Received: 2 February 2019 | Revised: 27 April 2019 | Accepted: 16 May 2019 | Published on: 1 July 2019

DOI: 10.1002/spy2.83

SURVEY PAPER

WILEY

Review on "Blockchain technology based medical healthcare system with privacy issues"

Arijit Saha | Ruhul Amin | Sourav Kunal | Satyanarayana Vollala | Sanjeev K. Dwivedi

Computer Science & Engineering, DR SPM International Institute of Information Technology, Chattisgarh, India

Correspondence
Ruhul Amin, Computer Science & Engineering, DR SPM International Institute of Information Technology, Chattisgarh, India.
Email: amin_ruhul@live.com

Healthcare has been the industry with the highest boom in terms of both revenue and data. With so much of electronic health records, the security has been the need of the hour. To make this critical information more secure, there has been an urge to use the blockchain technology. Therefore, researches came up with a solution of blockchain technology in medical healthcare that will not only protect data from being tampered but will also ensure that the data leakage is stopped. This technology could preserve data and thus guarantee reliability. And if this technology is used along with cloud computing technology, problems related to storage can also be vanished, because cloud is trusted for storing and managing data. Also, the blockchain can address the security issues of the cloud. Indeed, medical data sharing and storing with Blockchain-based cloud can address a lot of issues of medical data. The main aim of this paper is to present the current state-of-the-art on blockchain-based medical healthcare system. We have clearly discussed several existing works on the same domain and also presented a comparative study among the published works.

KEYWORDS
architecture, blockchain, healthcare system, security

1 | INTRODUCTION

Medical care has been an indispensable part of our lives and so the medical data, for example, prescriptions, previous medical records has also become a vital part for patient's diagnosis and for further proceedings. Traditionally, medical data were recorded on paper, which were prone to get damaged and modified. Therefore, it was necessary to preserve the data electronically. However, the medical database could be tampered or deleted permanently. Then, there was also a concern on information blocking. Information blocking occurs when an entity, for example, a person may be with or without his intention to access the data which should not have been seen without the patient's or hospital's concern.[1] Technology always plays a very significant role if it is about enhancing the quality or about resolving issues such as resource allocation along with information blocking, here in medical-care data sharing technology needed to be evolved with time. Generally, patients may have a lot of service providers in terms of medical healthcare that include general physicians or specialists or even therapists. Since a disease could be because of the previous disease,[2] so they all need to share health record securely without any manipulation. Patient need not be always a professional or to have a good memory to remember all the data properly if all the data are stored and shared securely. Patients need to keep updating their own medical data history. According to the Fundamental Right to Life and Liberty under Article 21 and freedom of expression and movement under Articles 19(1)(a) and (b) of the Constitution of India, a patient has right to consult or get transferred to another hospital for his treatment. Now, again it is patients' wish to share his data. Also, if a hospital wants to share his data for research there must be consent from the patient. Again, if consent is also there then the data transferring process takes a lot of time. Moreover, if the data that are transferred are in paper mode or even through

email, there is time, speed, storage, and security issues. Storing data in a database has many limitations such as storage and prone to cyber-attacks. Attackers may intrude into the system and get some patient's sensitive data. One can also not rely upon a centralized database because practically different access controls for different users, searching procedure over an encrypted channel, large memory for medical data storage etc. is difficult. Also, Al Omar et al[3] discuss various problems that occur when data are stored in an encrypted format. Access to a distributed ledger for sharing of medical data in a transparent manner can guarantee data security[4] as bitcoin was thought to be secured for transaction. Since this is used for medical data, patient should be prioritized. A patient purpose centric access model should be designed. Also, every record of a patient cannot be made public and it should be flexible,[1] where the patient should know which data are being provided to the insurance company and which data are to be provided to blood bank, etc.

Therefore, researches came up with a solution of blockchain technology in medical healthcare, which will not only protect data from being tampered but will also ensure that the data leakage is stopped. This technology could preserve data and thus guarantee reliability. And if this technology is used along with cloud computing technology,[5] problems related to storage can also be vanished, because cloud is trusted for storing and managing data. Also, the blockchain can address the security issues of the cloud. Indeed, medical data sharing and storing with Blockchain-based cloud can address a lot of issues of medical data. Furthermore, this technology can be implemented in the wearable device of the patient keeping his information.[6] Patient's body will be scanned for the biometric signature. This signature will be required while scanning of this wearable device embedded with IoT technology, where data are stored for further analysis. Also, wireless mobile technology is developing, Telecare Medical Information Systems can be used more and more, which can help track the patients and their data.[7] This location can help track those patients suffering from chronic disease or an infectious disease etc. This telemedical data can also be manipulated or destroyed by the attackers. Again, the blockchain comes into picture when we discuss about confidentiality and privacy of the patients' data, while data sharing through the telemedical technology.

2 | BLOCKCHAIN BACKGROUND STUDY

Blockchain or a ledger for transaction was proposed by Nakamoto et al[8] as a decentralized cryptocurrency in a distributed manner. This technology guarantees that an adversary or an attacker cannot intrude into the database.[9] His model worked as a permissionless model where leaving and joining of the node was flexible without any apriori knowledge of consensus nodes. Out of several consensuses to manage the ledgers Santoshi adopted proof-of-work (POW),[10] which is now also used by several other cryptocurrencies. Main consideration of this POW is the speed in which the transactions are processed. So, the speed transaction tradeoffs should be secure in blockchain.[11] Chain of digital signatures was used to define an electronic coin. Each coin is transferred by its owner to another by signing digitally a hash of its previous transaction with the public key of the next owner and finally adding it to the end of this coin. A trusted third party, that is, central authority checks each transaction so that double spending can be stopped. After each transaction, these coins were required to be submitted to the central authority who then issues a fresh new coin as described in Figure 1. Hash-cash[12] initially was used to tackle the unmetered resources of the Internet such as email which is now also used in bitcoin.

Since the company or the party who is providing the coin knows all the data and can even manipulate the data, so for this problem Santoshi proposed a Timestamp Server concept. This timestamp server takes the hash of all the entities that are to be timestamped and broadcasts the hash. So, every timestamp has the hash of its previous timestamp and forms a chain. Let us take an instance that an attacker generates a chain that is faster than an honest chain. Still, the attacker cannot take the money

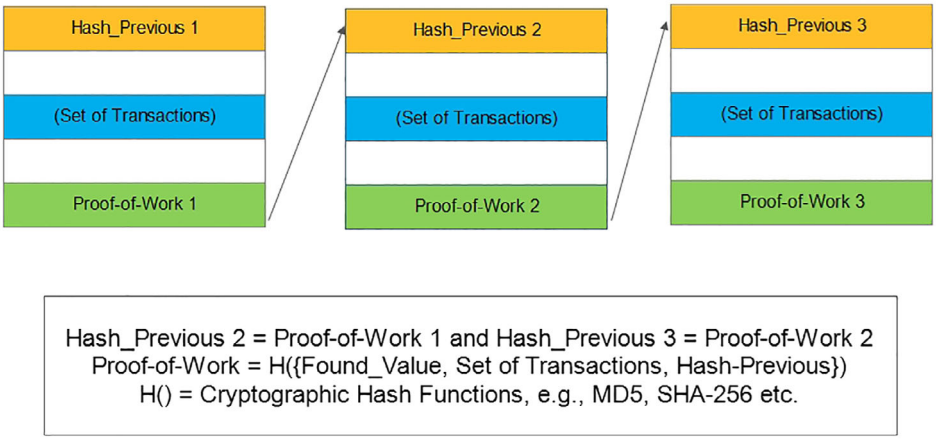

FIGURE 1 Uses of cryptographic hash function in blockchain

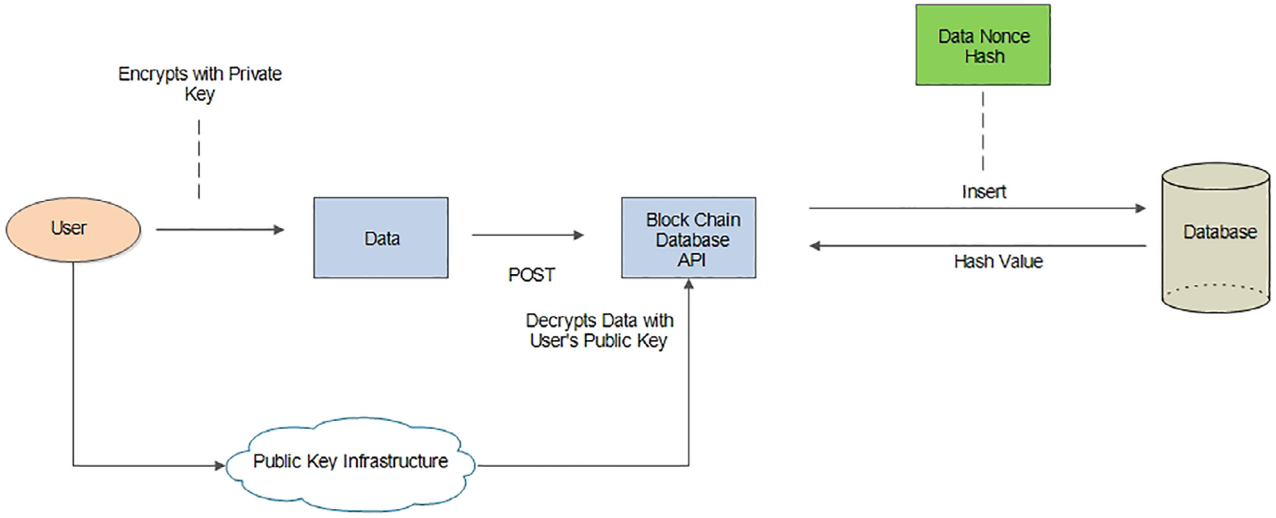

FIGURE 2 Typical blockchain diagram

because nodes do not accept payment if there is an invalid transaction and node will then not be accepted by the honest node. All these nodes work in coordination, can join, leave, and even rejoin the network. Also, malicious nodes can be detected by using the clustering protocol.[13] So, we can sum up all the features of Blockchain[14] as follows:

- *Decentralized*. It is the main feature of blockchain that it does not rely upon centralized node.
- *Transparent*. All the data that are stored are secured and transparent to all the nodes.
- *Open-source*. Anyone can use this blockchain technology to create any application.
- *Autonomous*. In blockchain, every block can update or transfer its own data securely.
- *Immutable*. Since records in blockchain will be stored forever and cannot be changed.
- *Anonymous*. Blockchain to be anonymous, it successfully maintains trust between node-to-node.

Blockchain should not be restricted only to the financial sector, it should be extended beyond bitcoin,[15] for public healthcare[16] and many more applications.[17] Blockchain-based medical system is an emerging topic. All the medical data that are created to be credible needs to be verifiable and untampered. Patient or his family members or a researcher or even any user who requires the data should be able to verify that the data are correct. Several researchers are merging various other technologies with blockchain technology to make their specific zone secured for sharing data. Several researchers have embedded blockchain with other technology such as Tian [5] used radio frequency identification with blockchain in the field of agri-food supply chain tracing. Blockchain, cloud technology along with IoT,[18,19] blockchain in smart contracts,[20,21] blockchain in vehicular ecosystem,[22] etc. The basic architecture of blockchain is shown in Figure 2.

3 | RELATED WORKS

Healthcare has been the industry with the highest boom in terms of both revenue and data. With the growing needs of the healthcare industry, there has also been the need to secure the data. With so much of electronic health records (EHR), the security has been the need of the hour. With better facilities, data sharing is almost required aspect of the healthcare industry. The informations related to patients and all other relevant things have slowly drifted toward cloud storage. To make this critical information more secure, there has been an urge to use the blockchain technology. We have given a tree model for the history of medical blockchain technology in Figure 3 for better understanding.

3.1 | Azaria et al[1]

The authors faced an urgent need to digitize the records in the healthcare industry on top of security and privacy of patient's data. To incorporate innovation in the field of the healthcare industry, they proposed a system to oversee the healthcare data using the blockchain technology. In their work, they achieve authentication, confidentiality, and accountability for the required data sharing. They made convenient and adaptable architecture to integrate the data with the local, existing data storages. Their

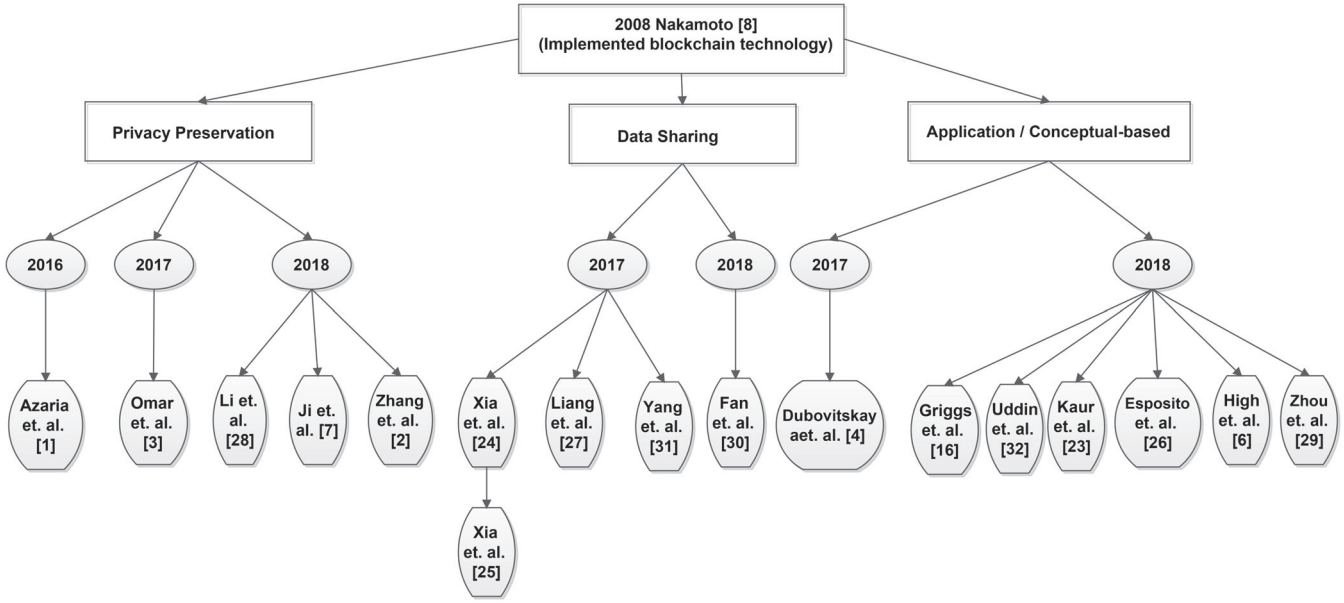

FIGURE 3 Tree model of state-of-the-art of blockchain-based medical system

framework considers the researchers, public health authorities, medical stakeholders to participate in the system as blockchain miners. The system proposed by the authors gives secure access to the medical history of all the patients. This makes sure that the patients are being taken in confidence as now they are fully aware of their own medical history, also if any changes made to it. Proper permission management has been implemented in the proposed system which checks on what type of data will be shown to which blockchain miners. A connection has also been done with the existing data storage infrastructure. The system can take input data from various sources such as physician offices, hospital servers, etc. The proposed system achieves the decentralization of medical records in a secured manner. Their framework used the smart contract mechanism and POW–based consensus algorithm to validate a new block in their blockchain-based system.

3.2 | Kaur et al[23]

The authors discussed healthcare data as an important asset and so there is an urgent requirement to effectively store such data with secure techniques. Data in the healthcare are very heterogeneous, which proved to be a challenge for the researchers. So, this needs to be overcome. They thought that if the blockchain technology and Cloud environment are used together, this problem can overcome to an extent. They proposed a blockchain-based platform that can store and manage huge healthcare data with ease, accuracy and also providing security for the data stored. Currently, all healthcare data are stored on centralized servers. The authors have proposed an architecture that ensures decentralization. This has the data in a distributed environment, which would also increase the interoperability. Here, the files are fragmented, where if any transaction happens it gets stored on the various nodes. In this proposed architecture, after the user requests for a transaction, an identity check of the user is being done using cryptographic techniques. After the user has been verified by the system, a new block on the existing blockchain gets added about the transaction that is being made. Then, the user is provided with the required information needed. The proposed architecture by the authors has been given in Figure 4.

3.3 | Xia et al[24]

The authors suggest that the privacy of the medical data is almost on top priority because it endangers to breach the patient's condition. If this breach happens, it impacts all the patients, stakeholders, and the miners negatively. To avoid such a situation, the authors propose a blockchain-based framework to protect the autonomy of data using a cloud environment. The proposed framework only allows verified users or stakeholders to access a system. The actions of the users can be monitored by the proposed blockchain-based framework. Sharing of patient's data is verified, by adopting the cryptographic techniques. The system is a mediator between users and sensitive healthcare data. The system proposed by them used a lightweight blockchain that ensures fast transactions and proper efficiency. The authors have kept the communication and the authentication protocols as a further study. The authors have kept three layers here, namely, user layer, system management layer, and the storage layer. The user

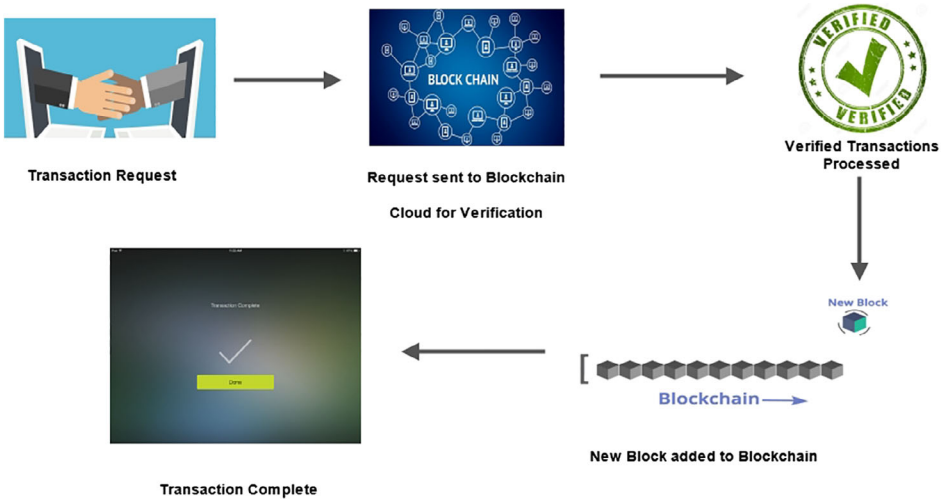

FIGURE 4 Proposed architecture by Kaur et al[23]

layer consists of all those entities or the blockchain miners who will try to access or request the data. The system management is the central and the most important layer where all connections are established for secure transactions. The last layer, that is, the storage layer consists of the entire data which are being securely stored on the cloud for further diverse applications.

3.4 | Xia et al[25]

The authors suggest that there is a tremendous amount of risk involved with the healthcare data as if malicious activities are performed on the data it can cause severe damage to revenues and activities involved. The current methods involved to protect the privacy of the data are not sufficient and also not efficient. The authors proposed a system named, MeDShare, which ensures authenticity, accountability, and efficiency to the healthcare data in a blockchain-based framework using the cloud repositories. The system monitors every user accurately to ensure there are no malicious activities. In this system, the data sharing records are stored in a tamper proof way. This system has the minimal risk to the healthcare data. The system proposed by the authors consists of four layers to provide proper data privacy and security. These are, namely, user layer, data query layer, data provenance and structuring layer, and existing database infrastructure layer. The user layer consists mainly various entities or blockchain miners who want to access the blockchain data and request to make a transaction. The next layer, the data query layer usually processes and forwards the different query it receives from the various blockchain miners. This layer has two components, Querying layer, which processes the requests and queries, and trigger, which acts as a mediator between the real world and the blockchain. The next layer, data provenance and structuring layer, has five components, namely, authenticator, processing, and consensus nodes, Smart contracts, smart contracts permissioned database, and blockchain network. The last layer, existing database infrastructure layer, contains the already existing data.

3.5 | Dubovitskaya et al[4]

The authors suggest that healthcare information is very sensitive and critical, and sometimes, the health information needs to be shared among the various shareholders for their special purposes. To achieve the above-mentioned issue, they proposed a blockchain-based health management system, which ensures trust, accountability, and transparency in health information. A framework has been designed, keeping in mind cancer-affected patients. The prototype of the framework ensures that security, privacy, and also reduce the turnaround time for healthcare data sharing. The proposed system consists of membership service databases for medical data storage, nodes, and various application programming interfaces (APIs). The membership service has the functionality to verify the various users or the blockchain miners who are accessing the data in the blockchain system. Here, if a doctor tries to request any query, first the profile will be verified using symmetric key encryption pair and authorizing digital signatures. A similar process is observed while verifying the various users. The entire sensitive healthcare data are stored on two databases, namely, a local database and a cloud server. The local database contains cancer-related data and the cloud server usually contains organized categorical data. All these data are encrypted with the symmetric key pair, which vary from patient to patient. Access to the data depends on what type of access control has been defined by the patients. Entire performance evaluation has been done by the authors on the grounds of privacy, security, and scalability. The proposed architecture by the author has been given in Figure 5.

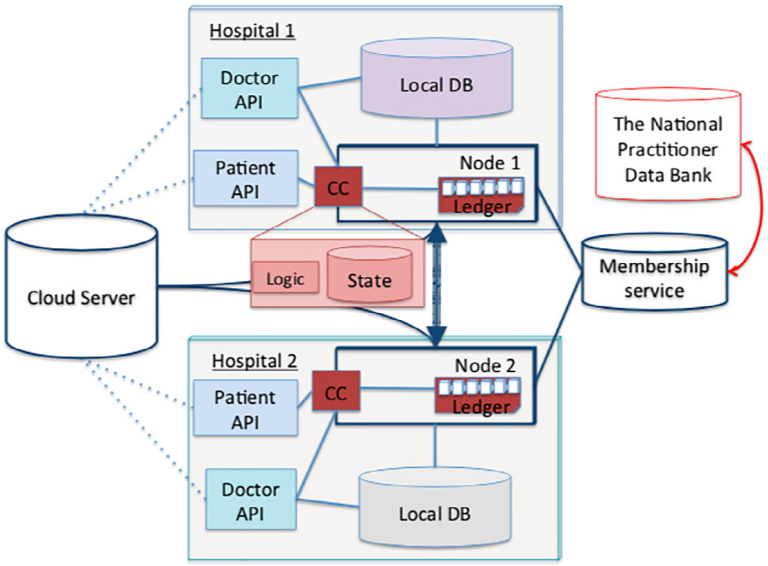

FIGURE 5 Proposed architecture by Dubovitskaya et al[4]

3.6 | Esposito et al[26]

The authors observed that there is a significant shift of the healthcare data to the cloud services. But these mechanisms may not be so secure in terms of data security and privacy. The authors use the blockchain technology to provide security and privacy to the healthcare data. The proposed architecture by the authors to provide privacy and security in the domain of healthcare data management consists of various users who are patients and wants their medical data to get stored on the blockchain. Whenever a new patient is added, a new block gets added on the existing blockchain architecture. The blocks are connected with each other and have a distributed and decentralized network. Every block in the existing blockchain has a timestamp which gets verified with cryptographic mechanisms and also contains the hash information of the previous block. The key benefits that the authors have using this proposed system are: - avoiding single point of failure, patients have the right to access over their own data, the entire healthcare data are easy to access, secure, distributed, and efficient, any illegal changes made to the blockchain data will be easily detectable and identified.

3.7 | Omar et al[3]

The authors believe that the cyber attackers have a specific interest toward the healthcare data as it involves huge revenue. The author suggests that the property of decentralization can make the healthcare a bit more secure. So, they have implemented this by proposing a healthcare data management system using the blockchain technology as it supports accountability and integrity. Anonymity is ensured by protecting the patient data with different cryptographic mechanisms. The protocol proposed by the authors has various entities and roles in it. Data sender layer plays an important role, it takes in all the medical-related data of the user and encrypts it using the cryptographic mechanisms and preserves it. It also checks whether the data or information entered by the user is correct or not. The data receiver layer will be authenticating the system and then receive the data from the users. Next is the registration unit, which has the responsibility to store the credentials of all the new users who want to access data from the system. This unit will store the identity, password, and biometric informations of the users. After entering the credentials for one time, the user just has to log on through the secured channel for making any transaction. Private accessible unit is the layer where two parties can interact and flow of data can take in terms of a transaction through the secured channel. It acts as a mediator unit that serves as a bridge between the user and the sensitive data stored in the existing blockchain. The blockchain returns an identifier that helps user to access the requested data.

3.8 | Liang et al[27]

The authors believe that mobile and wearable technology play a crucial role, in improving the quality of healthcare services, also there should be a secure mechanism to share healthcare data. The authors have noticed that privacy issues in the medical healthcare data, for both storage and sharing of it. So they proposed a user-centric system, using the blockchain technology, which is decentralized and accountable. They proposed mobile application that synchronized with the wearable devices. They used the tree-based method and batching method to ensure performance scalability. The authors have tried to propose a user-centric

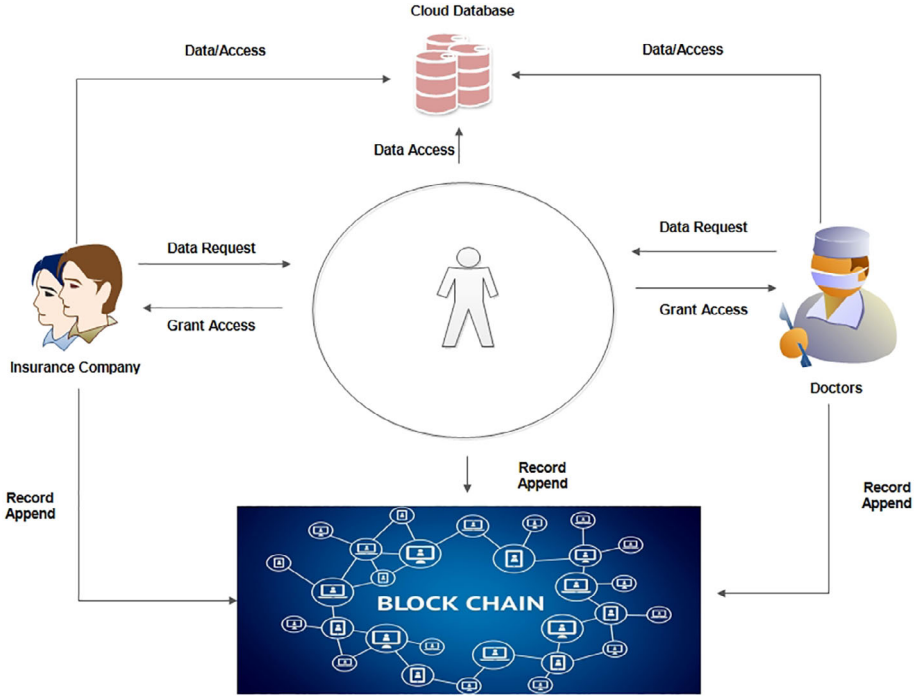

FIGURE 6 Proposed architecture by Liang et al[27]

system to implement the security and privacy of the healthcare data using the blockchain technology. They used six entities to implement the system. Starting with the user, it gives the input of the various health-related data using wearable devices. These devices closely keep a check on the heartbeat rate, walking speed and distances, sleep timings, etc. Such sensitive healthcare data get uploaded on the cloud using the wearable devices. The user has all the access rights on these data. When the patient's needs treatment, they can easily share their stored medical records with the doctors. Next entity is the wearable device that serves as an interface to store and display, all the information that gets timely stored. Whenever any new data get uploaded, at the same time, the blockchain also updated immediately, which provides efficiency of the proposed system. Healthcare provider is the next layer, which is responsible to store the patient's treatment data. Next layer is the health insurance layer, which gets access to the treatment data with proper verification techniques. The blockchain layer is the one which stores the entire data in the form of the blocks and updates itself whenever new data get added. The last entity is the Cloud database that consists of all the transactions in the form of user queries, requests. The proposed architecture by the author has been given in Figure 6.

3.9 | Nakamoto et al[8]

The concept of the blockchain technology first came out in a white paper reported by Nakamoto et al,[8] which rectifies the challenges that were faced by the crypto currencies. The author proposed a technology so that the transaction could be securely completed. Due to this major development, different domains across the globe have preferred blockchain technology over other existing technologies to share and store data securely and also ensure trust, accountability, authenticity, integrity, and anonymity. To incorporate innovation in the field of healthcare industry, they proposed a system to handle all the healthcare data using the blockchain technology. Their proposed system had the required authentication, confidentiality, and accountability for the required data sharing. They made convenient and adaptable architecture to integrate the data with the local, existing data storages. Their proposed system would take into consideration the researchers, public health authorities, and blockchain miners. A blockchain-based framework is introduced to protect the autonomity of the data using a cloud environment. The proposed system only allows verified users or stakeholders to access. The actions of the users can be monitored by the proposed blockchain-based framework, which ensure accountability. The data sharing is verified using the cryptographic techniques.

3.10 | High et al[6]

The authors proposed a unique method to access the patient information that could not be communicated but can be stored securely on wearable device using blockchain. The information of the patient will be stored using encrypted private key and public key. The private key can be decrypted only by the patient's biometric signature. Using a combination of the public and the private key, the critical records of the patient can be accessed in emergency situations only. The authors have proposed an

architecture that ensures decentralization. This has the data in a distributed environment, which would also increase the interoperability. Here, the files are in fragmented manner, where the transaction happens and then gets stored on the various nodes. In this proposed architecture, after the user requests for a transaction, an identity check of the user is done using cryptographic techniques. After the user has been verified by the system, a new block on the existing blockchain gets added about the transaction that is being made. The system monitors every user accurately to ensure that there are no malicious activities. In this system, the data sharing records are stored in a tamper proof way. This system has minimal risk to the data related to the healthcare. The system acts as a mediator between users and sensitive healthcare data. The system proposed by the authors uses a lightweight blockchain that ensures fast transactions. This has also made sure a perfectly secure system with proper efficiency. The authors have kept the communication and the authentication protocols as a part of further study.

3.11 | Li et al[28]

The authors expresses that healthcare has been an essential space in the lives of individuals, which includes the storage of high measures of data. It has sensational effects in the lives of individuals. Be that as it may, this data can be effectively altered or stolen by the attackers which will result in wrong diagnosis and tremendous misfortune in income. In this way, the authors proposed a blockchain-based information preservation framework that guarantees solid stockpiling of information and furthermore gives protection to the users utilizing the blockchain architecture. This framework ensures user security utilizing cryptographic calculations. So, they have implemented this system on a platform named Ethereum. It provides effective and efficient performance results. It gives successful and proficient execution results. The proposed architecture by the authors to provide privacy and security in the domain of healthcare data management consists of various users who are patients and wants their medical data to get stored on the blockchain. Whenever a new patient is added, a new block gets added on the existing blockchain architecture. The blocks are connected with each other and have a distributed and decentralized network. Every block in the existing blockchain has a timestamp which gets verified with cryptographic mechanisms and also contains the hash information of the previous block. The system monitors every user accurately to ensure that there are no malicious activities. In this system, the data sharing records are stored in a tamper proof way. This system has the minimal risk to the healthcare data.

3.12 | Ji et al[7]

The authors believe that patients' location these days is a significant viewpoint while thinking about the mobile healthcare technologies. However, it has difficulties of security and protection. Thus, the authors have proposed a multilevel blockchain-based location sharing scheme. This guarantees total dependability, assurance, decentralization, and realness of the location of the patient. The performance evaluations of the above scheme are efficient and effective for the real life implementation. The protocol proposed by the authors has various entities and roles in it. Data sender layer plays an important role, it takes in all the medical-related data of the user and encrypts it using the cryptographic mechanisms and preserves it. It also checks whether the data or information entered by the user are correct or not. The data receiver layer will be authenticating the system and then receive the data from the users. Next is the registration unit, which has the responsibility to store the credentials of all the new users who want to access data from the system. This unit will store the identity, password, and biometric information of the users. After entering the credentials one time, the user just has to log in through the secured channel for making any transaction. Private accessible unit is where two parties can collaborate and stream of information can take in terms of an exchange through the verified channel. It acts as a mediator unit that serves as a bridge between the user and the sensitive data stored in the existing blockchain. The blockchain returns an identifier that helps user to access the requested data. The proposed architecture by the author has been given in Figure 7.

3.13 | Zhou et al[29]

The authors propose a blockchain-based medical insurance storage system. Because of the decentralization and credibility property of the blockchain, it is exceptionally successful for the users. The stakeholders of this framework are patients, emergency clinics, insurance agencies, and the servers. This framework guarantees legitimate information check likewise the framework requires exceptionally less memory and CPU. This has been actualized on the Ethereum platform and accordingly the performance evaluation has been done. The authors have kept three layers here, namely, user layer, system management layer, and the storage layer. The user layer consists of all those entities or the blockchain miners who will try to access or request the data. The system management is the central and the most important layer where all connections are established for secure transactions. The last layer, that is, the storage layer consists of the entire data which are being securely stored on the cloud

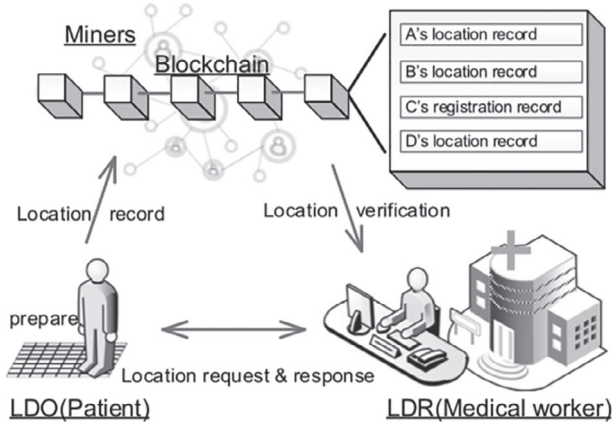

FIGURE 7 Proposed architecture by Ji et al[7]

for further diverse applications. It is suggested that there is a tremendous amount of risk involved with the healthcare data as if malicious activities are performed on the data, it can cause severe damage to revenues and activities involved. The current methods involved to protect the privacy of the data are not sufficient and also not efficient. The privacy of the medical data is almost priority nowadays, because it endangers to breach the patient's condition. If this breach happens, it impacts all the patients, stakeholders, and the miners negatively. To avoid such a situation, the authors propose a blockchain-based framework to protect the autonomity of the data using a cloud environment.

3.14 | Fan et al[30]

The authors trust that with the expansion being developed of the data innovation, there has additionally been a huge development in the electronic medical records. Sometimes same patient information is stored in different hospitals, that is, multiple databases. This leads to breach in security and privacy of the electronic medical records. Eventually, it becomes difficult for data sharing. To resolve this issue, the authors have proposed a blockchain-based system that provides security and privacy. This does not even consume much energy and also does not create network congestion. Efficiently, it protects the electronic medical records securely. The proposed architecture by the authors to provide privacy and security in the domain of healthcare data management consists of various users who are patients and want their medical data to get stored on the blockchain. Whenever a new patient is added, a new block gets added on the existing blockchain architecture. The blocks are connected with each other and have a distributed and decentralized network. Every block in the existing blockchain has a timestamp that gets verified with cryptographic mechanisms and also contains the hash information of the previous block. The key benefits that the authors have using this proposed system are: avoiding single point of failure, patients have the right to access over their own data, the entire healthcare data is easy to access, secure, distributed, and efficient, any illegal changes made to the blockchain data will be easily detectable and identified. Legitimate consent has been actualized in the proposed framework, which keeps an eye on what kind of information will be appeared to which blockchain miners. It approves specific users. A connection has also been done with the existing data storage infrastructure. The system proposed by the authors can input data from various sources such as physician offices, hospital servers, etc. This system achieves the important aspect, that is, decentralization.

3.15 | Yang and Yang[31]

The authors trust that electronic medicinal records sharing improves nature of healthcare and furthermore decreases the expense of medicinal services. But this is quite challenging because nowadays data are not secure and privacy is a myth. To ensure interoperability, integrity, and confidentiality of the data, the authors propose a blockchain-based approach. After implementing this, the electronic medical records will be secure against tampering and will provide authenticity to the data. The system will be flexible and will be maintaining clear audit. A framework has been designed keeping in mind the cancer-affected patients. The prototype of the framework ensures that security, privacy, and also reduces the turnaround time for healthcare data sharing and storing. The main framework of the proposed work consists of membership service, databases for medical data storage, nodes, and various APIs. The membership service has the functionality to verify the various users or the blockchain miners who will be accessing the data of the blockchain. Here, if a doctor tries to request any query, first the profile will be verified using symmetric key encryption pair and authorizing digital signatures. Similar process is observed while verifying the various users. The entire sensitive healthcare is stored on two databases, namely, a local database and a cloud server. The local database contains cancer-related data and the cloud server usually contains an organized categorical data. All these data are encrypted

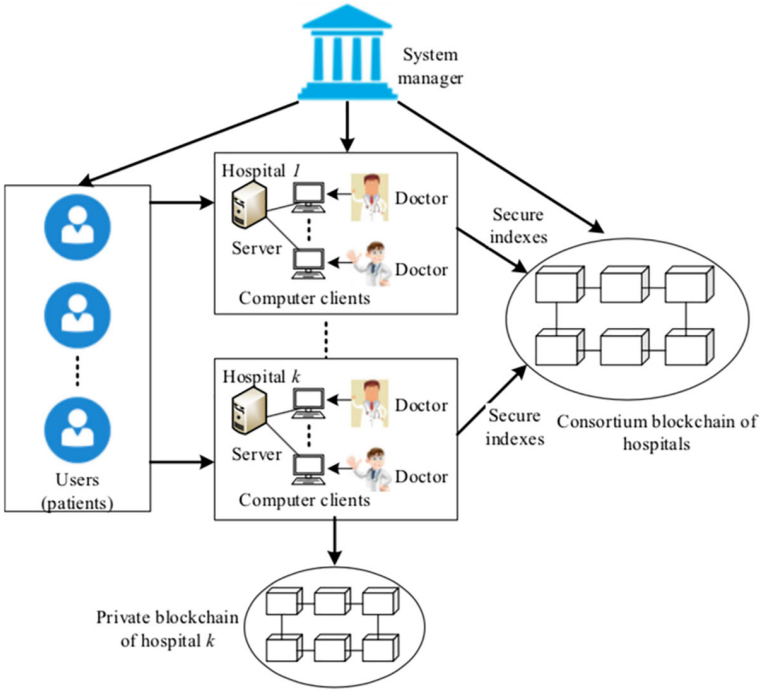

FIGURE 8 Proposed architecture by Zhang and Lin[2]

with the symmetric key pair, which vary patient to patient. The access to the data depends on what type of access control has been defined by the patients. An entire performance evaluation has been done by the authors on the grounds of privacy, security, and scalability.

3.16 | Zhang and Lin[2]

The authors trust that because of the execution of the electronic medical records, there has been a huge improvement in the diagnosis of the patients. This work proposes a blockchain-based secure privacy preserving sharing scheme for the electronic medical records. This scheme uses two blockchains: private blockchain and consortium blockchain. The private blockchain stores the health records of the patients, and the consortium blockchain creates the secure indexes for the data stored by the private blockchain. In order to make the scheme data secure, all the public health records and the patients' identity are public key encrypted with keyword search. This scheme has been implemented on JUICE to meet the security goals and evaluate the performance of the scheme effectively and efficiently. They proposed a blockchain-based platform that can store and manage huge healthcare data with ease, accuracy, and also providing security for the data stored. Currently, all healthcare data are stored on a centralized server. The authors have proposed an architecture that ensures decentralization. This has the data in a distributed environment, which would also increase the interoperability. Here, the files are fragmented, where the transaction happens and then gets stored on the various nodes. In this proposed architecture, after the user requests for a transaction, an identity check of the user is being done using cryptographic techniques. After the user has been verified by the system, a new block on the existing blockchain gets added about the transaction that is being made. Then, the user is provided with the required information needed. The proposed architecture by the author has been given in Figure 8.

3.17 | Uddin et al[32]

They proposed the blockchain-based framework for remote patients in the healthcare system. In their architecture, they consider that every patient is having wearable devices (sensors) that are used for getting the health-related information. After the pre-processing from the system, the information is stored in the blockchain. The proposed scheme used miner mechanism for the creation of blocks. The proposed miner mechanism differs from the bitcoin-based miner concept. In the bitcoin system, more than one miner are participating in the system for generating the hash value of the current block. But in the proposed system, the same work is done by only one miner. This selection of suitable miner is done by the patient agent, based on some parameters (eg, previous performance of miners). The proposed scheme used patient-centric modal for the sharing of health information among health providers, but authors do not provide sufficient knowledge for the block validation. Authentication protocols are also not fully investigated in their architecture.

3.18 | Griggs et al[16]

Authors proposed the blockchain-based smart contracts for secure remote patient monitoring. Their framework uses permissioned blockchain in which patient is equipped with sensors for collecting the medical data. They use practical byzantine fault tolerance consensus mechanism for patients' data validation. The advised protocol works well only if all the users are already present in the permissioned network. Authentication and blockchain specific vulnerability are not discussed by the authors.

Table 1 shows the comparison of the existing blockchain-based electronic medical records (EMRs) system with their benefits and shortcoming, along with the blockchain specific challenge. Many researchers are trying to solve the patient's data sharing and privacy problem, heterogeneity of medical data, etc. The brief summary is shown in Table 1.

4 | DISCUSSION ON RESEARCH ISSUES

Potential research challenges include the following points:

- In the electronic medical record-based system, security and privacy of patient's data are the primary concern. Patient's data need to be stored in a secure manner such that unauthorized users are not performed malicious activity on it. Existing EMRs system tries to handle, this issue with the use of different cryptographic methodologies. Some authors try to solve the above-mentioned problem, with the adoption of blockchain technology in the EMRs system. Azaria et al[1] use the blockchain technology in the medical record system, but in their work, the security of the database is not guaranteed.
- Authentication and key-management are the second type of problem, which exist in the EMRs system. Many authors, Li et al[28] and Zhou et al[29] adopt a cryptographic mechanism to provide secure and reliable sharing of patient's data. The patients, in EMRs system, are increasing day-by-day. Managing patient's key pair is a big challenge in the EMRs system.
- Currently, many researchers are proposing the blockchain-based electronic medical record system. The inherent mechanism of blockchain is widely suitable in the EMRs system. The advantage of using blockchain is that it provides immutable patient's records. Smart contract and consensus are the core functions of the blockchain mechanism. But only a few authors, Zhang and Lin,[2] Griggs et al,[16] and Zhou et al[29] suggested smart contract and consensus for data validation and verification. Research in this direction is needed.
- Several existing EMRs are centric toward health providers. The health providers are performed the necessary actions, according to their need, unacquainted from patients. Many researchers used blockchain-based EMRs/EHRs system, where patients are in a central role, to provide their own records to other health providers. The authors in Liang et al[27] used patient-centric modal to preserve the privacy of patient's record.
- Today, medical data are growing rapidly day-by-day and it is heterogeneous in nature. Several authors proposed blockchain-based EMRs system, but only a few of them consider the heterogeneity nature of medical data. Kaur et al[23] used blockchain-based EMRs system based on the heterogeneous collection of medical data, stored in the cloud environment. A suitable architecture is needed, which considers the above-mentioned issue.
- Scalability is the next issue that is associated with the EMRs system. The patients are increasing at an exponential rate. The traditional EMRs-based system is not able to grapple with the above situation. To deal with the above-mentioned issue, a framework is needed, which is scalable in nature.

5 | CONCLUSIONS

Medical care has been an indispensable part of our lives and so the medical data, for example, prescriptions, previous medical records has also become a vital part for patients' diagnosis and for further proceedings. Traditionally, medical data were recorded on paper, which was prone to get damaged and modified. Therefore, it was necessary to preserve the data electronically. However, the medical database could be tampered or deleted permanently. Then, there was also a concern on information blocking. Information blocking occurs when an entity, for example, a person may be with or without his intention to access the data that should not have been seen without patients or hospitals concern. Technology always plays a very significant role if it is about enhancing the quality or about resolving issues such as resource allocation along with information blocking, here in medical-care data sharing technology needed to be evolved with time. This paper has reviewed all possible works on the medical healthcare using blockchain technology with a proper comparative study. Furthermore, the same paper also highlights privacy issues on the blockchain-based medical system.

TABLE 1 Shows the comparison of existing blockchain-based EMRs system with benefits and shortcoming

S.No.	Reference	Idea	Blockchain type	Blockchain-specific challenge addressed	Benefit	Shortcoming
1	Azaria et al[1]	Blockchain-based EMRs system to manage the decentralized medical data	Not Discussed	Mining incentive and smart contract	Provide easy accessing of patients' medical information to health providers	Security of database and legal issues are not addressed
2	Kaur et al[23]	Blockchain-based system is used for storing and managing the EMRs in cloud enviornment	Not discussed	Not discussed	Heterogeneous medical data is stored on blockchain in a distributed manner	Key generation and replacement are not addressed
3	Xia et al[24]	Blockchain-based data sharing framework for EMRs system in cloud envirnment	Permissioned blockchain	Not discussed	Adopt identity-based authentication and key agreement protocol for access control mechanism	Authentication and communication protocol are not fully investigated
4	Xia[25]	Blockchain-based medical data sharing framework for EMRs system among untrusted parties	Not discussed	Smart contract	Provide data provenance when sharing patients' medical data	Key generation and replacement are not addressed
5	Dubovitskaya et al[4]	Blockchain-based healthcare data management framework for EMRs system	Permissioned blockchain	Not discussed	Provide security and privacy for sharing patients' medical data	Heterogeneity of medical data and legal issues are not addressed
6	Al Omar et al[3]	Blockchain-based privacy preserving framework for patients' health data	Permissioned blockchain	Smart contract	Provide a patient-centric healthcare data management system along with cryptographic primitives	Key generation part is not fully investigated
7	Liang et al[27]	Permissioned blockchain-based data sharing framework for healthcare system	Permissioned blockchain	Hyperledger fabric	Adopt a patient-centric model for ensuring data ownership and integrity	Smart contracts are not fully investigated
8	Li et al[28]	Blockchain-based data preservation scheme for patients' medical data in EMRs system	Not discussed	Ethereum	Adopt cryptographic techniques to achieve data privacy	Authentication protocol and Heterogeneity of medical data, are not fully investigated
9	Ji et al [7]	Blockchain-based patients' location sharing scheme for telecare medical information system	Not discussed	Not discussed	Adopt an order-preserving encryption scheme to achieve multilevel location privacy	Security and privacy of patients' data are not addressed
10	Zhou et al[29]	Blockchain-based medical insurance storage system	Permissioned blockchain	Consensus	Adopt cryptographic techniques to achieve security and privacy of patients' data	Heterogeneity of medical data not addressed
11	Fan et al[30]	Blockchain-based secure patients' medical data sharing framework for EMRs system	Not discussed	Consensus	Provide data privacy by using the access control protocol and cryptographic mechanism	PBFT consensus is not fully investigated

TABLE 1 Continued

S.No.	Reference	Idea	Blockchain type	Blockchain-specific challenge addressed	Benefit	Shortcoming
12	Yang et al[31]	Blockchain-based scheme for secure sharing of healthcare data in EMRs system	Not discussed	Miner and smart contract	Provide data authenticity and confidentiality by using cryptographic primitives	Smart contract and consensus mechanism are not fully investigated
13	Zhang and Lin[2]	Blockchain-based e-health system for secure sharing of personal health information	Consortium blockchain	Consensus	Provide secure sharing of PHI by using cryptographic primitives	Scalability, in number of private blockchains, is not investigated
14	Uddin et al[32]	Blockchain-based remote healthcare framework for EHRs system	Not discussed	Miner	Provide a patient-centric scheme for remote patients' data management	Authentication and communication protocol are not fully investigated
15	Griggs et al[16]	Blockchain-based smart contracts for secure remote patient monitoring	Permissioned blockchain	Smart contract and consensus	Provide patients' data validation by using PBFT consensus mechanism	Authentication protocols are not addressed

Abbreviation: EMR, electronic medical record; PBFT, practical byzantine fault tolerance; PHI, personal health information.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

REFERENCES

1. Azaria A, Ekblaw A, Vieira T, Lippman A. *Medrec: Using Blockchain for Medical Data Access and Permission Management*. Vienna, Austria: IEEE; 2016.
2. Zhang A, Lin X. Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. *J Med Syst*. 2018;42(8):140.
3. Al Omar A, Rahman MS, Basu A, Kiyomoto S. *Medibchain: A Blockchain Based Privacy Preserving Platform for Healthcare Data*. Vol 10658. Guangzhou, China: Springer; 2017.
4. Dubovitskaya A, Xu Z, Ryu S, Schumacher M, Wang F. Secure and Trustable Electronic Medical Records Sharing Using Blockchain. AMIA Annual Symposium Proceedings, Maryland; 2017.
5. Tian F. *An Agri-Food Supply Chain Traceability System for China Based on RFID & Blockchain Technology*. Kunming, China: IEEE; 2016.
6. High DR, Wilkinson BW, Mattingly T, et al. *Obtaining a Medical Record Stored on a Blockchain from a Wearable Device*. 2018. US Patent App. 15/840, 589. Bentonville, AR: Patent application Publication.
7. Ji Y, Zhang J, Ma J, Yang C, Yao X. BMPLS: blockchain-based multi-level privacy-preserving location sharing scheme for telecare medical information systems. *J Med Syst*. 2018;42(8):147.
8. Nakamoto S. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008. http://www.bitcoin.org. Accessed February 11, 2019.
9. Watanabe H, Fujimura S, Nakadaira A, Miyazaki Y, Akutsu A, Kishigami J. *Blockchain Contract: Securing a Blockchain Applied to Smart Contracts*. Las Vegas, NV: IEEE; 2016.
10. Dorri A, Kanhere SS, Jurdak R, Gauravaram P. *Blockchain for IoT Security and Privacy: The Case Study of a Smart Home*. Kona, HI: IEEE; 2017.
11. Biswas K, Muthukkumarasamy V. *Securing Smart Cities Using Blockchain Technology*. Sydney, Australia: IEEE; 2016.
12. Atzei N, Bartoletti M, Cimoli T. *A Survey of Attacks on Ethereum Smart Contracts (sok)*. New York, NY: Springer-Verlag Inc; 2017.
13. Mettler M. *Blockchain Technology in Healthcare: The Revolution Starts Here*. Munich, Germany: IEEE; 2016.
14. Park J, Park J. Blockchain security in cloud computing: use cases, challenges, and solutions. *Symmetry*. 2017;9(8):164.
15. Kiayias A, Panagiotakos G. Speed-security tradeoffs in Blockchain protocols. *IACR Cryptol*. 2015;2015:1019.
16. Griggs KN, Ossipova O, Kohlios CP, Baccarini AN, Howson EA, Hayajneh T. Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *J Med Syst*. 2018;42(7):130.
17. Dorri A, Steger M, Kanhere SS, Jurdak R. Blockchain: a distributed solution to automotive security and privacy. *IEEE Commun Mag*. 2017;55(12):119-125.
18. Spagnuolo M, Maggi F, Zanero S. *Bitiodine: extracting intelligence from the bitcoin network*. Berlin, Germany: Springer; 2014.
19. Lin IC, Liao TC. A survey of blockchain security issues and challenges. *IJ Netw Security*. 2017;19(5):653-659.

20. Gervais A, Karame GO, Wüst K, Glykantzis V, Ritzdorf H, Capkun S. On the security and performance of proof of work blockchains. CCS '16 Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria; October 24–28, 2016, ACM, New York; 2016: 3–16.
21. Puthal D, Malik N, Mohanty SP, Kougianos E, Yang C. The blockchain as a decentralized security framework [future directions]. *IEEE Consum Electr M*. 2018;7(2):18-21.
22. Zyskind G, Nathan O, Pentland A. *Decentralizing Privacy: Using Blockchain to Protect Personal Data*. San Jose, CA: IEEE; 2015.
23. Kaur H, Alam MA, Jameel R, Mourya AK, Chang V. A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment. *J Med Syst*. 2018;42(8):156.
24. Xia Q, Sifah E, Smahi A, Amofa S, Zhang X. BBDS: Blockchain-based data sharing for electronic medical records in cloud environments. *Information*. 2017;8(2):44.
25. Xia Q, Sifah EB, Asamoah KO, Gao J, Du X, Guizani M. MeDShare: trust-less medical data sharing among cloud service providers via blockchain. *IEEE Access*. 2017;5:14757-14767.
26. Esposito C, De Santis A, Tortora G, Chang H, Choo KKR. Blockchain: a panacea for healthcare cloud-based data security and privacy? *IEEE Cloud Comput*. 2018;5(1):31-37.
27. Liang X, Zhao J, Shetty S, Liu J, Li D. *Integrating Blockchain for Data Sharing and Collaboration in Mobile Healthcare Applications*. Montreal, QC: IEEE; 2017.
28. Li H, Zhu L, Shen M, Gao F, Tao X, Liu S. Blockchain-based data preservation system for medical data. *J Med Syst*. 2018;42(8):141.
29. Zhou L, Wang L, Sun Y. Mistore: a blockchain-based medical insurance storage system. *J Med Syst*. 2018;42(8):149.
30. Fan K, Wang S, Ren Y, Li H, Yang Y. Medblock: efficient and secure medical data sharing via blockchain. *J Med Syst*. 2018;42(8):136.
31. Yang H, Yang B. *A Blockchain-Based Approach to the Secure Sharing of Healthcare Data*. Oslo, Norway: Norwegian Research Council; 2017.
32. Uddin MA, Stranieri A, Gondal I, Balasubramanian V. A patient agent to manage Blockchains for remote patient monitoring. *Stud Health Technol Inform*. 2018;254:105-115.

How to cite this article: Saha A, Amin R, Kunal S, Vollala S, Dwivedi SK. Review on "Blockchain technology based medical healthcare system with privacy issues". *Security and Privacy*. 2019;2:e83. https://doi.org/10.1002/spy2.83