in the PoI network is given a trust score. The higher the value, the higher the chance of getting a reward. NEM[9] blockchain platform use this algorithm.

D. SMART CONTRACTS

Smart contracts make our daily life contracts in a digital form. These are small computer programs written for different blockchains to be implemented automatically for healthcare, government organizations, and so on, based on some previous agreements [33]. The need for smart contracts is to eradicate trust problems, third parties, and fraud in financial transactions. One may find the difference between a smart contract and a standard business agreement. Theoretically, both are the same, but smart contracts support automatic execution of the predefined agreement, and this can be done for multiple business organizations at a time.

E. DIGITAL SIGNATURES

A digital signature brings authenticity and integrity to digital assets like messages, software, documents, etc. Asymmetric cryptography enables to authenticate transactions in an untrustworthy environment [34]. Blockchain uses asymmetric cryptography to sign digital transactions—the user's private key signs the transaction before being shared with the distributed network. Once the transaction is signed, it is then sent to all other peers in the network for verification. Peers then verify it with the available public key of the transaction initiator. If the transaction signature is valid from maximum nodes, it is added in a new block in the blockchain; otherwise, the transaction is discarded.

F. ELECTRONIC HEALTH RECORDS

The EHR collects patients' medical diagnostic reports in electronic form (e.g., JPEG, PDF). Electronic Medical Record (EMR) can serve as a collection of data sources for EHR in different medical organizations. It also contains personal health information collected from wearable devices (e.g., smartwatches, smart bands), which patients manage. EHRs are real-time, patient-centered records available to authorized users (e.g., doctors, health providers) as required. EHRs may comprise a wide range of data, including the diagnosis reports, immunity level of patients, medication history, age, weight, and demographic history.

EHR should comply with three essential attributes: confidentiality, integrity, and availability. EHR must only be accessible by authorized users (e.g., medical practitioners and nurses) with proper access control mechanisms. Implementation of EHR systems can reduce the loss of medical history, data malfunction, etc. However, ensuring the privacy and security of these critical data is challenging. In addition, cyber-attacks on smart healthcare devices [35] are increasingly a concern because they could pose severe life-threatening implications for patient safety. For instance, malicious users will target patients' wearable devices that are connected to EHR servers. Afterward, hackers can install some malicious program in those devices and acquire control over them.[10]

1) BENEFIT OF EHR

About the benefit of EHR, the New England Journal of Medicine published a study report in 2011, where the study found that the use of EHR provides better care [36]. Moreover, EHR ensures the availability of many medical records at a single point, which can be used to design machine learning algorithms and predict better medical advice for patients. Since with EHR, anyone with access rights can have access to a patient's entire chart, reducing the probability of guessing medical history and consulting with multiple specialists. Emergency care can be provided to any patients more efficiently by consulting EHRs from anywhere.[11]

III. MANAGING EHR USING BLOCKCHAIN

EHR contains sensitive personal data (e.g., medical history of patients). Therefore, the security and privacy of such data are crucial. In developing countries, medical institutions are bound to obey the rules set by the government. As a result, storing and distributing EHR data are challenging. On the other hand, EHR management faces lots of technical difficulties. For instance, central medical servers are low in capacity, susceptible to single-point failure, and vulnerable to insider attacks. Even patients do not know exactly where their sensitive data is being stored and how it is shared. However, this has become important as people nowadays are mobile, so inseparability among various healthcare providers can provide better health suggestions.

[8]What is POI?: https://docs.nem.io/ja/gen-info/what-is-poi, Accessed 19 May 2021.

[9]NEM, https://docs.nem.io/en, Accessed 11 May 2021.

[10]Cyber safety and resilience, https://www.raeng.org.uk/publications/reports/cyber-safety-and-resilience, Accessed 20 May 2021.

[11]Improve Care Coordination, https://www.healthit.gov/topic/health-it-basics/improve-care-coordination, Accessed 22 May 2021.

By considering the above scenario, Health Insurance Portability and Accountability Act (HIPAA)[12] was built in the USA. HIPAA created five sections of the act to guarantee electronic protected health information [37]. Along with ensuring confidentiality, integrity, and availability of health information, it makes sure that healthcare providers and other authorized individuals can have access to it. Besides, a framework (and relevant standards) for the sharing, synchronization, distribution, and retrieval of electronic health information is provided by Health Level Seven (HL7)[13] and its members. This is committed to offering a comprehensive structure and associated criteria for exchanging, synchronizing, transmitting, and retrieving electronic health information to facilitate clinical practice, health care administration, implementation, and assessment. The vision of HL7 is to make an environment where everybody can access and use the best health data safely when they need to.

On the other hand, the standard ISO 18308:2011[14] specifies the collection of specifications to be fulfilled by the processing, maintenance, and communication of EHR information architecture for systems and services. This standard is made to ensure the trustworthiness of EHR for healthcare delivery, clinically valid and reliable, ethically sound, and to support data analysis for various purposes. The EHR is defined according to this standard as: ''one or more repositories, physically or virtually integrated, of information in computer processable form, relevant to the wellness, health, and healthcare of an individual, capable of being stored and communicated securely and of being accessible by multiple authorized users, represented according to a standardized or commonly agreed logical information model. Similarly, the standard ISO 27789:2013[15] provides a joint audit trails framework for EHR. In summary, specific requirements should be met for the next-generation EHR systems. Those requirements include accuracy, integrity, privacy, security, user accessibility, availability, auditability, and accountability.

The above properties can be achieved through blockchain, thanks to its properties like immutability, transparency, security, auditability, and incentive mechanisms.

A. RESEARCH METHODOLOGY

We adopt SLR guidelines [38], and the Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines [39] in conducting this review. An SLR refers to a methodology for discovering, analyzing, and assessing all recent literature related to a research issue or subject field.

[12]Health Information Privacy, https://www.hhs.gov/hipaa/index.html, Accessed 23 May 2021.

[13]HL7 Standards - Section 1b: EHR - Electronic Health Records, https://www.hl7.org/implement/standards/product_section.cfm?section=11, Accessed 20 May 2021.

[14]Health informatics — Requirements for an electronic health record architecture, https://www.iso.org/obp/ui/#iso:std:iso:18308:ed-1:v1:en, Accessed 15 May 2021.

[15]Audit trails for Electronic Health Records, https://www.nrces.in/standards/iso/iso-27789, Accessed 11 May 2021.

All review papers were selected by searching for relevant and reliable academic repositories like PubMed, Google Scholar, IEEE, ACM, Science Open, Science Direct, Springer, Hindawi, Wiley Online Library, and MDPI in December 2020.

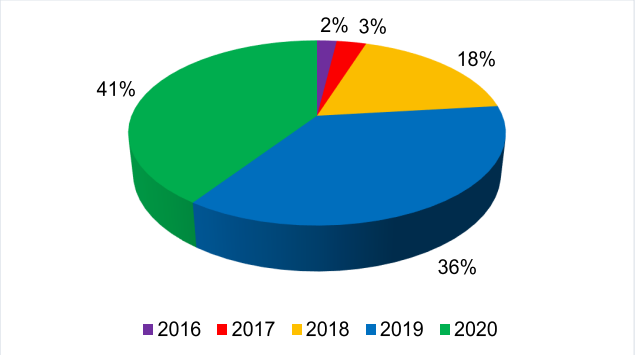

FIGURE 2. Publications per year between 2016 and 2020.

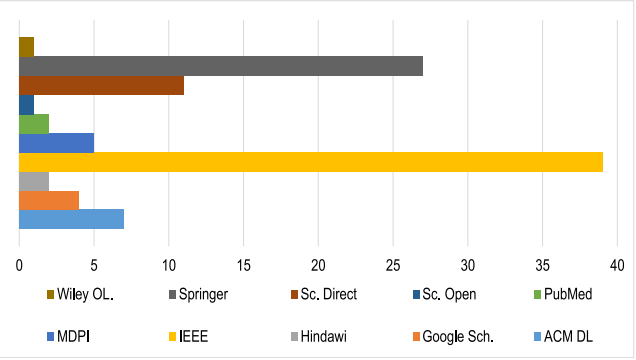

FIGURE 3. Number of articles according to publishers.

B. RESEARCH QUESTIONS

The objective of the study was to address the following research questions:

1) **RQ1**: To what extent is the blockchain developed for managing EHRs and how has it changed over time?
2) **RQ2**: What standardization is followed for storing EHRs in the blockchain?
3) **RQ3**: How big data related to EHRs were handled?
4) **RQ4**: What platforms/mechanisms of blockchain were used to handle EHRs Management?

C. SCREENING THE ARTICLES

Selected papers are presented in this segment after screening from various categories. The selection query for articles was purposely long enough to consider as many research questions as possible as described in Section III-B. Using the searching mechanism, we were able to retrieve 1282 research articles from the scientific repositories, as shown in Fig. 4. After the first screening step, we removed duplicates and retrieved 139 papers. Using the second and third screening

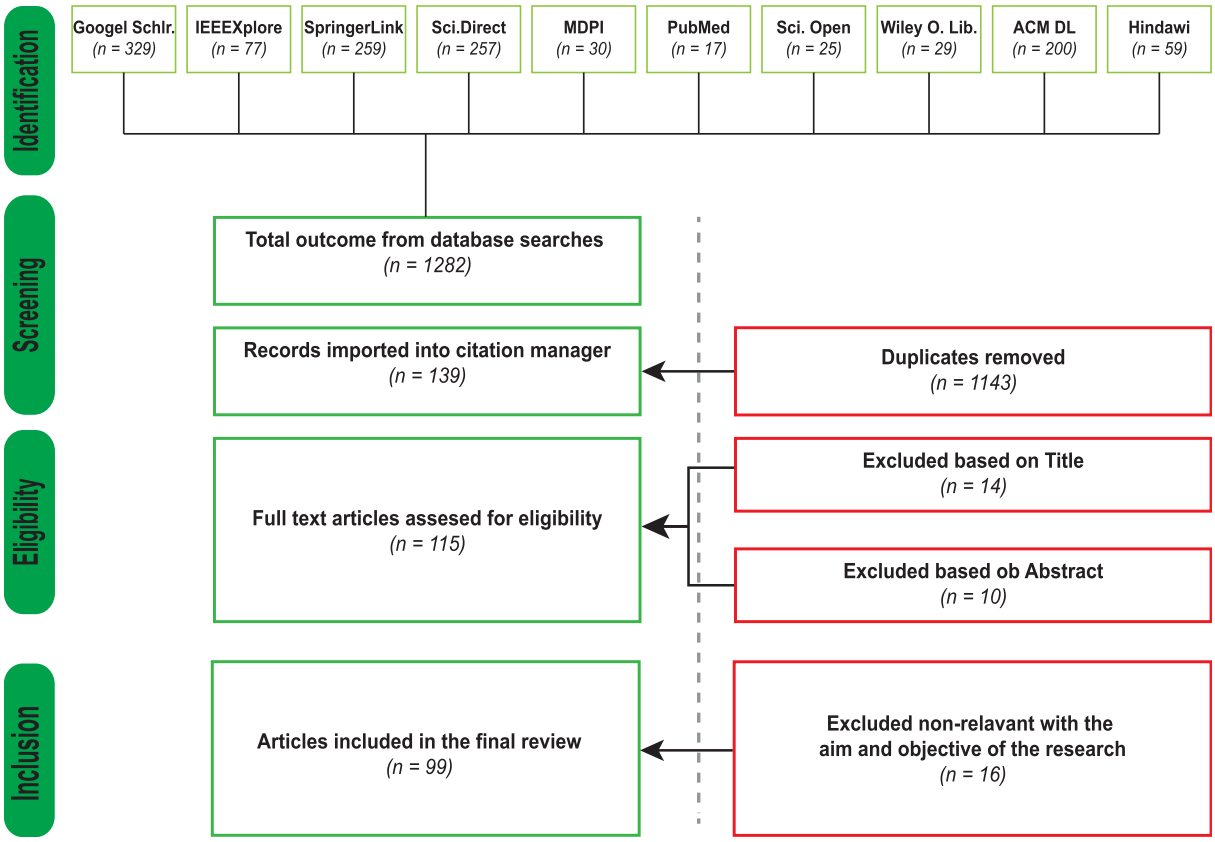

FIGURE 4. PRISMA chart for the SLR process.

methods (here, exclusion was based on title and abstract), a total of 24 articles were deleted accordingly, leaving 115 papers for further processing. We uploaded the remaining papers to the Mendeley software[16] for thorough reading. Finally, all articles that did not serve the purpose of the SLR were deducted, and a total of 99 articles was there.

Table 1 includes a complete list of selected papers and some essential details on those articles. Necessary details include authors' initials, year of publication, number of citations per paper up to 05 June 2021, type of publication, a blockchain platform, blockchain type, class (1 = Conceptual, 2 = Prototype or Experimental, 3 = Implementation), and the consensus algorithm. The number of articles from several publishers has been shown in Fig. 3. It is mentionable from the Fig. 3 that IEEE and Springer published a maximum number of articles related to EHRs, whereas MDPI and Wiley Online Library equally published a fewer number of papers. Several publications per year have been shown in Fig. 2. The publication has increased gradually over five years. In 2020, the highest number of papers had been published, 41% to be precise.

Further analysis for the selected papers are shown in Table 2. The table compares papers chosen based on five essential properties. These properties are really crucial for EHRs. The properties are discussed below:

1) PRIVACY

Privacy refers to the right that someone can decide when, how and at which levels accessing the personal EHRs, transforming them and sharing them with others are given. [40]. Privacy can be breached in various situations; for example, a healthcare provider may either intentionally or by mistake abuse EHRs [41]. In a survey paper, Win [42] mentioned that around two-thirds of patients pay attention to their personal EHRs. In another survey, Ancker *et al.* [43] mentioned that close to fifty percent of the participants believe that exchanging health data would worsen their data privacy. Thus, privacy is a great factor to consider when comparing blockchain-based solutions that claim to maintain the privacy of EHRs.

2) SECURITY

Security, on the other hand, defines the level at which someone's EHRs are restricted and allowed only to authorized personnel. Perera *et al.* [44], in their study, mentioned that around fifty percent of the patients are worried about the security of their EHRs as these need to travel through the Internet. Wikina [45] mentioned that physicians are more interested in the security of EHRs than patients, and a majority portion

[16]Mendeley Desktop for Windows, https://www.mendeley.com/download-desktop-new/, Accessed 11 May 2021.

of doctors prefer paper-based records than EHRs as they think they are more secure. Indeed, to support doctors' preference, digital forms of health records are exposed to security breaches [46]. That is why Liu *et al.* [47] suggested that methods of providing security that is related to EHRs need to be well understood first. These factors indicate that we should consider security related to EHRs seriously.

3) STORAGE SCALABILITY

As blockchain technology has grown over the last few years, it has raised scalability issues. When Nakamoto [1] started the Bitcoin blockchain, the data storage for a single block was limited to 1MB only. However, since then, the blockchain has grown in popularity & participants and its blocks. A participant has to download all the chains to learn and validate a transaction that requires huge memory and time. However, general blockchain applications have two solutions to mitigate storage scalability: on-chain and off-chain. The on-chain storage means all data a user uploads will be directly stored in the blockchain. On the other hand, off-chain storage means the real data is stored somewhere other than the blockchain such that it is linked to the main chain. However, off-chain storage has weaker security. While storing EHRs on-chain requires a large data space. Therefore, hosting data outside the blockchain and maintaining high-level security is a concern to look at.

4) ACCESSIBILITY

Accessibility requires to control and manage access to critical or sensitive data [48]. It provides the technique for restrictive access to data. Commonly known techniques for healthcare systems are role-based, attribute-based, and identity-based access control [49]. Since EHRs deal with patients' health data containing very sensitive information, access control is a significant factor to consider.

5) COST ANALYSIS

Apart from the legal and ethical aspects, the cost for EHRs is one of the most significant factors for which the widespread adoption is still failing. A major issue is that who pays for the implementation of EHRs is still unresolved [50]. The cost for five-person practice to implement an EHR system is close to $162,000 in the first year and an annual maintenance cost of around $85,000. These can touch millions or even more for an individual hospital.[17]

D. DISCUSSION

From the selected articles, this section provides a discussion about how the papers answer the research questions from Section III-B.

RQ1: *To what extent is the blockchain developed for managing EHRs, and how has it changed over time?*

[17]Electronic health records were supposed to be everywhere.., https://www.washingtonpost.com/news/wonk/wp/2014/08/07/electronic-health-records-were-supposed-to-be-everywhere-this-year-theyre-not-but-its-okay/, Accessed 7 April 2021.

The study reviewed the current extent of blockchain technology and the transition for managing EHRs, over five years (2016-2020). Among all papers reviewed, more than half are prototype or experimental, around one-third are conceptual, and the rest are implemented as shown in Fig. 5. The highest proportion of articles in this review is published after 2018, which indicates that blockchain technology is still emerging. As blockchain technology is going through the development phases and the usability in real-time is still under development, most articles focused on designing a prototype for managing EHRs. Researchers highly focused on managing EHRs using the blockchain, mainly after 2018, and the research trend skyrocketed during the pandemic situation of COVID-19 in 2020.

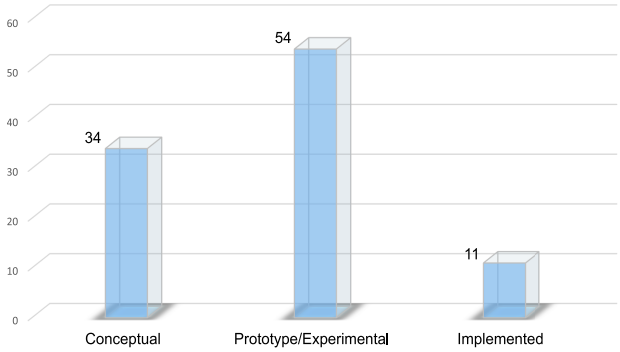

FIGURE 5. Classifications of published papers.

For managing EHRs, the authors tried to propose solutions from various perspectives. While most authors focused on the access control mechanism using Certificate Authority (CA) in storing and managing EHRs using blockchain, others focused only on EHRs data encryption mechanisms before uploading EHRs into the blockchain. Many followed symmetric encryption schemes for data encryption, while others used asymmetric encryption schemes. A few authors provided solutions for the scalability of the blockchain when managing EHRs. Some people came with smart contracts, but some used chain-code for EHR preserving mechanisms.

Regarding the storage of EHRs, two types of solutions were found, such as on-chain storage and off-chain storage. While an on-chain storage scheme focused on storing data over the blockchain, an off-chain storage scheme stored data either over the cloud or in the local database and linked the data's address to the blockchain. Current development for storing data in blockchain involves a high cost, and the solutions need more research as it is not yet up to the mark.

From 2016, which was the starting year for providing the blockchain-based solutions for managing EHRs, until 2020, there has been an enormous development. In 2016, two articles [51], [52] started the idea of using blockchain as a platform to manage health data. Later in 2017, two articles [53], [54] mentioned about the applicability of private blockchain for EHRs. Afterward, researchers tried to prove the applicability of blockchain for handling EHRs.

TABLE 1. List of selected articles.

Ref.	Authors	Year	Citation	Publication Type	Platform	Type	Class[18]	CA[19]
1 [65]	L. Ismail and H. Materwala	2020	1	Conference	Hyperledger Fabric	N/D	1	N/D
2 [66]	L. Ismail et al.	2020	1	Conference	Hyperledger Fabric	N/D	2	PBFT
3 [67]	Z. Li and L. Zhang	2020	0	Conference	Consortium	N/D	1	PoS
4 [68]	X. YANG et al.	2020	1	Journal	Ethereum	Public	2	PoW
5 [69]	M. Al. Baqari and E. Barka	2020	1	Conference	N/D	N/D	1	N/D
6 [70]	O. Ajayi et al.	2020	0	Conference	Hyperledger Fabric	Private	2	N/D
7 [71]	V. Jaiman and V. Urovi	2020	6	Journal	Ethereum	Public	2	N/D
8 [14]	A. Fernandes et al.	2020	1	Conference	Hyperledger Fabric	Private	2	N/D
9 [72]	RK Marangappanavar and M. Kiran	2020	3	Conference	Ethereum	Public	1	N/D
10 [73]	AI. El Sayed et al.	2020	1	Conference	Hyperledger Fabric	Private	2	N/D
11 [74]	H. Guo et al.	2020	7	Conference	Hyperledger Fabric	Private	2	N/D
12 [59]	R. Jabbar et al.	2020	4	Conference	Ethereum	Private	3	N/D
13 [75]	S. Cao et al.	2020	0	Conference	Polkadot	Private	2	BFT
14 [60]	Y. Zhuang et al.	2020	12	Journal	Ethereum	Private	3	N/D
15 [76]	M. Qazi et al.	2020	1	Conference	N/D	N/D	1	PoA
16 [62]	P. Meier et al.	2020	2	Journal	Hyperledger Fabric	Private	3	N/D
17 [77]	G. Nagasubramanian et al.	2020	63	Journal	KSI	Private	2	N/D
18 [78]	S. Lokhande et al.	2020	3	Conference	Hyperledger Fabric	Private	1	N/D
19 [79]	X. Wu et al.	2020	9	Conference	Ethereum	Private	2	N/D
20 [63]	R. Kumar and R. Tripathi	2020	3	Chapter	Hyperledger Fabric	Private	3	N/D
21 [80]	R. Haque et al.	2020	2	Conference	N/D	N/D	1	N/D
22 [81]	H. Jin et al.	2020	0	Conference	Ethereum	Public	2	PoW
23 [82]	HH Kung et al.	2020	1	Conference	Ethereum	Private	2	N/D
24 [83]	B. Arunkumar and G. Kousalya	2020	2	Conference	Ethereum	Public	2	PoW and PoS
25 [84]	SM Pournaghi et al.	2020	24	Journal	N/D	Private	2	PBFT
26 [85]	A. A. Mamun et al.	2020	2	Book	Consortium	Private	2	N/D
27 [86]	A. Keerthika and R. Chendhavarayan	2020	0	Journal	Consortium	Private	2	N/D
28 [87]	M. Madine et al.	2020	6	Journal	Ethereum	Public	2	PoW
29 [88]	L. Huang and H. H. Lee	2020	0	Special Issue	N/D	N/D	2	N/D
30 [61]	O. Gutiérrez et al.	2020	1	Journal	Ethereum	Private	3	PoA
31 [64]	TT Thwin and S. Vasupongayya	2020	1	Journal	Hyperledger Fabric	Private	3	dummy
32 [89]	F. Junsong et al.	2020	8	Journal	Bitcoin	Public	1	PoW

[18]Class (1=Conceptual, 2=Prototype or Experimental, 3=Implementation)
[19]Consensus Algorithm

In the rest of the paper, most papers proposed using either Ethereum or Hyperledger Fabric, those are private blockchains. The practical implementation with blockchain started with Ethereum blockchain in 2018 [55], [56]. Between 2019 and 2020 more 9 papers proposed implemented solutions [57]–[64]. The authors proved that the blockchain is a better solution for managing EHR data by this time. While there were only two papers in 2016, the number was 40 in 2020. Though most publications focused on prototype designing, a few articles tried to implement the ideas. As time passed, the interest has grown in blockchain technology for EHR management.

RQ2: *What standardization is followed for storing EHRs in the blockchain?*

The standards related to the data format and interoperability principle remain an issue for sharing and storing EHRs. While most authors did not even consider any of the standards provided by HIPAA, Fast Health Interoperability Resources (FHIR), and HL7, some authors either discussed or applied the standards in their proposed solutions. Most authors consider FHIR and HL7 when they defined standard for EHRs data format [51], [55], [103], [107], [145]. A significant number of authors followed HIPAA standard for their proposed framework [81]–[83], [120], [122], [134]. However, only a few authors followed the standard of HL7 [12], [77], [97], [144], whereas a small number considered the standard of FHIR [95], [96], [128]. A standard from NeHA (National eHealth Authority) that works as a promotional, regulatory and standard-setting organization in the health sector in India applied in [116]. vMR (Virtual Medical Record) found in [59] is a simplified, standardized EHR data model designed to support interfacing to the clinical decision support system. Among the rest of the papers, authors in [61] described the standard of ISO 18308: 2011, HL7 and HIPAA, but did not implement those principles. Finally, researchers in [62] followed the openEHR standard. By contrast, the remaining papers did not follow or describe the EHRs standards.

Having mentioned the above references, the expected standard for EHRs exchanging, uploading, storing, authenticity checking, and formatting remain a crucial issue for

TABLE 1. ***(Continued.)*** **List of selected articles.**

Ref.	Authors	Year	Citation	Publication Type	Platform	Type	Class	CA
33 [90]	S. Tanwar et al.	2020	157	Journal	Hyperledger Fabric	Private	2	CFT and BFT
34 [91]	S. Shamshad et al.	2020	9	Journal	Private + Consortium	Private	2	N/D
35 [92]	Y. Sharmaa and Prof. B. Balamurugan	2020	5	Journal	Hyperledger Fabric	Private	2	N/D
36 [93]	H. Huang et al.	2020	1	Journal	N/D	N/D	1	N/D
37 [94]	U. Muhammad and Q. Usman	2020	8	Conference	Hyperledger Fabric	Private	2	PBFT
38 [95]	L. Hsiu-An et.al	2020	7	Journal	Ethereum	Private	2	PoA
39 [96]	A Dubovitskaya et al.	2020	8	Journal	Hyperledger Fabric	Private	2	PBFT
40 [97]	D Tith et al.	2020	9	Journal	Hyperledger Fabric	Private	2	PBFT
41 [11]	MS. Rahman et al.	2019	5	Conference	Ethereum	N/D	2	PoW
42 [12]	H. Wu et al.	2019	2	Conference	Ethereum	N/D	2	DPoS
43 [13]	S. Wu and J. Du	2019	16	Conference	Bitcoin	N/D	1	DPoS
44 [98]	YY. Zhao et al.	2019	0	Conference	N/D	N/D	1	N/D
45 [99]	A. SHAHNAZ et al.	2019	72	Journal	Ethereum	N/D	3	PoW
46 [100]	D. C. NGUYEN et al.	2019	112	Journal	Ethereum	N/D	2	PoW
47 [101]	R. Adlam and B. Haskins	2019	4	Conference	Hyperledger Fabric	N/D	1	Kafka
48 [102]	R. N. Nortey	2019	11	Conference	Hyperledger Fabric	N/D	1	N/D
49 [103]	G. Carter et al.	2019	9	Conference	Ethereum	N/D	1	PoW
50 [104]	J. Huang et al.	2019	11	Conference	Hyperledger Fabric	N/D	1	PBFT
51 [105]	H. Guo et al.	2019	34	Conference	Hyperledger Composer Fabric	Private	2	N/D
52 [106]	MT. de Oliveira et al.	2019	14	Conference	Multichain	Private	2	PoA
53 [107]	A. Donawa et al.	2019	6	Conference	Consortium	Private	1	PoA
54 [108]	X. LIU et al.	2019	41	Journal	Private Blockchain	Private	2	Improved DPoS
55 [109]	A. Buzachis et al.	2019	2	Conference	Ethereum	Private	2	PoA
56 [110]	S. Jiang et al.	2019	6	Conference	Ethereum	Private	2	N/D
57 [111]	B. Toshniwal et al.	2019	4	Conference	Ethereum	Private	2	N/D
58 [112]	F. TANG et al.	2019	36	Journal	Consortium	Private	2	N/D
59 [113]	A. R. RAJPUT et al.	2019	40	Journal	Hyperledger Fabric	Private	2	N/D
60 [114]	X. YANG et al.	2019	5	Conference	N/D	N/D	1	N/D
61 [115]	Y. WANG et al.	2019	34	Journal	Ethereum	Private	2	PoA
62 [116]	G. S. Reen et al.	2019	4	Conference	Ethereum	Private	2	PoA
63 [117]	J. Xu et al.	2019	61	Journal	Userchain + Docchain	Pub. + Pri.	2	PoW & PBFT
64 [118]	H. Tian et al.	2019	42	Journal	Hyperledger Fabric	Private	2	N/D
65 [119]	M. Nagori et al.	2019	1	Conference	Multichain	Private	1	N/D
66 [58]	T. Zhou et al.	2019	10	Journal	Permissioned	Public	3	DPoS-Quorum
67 [120]	TPA Rahoof and VR Deepthi	2019	1	Conference	Private + Consortium	Private	2	N/D

blockchain-enabled EHRs solutions until now. It may be because of the evolving nature of blockchain and the lack of standardized developing platforms. While blockchain is a promising technology for EHR management, it still needs to go on a long run to reach a stable position to maintain a standardized framework.

RQ3: *How big data related to EHRs were handled?*

EHRs generate big data continuously as the number of people, hospitals, and healthcare centers is countless. Every moment, thousands of patients are taking medical care from hospitals worldwide, and EHRs are generated for diagnosis purposes. Handling these large amounts of data itself is a big challenge. When it comes to handling this big data through blockchain, it becomes more challenging as storing data over the blockchain is expensive. The blockchain was initially developed to keep data tiny in size, basically the financial transaction information. However, to enjoy the merits of blockchain and overcome the limitations of data storing capacity, researchers came with several ideas.

While many haven't considered the scalability issue of blockchain for data storage, others focused on storing data either over the cloud or in local databases and linking the address from that storage to the blockchain.

Among the papers we have analyzed for the review, slightly less than 50% of papers haven't considered the big data storage issue. Authors in 5 papers [105], [107], [113], [124], [135] have considered the issue, but they haven't mentioned about the data storage services. In addition, there were seven papers where authors have chosen the Interplanetary File System (IPFS) as a medium of data storage and then linked the address with the blockchain [72], [79], [85], [87], [116], [117], [120], [144]. Among all the papers, only three proposed to use Amazon Cloud services before uploading data into the blockchain network [59], [96], [100]. Around one-fourth of the total papers suggested using the local database for storing EHRs data before blockchain. The rest of the papers proposed using private blockchain or off-chain storage to handle scalability issues.

The solutions provided above to overcome the big data issues are significant, but it needs more research to handle a considerable amount of EHRs data.

TABLE 1. *(Continued.)* **List of selected articles.**

Ref.	Authors	Year	Citation	Publication Type	Platform	Type	Class	CA
68 [121]	M. Shah et al.	2019	3	Conference	N/D	N/D	1	N/D
69 [122]	D. R. Chawdhuri	2019	2	Conference	N/D	Public	1	N/D
70 [123]	WC. Wu and YC. Wei	2019	0	Conference	N/D	N/D	1	N/D
71 [57]	T. T. Thwin and S. Vasupongayya	2019	29	Journal	Hyperledger Fabric	Private	3	N/D
72 [124]	B. Shen et al.	2019	80	Journal	N/D	N/D	2	BFT
73 [125]	L. Chen et al.	2019	132	Journal	Ethereum	N/D	2	N/D
74 [126]	A. A. Omar et al.	2019	118	Journal	Ethereum	N/D	2	N/D
75 [127]	S. Cao et al.	2019	59	Journal	Ethereum	Public	2	PoW
76 [128]	Y. Guang et al.	2019	7	Special Issue	Hyperledger Fabric	Private	2	PoI
77 [129]	X. Zhang and S. Poslad	2018	57	Conference	N/D	N/D	1	N/D
78 [130]	R. GUO et al.	2018	269	Journal	N/D	N/D	1	N/D
79 [131]	X. Zhang et al.	2018	14	Conference	N/D	N/D	1	N/D
80 [132]	G. Yang and C. Li	2018	27	Conference	N/D	N/D	1	N/D
81 [133]	J. Liu et al.	2018	77	Conference	Consortium	N/D	1	Improved DPoS
82 [134]	O. Gutierrez et al.	2018	5	Conference	N/D	N/D	1	N/D
83 [135]	J. Vora et al.	2018	127	Conference	Ethereum	N/D	2	PoV
84 [136]	Z. Xiao et al.	2018	16	Conference	Hyperledger Fabric	Private	2	PBFT
85 [56]	A. Zhang and X. Lin	2018	175	Journal	N/D	Private and consortium	3	Proof of Conformance
86 [137]	H. Li et al.	2018	122	Journal	Ethereum	Public	2	Proof of primitiveness of data
87 [138]	H. Kaur et al.	2018	114	Journal	N/D	N/D	1	N/D
88 [139]	Y. Chen et al.	2018	146	Journal	N/D	N/D	1	DPoS
89 [140]	K. Fan et al.	2018	190	Journal	N/D	N/D	1	Hybrid Consensus
90 [141]	H. Han et al.	2018	11	Conference	Private + Consortium	Private	1	PoW
91 [142]	H. Wang and Y. Song	2018	127	Journal	N/D	N/D	1	N/D
92 [143]	S. Rahmadika and K. H. Rhee	2018	41	Journal	N/D	Private	1	PoW
93 [55]	P. Zhang et al.	2018	284	Journal	Ethereum	Private	3	N/D
94 [144]	GG Dagher et al.	2018	300	Journal	Ethereum	Private	2	QuorumChain
95 [53]	KJ Kim and S. P. Hong	2017	10	Journal	Ethereum	Private	2	N/D
96 [54]	Q. Xia et al.	2017	279	Journal	Private Blockchain	Private	2	N/D
97 [145]	A. Roehrs et al.	2017	182	Journal	Bitcoin	Public	2	N/D
98 [51]	A. Azaria et al.	2016	1274	Conference	Ethereum	N/D	2	PoW
99 [52]	A. Al Omar et al.	2016	139	Conference	N/D	N/D	1	N/D

RQ4: *What platforms/mechanisms of blockchain were used to handle EHRs management?*

Various platforms/mechanisms exist now to offer blockchain-based solutions. Different categories of existing blockchains are explained in Section 11 II-B. Among all the various types, Ehtereum (public and private), Hyperledger Fabric [19], and consortium blockchains [21], [22] is by far the most popular for EHR data management. Due to the nature of EHRs, which contain sensitive personal information, a private blockchain resides on top of the popularity index. Moreover, a private blockchain can provide access control rules, so only specific people can join the network by following good security policies. By contrast, a public blockchain does not provide strict access control rules, so anybody can join the web and get access to the data. Apart from that, a consortium blockchain also provides a private network and limits access to network data. Therefore, these three types are found appealing among researchers.

Several proposed models or architectures have been offered in the literature review. Most of the authors focused on the integrity, availability, transparency, privacy, and security of EHRs. Almost all the proposed models support the storage of EHRs from medical institutions and wearable devices. Various types of blockchain platforms used in the literature review are shown in Fig. 7. A significant number of papers used the Ethereum platform for the proposed solutions. The number was equal for Hyperledger Fabric and Not Defined (N/D), 24 in each category. The rest of the offered solutions include Bitcoin [13], [89], [145], consortium blockchain [67], [85], [86], [107], [112], [133], private & consortium blockchain [91], [120], [141], Multichain [106], [119], private blockchain [54], [108], Userchain and Docchain [117], Permissioned Blockchain [58], Polkadot [75], and KSI [77].

It includes numerous consensus algorithms for finding an agreement among miners before adding a block to the blockchain. Various consensus algorithms used in the given literature review are shown in Section II-C. Various types of consensus algorithms found in literature review is shown in Fig. 8. Among all the different consensus used for adding EHRs in the blockchain, PoW has been found by far the most popular. Authors chose the PoW as the consensus algorithm in twelve research articles [11], [51], [68], [81], [87], [89], [99], [100], [103], [127], [141], [143]. Researchers used PoA in 8 papers [61], [76], [95], [106], [107], [109], [115], [116], whereas PBFT

TABLE 2. Comparison of articles.

Reference	Privacy	Security	Scalability	Accessibility	Cost Analysis
[11]	✓	✓	✓(Cloud)	✓	x
[12]	✓	✓	✓(Cloud)	✓	x
[13]	✓	✓	✓(Cloud)	✓	x
[65]	✓	✓	x	✓	x
[66]	✓	✓	x	✓	x
[98]	x	✓	x	x	x
[67]	✓	✓	✓(Cloud)	✓	x
[51]	✓	✓	x	✓	x
[129]	✓	✓	x	x	x
[130]	✓	✓	x	x	✓
[131]	✓	✓	x	x	✓
[132]	✓	✓	x	x	x
[133]	✓	✓	✓(Cloud)	✓	x
[134]	✓	✓	x	✓	x
[99]	✓	✓	✓(IPFS)	✓	✓
[135]	✓	✓	✓	✓	x
[100]	✓	✓	✓(Amazon Cloud)	✓	x
[101]	✓	✓	✓(Cloud)	✓	x
[102]	✓	✓	x	✓	x
[103]	x	✓	✓(Cloud)	✓	x
[104]	✓	✓	x	✓	x
[105]	✓	✓	✓	✓	x
[68]	✓	✓	✓(Cloud)	✓	✓
[106]	✓	✓	x	✓	x
[107]	✓	✓	✓	✓	x
[108]	✓	✓	x	✓	✓
[109]	✓	✓	x	✓	x
[110]	✓	✓	✓(Cloud)	✓	✓
[136]	✓	✓	✓(Government or Individual)	✓	x
[111]	✓	✓	x	✓	x
[112]	✓	✓	x	✓	✓
[113]	✓	✓	✓	✓	x
[114]	✓	✓	✓(Cloud)	✓	x
[115]	✓	✓	✓(Cloud)	✓	✓
[116]	✓	✓	IPFS	✓	x
[69]	✓	✓	x	✓	x
[70]	x	✓	x	✓	x
[71]	✓	✓	x	✓	✓
[14]	✓	✓	✓(Dropbox)	✓	x
[72]	✓	✓	✓(IPFS)	✓	x
[73]	✓	✓	✓(Cloud)	✓	x
[74]	✓	✓	✓(Off-chain Storage)	✓	x
[59]	✓	✓	✓(Amazon Cloud)	✓	✓
[75]	✓	✓	✓(CSP)	✓	✓
[60]	✓	✓	x	✓	x
[117]	✓	✓	✓(IPFS)	✓	✓
[52]	✓	✓	x	✓	x
[56]	✓	✓	x	✓	✓
[137]	✓	✓	x	✓	✓
[138]	✓	✓	x	✓	x
[139]	✓	✓	✓(Cloud)	✓	x

TABLE 2. *(Continued.)* **Comparison of articles.**

Reference	Privacy	Security	Scalability	Accessibility	Cost Analysis
[140]	✓	✓	✓(Cloud or Local Database)	✓	x
[141]	✓	✓	✓(Private Blockchain)	✓	x
[118]	✓	✓	x	✓	✓
[119]	✓	✓	✓(Off-chain Storage)	✓	x
[58]	✓	✓	✓(Off-chain Storage)	✓	x
[120]	✓	✓	✓(IPFS)	✓	x
[121]	✓	✓	✓(Existing Database)	✓	x
[122]	✓	✓	x	✓	x
[123]	✓	✓	x	x	x
[76]	✓	x	x	✓	x
[62]	✓	✓	x	✓	x
[77]	✓	✓	✓(Cloud)	✓	✓
[78]	✓	✓	x	✓	x
[79]	✓	✓	✓(IPFS)	✓	x
[63]	✓	✓	x	✓	x
[80]	x	✓	x	✓	x
[81]	✓	✓	x	✓	✓
[82]	✓	✓	x	✓	x
[83]	✓	✓	✓(Cloud)	✓	x
[84]	✓	✓	✓(Cloud)	✓	✓
[142]	✓	✓	✓(Cloud)	✓	x
[85]	✓	✓	✓(IPFS)	✓	x
[53]	✓	✓	x	✓	x
[143]	x	✓	x	✓	x
[86]	✓	✓	x	✓	✓
[87]	✓	✓	✓(IPFS)	✓	✓
[88]	✓	✓	✓(Cloud	✓	x
[57]	✓	✓	✓(Cloud)	✓	x
[54]	✓	✓	✓(speed✓Transaction)	✓	x
[124]	✓	✓	✓	✓	✓
[61]	✓	✓	x	✓	x
[64]	✓	✓	x	✓	x
[89]	✓	✓	✓(Message Sharing)	✓	x
[145]	✓	✓	✓(Chord Algorithm)	✓	x
[55]	✓	✓	✓(Local Storage)	✓	x
[144]	✓	✓	✓(Local Database)	✓	x
[125]	✓	✓	x	✓	x
[126]	✓	✓	✓(Cloud)	✓	✓
[90]	✓	✓	x	✓	x
[91]	✓	✓	x	✓	✓
[127]	✓	✓	✓(Cloud)	✓	✓
[92]	✓	✓	x	✓	x
[93]	✓	✓	x	✓	x
[94]	✓	✓	x	✓	x
[95]	✓	✓	x	✓	x
[128]	✓	✓	x	✓	x
[96]	✓	✓	✓(Amazon AWS)	✓	x
[97]	✓	✓	✓(Cloud)	✓	x

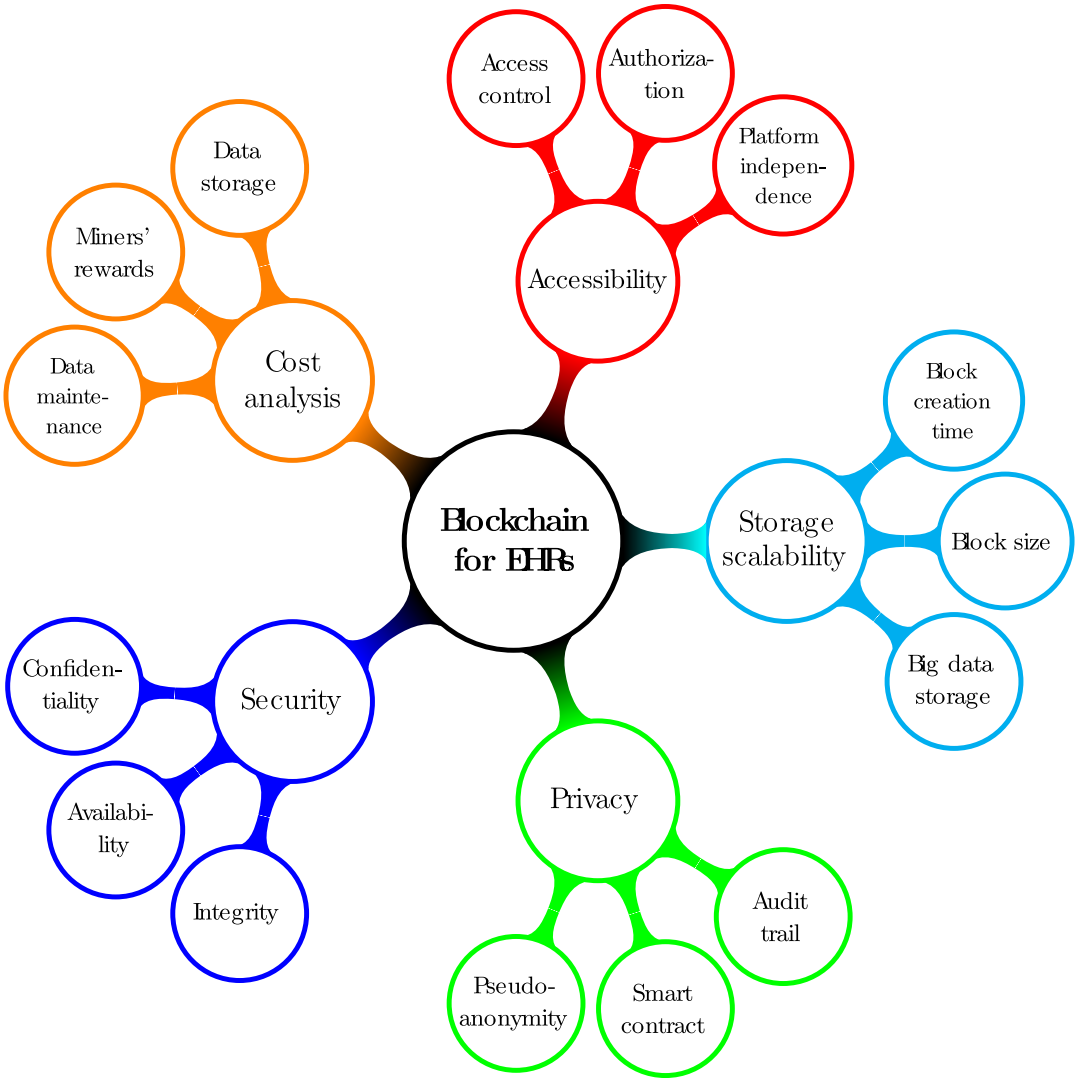

FIGURE 6. Taxonomy for five unique properties of blockchain based EHR solutions.

was suggested in 7 research papers [66], [84], [94], [96], [97], [104], [136]. DPoS, BFT, and improved DPoS were less popular, the number was three [12], [13], [139], two [75], [124], and two [108], [133] accordingly. Other algorithms found in the SLR were DPoS-Qoram, KAFKA, PoI, PoS, PoV, POW and PBFT, PoW and PoS, Proof of Primitiveness of data, Proof of Conformance, QuorumChain, and Hybrid Consensus, each of these found in a single paper among all. However, among more than 50% papers, authors haven't mentioned or used any consensus algorithms.

RQ5: *How Privacy, Security, Storage Scalibility, Accessibility, and Cost analysis were handled?*

We intended to find how researchers handled privacy, Security, Storage Scalability, Accessibility, and Cost analysis properties in blockchain-enabled EHR solutions. These five unique characteristics are very crucial when it comes to providing a solution for EHRs using blockchain. The mindmap for the details of these characteristics is shown in Fig. 6.

privacy is the primary concern for blockchain-based solutions as the EHRs involve sensitive personal information that patients may or may not wish to share in public. We found that authors in the list of papers used three properties to ensure privacy, such as Pseudo-anonymity, Smart Contract, and Audit trail. *Pseudo-anonymity* is a property of blockchain transactions where an alphanumeric number represents every user. Whenever a user opens a Bitcoin wallet, an automatic alphanumeric number is assigned to her to conceal his real identity and to allow him to send and receive Bitcoins. Anyone with the public key can know the history of transactions in the blockchain, but not the identity of the person behind it.[20] Similarly, it ensures the identity of a patient not to be directly exposed to the public from his EHRs [13], [89]. *Smart contracts* are another privacy mechanism that authors

[20] Anonymity vs. Pseudonymity In Crypto, https://www.gemini.com/cryptopedia/anonymity-vs-pseudonymity-basic-differences, Accessed 10 May 2021.

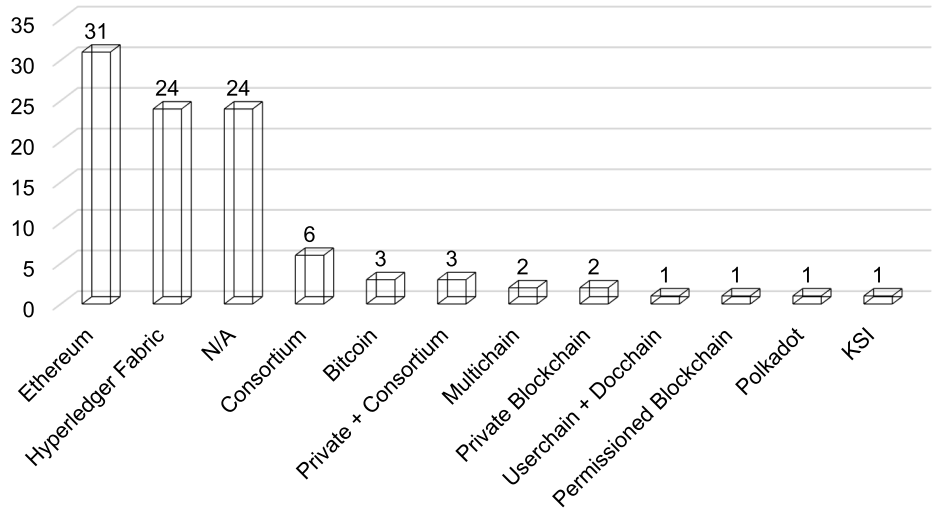

FIGURE 7. Types of blockchain platforms/mechanisms used.

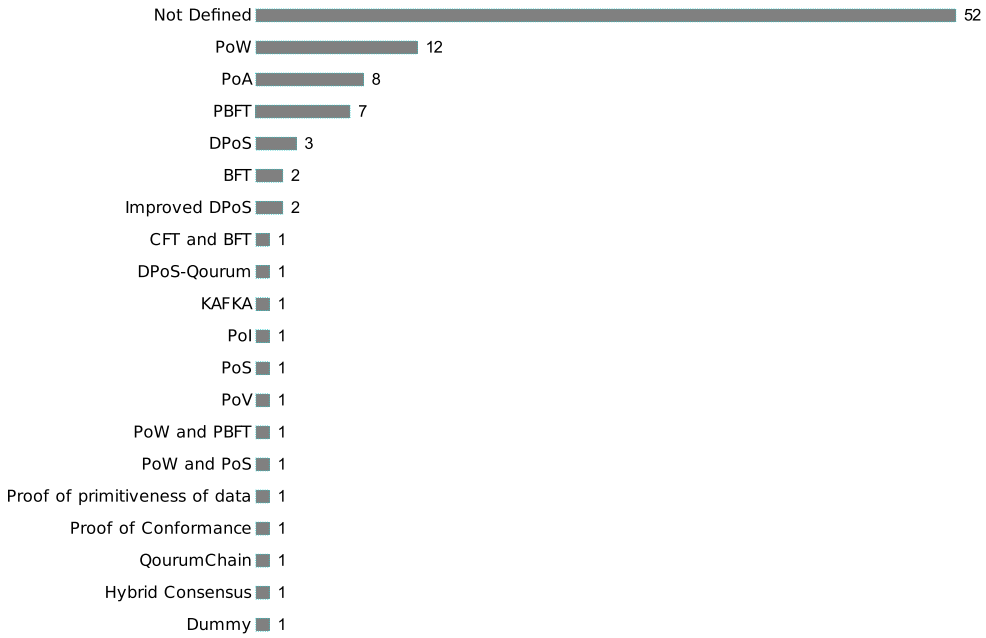

FIGURE 8. Types of consensus algorithm used in literature review.

used for safe EHR sharing in blockchain-based applications [72], [102]. These are simple computer programs installed on a blockchain that run when some preconditions are met. Using predefined smart contracts, a patient can determine who will access his EHRs and who will be restricted from them. *Audit trail* is another significant privacy property for blockchain-based EHR solutions. It provides information about who, when, and from where users access EHRs. Therefore, the privacy of patients' records is maintained using this property. Nevertheless, among the articles we analysed, five papers [98], [103], [70], [80], [143] have not considered privacy in their proposed solutions.

Security is the second most important property to consider for EHR-based applications using blockchain. It has three sub-categories: confidentiality, integrity, and availability. *Confidentiality* means the EHR data will only be accessible by authorized users. It is highly significant for EHRs as patients' information with doctors and other medical practitioners is highly sensitive, and exposing those can hamper the security and lead to data misuse or modification.

In most blockchain-based solutions, confidentiality is maintained using cryptographic tools to ensure that data is not readable by unauthorized users [99], [108], [135]. We found that most popular encryption algorithms are Attribute-based Encryption (ABE) [88], Proxy Re-Encryption (PRE) [87], and symmetric encryption (e.g., AES) [11]. *Integrity* of EHR data is all about accuracy, consistency, and completeness and also refers to their safety. Data integrity can be broken due to human errors, bugs, and hardware failure, leading to the loss of critical health records and sensitive personal information. Blockchain ensures the integrity of information found in blocks using hash functions (e.g., SHA-256). Besides, every node in the blockchain network has either a copy of EHRs when they are stored on the blockchain [53], [143], or a copy of the pointer to EHRs when stored externally (e.g., cloud) [11], [71]. *Availability* means that EHRs are available when and where the user needs them. If the data is not known when the user wants it, there is no use in storing it; moreover, the user may face tragic consequences such as wrong medication or incomplete medical consultation. As blockchain is a distributed ledger, there is a slight chance of losing data or accessing it. However, Even though off-chain data storage does not ensure data availability, it can ensure that if the data is missing from the host database, digital data forensic can be done using the data pointers. Most blockchain-based applications for EHRs focused on the system being fault-tolerant during any system failure [65], [98]. All papers, except one [76], considered security when proposing their blockchain-based solutions.

Storage scalability is a big concern for blockchain-based solutions. A blockchain is a distributed ledger that increases in size each time a block is created. The literature review considers three main challenges: block creation time, block size, and ample data storage. *Block creation time* corresponds to the time needed to store either EHRs directly or some auxiliary data linking EHRs stored externally from the blockchain. It is crucial as EHRs data are generated continuously across the world. If the time taken for storing these data is long (e.g., When EHRs are developed every minute, blocks creation time needs to be shorter than that), it will cause problems for both patients and doctors. Similarly, *block size* refers to the capacity limit of data in a block. This is also important as EHR data vary in size. Various blockchain-based solutions have been proposed with these issues in mind but different results. For instance, Bitcoin takes around ten minutes to create a new block, and the maximum block size is 1 MB [1], whereas Ethereum takes about 10-20 seconds to create a new block[21] and the average block size is about 50-60 KB.[22] Finally, *big data storage* refers to storing huge EHR data generated all around the globe. It is mandatory to analyze the capacity and the scalability of the data storage options of a blockchain to handle these big data by storing a large set of dummy data[23] before deploying. Failing to do so will not be fruitful for patients worldwide. Authors such as [100], [108], decided to put the EHRs in external databases, such as local or cloud databases, in order to cope with the limited storage of blockchains. However, when storing data outside the blockchain network, it is crucial to consider the security of the storage options (e.g., encryption, access control). For storage scalability, several authors [105], [108] proposed solutions that are costly but easy data access.

Accessibility is another important property related to the EHR data access policies in the blockchain. We found three major sub-properties to ensure the proper accessibility of EHRs: access control, authorization, and platform independence. *Access control* verifies EHR access rights. It has two aspects: patients accessing their own EHRs [37] and other users accessing those same EHRs [12], [98]. The former case is pretty simple as the patients should have all the rights to access their own EHRs, but the latter requires careful investigation. Often, a third party who requests access to the owner of EHRs, follows a public-key encryption process [98]. For instance, ABE [88] allows third parties to get access rights from some attributes such as ''doctor'' and ''hospital.'' *Authorization* is the process where a patient or hospital authorizes someone to get access to his EHRs. It is sometimes (depending on the country's legislation) illegal to access someone's EHRs without his consent [37], as this may then expose the data to malicious users. Furthermore, *platform independence* is the property of a blockchain-based solution that makes sure it runs on all platforms for smartphones and computers, such as Android, Windows, and MAC. Failing to do so will create accessibility problems not only for patients but also for physicians. All papers except five, [98], [123], [129]–[132] considered accessibility carefully when designing their blockchain-based solutions.

Finally, **cost analysis** is a significant feature to offer in blockchain-based EHRs solutions. Costs are involved in adding a block to the blockchain, rewarding miners, and uploading and maintaining a database when EHRs are stored externally. *Data storage* cost is higher when directly stored in blockchains [85], so authors [100], [108] came with off-chain data storage. However, even if EHRs are stored in external databases, it is pretty expensive to store huge amounts of EHR data generated every day worldwide.[24] *Data Maintenance* in local or cloud databases involves a huge cost such as workforce, computing resources, and resources for data sharing. This is a significant issue when making EHR management using blockchain. Finally, *miners' rewards* are the expense for people who mine a block before accepting and uploading it to the blockchain. Miners are there to ensure that they will upload only the eligible and authentic data to the blockchain. If we consider a large-scale blockchain-based solution for

[21] Ethereum Average Block Time Chart, https://etherscan.io/chart/blocktime, Accessed 15 May 2021.

[22] Ethereum Average Block Size Chart, https://etherscan.io/chart/blocksize, Accessed 15 May 2021.

[23] 4 ways to create random dummy files.. https://www.digitalcitizen.life/3-ways-create-random-dummy-files-windows-given-size/, Accessed 12 May 2021.

[24] Why new off-chain storage is required for blockchains, https://www.ibm.com/downloads/cas/RXOVXAPM, Accessed 23 May 2021.

EHRs, these costs (e.g., transaction fees, miners' reward, and database maintenance) are significant to consider. However, only 24 papers [56], [59], [68], [71], [75], [77], [81], [84], [86], [87], [91], [99], [108], [110], [112], [115], [117], [118], [124], [126], [127], [130], [131], [137] discussed or analyzed the cost induced by their solutions using blockchain. The remaining 75 papers did not focus on the cost issue.

IV. FUTURE RESEARCH DIRECTION

This section discusses about directions for designer of blockchain applications to handle EHRs.

A. ARTIFICIAL INTELLIGENCE

When blockchain systems are integrated with Artificial Intelligence (AI) in different real-world healthcare solutions, they will become more efficient and stable [146]. Machine learning (ML) and deep learning (DL) are two main domains of AI which are helping to automate real-world applications. ML could be a potential technology in combination with blockchain to handle EHRs in the near future. Despite the challenges like storing, sharing, and training critical EHR data for designing practical applications, interest is growing among researchers to develop ML, and blockchain-based EHR applications [147], [148]. IBM has recently announced plans to deploy intelligent blockchain, where some AI agent performs various tasks like legislation, improved records, suspicious activities and make suggestions for updating smart contracts in a large network.[25] AI is used to develop a next-generation blockchain in the MATRIX project [149], which facilitates the automated generation of intelligent contacts, improves the protection against malicious threats, and enables highly scalable operations.

Using various ML algorithms, one can find fraudulent EHRs data, and only valid EHRs will be stored in the blockchain. Using DL, previous damaged medical records can be recovered and stored in blockchain for knowledge improvement (e.g., for drug analysis and prediction) [150]. Deep Learning as-a-Service (DaaS) is also used on stored EHRs to precisely predict future diseases based on current diagnosis reports of patients [151]. Finally, ML algorithms can be used to prevent major attacks in blockchain networks [152]. There are some existing projects where AI and blockchain are combined. For instance, SingularityNET [153], which focuses on creating networking with AI and blockchain for the robot brain, and DeepBrain Chain,[26] which focuses on creating a platform to develop AI algorithms. Besides, some ML and DL based works related to health are underway, such as Gamalon project,[27] TraneAI [154], Neureal [155], etc.

[25] AI & Intelligent Automation, https://www.tractica.com/artificial-intelligence/four-examples-o-fblockchain-artificial-intelligence-deployments/, Accessed 25 May 2021.

[26] Artificial Intelligence Computing Platform Driven By BlockChain-DeepBrain Chain, https://cryptorating.eu/whitepapers/DeepBrain-Chain/DeepBrainChainWhitepaper.pdf, Accessed 26 May 2021.

[27] ABOUT GAMALON, https://gamalon.com/company/,Accessed 26 May 2021.

B. EDGE COMPUTING

Sharing large amounts of EHRs among various health care organizations is challenging because of network loads and data size. Recent solutions for EHR management, in particular, have poor scalability, high computational cost, and extended response times. Edge computing could be a solution for the issues mentioned above. It can process a large amount of data from diverse locations, as edge computing consists of a group of servers/computers for its operations [156]. Gai *et al.* [157] suggest edge computing to expand cloud services to the network's edge, providing processing capacity and enhancing device Quality of Operation.

Edge Computing has the advantage of big data storing, long networking, and high computing power, and it supports the scalability for distributed applications in a secure and controlled manner. Even though edge computing has several flaws such as security, vulnerability to various attacks during message transmission, and integrity, blockchain-based solutions face numerous problems such as storage, scalability, constraints of block size, and block creation time that can be solved using edge computing. Similar mechanisms for decentralized technologies can enhance privacy, security, and automatic resource handling [158]. Combining both can have several merits. Firstly, we can build distributed controls at various edge nodes using blockchain. The mining process of blockchain confirms data accuracy, consistency, and reliability. Secondly, user privacy can even become higher as users control the data using cryptographic keys. Finally, edge computing involves resource sharing among other nodes, which can be achieved securely using smart contracts on blockchain [159].

C. IoMT

Internet of Medical Things (IoMT) is a series of medical equipment and software that use online computing networks to link to various healthcare providers. The basis of IoMT is the Machine-to-Machine (M2M) communication among wireless medical devices. Through the IoMT, medical care providers & authorities can get the real-time health update of patients from remote locations through wearable devices.

However, besides the advantages of IoMT, there are several downsides to it, as IoMT devices are vulnerable to security threats. During the pandemic situation of Covid-19, not only the demand for innovative medical devices has increased enormously, but the cyber threats related to them also increased significantly [160].

Blockchain can be considered a savior for the threats related to IoMT devices. The decentralized key management, inseparability, and integrity properties of blockchain can ensure secure communications among smart Medical devices.

V. LIMITATIONS

The SLR solely focused on applying blockchain for EHR management and did not include any other potential

blockchain applications related to other healthcare sectors (e.g., supply chain management for medicine) or any other fields (e.g., transaction handling). The review was strictly limited to articles that only addressed EHR and blockchain ideas.

We identified several limitations of blockchain-based EHR solutions. Limitations include common standard, scalability in terms of storage, block creation time, data storage, user adaptation, and storing and maintaining EHR data costs. Most of the solutions are still in either a theoretical or prototype state. Blockchain technology is still in a developing state that lacks user-friendliness and has limitations regarding EHR privacy and security of EHR data. No solutions have been found to either delete fraud EHR data from the blockchain or for dead patients.

Besides, no acceptable solutions were found for the scenario where a patient is in a coma, unconscious, or illiterate, and his EHRs need to be accessed by the doctors or physician. One possibility is that the patient has an ID card with a unique identification number, and the doctor can read the EHRs using it. Finally, aggregation of technologies like ML, AI, and Edge Computing may help overcome problems like scalability, fraud EHRs detection, and many more.

VI. CONCLUSION

This study answers the question of the current state of the art in blockchain-based EHR management research and future directions. We showed the distribution of blockchain types and platforms adopted by the reviewed articles. The potential benefits of blockchain to manage EHRs have met stakeholders' expectations in the healthcare sectors, while we also found that several challenges require further research. For instance, cross-border sharing of EHR data may be hampered by varying and often conflicting legislation. Besides, the privacy policies also vary based on the specific government regulation. Hence, further investigation on regulation, standardization, and cross-border accessibility of EHRs is crucial.

However, After thorough scrutiny of selected articles, we concluded that the most prominent blockchain platform for EHR management is Ethereum (private) and Hyperledger Fabric because these two platforms meet almost all the requirements. We also found that handling big EHR data on a large scale with blockchain has limitations such as limited storage capacity, computation cost, and communication cost. However, there are potential solutions to overcome these limitations, such as artificial intelligence, IoMT, and edge computing.

The study may serve as a reference for future research in this field. The accumulation of all related papers, their contributions, and limitations will help the potential researchers to design a new architecture or model. Moreover, future research directions to combine blockchain could help propose more exciting solutions for the existing problems.

DECLARATION OF COMPETING INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have influenced the work reported in this paper.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Bus. Rev.*, 2008, Art. no. 21260.

[2] A. A. Vazirani, O. O'Donoghue, D. Brindley, and E. Meinert, "Implementing blockchains for efficient health care: Systematic review," *J. Med. Internet Res.*, vol. 21, no. 2, Feb. 2019, Art. no. e12439.

[3] M. Hölbl, M. Kompara, A. Kamišalić, and L. N. Zlatolas, "A systematic review of the use of blockchain in healthcare," *Symmetry*, vol. 10, no. 10, p. 470, Oct. 2018.

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

[5] E. Chukwu and L. Garg, "A systematic review of blockchain in healthcare: Frameworks, prototypes, and implementations," *IEEE Access*, vol. 8, pp. 21196–21214, 2020.

[6] S. Khezr, A. Yassine, and R. Benlamri, "Blockchain technology in healthcare: A comprehensive review and directions for future research," *Appl. Sci.*, vol. 9, no. 9, p. 1736, 2019.

[7] I. Ahmed, M. Ahmad, G. Jeon, and F. Piccialli, "A framework for pandemic prediction using big data analytics," *Big Data Res.*, vol. 25, Jul. 2021, Art. no. 100190.

[8] R. Vaishya, M. Javaid, I. H. Khan, and A. Haleem, "Artificial intelligence (AI) applications for COVID-19 pandemic," *Diabetes Metabolic Syndrome: Clin. Res. Rev.*, vol. 14, no. 4, pp. 337–339, Jul. 2020.

[9] L. Houston, Y. Probst, and A. Humphries, "Measuring data quality through a source data verification audit in a clinical research setting," *Stud. Health Technol. Inform.*, vol. 214, pp. 13–107, Jan. 2015.

[10] M. Muthuppalaniappan and K. Stevenson, "Healthcare cyber-attacks and the COVID-19 pandemic: An urgent threat to global health," *Int. J. Qual. Health Care*, vol. 33, no. 1, Feb. 2021.

[11] M. S. Rahman, I. Khalil, P. C. Mahawaga Arachchige, A. Bouras, and X. Yi, "A novel architecture for tamper proof electronic health record management system using blockchain wrapper," in *Proc. ACM Int. Symp. Blockchain Secure Crit. Infrastruct. (BSCI)*, 2019, pp. 97–105.

[12] H. Wu, Y. Shang, L. Wang, L. Shi, K. Jiang, and J. Dong, "A patient-centric interoperable framework for health information exchange via blockchain," in *Proc. 2nd Int. Conf. Blockchain Technol. Appl.*, Dec. 2019, pp. 76–80.

[13] 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.

[14] A. Fernandes, V. Rocha, A. F. D. Conceicao, and F. Horita, "Scalable architecture for sharing EHR using the hyperledger blockchain," in *Proc. IEEE Int. Conf. Softw. Archit. Companion (ICSA-C)*, Mar. 2020, pp. 130–138.

[15] A. A. Mamun, A. Al Mamun, S. R. Hasan, S. R. Hasan, M. S. Bhuiyan, M. S. Bhuiyan, M. S. Kaiser, M. S. Kaiser, M. Abu Yousuf, and M. A. Yousuf, "Secure and transparent KYC for banking system using IPFS and blockchain technology," in *Proc. IEEE Region 10 Symp. (TENSYMP)*, 2020, pp. 348–351.

[16] Wikipedia. *Cryptographic Nonce*. Accessed: Jan. 10, 2021. [Online]. Available: https://en.wikipedia.org/wiki/Cryptographic_nonce

[17] V. Buterin. (2016). *What is Ethereum*. [Online]. Available: http://www.ethdocs.org/en/latest/introduction/what-is-ethereum.html

[18] Litecoin. *Litecoin–Open Source P2P Digital Currency*. Accessed: Jan. 8, 2021. [Online]. Available: https://litecoin.org/

[19] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, and K. Christidis, "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proc. 13th EuroSys Conf.*, 2018, pp. 1–15.

[20] F. Armknecht, G. O. Karame, A. Mandal, F. Youssef, and E. Zenner, "Ripple: Overview and outlook," in *Proc. Int. Conf. Trust Trustworthy Comput.* Heraklion, Greece: Springer, 2015, pp. 163–180.

[21] Quorum. *Build on Quorum, the Complete Open Source Blockchain Platform for Business*. Accessed: Jan. 7, 2021. [Online]. Available: https://consensys.net/quorum/

[22] R. G. Brown, "The corda platform: An introduction," *Retrieved*, vol. 27, p. 2018, May 2018.

[23] S. Nadal and S. King, "PPCoin: Peer-to-peer crypto-currency with proof-of-stake," *Self Published Paper*, vol. 19, 2012.
[24] F. Saleh, "Blockchain without waste: Proof-of-stake," in *The Review of Financial Studies*. Oxford, U.K.: Oxford Univ. Press, 2018.
[25] G. Wood, "Polkadot: Vision for a heterogeneous multi-chain framework," Parity Technol., London, U.K., White Paper 21, 2016.
[26] C. Li and B. Palanisamy, "Incentivized blockchain-based social media platforms: A case study of steemit," Apr. 2019.
[27] Quordantheman. *Dpos Consensus Algorithm–The Missing White Paper*. Accessed: Jan. 7, 2021. [Online]. Available: https://steemit.com/dpos/@dantheman/dpos-consensus-algorithm-this-missing-white-paper
[28] F. Schuh and D. Larimer. (2017). *Bitshares 2.0: General Overview*. Accessed: Jun. 2017. [Online]. Available: http://docs.bitshares.org/downloads/bitshares-general.pdf
[29] C. Jepson. (2015). *Dtb001: Decred Technical Brief*. [Online]. Available: https://coss.io/documents/white-papers/decred.pdf and [Online]. Available: https://www.decred.org
[30] K. Li, H. Li, H. Hou, K. Li, and Y. Chen, "Proof of vote: A high-performance consensus protocol based on vote mechanism & consortium blockchain," in *Proc. IEEE 19th Int. Conf. High Perform. Comput. Commun.; IEEE 15th Int. Conf. Smart City; IEEE 3rd Int. Conf. Data Sci. Syst. (HPCC/SmartCity/DSS)*, Dec. 2017, pp. 466–473.
[31] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in *Proc. OSDI*, vol. 99, 1999, pp. 173–186.
[32] L. Goodman. (2014). *Tezos-a Self-Amending Crypto-Ledger White Paper*. [Online]. Available: https://www.tezos.com/static/papers/white paper.pdf
[33] M. Röscheisen, M. Baldonado, K. Chang, L. Gravano, S. Ketchpel, and A. Paepcke, "The Stanford InfoBus and its service layers: Augmenting the internet with higher-level information management protocols," in *Digital Libraries in Computer Science: The MeDoc Approach*. Stanford, CA, USA: Stanford InfoLab, 1998, pp. 213–230.
[34] E. Paul, "What is digital signature-how it works, benefits, objectives, concept," EMP Trust HR, Gaithersburg, MD, USA, Tech. Rep., 2017. [Online]. Available: https://www.emptrust.com/blog/benefits-of-using-digital-signatures/
[35] J. Beavers and S. Pournouri, "Recent cyber attacks and vulnerabilities in medical devices and healthcare institutions," in *Blockchain and Clinical Trial*. Cham, Switzerland: Springer, 2019, pp. 249–267.
[36] R. D. Cebul, T. E. Love, A. K. Jain, and C. J. Hebert, "Electronic health records and quality of diabetes care," *New England J. Med.*, vol. 365, no. 9, pp. 825–833, Sep. 2011.
[37] H. M. Edemekong and P. Annamaraju. *Health Insurance Portability and Accountability Act*. Accessed: Jan. 15, 2021. [Online]. Available: https://www.ncbi.nlm.nih.gov/books/NBK500019/#:~:text=HHS%20initiated%
[38] S. Keele *et al.*, "Guidelines for performing systematic literature reviews in software engineering," Citeseer, 2007.
[39] D. Moher, A. Liberati, J. Tetzlaff, and D. G. Altman, "Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement," *Int. J. Surg.*, vol. 8, no. 5, pp. 336–341, 2010.
[40] I. Keshta and A. Odeh, "Security and privacy of electronic health records: Concerns and challenges," *Egyptian Informat. J.*, vol. 22, no. 2, pp. 177–183, Jul. 2021.
[41] M. Cifuentes, M. Davis, D. Fernald, R. Gunn, P. Dickinson, and D. J. Cohen, "Electronic health record challenges, workarounds, and solutions observed in practices integrating behavioral health and primary care," *J. Amer. Board Family Med.*, vol. 28, pp. S63–S72, Sep. 2015.
[42] K. T. Win, "A review of security of electronic health records," *Health Inf. Manage.*, vol. 34, no. 1, pp. 13–18, Mar. 2005.
[43] J. S. Ancker, M. Silver, M. C. Miller, and R. Kaushal, "Consumer experience with and attitudes toward health information technology: A nationwide survey," *J. Amer. Med. Inform. Assoc.*, vol. 20, no. 1, pp. 152–156, Jan. 2013.
[44] G. Perera, A. Holbrook, L. Thabane, G. Foster, and D. J. Willison, "Views on health information sharing and privacy from primary care practices using electronic medical records," *Int. J. Med. Informat.*, vol. 80, no. 2, pp. 94–101, Feb. 2011.
[45] S. B. Wikina, "What caused the breach? An examination of use of information technology and health data breaches," *Perspect. Health Inf. Manage.*, vol. 11, pp. 1–16, Oct. 2014.
[46] C. S. Kruse, B. Smith, H. Vanderlinden, and A. Nealand, "Security techniques for the electronic health records," *J. Med. Syst.*, vol. 41, no. 8, pp. 1–9, Aug. 2017.
[47] V. Liu, M. A. Musen, and T. Chou, "Data breaches of protected health information in the United States," *Jama*, vol. 313, no. 14, pp. 1471–1473, 2015.
[48] D. D. F. Maesa, P. Mori, and L. Ricci, "Blockchain based access control," in *Proc. IFIP Int. Conf. Distrib. Appl. Interoperable Syst.* Neuchâtel, Switzerland: Springer, 2017, pp. 206–220.
[49] B. Yüksel, A. Küpçü, and Ö. Özkasap, "Research issues for privacy and security of electronic health services," *Future Gener. Comput. Syst.*, vol. 68, pp. 1–13, Mar. 2017.
[50] D. F. Sittig and H. Singh, "Legal, ethical, and financial dilemmas in electronic health record adoption and use," *Pediatrics*, vol. 127, no. 4, pp. e1042–e1047, 2011.
[51] 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.
[52] A. Al Omar, M. S. Rahman, A. Basu, and S. Kiyomoto, "Medibchain: A blockchain based privacy preserving platform for healthcare data," in *Proc. Int. Conf. Secur., Privacy Anonymity Comput., Commun. Storage*. Guangzhou, China: Springer, 2017, pp. 534–543.
[53] K. Kim and S.-P. Hong, "A trusted sharing model for patient records based on permissioned blockchain," *J. Internet Comput. Services*, vol. 18, no. 6, pp. 75–84, 2017.
[54] Q. Xia, E. B. 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, 2017.
[55] 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, Jul. 2018.
[56] A. Zhang and X. Lin, "Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain," *J. Med. Syst.*, vol. 42, no. 8, p. 140, 2018.
[57] T. T. Thwin and S. Vasupongayya, "Blockchain-based access control model to preserve privacy for personal health record systems," *Secur. Commun. Netw.*, vol. 2019, pp. 1–15, Jun. 2019.
[58] T. Zhou, X. Li, and H. Zhao, "Med-PPPHIS: Blockchain-based personal healthcare information system for national physique monitoring and scientific exercise guiding," *J. Med. Syst.*, vol. 43, no. 9, p. 305, Sep. 2019.
[59] R. Jabbar, N. Fetais, M. Krichen, and K. Barkaoui, "Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity," in *Proc. IEEE Int. Conf. Informat., IoT, Enabling Technol. (ICIoT)*, Feb. 2020, pp. 310–317.
[60] Y. Zhuang, L. R. Sheets, Y.-W. Chen, Z.-Y. Shae, J. J. P. Tsai, and C.-R. Shyu, "A patient-centric health information exchange framework using blockchain technology," *IEEE J. Biomed. Health Informat.*, vol. 24, no. 8, pp. 2169–2176, Aug. 2020.
[61] O. Gutiérrez, G. Romero, L. Pérez, A. Salazar, M. Charris, and P. Wightman, "HealthyBlock: Blockchain-based IT architecture for electronic medical records resilient to connectivity failures," *Int. J. Environ. Res. Public Health*, vol. 17, no. 19, p. 7132, Sep. 2020.
[62] P. Meier, J. H. Beinke, C. Fitte, and F. Teuteberg, "Generating design knowledge for blockchain-based access control to personal health records," *Inf. Syst. e-Bus. Manage.*, vol. 19, pp. 13–41, Aug. 2020.
[63] R. Kumar and R. Tripathi, "Secure healthcare framework using blockchain and public key cryptography," in *Blockchain Cybersecurity, Trust Privacy*. Cham, Switzerland: Springer, 2020, pp. 185–202.
[64] T. T. Thwin and S. Vasupongayya, "Performance analysis of blockchain-based access control model for personal health record system with architectural modelling and simulation," *Int. J. Netw. Distrib. Comput.*, vol. 8, no. 3, p. 139, 2020.
[65] L. Ismail, H. Materwala, and M. A. Khan, "Performance evaluation of a patient-centric blockchain-based healthcare records management framework," in *Proc. 2nd Int. Electron. Commun. Conf.*, Jul. 2020, pp. 39–50.
[66] L. Ismail and H. Materwala, "BlockHR: A blockchain-based framework for health records management," in *Proc. 12th Int. Conf. Comput. Modeling Simulation*, 2020, pp. 164–168.
[67] Z. Li and L. Zhang, "An EMR sharing and privacy protection mechanism based on medical consortium blockchain," in *Proc. 6th Int. Conf. Comput. Technol. Appl.*, Apr. 2020, pp. 160–164.
[68] X. Yang, T. Li, W. Xi, A. Chen, and C. Wang, "A blockchain-assisted verifiable outsourced attribute-based signcryption scheme for EHRs sharing in the cloud," *IEEE Access*, vol. 8, pp. 170713–170731, 2020.
[69] M. Al Baqari and E. Barka, "Biometric-based blockchain EHR system (BBEHR)," in *Proc. Int. Wireless Commun. Mobile Comput. (IWCMC)*, Jun. 2020, pp. 2228–2234.

[70] O. Ajayi, M. Abouali, and T. Saadawi, "Secure architecture for inter-healthcare electronic health records exchange," in *Proc. IEEE Int. IoT, Electron. Mechatronics Conf. (IEMTRONICS)*, Sep. 2020, pp. 1–6.

[71] V. Jaiman and V. Urovi, "A consent model for blockchain-based health data sharing platforms," *IEEE Access*, vol. 8, pp. 143734–143745, 2020.

[72] R. K. Marangappanavar and M. Kiran, "Inter-planetary file system enabled blockchain solution for securing healthcare records," in *Proc. 3rd ISEA Conf. Secur. Privacy (ISEA-ISAP)*, Feb. 2020, pp. 171–178.

[73] A. I. El Sayed, M. Abdelaziz, M. H. Megahed, and M. H. A. Azeem, "A new supervision strategy based on blockchain for electronic health records," in *Proc. 12th Int. Conf. Electr. Eng. (ICEENG)*, Jul. 2020, pp. 151–156.

[74] H. Guo, W. Li, E. Meamari, C.-C. Shen, and M. Nejad, "Attribute-based multi-signature and encryption for EHR management: A blockchain-based solution," 2020, *arXiv:2002.11078*.

[75] S. Cao, J. Wang, X. Du, X. Zhang, and X. Qin, "CEPS: A cross-blockchain based electronic health records privacy-preserving scheme," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2020, pp. 1–6.

[76] M. Qazi, D. Kulkarni, and M. Nagori, "Proof of authenticity-based electronic medical records storage on blockchain," in *Smart Trends in Computing and Communications*. Singapore: Springer, 2020, pp. 297–306.

[77] 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.

[78] S. Lokhande, S. Mukadam, M. Chikane, and M. Bhonsle, "Enhanced data sharing with blockchain in healthcare," in *Proc. ICCCE*. Singapore: Springer, 2020, pp. 277–283.

[79] X. Wu, Y. Han, M. Zhang, and S. Zhu, "Secure personal health records sharing based on blockchain and IPFS," in *Proc. Chin. Conf. Trusted Comput. Inf. Secur.* Shanghai, China: Springer, 2019, pp. 340–354.

[80] R. Haque, H. Sarwar, S. R. Kabir, R. Forhat, M. J. Sadeq, M. Akhtaruzzaman, and N. Haque, "Blockchain-based information security of electronic medical records (EMR) in a healthcare communication system," in *Intelligent Computing and Innovation on Data Science*. Singapore: Springer, 2020, pp. 641–650.

[81] H. Jin, C. Xu, Y. Luo, and P. Li, "Blockchain-based secure and privacy-preserving clinical data sharing and integration," in *Proc. Int. Conf. Algorithms Archit. Parallel Process.* NY, USA: Springer, 2020, pp. 93–109.

[82] H. H. Kung, Y.-F. Cheng, H.-A. Lee, and C.-Y. Hsu, "Personal health record in FHIR format based on blockchain architecture," in *Proc. Int. Conf. Frontier Comput.* Kyushu, Japan: Springer, 2019, pp. 1776–1788.

[83] B. Arunkumar and G. Kousalya, "Blockchain-based decentralized and secure lightweight e-health system for electronic health records," in *Intelligent Systems, Technologies and Applications*. Singapore: Springer, 2020, pp. 273–289.

[84] S. M. Pournaghi, M. Bayat, and Y. Farjami, "MedSBA: A novel and secure scheme to share medical data based on blockchain technology and attribute-based encryption," *J. Ambient Intell. Humanized Comput.*, vol. 11, pp. 4613–4641, Jan. 2020.

[85] A. Al Mamun, M. U. F. Jahangir, S. Azam, M. S. Kaiser, and A. Karim, "A combined framework of interplanetary file system and blockchain to securely manage electronic medical records," in *Proc. Int. Conf. Trends Comput. Cogn. Eng.* Savar, Bangladesh: Springer, 2021, pp. 501–511.

[86] A. Keerthika and R. Chendhavarayan, "An efficient authentication scheme for block chain-based electronic health records," *Int. J. Eng. Appl. Sci. Technol.*, vol. 4, no. 9, pp. 465–470, Jan. 2020.

[87] M. M. Madine, A. A. Battah, I. Yaqoob, K. Salah, R. Jayaraman, Y. Al-Hammadi, S. Pesic, and S. Ellahham, "Blockchain for giving patients control over their medical records," *IEEE Access*, vol. 8, pp. 193102–193115, 2020.

[88] L. Huang and H.-H. Lee, "A medical data privacy protection scheme based on blockchain and cloud computing," *Wireless Commun. Mobile Comput.*, vol. 2020, pp. 1–11, Sep. 2020.

[89] J. Fu, N. Wang, and Y. Cai, "Privacy-preserving in healthcare blockchain systems based on lightweight message sharing," *Sensors*, vol. 20, no. 7, p. 1898, Mar. 2020.

[90] S. Tanwar, K. Parekh, and R. Evans, "Blockchain-based electronic healthcare record system for healthcare 4.0 applications," *J. Inf. Secur. Appl.*, vol. 50, Feb. 2020, Art. no. 102407.

[91] S. Shamshad, K. Mahmood, S. Kumari, and C.-M. Chen, "A secure blockchain-based e-health records storage and sharing scheme," *J. Inf. Secur. Appl.*, vol. 55, Dec. 2020, Art. no. 102590.

[92] Y. Sharma and B. Balamurugan, "Preserving the privacy of electronic health records using blockchain," *Proc. Comput. Sci.*, vol. 173, pp. 171–180, Jan. 2020.

[93] H. Huang, X. Sun, F. Xiao, P. Zhu, and W. Wang, "Blockchain-based eHealth system for auditable EHRs manipulation in cloud environments," *J. Parallel Distrib. Comput.*, vol. 148, pp. 46–57, Feb. 2021.

[94] M. Usman and U. Qamar, "Secure electronic medical records storage and sharing using blockchain technology," *Proc. Comput. Sci.*, vol. 174, pp. 321–327, Jan. 2020.

[95] H.-A. Lee, H.-H. Kung, J. G. Udayasankaran, B. Kijsanayotin, A. B. Marcelo, L. R. Chao, and C.-Y. Hsu, "An architecture and management platform for blockchain-based personal health record exchange: Development and usability study," *J. Med. Internet Res.*, vol. 22, no. 6, Jun. 2020, Art. no. e16748.

[96] A. Dubovitskaya, F. Baig, Z. Xu, R. Shukla, P. S. Zambani, A. Swaminathan, M. M. Jahangir, K. Chowdhry, R. Lachhani, N. Idnani, M. Schumacher, K. Aberer, S. D. Stoller, S. Ryu, and F. Wang, "ACTION-EHR: Patient-centric blockchain-based electronic health record data management for cancer care," *J. Med. Internet Res.*, vol. 22, no. 8, Aug. 2020, Art. no. e13598.

[97] D. Tith, J.-S. Lee, H. Suzuki, W. Wijesundara, N. Taira, T. Obi, and N. Ohyama, "Application of blockchain to maintaining patient records in electronic health record for enhanced privacy, scalability, and availability," *Healthcare Informat. Res.*, vol. 26, pp. 3–12, Jan. 2020.

[98] Y. Y. Zhao, W. Z. Li, T. Gao, X. Y. Deng, Z. Q. Hai, and X. Zhao, "A multi-layered block chain network for individual-oriented health-care records storage and management," in *Proc. 2nd Int. Conf. Blockchain Technol. Appl.*, Dec. 2019, pp. 64–69.

[99] A. Shahnaz, U. Qamar, and A. Khalid, "Using blockchain for electronic health records," *IEEE Access*, vol. 7, pp. 147782–147795, 2019.

[100] 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.

[101] R. Adlam and B. Haskins, "A permissioned blockchain approach to the authorization process in electronic health records," in *Proc. Int. Multidisciplinary Inf. Technol. Eng. Conf. (IMITEC)*, Nov. 2019, pp. 1–8.

[102] 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.

[103] G. Carter, H. Shahriar, and S. Sneha, "Blockchain-based interoperable electronic health record sharing framework," in *Proc. IEEE 43rd Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, Jul. 2019, pp. 452–457.

[104] J. Huang, Y. W. Qi, M. R. Asghar, A. Meads, and Y.-C. Tu, "MedBloc: A blockchain-based secure EHR system for sharing and accessing medical data," in *Proc. 18th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./13th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2019, pp. 594–601.

[105] H. Guo, W. Li, M. Nejad, and C.-C. Shen, "Access control for electronic health records with hybrid blockchain-edge architecture," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Jul. 2019, pp. 44–51.

[106] M. T. de Oliveira, L. H. A. Reis, R. C. Carrano, F. L. Seixas, D. C. M. Saade, C. V. Albuquerque, N. C. Fernandes, S. D. Olabarriaga, D. S. V. Medeiros, and D. M. F. Mattos, "Towards a blockchain-based secure electronic medical record for healthcare applications," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2019, pp. 1–6.

[107] A. Donawa, I. Orukari, and C. E. Baker, "Scaling blockchains to support electronic health records for hospital systems," in *Proc. IEEE 10th Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf. (UEMCON)*, Oct. 2019, pp. 0550–0556.

[108] X. Liu, Z. Wang, C. Jin, F. Li, and G. Li, "A blockchain-based medical data sharing and protection scheme," *IEEE Access*, vol. 7, pp. 118943–118953, 2019.

[109] A. Buzachis, A. Celesti, M. Fazio, and M. Villari, "On the design of a blockchain-as-a-service-based health information exchange (BaaS-HIE) system for patient monitoring," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jun. 2019, pp. 1–6.

[110] S. Jiang, H. Wu, and L. Wang, "Patients-controlled secure and privacy-preserving EHRs sharing scheme based on consortium blockchain," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2019, pp. 1–6.

[111] B. Toshniwal, P. Podili, R. J. Reddy, and K. Kataoka, "PACEX: PAtient-centric EMR eXchange in healthcare systems using blockchain," in *Proc. IEEE 10th Annu. Inf. Technol., Electron. Mobile Commun. Conf. (IEMCON)*, Oct. 2019, pp. 0954–0960.

[112] 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.
[113] A. R. Rajput, Q. Li, M. T. 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.
[114] X. Yang, T. Li, R. Liu, and M. Wang, "Blockchain-based secure and searchable EHR sharing scheme," in *Proc. 4th Int. Conf. Mech., Control Comput. Eng. (ICMCCE)*, Oct. 2019, pp. 822–8223.
[115] Y. Wang, A. Zhang, P. Zhang, and H. Wang, "Cloud-assisted EHR sharing with security and privacy preservation via consortium blockchain," *IEEE Access*, vol. 7, pp. 136704–136719, 2019.
[116] G. S. Reen, M. Mohandas, and S. Venkatesan, "Decentralized patient centric e-health record management system using blockchain and IPFS," in *Proc. IEEE Conf. Inf. Commun. Technol.*, Dec. 2019, pp. 1–7.
[117] J. Xu, K. Xue, S. Li, H. Tian, J. Hong, P. Hong, and N. Yu, "Healthchain: A blockchain-based privacy preserving scheme for large-scale health data," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8770–8781, Oct. 2019.
[118] 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.
[119] M. Nagori, A. Patil, S. Deshmukh, G. Vaidya, M. Rahangdale, C. Kulkarni, and V. Kshirsagar, "Mutichain enabled EHR management system and predictive analytics," in *Smart Trends in Computing and Communications*. Singapore: Springer, 2020, pp. 179–187.
[120] T. A. Rahoof and V. Deepthi, "HealthChain: A secure scalable health care data management system using blockchain," in *Proc. Int. Conf. Distrib. Comput. Internet Technol.* Bhubaneswar, India: Springer, 2020, pp. 380–391.
[121] M. Shah, C. Li, M. Sheng, Y. Zhang, and C. Xing, "CrowdMed: A blockchain-based approach to consent management for health data sharing," in *Proc. Int. Conf. Smart Health*. Shenzhen, China: Springer, 2019, pp. 345–356.
[122] D. R. Chawdhuri, "Patient privacy and ownership of electronic health records on a blockchain," in *Proc. Int. Conf. Blockchain*. San Diego, CA, USA: Springer, 2019, pp. 95–111.
[123] W.-C. Wu and Y.-C. Wei, "A health information exchange based on block chain and cryptography," in *Proc. Int. Conf. Frontier Comput.* Kuala Lumpur, Malaysia: Springer, 2018, pp. 1985–1990.
[124] B. Shen, J. Guo, and Y. Yang, "MedChain: Efficient healthcare data sharing via blockchain," *Appl. Sci.*, vol. 9, no. 6, p. 1207, Dec. 2018.
[125] L. X. 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.
[126] A. A. Alomar, M. Z. A. Bhuiyan, and A. Basu, S. Kiyomoto, and M. S. Rahman, "Privacy-friendly platform for healthcare data in cloud based on blockchain environment," *Future Gener. Comput. Syst.*, vol. 95, pp. 511–521, Jun. 2019.
[127] 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.
[128] G. Yang, C. Li, and K. E. Marstein, "A blockchain-based architecture for securing electronic health record systems," *Concurrency Comput., Pract. Exper.*, vol. 33, no. 14, p. e5479, 2019.
[129] 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.
[130] 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.
[131] 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.
[132] 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.
[133] 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," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2018, pp. 1–6.
[134] O. Gutierrez, J. J. Saavedra, M. Zurbaran, A. Salazar, and P. M. Wightman, "User-centered differential privacy mechanisms for electronic medical records," in *Proc. Int. Carnahan Conf. Secur. Technol. (ICCST)*, Oct. 2018, pp. 1–5.
[135] 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.
[136] Z. Xiao, Z. Li, Y. Liu, L. Feng, W. Zhang, T. Lertwuthikarn, and R. S. Mong 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.
[137] 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, no. 8, p. 141, Aug. 2018.
[138] 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, p. 156, Aug. 2018.
[139] 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, Jan. 2019.
[140] 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, Aug. 2018.
[141] H. Han, M. Huang, Y. Zhang, and U. A. Bhatti, "An architecture of secure health information storage system based on blockchain technology," in *Proc. Int. Conf. Cloud Comput. Secur.* Haikou, China: Springer, 2018, pp. 578–588.
[142] H. Wang and Y. Song, "Secure cloud-based EHR system using attribute-based cryptosystem and blockchain," *J. Med. Syst.*, vol. 42, no. 8, p. 152, 2018.
[143] 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, Jul. 2018, Art. no. 1847979018790589.
[144] 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.
[145] 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.
[146] M. N. K. Boulos, J. T. Wilson, and K. A. Clauson, "Geospatial blockchain: Promises, challenges, and scenarios in health and healthcare," *Int. J. Health Geographics*, vol. 17, no. 1, pp. 1–10, 2018.
[147] X. Zheng, X. Geng, L. Xie, D. Duan, L. Yang, and S. Cui, "A SVM-based setting of protection relays in distribution systems," in *Proc. IEEE Texas Power Energy Conf. (TPEC)*, Feb. 2018, pp. 1–6.
[148] 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, 2018, Art. no. 1550147718767044.
[149] L. Tzu. (2017). *Matrix Technical Whitepaper*. [Online]. Available: https://www.matrix.io/html/MATRIXTechnicalWhitePaper.pdf
[150] D. E. O'Leary, "Artificial intelligence and big data," *IEEE Intell. Syst.*, vol. 28, no. 2, pp. 96–99, Mar. 2013.
[151] P. Bhattacharya, S. Tanwar, U. Bodkhe, S. Tyagi, and N. Kumar, "BinDaaS: Blockchain-based deep-learning as-a-service in healthcare 4.0 applications," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 2, pp. 1242–1255, Apr. 2021.
[152] S. Dey, "Securing majority-attack in blockchain using machine learning and algorithmic game theory: A proof of work," in *Proc. 10th Comput. Sci. Electron. Eng. (CEEC)*, Sep. 2018, pp. 7–10.
[153] Singularitynet. (2017). *A Decentralized, Open Market and Inter-Network for AIS*. [Online]. Available: https://public.singularitynet.io/whitepaper.pdf
[154] F. Corea. (2017). *The Convergence of AI and Blockchain: What is the Deal*. [Online]. Available: https://francesco-ai.medium.com/the-convergence-of-ai-and-blockchain-whats-the-deal-60c618e3accc
[155] N. Team. *What is Neureal*. Accessed: Feb. 16, 2021. [Online]. Available: https://neureal.net/
[156] A. Awad Abdellatif, L. Samara, A. Mohamed, A. Erbad, C. F. Chiasserini, M. Guizani, M. D. O'Connor, and J. Laughton, "MEdge-chain: Leveraging edge computing and blockchain for efficient medical data exchange," *IEEE Internet Things J.*, vol. 8, no. 21, pp. 15762–15775, Nov. 2021.
[157] K. Gai, Y. Wu, L. Zhu, L. Xu, and Y. Zhang, "Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7992–8004, Oct. 2019.

[158] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, "Integrated blockchain and edge computing systems: A survey, some research issues and challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1508–1532, 2nd Quart., 2019.
[159] P. De Filippi, "The interplay between decentralization and privacy: The case of blockchain technologies," *J. Peer Prod.*, no. 7, 2016. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2852689
[160] P. Dialani. *IoMT Devices are Vulnerable to Cybersecurity Risks*. [Online]. Available: https://www.analyticsinsight.net/iomt-devices-are-vulnerable-to-cybersecurity-risks/

ABDULLAH AL MAMUN is currently a Ph.D. Researcher with the Victoria University of Wellington, New Zealand. He is also working towards designing a proactive honeypot based on artificial intelligence and blockchain-based electronic health records management. His research interests include honeypots, machine learning, cybersecurity, information security, data privacy, and blockchain.

SAMI AZAM (Member, IEEE) is currently a Leading Researcher and a Senior Lecturer with the College of Engineering, IT and Environment, Charles Darwin University, Australia. He has number of publications in peer-reviewed journals and international conference proceedings. His research interests include computer vision, data privacy and security, signal processing, artificial intelligence, and biomedical engineering.

CLEMENTINE GRITTI received the M.Sc. degree in computer science from Grenoble Alpes University, France, in 2012, and the Ph.D. degree in computer science from the University of Wollongong, Australia, in 2016. She is currently a Lecturer at the Computer Science and Software Engineering Department, University of Canterbury. Prior to joining the University of Canterbury last year, she worked at the Norwegian University of Science and Technology, Norway, and at the Graduate School and the Research Center in Digital Sciences Eurecom, France. She previously worked on several research projects dealing with information security and privacy for electronic health and electronic voting. Her current research interests include design and evaluation of public-key cryptographic protocols for security and privacy in various environments, such as cloud computing, the Internet of Things, and blockchain. She has been a Program Chair Member for security conferences, such as the Australasian Conference on Information Security and Privacy and International Conference on Cryptology in India. She has been a Reviewer for various journals, such as IEEE Access, the IEEE Internet of Things, and *Computers and Security* (Elsevier).