ISSN No:-2456-2165

The Blockchain-Based Solution and Applications for EMR: Issues and Challenges

Sohaib Saleem[1, *], Songfeng Lu[2], Imdad Hussain[3], Ubaid Ur Rahman[3], Inam Ul Haq[3], Asif Javed[3]
[1]PhD Scholar, Hubei Engineering Research Center on Big Data Security, School of Cyber Science and Engineering, Huazhong University of Science and Technology, Wuhan, 430074, China
[2]Professor, School of Cyber Science and Engineering, Huazhong University of Science and Technology, Wuhan, 430074, China
[3]Department of Computer Science, University of Okara, Okara, Punjab, Pakistan

Abstract:- Electronic medical records (EMR) are the digital form of the most crucial, sensitive and private healthcare data. The EMR contains both medical and clinical data related to patients. The EMR data is stored to access over the network for multiple stakeholders such as service providers, researchers, vendors, payers, pharmacies, and patients' families, etc. The sharing of EMR records is one of the significant and sensitive portions of the healthcare system to improve the patient's health. The current sharing method of the EMR system is in infancy or insufficient due to centralized storage or proprietorship. This arises the issues and challenges of security, privacy, and interoperability of EMR. The foundation of digital currencies like Bitcoin based on Blockchain is one of the most cutting-edge technologies currently available. The decentralized, immutable, shareable, transparent, and secure record management system provided by Blockchain technology may provide for allowing EMR data to be distributed among various parties without violating security and privacy. So, this paper reviews the blockchain-based solutions for managing and sharing the EMR data. First, we highlight the major issues that are being met by different stakeholders in the healthcare sector. Secondly, we explore the features and opportunities of this technology that can be used to resolve these highlighted issues. Thirdly, the blockchain-based applications need to be identified that have been developed for the EMR healthcare sectors.

Keywords:- *EMR Issues, Blockchain, EMR Blockchain, Systematic literature reviews, Information and Privacy Issues, Information Violations, Privacy Violations, Sharing of Information.*

I. INTRODUCTION

Blockchain technology is a decentralized public ledger or database that is distributed where every transaction is stored and verified anonymously by the nodes of the network [1]. "Satoshi Nakamoto" an anonymous person, designed a peer-to-peer decentralized electronic cash system without involving any third party. The first digital currency named as Bitcoin was introduced by this system in 2008 [1][2].

The evolution of blockchain technology is not restricted to cryptocurrency. Blockchain (BC), the newly born technology, has gained a lot of attention and captivated the rational attraction of domain experts and researchers in several fields including banks, manufacturers, supply chain, Internet of Things, government, education, and healthcare. Blockchain technology combines diverse characteristics of decentralization, immutability, robustness, security, transparency and trustless protocol. It has the potentials to eradicate the current problems of the healthcare sectors [3][4][5].

The current EMR system is not as efficient where the patient can share their medical data with confidence. Because different hospitals and medical sectors are using different programs and systems. Some hospitals are using their EMR system and some are already developed ready-to-use EMR systems [6]. It cannot be connected to access and share the data during the treatment of the patient. In case, if a patient gets sick and traveled or referred to another hospital, then information from their EMR system of the hospital could not be shared [7]. The patient wants to be in charge of their personal information and share it with the specific authorized user as needed. But in the conventional system, the patient lacks confidence in the confidentiality and privacy of his or her personal information [7] [8].

This systematic literature review examines how the blockchain-based EMR system can transform the current healthcare (HC) setup. This study attempts to identify the benefits and opportunities to use the blockchain in an EMR environment for all healthcare players and to identify the developed blockchain-based EMR's applications.

The remainder of the paper is structured into five sections. Section 1 presents the blockchain technology and its importance in electronic medical records. Section 2 explores the literature reviewed for this study and blockchain features present the opportunities which might be envisioned by using blockchain technology to revolutionize the current EMR healthcare system. Section 3 describes the methodology of research as well as sections characterized as; the need for conducting a systematic literature review, motivation and research questions, search strategy, inclusion and exclusion criteria, classification criteria, data extraction. Section 4 discovers the result to answer the formulated research questions. Section 5 describes the threats to the validity of this research. Finally, conclusion and future work are documented.

II. BACKGROUND

This chapter consists of two parts. The first part defines major fundamentals and concept theories of blockchain technology to understand the rest of the paper based on the review studies about blockchain technology.

The second part describes the use of EMR-based blockchains in the healthcare sector and analyzed some blockchain implementations and the existing application of blockchain in EMR healthcare.

A. Blockchain

Blockchain technology works on a consensus algorithm to replace the third-party. Blockchain manages and shares the records in the form of a distributed ledger. Blocks are validated by the consensus of all nodes of the network. Security, auditability, and anonymous transparency are all provided on all the network's permissioned nodes via this chain of blocks joined together using an irreversible hash function [9] [11]. The distributed ledger and the consensus process are the two fundamental components of this distributed ledger technology. The distinction between centralized and distributed ledgers is seen in Figure 1.

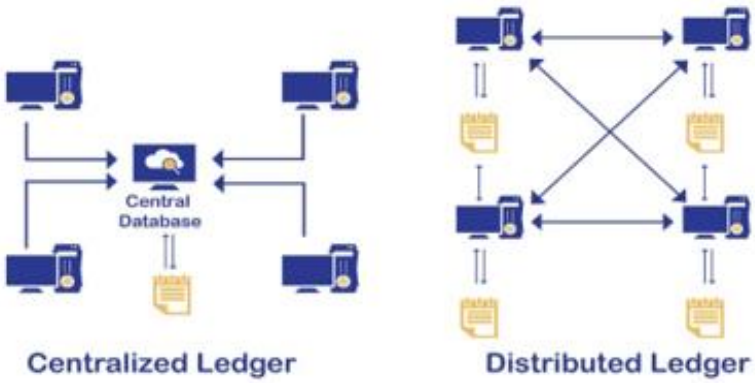

Fig. 1: Centralized vs. Distributed Ledger

B. Use of Blockchain in EMR Healthcare

In the healthcare sector, EMR is the very important aspect of patient care for diagnosis and treatment which needs to be circulated and shared among the different stakeholders e.g.; service providers, payers, pharmacies, researchers, patients' families, etc. [10]. The EMR data can be shared among different stakeholders when the patient is moved or transferred from one hospital to another hospital. The patient can control his/her medical record and grant or revoke access to other parties on the network to achieve security and privacy [9] [10].

Healthcare stakeholders and experts may prefer the blockchain to resolve the issues of security, privacy, data ownership and interoperability of healthcare sectors without the loss or delay of medical data. Blockchain technology can be proved as a game-changer when the multiple parties and healthcare provider generate or share the information in a trusted environment, where intermediaries are no longer required. This technological advantage improves the security and privacy of patient data [12].

The blockchain is using these days in the healthcare sector to overcomes all challenges and issues that are faced by the current EMR system [13]. In this perspective, Dubovitskaya et al. [14] Purposed a framework for maintaining the management of healthcare data and EMR data distribution between different healthcare providers based on the permissioned blockchain technology to achieves security and privacy and can decrease the turnaround time for EMR sharing. This paper also presented the different scenarios of using blockchain application in the healthcare sector such as primary patient care to manage and control the access his data, data aggregation for research purpose to participate in data sharing, connected different healthcare parities using the permissioned blockchain technology for patient care and cost management.

Xia et al. [15] used the permissioned blockchain for a secure and scalable access control system called Blockchain-based Data Sharing (BBDS). By utilizing cryptographic keys and digital signatures, this scalable and secure system safely allows data sharing while safeguarding the confidentiality of EMR data. The users/owners of the data can obtain their own EMR data from the shared pool after verifying and authenticating their cryptographic keys for security reasons in this permissioned blockchain-based data-sharing system.

Zhang et al. [16] Designed the blockchain-oriented architecture for EMR called GAA-FQ (Granular Access Authorization supporting Flexible Queries), which is used for the granularity of authorization of access control scheme for different stakeholder on the EMR system. To achieve a more flexible and accurate granularity for searches and access authorisation, a secure EMR system uses this design. The access authorization method known as GAA-FQ has been developed for secure EMR. It uses authorization, encryption, and decryption algorithms and supports flexible data queries.

McFarlane et al. [7] Implemented a network storage system for peer-to-peer EMR systems based on the blockchain for the Health information exchange (HIE) to achieve interoperability and security. In this paper, the author discovered the patient-provider system for achieving privacy and security according to HIPPA rules and regulations. With the help of this system, the current patient-provider connection may do without the expenses associated with third parties. There are potentials in the system to upgrade the data integrity, reduced costs of transaction, decentralization, and trust. The patientory network [7], a patient-centered protocol supported by blockchain technology, is transforming how healthcare stakeholders handle electronic medical data and effectively communicate with the clinical care team.

C. Compared to Secondary Studies

Blockchain appeared as the backbone of cryptocurrency when the first application bitcoin was launched in 2009. Blockchain is the fastest growing technology that came in the healthcare sector in 2014. In the healthcare department, this technology provides the facilities for the healthcare stakeholders to manage the healthcare data, clinical trials, electronic medical records (EMRs) and electronic health records (EHRs) while upholding the regulatory compliance.

There are only nine secondary studies were shortlisted for comparison, we found that these studies discussed the different attributes of this blockchain technology is the healthcare sector. Table 1 shows the different attributes that have been studied by existing researchers for classifications of its context and also compares to this study. The first attribute is Features and Benefits of BC, which shows that almost all these secondary studies incompletely describe the feature of blockchain technology and as compared to this study. The next attributes are EMR-related issues faced by the patient, opportunities are offered by the blockchain to eradicate these issues and challenges, highlight the blockchain-based EMR applications in the healthcare sector. These attributed did not address in these studies. So, our major goal is to focus on these four attributes (EMR-related issues are faced by the patient, opportunities are offered by the blockchain to eradicate these issues, blockchain-based EMR applications.) as well as we explain the features of blockchain technology.

Table 1: Compared Secondary Studies

Reference	Attributes				
	Features and Benefits of BC in HC	**EMR-related issues faced by the patient**	**Opportunities are offered by the blockchain to eradicate these issues?**	**Identified Blockchain-Based Applications**	**Research Methodology**
Rabah et al. [4],	Incompletely Yes	No	No	No	No
Zhang et al. [5].	Incompletely Yes	No	No	No	No
Arsheen et al. [6]	No	No	No	Yes	No
Boonstra et al. [12]	No	Yes	No	No	Yes
Baysal et al. [13]	Incompletely Yes	No	No	Yes	Yes
Yaqoob et al. [18]	Yes	No	Yes	Incompletely Yes	No
Al Mamun et al. [19]	Yes	No	No	No	Yes
Khatri, S. et al. [20]	Incompletely Yes	No	NO	Yes	Yes
Reegu et al. [21]	No	No	NO	No	Yes
This Study	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**

As earlier discussed, we identified that they only highlight the blockchain technology for healthcare sectors without focusing on the issues as well as the opportunities for Blockchain-based EMR systems did not address. No such study exists until the date that aims is to identify the blockchain-based applications which comprehend the importance of the healthcare sector and its stakeholders in the to revolutionize the ecosystem. Additionally, the results of previous investigations have been extracted using the qualitative research approach. As a result, we created a quantitative research approach using a systematic literature review as opposed to a non-structured review process.

III. RESEARCH METHODOLOGY

The research methodology is the way or technique that is used to solve a research problem(s) systematically. The systematic literature review (SLR) is the type of secondary study that uses any kind of research methodology to collect the data, finding and interprets the gap in the current research to answer the formulated research question. Finding related literature in the field is the primary objective of a systematic literature review. There are many guidelines are available for conducting the SLR. Following the methodology suggested by Barbara Kitchenham [22] and advised by [23] to seek the pertinent research for filling the lacking gap, this SLR was carried out. Figure 2 shows all the processing steps *and their outcomes* of *Barbara Kitchenham* methodology *which are implemented in this study.*

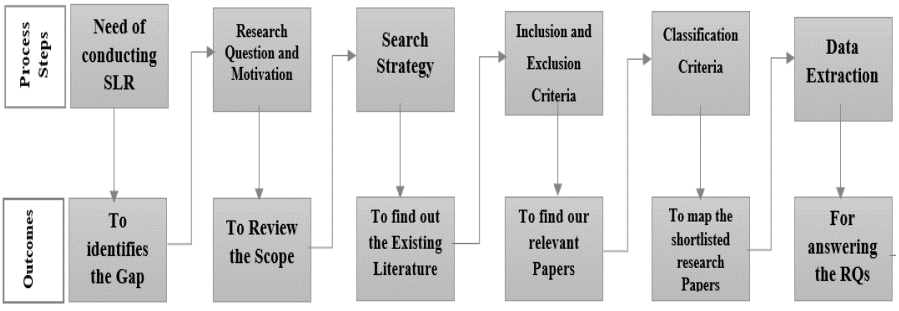

Fig. 2: Implemented Processing Steps of Barbara Kitchenham Methodology

A. Need of Conducting SLR

After scrutinizing the existing secondary studies or literature related to EMR Healthcare, it is identified that some gaps are missing yet (Table I presents) and need to be filled for further consequences. These existing studies only discussed the revolution of blockchain technology in the EMR system of the healthcare sector without focusing on the issues as well as the opportunities for Blockchain-based EMR systems. No such study exists until the date that aims is to highlight and discuss the applications of the EMR system based on the blockchain distributed technology.

Therefore, we are focusing on elaborating on the key characteristics of blockchain technology and the problems that the existing standard EMR system faces. The blockchain provides opportunity to solve these problems and uncover the full potential in the EMR health records system. The primary goals of this study are to pinpoint the blockchain applications that must be thoroughly examined in order to completely transform the EMR record system. Last but not least, compared to past non-structured review research, this systematic literature review employs a broad and exact order of activities to extract the outcomes. Table 1 present the different attributes of secondary studies in accordance with the scope of this study and tells us the gaps in the existing studies that are not filled until now.

B. Research Question and Motivation

The three research questions that guided our work and helped us accomplish the objectives of the systematic literature review are presented in this section. The following research questions are posed and addressed by this SLR. Table 2 present the research questions as well as the main motivation of research.

Table 2: Research Question and Motivation

Sr. #	Research Question	Motivation
1	What EMR-related issues are faced by the patient?	To highlights and address the issues that are faced by the patient in the current EMR system.
2	What opportunities are offered by the blockchain to eradicate these issues?	This research question seeks to explore the benefits and opportunities of this blockchain technology to resolve the highlighted issues and challenges.
3	What Blockchain-Based applications have been developed for EMR?	To highlights the developed Blockchain-Based EMR applications that have been proposed in the scientific literature.

C. Search Strategy

The search strategy is an essential part of conducting a systematic review. After ensuring the research questions, keywords are formulated to find out the relevant existing research work by using the tag-based approach. We used different digital libraries and web source for collecting the primary studies as well as secondary studies. Some of the digital libraries that we used are; IEEE Xplore Digital Library, ACM Digital Library, ScienceDirect (Elsevier), Scopus, and Springer, etc. By using these digital libraries and databases, our purpose was to find and collect only peer-reviewed studies that have been published in authentic and impact factor-based journals, conferences, books, and workshops. The search string; "EMR" AND ("issues*" OR "blockchain*" OR "security and privacy*" OR "health*") is used to find out the relevant literature of our problem statement. Furthermore, we selected Google Scholar Web sources to extend the research. All of the papers—regardless of quality or year of publication—were gathered and explored from multiple journals and conferences.

D. Inclusion and Exclusion Criteria

The next stage was to examine and screen the research papers for relevance after gathering papers from various databases using our search strategy and search methodology. This step's first stage involved screening studies and publications for inclusion based on their titles for relevancy. Based on our research questions, all the primary studies were collected and shortlisted that containing our targeted keywords especially; "EMR Issues, Electronic Medical Records issues, EMR Blockchain, Electronic Medical Records blockchain, and EMR Privacy and Security".

For inclusion purposes, after reading and analyzing the title and abstract of each study we concluded that only 26 primary studies were considered for data gathering that is relevant to our context i.e.: EMR Issues, Electronic Medical Records issues, EMR Blockchain. Table 3 presents the primary papers with corresponding Paper #, Authors, Publication year, Use cases, and Publication type/channel. Remaining studies were discarded because they were irrelevant or out of context to our specified criteria or did not include our searched keywords in their title or abstract.

Shortlisted papers whose title are not matched to our search strategy or research question was discarded. From them, some of the papers or studies were discarded that were not related to the EMR and blockchain technology in the healthcare industry.

At last, by applying the following exclusion criteria, we discarded the received set of results:

- Papers are written in other languages than English.
- Master and doctoral dissertations.
- Duplicated articles obtained from Google Scholar.
- Studies that are not peer-reviewed, such as surveys, interviews and press releases.
- Studies without full manuscript accessibility. Main emphasis are not correlated to our motivation such as EMR and blockchain for EMR system.

E. Classification Criteria

The objective of this research is to discuss the issues of the current EMR health system and the potential of blockchain technology for the EMR system, the blockchain-based EMR applications. Nominated studies were classified according to research questions. This step was planned to map the

shortlisted research paper into the classification criteria. We now provide the chosen paper's classification criteria. The papers that were selected for shortlisting were grouped into various classes or categories based on the search strategy and keywords. Each nominated and included paper was read in depth after being grouped into distinct classes, and if the text or content of the paper is relevant to our context, then these papers fulfill our classification criteria.

Table 3: Primary Papers with Corresponding Information

Paper #	Authors	Publication Years	Publication Channel	Use Case
1	Xia et al. [15]	2017	Journal	Data Sharing
2	Yue et al. [41]	2016	Journal	Privacy
3	Zhang et al. [16]	2018	Conferences	Access Control
4	Dubovitskaya et al. [14]	2018	Journal	Security and Sharing
5	Jiang et al. [52]	2018	Conference	Healthcare Information Exchange
6	Liu et al. [8]	2018	Conference	Privacy Sharing
7	McFarlane et al. [7]	2017	Journal	Data Storage
8	Azaria et al. [9]	2016	Conference	Data Access and Permission
9	Ahram et al. [48]	2017	Conference	Managing and Access Control
10	Kim et al. [39]	2017	Journal	Trusted Data Sharing
11	Xia et al. [34]	2017	Journal	Data Sharing
12	Chen et al. [38]	2019	Journal	Data Sharing
13	de Oliveira et al. [45]	2019	Conference	Security
14	Fan et al. [50]	2018	Journal	Secure Medical Data Sharing
15	Li et al. [36]	2018	Journal	Data Preservation
16	Ito et al. [35]	2018	Conference	Privacy
17	Rifi et al [42]	2017	Conference	Data Access
18	Rouhani et al. [43]	2017	Conference	Security
19	Ananth et al. [47]	2018	Journal	Security
20	Xiao et al [40]	2018	Conference	Sharing and Management
21	Zhang et al. [51]	2018	Journal	Security
22	Chen et al. [56]	2021	Journal	Security, Sharing, Storage
23	Zaabar et al. [53]	2021	Journal	Security and Privacy
24	Sadeghi et al. [57]	2022	Journal	Secure Health Management Information Systems
25	Karmakar et al. [54]	2023	Journal	Data Storage, Integrity
26	Pawar, V., & Sachdeva [55]	2023	Journal	Scalability

F. Data Extraction

After labeling the relevant studies, this phase is used for extracting and recording the required information from the selected studies that are used for answering the formulated questions through this SLR paper. Data were extracted from the literature primarily focusing on the EMR Issues, EMR Blockchain, and Electronic Medical Records Blockchain, EMR Privacy, and Security. Furthermore, we explored these studies to find the key benefits of blockchain technology in the EMR environment. The following criteria are used to extract the data from studies:

- Primary information from shortlisted studies (i-e; publication title and authors)
- Information associated with the study (main contribution, objective)
- Results (issues that have been addressed, benefits of blockchain technology for EMR in HC)

The information data from the labeled research article were retrieved during this final stage of the systematic literature review process in order to conduct a meta-analysis and respond to the established research question.

IV. RESULTS

This chapter explains the research questions that are defined in section 4. The first research question of this study is to highlights and addresses the issues that are faced by the patient in the current EMR system. The second research question seeks to highlight the opportunities that are offered by the BC for EMR. The next research question is to identify the Blockchain-Based applications that have been developed for electronic medical records.

A. What EMR-related issues are faced by the patient?

The healthcare sector consists of multiples players creating the ecosystem i-e patients, providers, payers, supply chain bearers and research institutes, governments, that is using the EMR records of patients without the permission or consent of the patient [17]. Each stakeholder creating multiple issues while storing, sharing or management of data in the area of concern. These records contain all the medical history of the patient throughout the medical system. So, the idea of centralizing all the medical records or information of EMR was revolutionized in the healthcare sectors. But the control of the current centralized EMR system is in the hand of third-party providers or players which creating numerous issues and challenges [18] [24]. Existing literature was

collected and analyzed to gather results is to rectify the issues that are facing by the patient in the current EMR system. These issues are discussed below:

➢ *Privacy and Confidentiality*

The EMR data of the patient is the most sensitive, private and confidential asset of patient care, thus the leakage of this data might hurt the patient reputation and money. Because this data is scattered and stored among the multiple servers or computers over the network [25]. Secondly, the existing scenarios of EMR systems in the healthcare sectors are developed on centralized architecture which is controlled by a single authority that is more vulnerable to privacy and confidentiality [26].

Multiple healthcare stakeholders need to access or share the medical information of patients without any modification. The unauthorized users' access might break the patient reputation and hurts the quality of care by using his/her data, so the audit trail of data access may cause the breakage of confidentiality [6]. EMR data and access to medical data to other parties on the network should be control by the patient to achieve privacy and confidentiality [27].

The medical data of any patient is vulnerable to misuse by those people who are taking profit from this data. For example, some pharmaceutical companies buying and selling the patient data to the research companies without the acknowledgment of patient, which create privacy issues. The World privacy forum warns that electronic medical data is more sensitive and private to the patient, especially when this data is stored on the central system [28].

The medical information always should be shared or exchanged only with the permission of the patient. When the patient is unable to shares their data, then the authorized representatives or the guardians of the patient share the information [29]. The primary way to preserve confidentiality is to allow the only authorized users to access personal information. This may lead to privacy and confidentiality [30]. To achieve this goal, the United States Department of Health and Human Services (HHS) created the rules and guidelines related to sharing and access control of patient data. According to HHS, the patient has access and control over their medical data. This may guarantee the privacy and confidentiality of patient health data [31].

The Health Insurance Portability and Accountability Act (HIPAA) privacy rules are used to define the restrictions or guidelines to bound or restrict the companies or service providers to fulfill the law related to the privacy of patient's data especially when they share the data between different parties. This HIPAA rule classifies the four fundamental parties that have access rights to access the medical information of patients i-e: health care providers, insurers, health claims clearinghouses, and business associates [29] [31].

➢ *Data Security*

Electronic medical records are open to threats and potential misuse due to a large amount of sensitive healthcare data stored in the central data center of the hospital which is vulnerable to security [28]. From the last few years, hundreds of thousands of patients have been compromised on their medical data because of the violation of security at hospitals, insurance companies, and different government healthcare organizations. This EMR data is also vulnerable to misuse by those people who are seeking to profit from these data by selling or buying doctor's prescribing data to the research organizations or pharmaceutical companies [25] [28].

The storage or accessing of EMR data system facing the issues [28] [31] these days are:

- Alteration or modification of patient data and destroying the medical data without the involvement of patients through the hacking.
- Misuse of EMR records by the unauthorized users of the system, whose motive is to hurt or destroy the patient reputation.
- Management of data takes extra time by the legacy EMR system which may lead to insecurity.
- Government institution creates the disturbance of private healthcare data.

During the treatment process of individuals, the patient, as well as physicians or doctors are uncertain about the secure storage of EMR records [28] [32]. They are in stress about the data that may be unauthorized users access the private medical data of the patient which creates a serious problem related to patient reputation and trust in the doctors.

The security of the EMR's data contains the integrity, availability, and confidentiality of the information that needs to ensure. So, to ensure the availability, confidentiality, and integrity of private information is a very challenging task [26].

➢ *Lack of interoperability or Data Sharing Limitation*

One of the biggest and major issues of electronic medical records is the lack of interoperability or data sharing limitations between similar or dissimilar kinds of systems. To check the medical's history of the patient, the system must communicate efficiently or effectively with each other during the treatment [28] [33].

The medical records of EMR data are scattered or fragmented in silos form on the different systems, so the communication among these systems is difficult because these data are located on different sides. If the patient moved or referred from one hospital or physician to another, then the patient needs to access their medical data from the previous hospital but the systems of EMR are not mutually connected for effective communication, so there are the biggest issues is lack of interoperability. In another scenario, some hospitals or providers don't want to share data from their system, even though the owner of this data is patient and cannot share their data when they want [33].

In healthcare sectors, another reason of the lack of interoperability is that the healthcare organizations use their independent different infrastructure (i.e.; protocols, OS, programming language, databases, software, etc.) to store the medical data, which arise the problems of interoperability and availability of patient medical data among the different stakeholders [34].

Different providers of EMR use their EMR management tools or take the services of already developed EMR systems from the other vendors. Different vendors use different environments, tools, hardware software, protocols, procedures, operating system, so the interoperability between a different kind of EMR hardware or software cannot be user-friendly for the patient [6] [7].

So, non-interoperability can cause a lack of coordination and communication among healthcare stakeholders in traditional systems. The poor or lack of coordination or communication among the different medical stakeholder results in the lack of quality care of the patient because patient themselves is not considered as data owner for sharing their data among the different healthcare providers.

- *Interruption of the Physician-Patient Relationship*

The physician-patient relationship creates interaction problems during the medication or treatment of the patient [7]. According to literature, 92% of the physicians or doctors feel the disturbance or to avoid the use of the EMR system when they communicate with their patients. The main reason behind the problem of the physician-patient relationship is that the physicians use the legacy system to store the data during the diagnosis of the patient which disturbs the communication [31]. These legacy systems or computer for EMR data storage is time-consuming especially when they are using the computer during the diagnosis and maybe the physicians have limited computer skills [26]. These legacy systems are less user-friendly or some physician has no computer skills for using the menus or system [12].

- *Lack of Availability of EMR data*

The availability of EMR's data depends upon the proper coordination and communications between the system. Because the system of the EMRs is primarily designed and developed for patient treatment and patient care [31].

According to the survey that occurred in 2010, a 50% EMR system is the physician's office-based that worked including under the fully difficult and different level of functionality [12]. So, the availability of patient medical data, prescriptions, history, treatment, and diagnosis data will be valuable for the patient and doctors if the data is delivered and shares at the same time of needs. In the healthcare department, the main factors which create the problem of the availability of EMR data for the different healthcare providers are the administrative decisions, legacy system, physical equipment, and technology [26].
The availability, integrity, security, privacy of sensitive information are very challenging or serious issues while sharing the information.

B. What Opportunities are Offered by the Blockchain to Eradicate these Issues?

Blockchain has seemed a decade before in computing whereas it came within the healthcare sector in 2014 with the start of the non-financial version of the technology. Researchers are found eager to get aware of this distinctive technology to grasp the potentials and challenges to extract the supreme benefits [35]. It is envisaged that EMR embedded with blockchain technology can exhibit healthcare intellect to plan better outcomes for patient care as it is the sole purpose of the whole ecosystem to serve humanity [36]. Some EMR health blockchain opportunities are the highlight for a specific demand of users to show the potentials of this emergence.

These opportunities are grouped below by its uses:

- *Data Exchange*

Blockchain decentralized technology used to solve the issues of incompatible scattered and fragmented medical records of a patient that are stored over the multiple locations on the network [37] [39]. This technology has the potentials to resolve the issue of medical data sharing by using the distributed ledger and improved the patient quality of care and coordination among the different parties of the EMR systems [38] [40]. This coordinated and synchronized structure of blockchain technology will improve real-time communication for the diagnosis, treatment, information sharing, latest health notifications, as well as the history of the patient [41].

On the ledger of blockchain technology, all the nodes are connected in a decentralized manner, and when the patient wants to share the information from one point to another, then-latest information is shared by giving the authorization access [40] [36] to the particular physicians of the patient. Moreover, this technology help to avoiding the single point of failure, because the multiple copies of patient data are available every time on different nodes [42]. So, the interoperability features of blockchain provide a more suitable and reliable environment for the information sharing of the patient when they need to share the information [38] [16] [34].
The shared immutable ledger is used for the information sharing in which once the records are stored, after that the information does not delete [39].

- *Decentralization*

In the healthcare sector, the different distributed medical stakeholders are located on the multiples site needs a decentralized management system for data storage [43]. Decentralization feature is the backbone of the blockchain technology [36] [34]. To highlight or resolved the issue of data management for healthcare, blockchain technology is the perfect solution for the decentralization management system for all the stakeholders [16]. In this nature of blockchain-based EMR healthcare systems, different providers, patients or other medical stakeholders can access the same health records because the multiple copies of each data lakes distributed over the multiples nodes of the network [13].

So, health data management is the basic needs of every healthcare sectors, which requires a lot of resources in terms of human resources and technical or computer resources [44].

Therefore, this technology is based on decentralization, which means there is no central or third party to store or manage the health data of the patient [41]. Decentralized data management can communicate the providers and patients more efficiently and productively [35]. The same information

or data can be shared and update the data in real-time, this feature can also increase the fraud detections and trace the counterfeit drugs [40]. Moreover, this blockchain technology for EMR management has the potential to transform the current costly and expensive management system into an easy and inexpensive system [37].

- *Improved Data Security and Privacy*

The security of patient medical data kept on the EMR system is generally improved by the immutability features of blockchain technology. Because the blockchain ledger is an immutable record of transactions, it is impossible to change the records once they have been put there. [35] Any modifications made to block are irreversible and permanent. Any modifications, whether significant or not, are permanently recorded in a new block [39].

With immutability, once the patient medical data or information stored on the ledger of the blockchain, it cannot be corrupted, altered or changed [37] [43]. If any malicious user or attackers want to access or destroy the data then it is impossible for them, because at the same time there are multiple healthcare nodes are connected within the ledger that contains the copy of data [41]. They immediately received the notification if anyone wants to alter the data [34]. Because every information recorded on the blockchain is time-stamped, encrypted, and added in chronological order. So, the beauty of these features is, data is stored in an appended form, which means it cannot be altered or changed [42] [45].

On the other hand, the patient data stored on blockchain by using the cryptographic keys and digital signatures that help to protect the identity and privacy of the patient. The patient controls their medical data including the latest information as well as the history of the data. If any medical stakeholder wants to access the patient data, then he/she need to take the grants of the intended data from the patient [46] [47].

Therefore, immutability promotes the blockchain as auditable and tamper-resistant.

- *Health Data Ownership*

Patient medical data controlled by the central party in the centralized environment of the traditional healthcare system. [34]. But the patient needs to control their data, to control the access of their data [43], sharing or exchange their data. The patient needs to ensure that their medical records, as well as medical history, are not accessed or misused by unauthorized users or other medical stakeholders [45].

By using the strong cryptographic encryption methods and digital signature with BC which are defined by the smart contract, the ownership of data is in the hand of the patient [36]. The smart contract is programmable computer code that is stored inside the blockchain and is activated and executed automatically when the necessary conditions are met. It is unnecessary to rely on a central authority or organization to carry out the contract when using a smart contract and the blockchain [9]. The execution of a contract between untrusted parties is made possible by smart contracts built on blockchain technology. The public key or private is signed to the healthcare providers by the patient with the appropriate access or permission for accessing the data [39] [43].

The secure patient-controlled access of data is sure by applying the consensus mechanism and cryptographic methods in blockchain distributed technology through the only private key of the specific user can decrypt the data [9]. The patient has the right and ability to grant and revoke access to other stakeholders (researchers, providers, and payers) in the EMR system.

- *Availability and Robustness*

Once the data is stored on the ledger of the blockchain networks, it is shared and replicated to every other node that exists on the network, so the availability of the health data of EMR stored on the blockchain is certain [36] [41]. On the blockchain network, there are multiple nodes present at the same time, if one node is down, at the same time the information should be accessible from other nodes means there is no single point of failure on the system of blockchain networks. Storage or existence of data at the same time on the multiples nodes must be guarantees that the availability of the data from any of the nodes because the data is distributed among every node on the network, so there is no chance of single point of failure on the system of EMR medical system [38] [45].

- *Transparency and Trust*

For the EMR environment, blockchain is an open and transparent technology that creates and ensures the trust even with the untrusted parties over the system. The transparency and openness nature of blockchains provides a trustworthy EMR environment among the distributed healthcare applications [47]. This feature of blockchain technology enables the applications of healthcare stakeholders accepted in a different area. The blockchain-based system for the EMR environment enhanced the transparency of data with end to end details of data storage and data access [36] [47].

After embedded the transparency feature of blockchain in electronic medical records, the healthcare sector becomes more transparent, efficient and removes the chances of fake or fraudulent activities with the patient data. in the supply chain of the health EMR system, everything is transparent to all the parties over the network [49].

The transparent system makes the system would be accessible or approachable to every node or parties that are involved in the network, no matter which type of electronic medical records they use [39]. So, this feature provides a trustworthy environment as well as achieve high security and transparency by using this system [16]. Also, the sharing of data among the nodes, origin of the data, history of the data, location of the data, circulation of counterfeit drugs or fake medicines recommended by providers to the patient on the network can be traceable and transparent to everyone.

Additionally, a blockchain based system's feature of data transparency can assist us in tracking down activities and stopping the distribution of fake drugs [38].

C. What Blockchain-Based Applications have been Developed for EMR?

Multiple applications of blockchain from the different areas have been proposed till the date in scientific studies. However, not all of these applications have been interpreted in the working environment. It is therefore important to address the real-world implementation of blockchain-based EMR healthcare applications from the literature. So, this research question helps to highlight the EMR applications and identify the areas where there are some research gap and that missing gap need to shift research focus to those areas.

- *BPDS [8]*

[8] Purposed a blockchain-based privacy-preserving data sharing method for the EMR system, named BPDS that is used for securely storing the EMR data on the cloud storage and indexed are created of this data using the tamper-proof consortium blockchain. The patients can have complete control over their EMRs or users for achieving security and privacy. By using the predefined access permission, sharing of data can be secure through the smart contract of the blockchain. The CP-ABE-based access control mechanism and the content extraction signature (CES) scheme in BPDS used to share the data selectively and protect the patient's privacy during the sharing of data.

- *MedRec [9]*

[9] The purposed decentralized record management system of EMRs using blockchain technology for atheization and data sharing among the multiples stakeholders, so-called MedRec. This platform provides the immutable and easy access approaches for patients to save their medical records and can also grant and revoke permissions to their data with confidentiality and accountability as the records are not stored on the blockchain instead pointers to the data storage locations, logs and permissions are only stored in this blockchain. The medical stakeholder takes incentive as rewards after participating on the network as a miner for verifying and securing the network through the proof of work on this platform.

- *MedShare [34]*

MedShare is also a blockchain-based EMR application that offers the data provenance, access control and data auditing of shared medical data in cloud repositories. MedShare monitors all activities of data sharing and transitions from one entity to another entity and recorded in a tamper-proof manner. Moreover, this application tracks the data access by applying the smart contract and access control mechanism in the subject to address the issues of medical data sharing. [34] proposed this application in a cloud environment for the purpose to exchange the medical data among the different medical custodians such as research and medical institutions with minimal risk to data privacy. The consensus nodes withing this system would be responsible for processing the request of data exchange and then broadcasting the data in the form of blocks into the blockchain network without the violation of data privacy.

- *DPS [36]*

A blockchain-based data preservation system (DPS) also implemented on the Ethereum platform for medical data, developed by [36]. The developed DPS system provides the temper proof secure storage to guarantee the verifiability and primitiveness of stored data, maintain the validity and integrity of data, preserving the privacy of the patient. This system uses the proof of primitiveness of data with blockchain that can detect the data tempering and can validate whether the current data is similar to original data or not. On the other hand, DPS uses the cryptographic hashing algorithm and storage mechanism to offer anonymity for the protection of sensitive data from being leaked or stolen by unauthorized parties.

- *HealthChain [48]*

The blockchain-based EMR application is HealthChain, which is implemented by permissioned and private blockchain on the IBM Bluemix platform using Hyperledger Fabric. The blockchain technology with the modular architecture of Hyperledger enables the HealthChain to achieves the confidentiality, security, and scalability of health data. This application using the Practical Byzantine Fault Tolerance (PBFT) consensus algorithm for the Protected Health Information PHI between healthcare network providers and mobile devices within the network. HealthChain also integrates the smart contracts to control the permissions and access rights on the blockchain network.

- *Ancile [49]*

Ancile is a blockchain-based framework proposed by Dagar et al. [49]. Ancile used the Ethereum blockchain's smart contract in the aforementioned case to fully offer the patient with access control, security, privacy, and interoperability of electronic medical records. This framework using the six types of smart contract i-e; consensus protocols, services history, permissions contract, classification, ownerships, and re-encryption. Using the smart contract, patient checks and control the access permission of their private data. Furthermore, the beauty of this framework is that patient transfer and grant or revoke the permission from one node to another node using the cryptographic hashes of medical records and query links.

- *MedBlock [50]*

MedBlock is another blockchain-based EMR application for secure information management to share the sensitive electronic medical records among authorized users which are proposed by Fan et al. [50]. The basic purpose of MedBlock is to handle the patient's information to solve the problems of data management and data sharing. The distributed ledger of MedBlock plays an important role for the authorized user to access and retrieval of EMRs effectively and efficiently. The ledger's retrieval system makes it simple for users to get involved and actively look for the information they need. The EMR data's privacy and security are ensured by the straightforward and efficient access control encryption technique, preventing the leakage of patients' sensitive information. Besides, this system uses the access control consensus protocol and cryptographic method to achieve high information security and achieve the consensus of EMR without much consumption of energy.

- *FHIRChain [51]*

The Health Level Seven International (HL7) group created the Fast Healthcare Interoperability Resources framework, often known as FHIRchain [51], for transferring clinical data to improve healthcare interoperability and efficiency. The Office of the National Coordinator for Health Information Technology's (ONC) roadmap's requirements for scalable and secure clinical data sharing, network node verification and authentication, and data source permissions are all addressed by the blockchain-based application FHIRchain. A decentralized app (DApp) based on FHIRchain that employs digital health identities and keys to authenticate and validate all participants and data access authorizations is also designed and shown by the author Zhang et al. [51] of this study. Also, this DApp used to support the healthcare interoperability for the patient clinical records for efficient data sharing.

- *BlocHIE [52]*

BlocHIE is yet another blockchain-based healthcare information exchange (HIE) system that has been put up by Shan et al. [52]. BlocHIE uses EMR-Chain and PHD-Chain to handle the difficulties of storing and exchanging electronic medical records (EMRs) and personal healthcare data (PHD). Two loosely coupled blockchains, EMR-chain and PHD-Chain, are utilized to store and manage the EMR and PHD records separately on the network. The EMR chain maintains the data produced by the hospital, and the PHD chain provides the patient with access to that data. In order to meet the needs of storing and exchanging medical data, various chains are utilized.

- *HealthBlock [53]*

HealthBlock is a blockchain-based platform for decentralized healthcare management. The suggested approach combines blockchain technology with IoT medical devices to produce an efficient and secure RPM (Remote patient monitoring) and EHR (Electronic Health Record) management. Using the concept of decentralized storage and a permissioned blockchain network as an access control system to manage patient vital signs data, the architecture of the recommended system was built. The proposed solution addresses security issues through resistance to a variety of well-known cyberthreats, including spoofing attacks using fabric certificates, tampering threats due to the usage of cryptographic techniques, and repudiation threats using fabric digital signature. The decentralization approach, which consists of a decentralized blockchain network, a decentralized Offchain database (OrbitDB with IPFS), and a decentralized Remote Patient Monitoring application, aims to address centralized security issues.

- *ChainSure [54]*

On an Ethereum test network, ChainSure, a proposed conceptual insurance model based on smart contracts, has been put to the test. We automate the entire operation by utilizing the potential of blockchain. Blockchain guarantees the system's accuracy and security. Since data is unchangeable and visible, there are less opportunities for cyberattacks on the ChainSure network. Data collecting and administrative tasks are particularly difficult and time-consuming in the traditional paradigm. The proposed system ends reliance on a single authority. Data are dispersed among all full nodes in the blockchain; therefore, it can withstand single points of failure. In the ChainSure system, network congestion has a significant impact on transaction speed; as a result, the slower the rate, the more participants or nodes there are. Private keys owned by individuals may provide a point of risk from a security standpoint in a decentralized setup. Once created during the creation of a wallet, they permit access to all data that has been stored. If it is stolen, it puts important data and digital currency at risk. Access to the wallet is permanently lost if it is lost.

- *ParallelChain [55]*

A new system that balances energy economy and scalability for managing healthcare data. In terms of the quantity of messages sent and received as well as processing efficiency, ParallelChain outperforms the consensus algorithms of Bitcoin, Bitcoin-NG, and Algorand. Network overhead, too. A more effective consensus technique is utilized in place of the Bitcoin's energy-intensive PoW consensus system. The ParallelChain is resistant to denial-of-service attacks, forks, and monopolistic issues. The quantity of data transfer, processing time, and the number of messages exchanged were all greatly increased by changing the consensus technique and the structure.

V. THREATS TO VALIDITY

Our major intention of conducting this SLR study is to highlight the EMR applications that are developed on the blockchain network in the healthcare domain. After analyzing the existing studies of blockchain-based EMR, we tried to gather as many primary studies for the extraction of data. But this emerging field in his initial stages, researchers are discovering its applications and very eagerly, so the threat of this study is that, related studies may be published in the future which is not presented and added here in the process of publication.

As the purposed research was in the investigated stages, therefore no peer-reviewed literature was found in this area, so might any type of work-related to this study to be published until the publication of this study. Our data extraction scenario based on the formulation of RQs so might be possibilities that researcher or reader find some points that we did not consider and can be helpful in the future. Also, the threat is that no quality score is used for the collection or gathering of primary studies as well as secondary studies which may consider the less quality result and synthesis.

VI. CONCLUSION

Blockchain technology is an emerging technology that extended its applications from financial to non-financials fields such as IoT, Governance, Education, Agriculture, and Healthcare, etc. In the traditional EMR healthcare system, the patient data is in the control of third-party or providers and scattered or fragmented among the several repositories. This situation has negatively affected on patient’s reputation and finance because of the leakage of his/her security and privacy. At the same time, interoperability among healthcare stakeholders remains a serious challenge.

The features of blockchain technology such as decentralization, immutability, transparency, smart contract, auditability is used with the EMR system to overcome the security, privacy and interoperability issues of patient data. So, the EMR health system in healthcare sectors is implemented in a more distributed and trustless way after the adoption of blockchain.

In this research, we pay attention to collect all the possible relevant primary literature to highlight the blockchain-based EMR system in the healthcare area that enables the users or stakeholders to share, access or store the patient data in a secure, private and auditable way to revolutionize the ecosystem. We got and investigated 28 primary studies from different scientific databases and web sources. This paper also presented the issues of the current EMR system after mapping the existing primary studies related to the EMR health system. Furthermore, we identified the blockchain-based applications that have been developed for EMR records of the patient. As future work, we plan to extend this work by finding the challenges and limitations of blockchain technology that is being faced by different healthcare stakeholders after the emergence of this technology in the EMR system.

REFERENCES

[1.] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

[2.] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). An overview of blockchain technology: Architecture, consensus, and future trends. In 2017 IEEE International Congress on Big Data (BigData Congress; pp. 557-564). IEEE.

[3.] Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain technology overview. arXiv preprint arXiv:1906.11078.

[4.] Rabah, K. (2017). Challenges & opportunities for blockchain powered healthcare systems: A review. Mara Research Journal of Medicine and Health Sciences, 1(1), 45-52.

[5.] Zhang, P., Schmidt, D. C., White, J., & Lenz, G. (2018). Blockchain technology use cases in healthcare. In Advances in Computers (Vol. 111, pp. 1-41). Elsevier.

[6.] Arsheen, S., & Ahmad, K. (2021, November). SLR: A systematic literature review on blockchain applications in healthcare. In 2021 International Conference on Information Science and Communications Technologies (ICISCT) (pp. 1-6). IEEE.

[7.] McFarlane, C., Beer, M., Brown, J., & Prendergast, N. (2017). Patientory: A Healthcare Peer-to-Peer EMR Storage Network v1. Entrust Inc.: Addison, TX, USA.

[8.] Liu, J., Li, X., Ye, L., Zhang, H., Du, X., & Guizani, M. (2018, December). Bpds: A blockchain based privacy-preserving data sharing for electronic medical records. In 2018 IEEE Global Communications Conference (GLOBECOM; pp. 1-6). IEEE.

[9.] Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016, August). Medrec: Using blockchain for medical data access and permission management. In 2016 2nd International Conference on Open and Big Data (OBD; pp. 25-30). IEEE.

[10.] Kamau, G., Boore, C., Maina, E., & Njenga, S. (2018, May). Blockchain Technology: Is this the Solution to EMR Interoperability and Security Issues in Developing Countries? In 2018 IST-Africa Week Conference (IST-Africa; pp. Page-1). IEEE.

[11.] Casino, F., Dasaklis, T. K., & Patsakis, C. (2018). A systematic literature review of blockchain-based applications: current status, classification and open issues. Telematics and Informatics.

[12.] Boonstra, A., & Broekhuis, M. (2010). Barriers to the acceptance of electronic medical records by physicians from systematic review to taxonomy and interventions. BMC health services research, 10(1), 231.

[13.] Baysal, M. V., Özcan-Top, Ö., & Betin-Can, A. (2023). Blockchain technology applications in the health domain: a multivocal literature review. The Journal of supercomputing, 79(3), 3112-3156.

[14.] Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., & Wang, F. (2017). Secure and trustable electronic medical records sharing using blockchain. In AMIA Annual Symposium Proceedings (Vol. 2017, p. 650). American Medical Informatics Association.

[15.] Xia, Q., Sifah, E., Smahi, A., Amofa, S., & Zhang, X. (2017). BBDS: Blockchain-based data sharing for electronic medical records in cloud environments. Information, 8(2), 44.

[16.] Zhang, X., & Poslad, S. (2018, May). Blockchain support for flexible queries with granular access control to electronic medical records (EMR). In 2018 IEEE International Conference on Communications (ICC; pp. 1-6). IEEE.

[17.] Tama, B. A., Kweka, B. J., Park, Y., & Rhee, K. H. (2017, August). A critical review of blockchain and its current applications. In 2017 International Conference on Electrical Engineering and Computer Science (ICECOS; pp. 109-113). IEEE.

[18.] Yaqoob, I., Salah, K., Jayaraman, R., & Al-Hammadi, Y. (2021). Blockchain for healthcare data management: opportunities, challenges, and future recommendations. Neural Computing and Applications, 1-16.

[19.] Al Mamun, A., Azam, S., & Gritti, C. (2022). Blockchain-based electronic health records management: a comprehensive review and future research direction. IEEE Access, 10, 5768-5789.

[20.] Khatri, S., Alzahrani, F. A., Ansari, M. T. J., Agrawal, A., Kumar, R., & Khan, R. A. (2021). A systematic analysis on blockchain integration with healthcare domain: scope and challenges. IEEE Access, 9, 84666-84687.

[21.] Reegu, F. A., Abas, H., Jabbari, A., Akmam, R., Uddin, M., Wu, C. M., ... & Khalaf, O. I. (2022). Interoperability Requirements for Blockchain-Enabled Electronic Health Records in Healthcare: A

Systematic Review and Open Research Challenges. Security and Communication Networks, 2022.
[22.] Kitchenham, B. (2004). Procedures for performing systematic reviews. Keele, UK, Keele University, 33(2004), 1-26.
[23.] Yaqoob, S., Khan, M. M., Talib, R., Butt, A. D., Saleem, S., Arif, F., & Nadeem, A. (2019). Use of blockchain in healthcare: a systematic literature review. International journal of advanced computer science and applications, 10(5).
[24.] Lu, Y. (2018). Blockchain and the related issues: a review of current research topics. Journal of Management Analytics, 5(4), 231-255.
[25.] Anderson, J. G. (2000). Security of the distributed electronic patient record: a case-based approach to identifying policy issues. International Journal of Medical Informatics, 60(2), 111-118.
[26.] Bensefia, A., & Zarrad, A. (2014). A proposed layered architecture to maintain privacy issues in electronic medical records. E-Health Telecommunication Systems and Networks, 3(04), 43.
[27.] Mashima, D., & Ahamad, M. (2012, January). Enhancing accountability of electronic health record usage via patient-centric monitoring. In Proceedings of the 2nd ACM SIGHIT International Health Informatics Symposium (pp. 409-418). ACM.
[28.] Benaloh, J., Chase, M., Horvitz, E., & Lauter, K. (2009, November). Patient controlled encryption: ensuring privacy of electronic medical records. In Proceedings of the 2009 ACM workshop on Cloud computing security (pp. 103-114). ACM.
[29.] Ozair, F. F., Jamshed, N., Sharma, A., & Aggarwal, P. (2015). Ethical issues in electronic health records: A general overview. Perspectives in clinical research, 6(2), 73.
[30.] Zaghloul, E., Li, T., Mutka, M., & Ren, J. (2019). $ d $-MABE: Distributed Multilevel Attribute-Based EMR Management and Applications. arXiv preprint arXiv:1904.11432.
[31.] Richards, M. M. (2009). Electronic medical records: Confidentiality issues in the time of HIPAA. Professional Psychology: Research and Practice, 40(6), 550.
[32.] Zaghloul, E., Li, T., Mutka, M., & Ren, J. (2019). $ d $-MABE: Distributed Multilevel Attribute-Based EMR Management and Applications. arXiv preprint arXiv:1904.11432.
[33.] Schwarz, C., & Schwarz, A. (2014). To adopt or not to adopt: A perception-based model of the EMR technology adoption decision utilizing the technology-organization-environment framework. Journal of Organizational and End User Computing (JOEUC), 26(4), 57-79.
[34.] Xia, Q. I., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., & Guizani, M. (2017). MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. IEEE Access, 5, 14757-14767.
[35.] Ito, K., Tago, K., & Jin, Q. (2018, October). i-Blockchain: a Blockchain-empowered individual-centric framework for privacy-preserved use of personal health data. In 2018 9th International Conference on Information Technology in Medicine and Education (ITME; pp. 829-833). IEEE.
[36.] Li, H., Zhu, L., Shen, M., Gao, F., Tao, X., & Liu, S. (2018). Blockchain-based data preservation system for medical data. Journal of medical systems, 42(8), 141.
[37.] Chen, Y., Ding, S., Xu, Z., Zheng, H., & Yang, S. (2019). Blockchain-based medical records secure storage and medical service framework. Journal of medical systems, 43(1), 5.
[38.] Chen, W., Mu, Y., Liang, X., & Gao, Y. (2019, July). Medical Data Sharing Model Based on Blockchain. In Journal of Physics: Conference Series (Vol. 1267, No. 1, p. 012014). IOP Publishing.
[39.] Kim, K. J., & Hong, S. P. (2017). A trusted sharing model for patient records based on permissioned Blockchain. J. Int. Comput. Service (JICS), 6, 75-84.
[40.] Xiao, Z., Li, Z., Liu, Y., Feng, L., Zhang, W., Lertwuthikarn, T., & Goh, R. S. M. (2018, December). EMRShare: A Cross-Organizational Medical Data Sharing and Management Framework Using Permissioned Blockchain. In 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS; pp. 998-1003). IEEE.
[41.] Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. Journal of medical systems, 40(10), 218.
[42.] Rifi, N., Rachkidi, E., Agoulmine, N., & Taher, N. C. (2017, October). Towards using blockchain technology for eHealth data access management. In 2017 Fourth International Conference on Advances in Biomedical Engineering (ICABME; pp. 1-4). IEEE.
[43.] Rouhani, S., Butterworth, L., Simmons, A. D., Humphery, D. G., & Deters, R. (2018, July). MediChain TM: A Secure Decentralized Medical Data Asset Management System. In 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData; pp. 1533-1538). IEEE.
[44.] De Aguiar, Erikson Júlio, Bruno S. Faiçal, Bhaskar Krishnamachari, and Jó Ueyama. "A Survey of Blockchain-Based Strategies for Healthcare." ACM Computing Surveys (CSUR) 53, no. 2 (2020): 1-27.
[45.] de Oliveira, M. T., Reis, L. H., Carrano, R. C., Seixas, F. L., Saade, D. C., Albuquerque, C. V., ... & Mattos, D. M. (2019, May). Towards a Blockchain-Based Secure Electronic Medical Record for Healthcare Applications. In ICC 2019-2019 IEEE International Conference on Communications (ICC; pp. 1-6). IEEE.
[46.] Yang, J., Onik, M. M. H., Lee, N. Y., Ahmed, M., & Kim, C. S. (2019). Proof-of-Familiarity: A Privacy-Preserved Blockchain Scheme for Collaborative Medical Decision-Making. Applied Sciences, 9(7), 1370.

[47.] Ananth, C., Karthikeyan, M., & Mohananthini, N. (2018). A secured healthcare system using private blockchain technology. J. Eng. Technol, 6, 42-54.
[48.] Ahram, T.; Sargolzaei, A.; Sargolzaei, S.; Daniels, J.; Amaba, B. Blockchain Technology Innovations. In Proceedings of the 2017 IEEE Technology & Engineering Management Conference (TEMSCON), Santa Clara, CA, USA, 8–10 June 2017; pp. 137–141.
[49.] Dagher, G.G.; Mohler, J.; Milojkovic, M.; Marella, P.B.; Marella, B. Ancile: Privacy-Preserving Framework for Access Control and Interoperability of Electronic Health Records Using Blockchain Technology. Sustain. Cities Soc. 2018, 39, 283–297.
[50.] Fan, K., Wang, S., Ren, Y., Li, H., & Yang, Y. (2018). Medblock: Efficient and secure medical data sharing via blockchain. Journal of medical systems, 42(8), 136.
[51.] Zhang, P.; White, J.; Schmidt, D.C.; Lenz, G.; Rosenbloom, S.T. FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data. Comput. Struct. Biotechnol. J. 2018, 16, 267–278
[52.] Jiang, Shan, Jiannong Cao, Hanqing Wu, Yanni Yang, Mingyu Ma, and Jianfei He. "Blochie: a blockchain-based platform for healthcare information exchange." In 2018 ieee international conference on smart computing (smartcomp), pp. 49-56. IEEE, 2018.
[53.] Zaabar, B., Cheikhrouhou, O., Jamil, F., Ammi, M., & Abid, M. (2021). HealthBlock: A secure blockchain-based healthcare data management system. Computer Networks, 200, 108500.
[54.] Karmakar, A., Ghosh, P., Banerjee, P. S., & De, D. (2023). ChainSure: Agent Free Insurance System using Blockchain for Healthcare 4.0. Intelligent Systems with Applications, 200177.
[55.] Pawar, V., & Sachdeva, S. (2023). ParallelChain: a scalable healthcare framework with low-energy consumption using blockchain. International Transactions in Operational Research.
[56.] Chen, M., Malook, T., Rehman, A. U., Muhammad, Y., Alshehri, M. D., Akbar, A., ... & Khan, M. A. (2021). Blockchain-Enabled healthcare system for detection of diabetes. Journal of Information Security and Applications, 58, 102771.
[57.] Sadeghi R, J. K., Prybutok, V. R., & Sauser, B. (2022). Theoretical and practical applications of blockchain in healthcare information management.