A View on the Blockchain as a Solution to the Healthcare Industry: Challenges and Opportunities

Sharmila(✉), Krista Chaudhary, Umang Kant, and Pramod Kumar

Krishna Engineering College, Ghaziabad, Uttar Pradesh, India
sharmila1ece@gmail.com

Abstract. Due to the advancement of technology, the large volume of digital data increases rapidly in every field. One of the most sensitive digital data field is the healthcare system. Healthcare information contains high delicate private data, and it needs to be shared among the peoples such as health specialists, pharmacist, family members, insurance companies, hospitals etc. Healthcare organization have not only their patient's medical details which include insurance and financial account information. The breach of healthcare information is one of the most important concern nowadays. Recently, the research studies are going on Blockchain technology to secure the health care system. Blockchain technology is an open and distributed online database system which comprises the list of blocks that are related to each other. This paper summarizes the impact of blockchain in the healthcare system and enfranchises the privacy of a patient's health data. This paper also addresses the issues, challenges, and research onset of blockchain in the area of the healthcare system.

Keywords: Blockchain · Breaching · Data storage

1 Introduction

Generally, the modern healthcare systems provide more facilities to the doctors to gather, analyze, and monitor the health information of remote patients due to the advanced computing approaches such as the Internet of Things (IoT) and clouds. Technology development has eroded the privacy and security protection of our data. The privacy and integrity of the healthcare systems information must be protected from an unauthorized user, the internal, and external attacks. The extensive research work is going on to secure the health care systems such as Electronic Medical Report (EMR), Electronic Health Records (EHR), Health Information System (HIS), and Personal Health Records (PHR) [1]. Recently, researchers have been proposed many cryptographic algorithms to ensure the privacy and security of the healthcare system. Healthcare system consists of a large diversity of data's are generated, scattered, stored and retrieved. For example, consider the patient undergoes to treatment; the patient needs to take

A. Saha et al. (Eds.): ICCISIoT 2019, CCIS 1192, pp. 160–169, 2020.
https://doi.org/10.1007/978-981-15-3666-3_14

various tests, scans, CT scan, etc. The data will be available at the test center as well as with a physician. The data could be accessed by a physician in the same hospital as well as a physician in another hospital. The advancement of technology plays a vital role to provide security, privacy, and integrity of health care data management system. Blockchain is a tamper-proof distributed or decentralized online database which is undisputable, non-rewritable, read a dissimilar data structure, consists of the large number of blocks which are linked together using non alterable key referencing mechanism. Blockchain is a network of independent entities which work together and form a peer to peer network. The blocks of data which is stored in the network are synchronized together using the consensus mechanism and offers a validity of data over the network. The blockchain [2] consists of a list of blocks called a data structure. The data structure of blockchain consists of the following elements: timestamp, the hash value of the previous block, transaction data. The properties of data structure are as follows: (1) secured blocks (data records) (2) peer to peer network (3) consensus mechanism (4) security mechanism which offers unchallengeable of the data. These four properties play vital role in blockchain mechanism for the important consequences. The data availability of blockchain is either permission or permissionless. The block-chain is distributed ledger, which does not depend on a third party to perform transaction between two entities. The transaction between the two parties can be carried out using consensus rules to ensure the trustworthy of the parties. The trustworthy can be ensured by the participants in the network instead of any centralized parties. The inherent characteristics of the blockchain technology are the transaction cannot be changed anymore. The security of blockchain [3] depends on the cryptographic encryption function and consensus mechanism. The large resources are needed to carry out the malicious attack on the block of transaction. The complexity of attacks as increases whenever the new block of the transaction is attached to the chain of an existing transaction block. The aforementioned features of blockchain offer the following services such as integrity, privacy, security, traceability, and non-repudiation of data while storing the information in a decentralized way. The exhaustive research works have been carried out in the field of the banking sector, real estate, government bid, and finance using blockchain. Recently, the researchers started to address the potential of using blockchain technology in the field of healthcare. The blockchain technology provides the solution to the existing challenges in healthcare applications. The main contribution of this paper is to addresses the challenges, possible solution and its of blockchain technology in the healthcare applications. The organization of this paper as follows: Sect. 2 describes the literature of the healthcare system. Section 3 discusses the literature of blockchain. Section 4 discusses the uses of blockchain for the healthcare industry. Section 5 concludes this paper.

2 Healthcare System Literature

Healthcare system needs a unique security requirement due to the sensitive and legal information of patients. In this modern era, the risk of malicious attack and private information being compromised increases day by day because of ease data sharing with cloud computing using the internet. The sharing of information is the main concern due to the development of technology, the patient can use smart devices to carry their health information to the different doctors. One of the most significant field is big data which can be applied in the healthcare data to improve the patient's outcome, predict the epidemic, avoid preventable diseases, and minimize the cost of healthcare delivery and improve the quality of life [3]. The security and privacy of healthcare data is a difficult task. Big data which can be useful. In order to ensure the security and privacy of data, it is necessary to identify the limitations of existing systems and envisage directions for research in future. The security requirement of the healthcare is as follows: access control, authentication, interoperability in terms of centralized storage of data, mobility, transfer of medical data, etc. Figure 1 shows the requirements of healthcare system. Medical information [6] consists of patient's personal details, medical records as well as medical data which received from wireless body area network or sensor nodes implanted in the body [7]. The medical records of the patients are transferred from traditional paper to electronic documents i.e., digital medium. Electronic records are stored in the form of databases. It needs more security as well as authorized access control of data. The risk of replication or modification of data can be reduced by means of access control. The traditional encryption techniques are not suitable for the medical record due to the different standards of encryption used in various systems.

Interoperability is generally defined as the process of sharing and transmitting the data between the various sources. In a centralized database, all the medical records are stored in one database. Centralized data storage is the main limitation of interoperability which causes data to need to be fragmented, difficult to perform data sharing and limit the speed of data access. The advancement of MEMS technology, the mobility of healthcare data is an important requirement of the health industry. The real-time healthcare data is collected from sensor nodes, Body Area Sensor Network (BASN), pervasive smart devices, and Internet-enabled devices. It is a challenging task to secure the real-time data collected from wireless devices or an IoT. The privacy and security of mhealth care [8] suffer from the centralized healthcare system. Wireless Sensor Networks (WSN) or IoT is resource constraint devices which need to perform more computation to provide security and privacy. The malicious attacker compromises the sensitive health data which affects the future vision of healthcare applications.

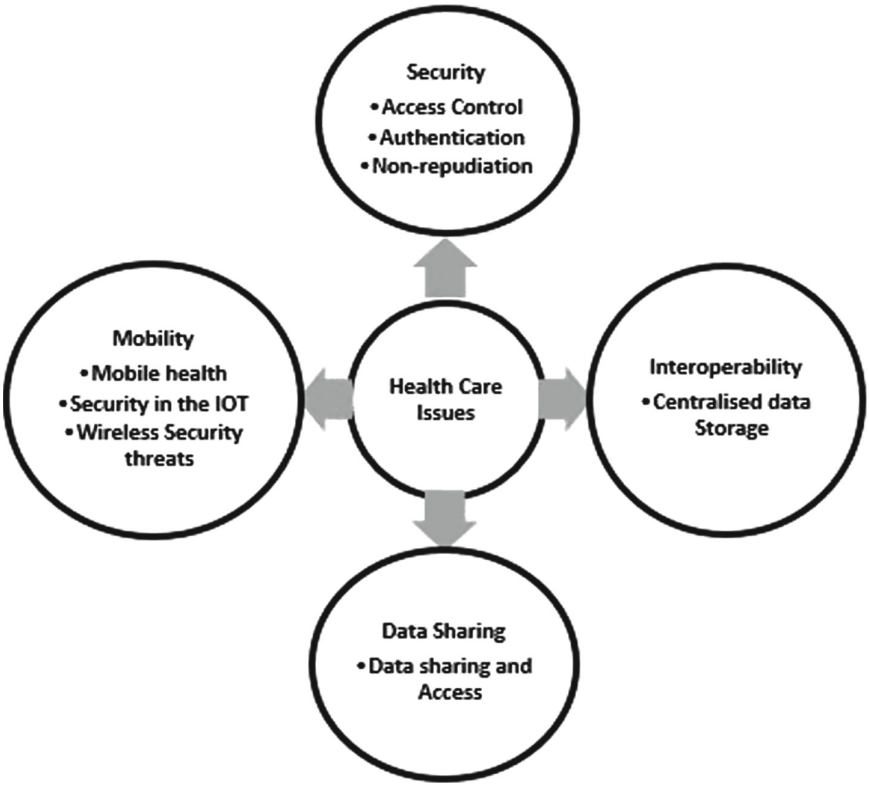

Fig. 1. Healthcare requirements.

3 Blockchain Architecture and Its Requirements

Blockchain is decentralized ledger in which transaction among a node to node in the network is carried out without any intervention of centralized authority. Generally, the two version of blockchains [6] such as cryptocurrencies version 1.0 and version 2.0. Zheng et al. [9] address four key parameters of blockchain methodology which will directly influence the healthcare industries in terms of decentralization, auditable, persistence, and obscurity. Figure 2 shows the blockchain architecture. The architecture of blockchain consists of the following components: blocks, header, transaction counter, and transaction data. The algorithms used in blockchain are the hash algorithm, digital signature, forking, and consensus algorithm. Figure 3 shows the requirements of blockchain. The components of blockchain as follows: Block: Each block stores the transaction information. It maintains an immutable and permanent record of data. It consists of three blocks as follows: 1. Header 2. Transaction Counter 3. Data Transaction

Header: Each header section maintains the following information.

- Version Number: It represents which regulation the block follows.
- Hash Block: It maintains and points the parent block hash values and their corresponding parent's block.
- Merkle tree root hash: It keeps blockchain values after double hash function using SHA256.
- Time Stamp: It records the time at which the particular block approved.
- Nonce: On time variable use.
- Threshold: It represents the mining difficulties.

Transaction counter: It sums the total number of the transaction completed successfully and maintain the details about the current transaction block.

Transaction Data: The transaction data varies depends on the applications such as Bitcoin, Smart contract, business data, and healthcare data.

Hash function: Hash function is used to provide the fixed length hash value.

Forking: Forking happens in blockchain whenever there is any contradict in consensus algorithm or any software changes. Depending on the problem, the forking is divided into the hard, soft fork, and usercentric fork.

Types of Blockchain: Blockchain mechanism is divided into three types depending on permission of the user such as public, private, and Consortium.

Consensus algorithm: Each node in the distributed network agree on the common rule based on consensus algorithm for a successful transaction. Therefore, it needs consensus algorithms to ensure the consistent data/state of transaction among the nodes. Some of the consensus models are Proof of work (PoW), Byzantine fault tolerance, Proof of Stake (PoS), Proof of Authority (PoA), ripple, and tender mint.

Digital Signature: Digital signature plays an important role to improve the security of sensitive data, increase the efficiency of administrative processes, and treatment, as well as E-prescribing and admission in hospitals. The digital signatures in healthcare need to obey with the Health Insurance Portability and Accountability Act of 1996.

3.1 Blockchain Features

Blockchain has many features that can be used for healthcare. The features of blockchain are as follows:

- Decentralized storage
- Authentication
- Disintermediation
- Cost reduction
- Immutability

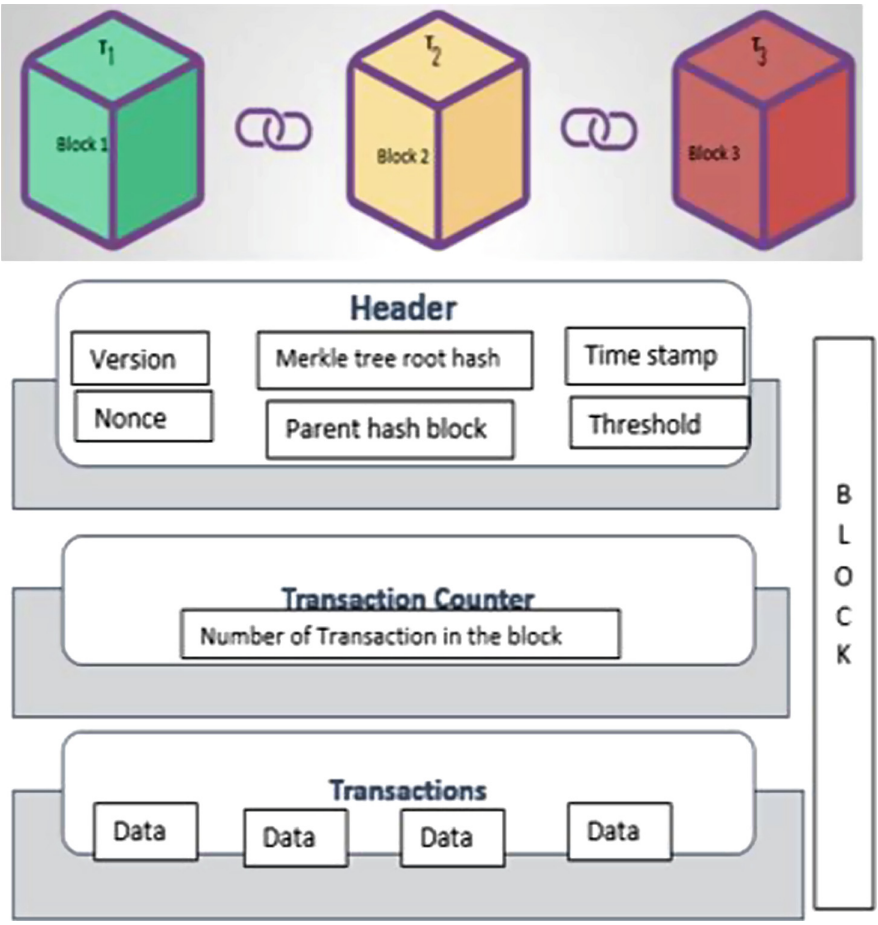

Fig. 2. Block chain Architecture.

3.2 Blockchain Limitations

In spite of all the advantages of Blockchain, still, it has limitations need to over-come. The limitation of blockchain as follows:

- Privacy leakage
- Lack of Standardization
- Key Management
- Scalability issues due to IoT
- Software Vulnerabilities

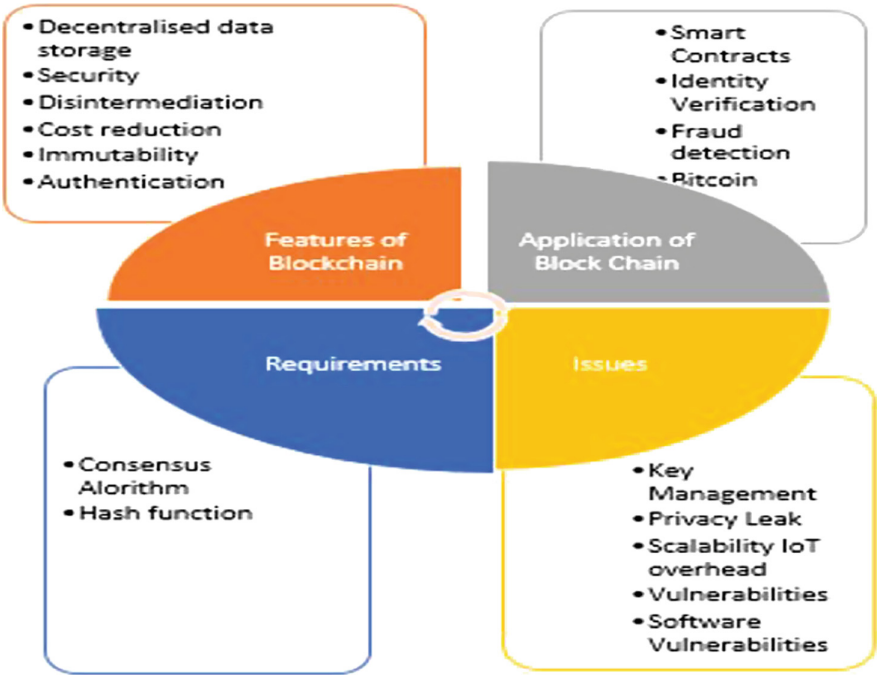

Fig. 3. Blockchain requirements.

4 Blockchain for the Healthcare Industry

Blockchain technology brings more advantages for the healthcare industry. Blockchain offers secure and trustworthy digital electronic data among healthcare data stakeholders. Figure 4 shows the impact of blockchain on the healthcare industry. Blockchain provides solutions for the challenges of the healthcare system. The existing software solutions for blockchain enabled healthcare solutions will be discussed in the following sections.

4.1 Gem Health Network

Healthcare industry deals with more number of records and medical documents which follow the Health Insurance Portability and Accountability (HIPAA) act of 1996 and offers confidentiality. Earlier, the data's are stored in a centralized system. The main issues of centralized health care database are security, interoperability, difficult to share the confidential record [6,7] among different physicians and hospitals. If the patient consults different physicians, it creates overhead in terms of resource rigorous authentication and consumes more time due to the creation of a duplicate copy or new records, communication protocols between the doctors need to change, and records need to update. The aforementioned problem can be solved by Gem health network [3] which used

the concept of Ethereum Blockchain technology. It creates a shared network infrastructure and overcomes the limitation of a centralized database. It facilitates the patients and doctors to access the real-time data at any place and any time. Estonia country has collaborated with healthcare platform named Guardtime, which uses blockchain technology to provide healthcare service. In Estonia, every citizen, physician, healthcare provider, and health insurance companies can retrieve the patients' medical treatment records by using blockchain technology. The major limitation of this technology is not addressed the scalability and key replacement. OmniPHR is designed to share patient up to date medical records distributed among healthcare care providers and addressed the scalability issues. OmniPHR [4] was developed by Roehrs, Costa, and Righi. OmniPHR addressed the difference between Electronic Health Records (EHR) and Personal Health Record (PHR). Electronic Health records are maintained and updated by a doctor without the intervention of patients. In PHR, medical records are maintained by patients. OmniPHR offers an integrated view of health records which are distributed across the different health care organization. The main limitation of OmniPHR is that the data needs to follow the standards reinforced by the model. It would not share the data if it does not support the scope of the standards. In the case of key lost or leaked, the key management and recovery problems are not addressed by OmniPHR.

4.2 MedRec

MedRec [5] is decentralized data management system used to handle EMRs using blockchain which was proposed by Azaria, Ekblaw, Vieira, and Lippman. In this MedRec, the stakeholders of the healthcare industry participated as the miners and access, aggregate, mining data as an anonymous and securing network using PoW. The main limitation not addressed by MedRec is a key replacement and legal issues.

4.3 Research Scope and Solutions

Blockchain technology for healthcare applications has been widely acknowledged by means of many of the organizations. Though, blockchain technology for the healthcare industry still in their primary stages. Many existing challenges have been not yet addressed. Figure 5 shows the solution offered by blockchain for the healthcare industry. This section gives several challenges and its future research directions of blockchain technology for healthcare applications.

- Need to focus on the scalability of blockchain enabled healthcare.
- Required to conduct and verify the result on analysis of real-time datasets.
- More focus on key management and security(lost key and key recovery).
- More focus needed on the privacy of patients and identity verification.
- Need to work on doctor access authorized data in an emergencies situation without authorization.

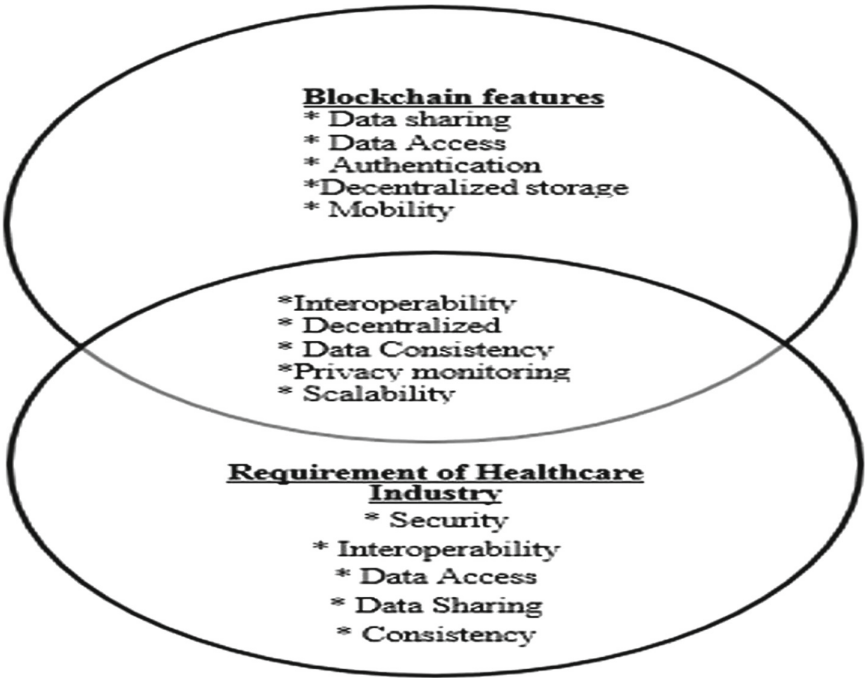

Fig. 4. Blockchain requirements.

Challenges of Healthcare	Solutions offered by Blockchain
Data dissemination	The decentralized system forms a network among all the nodes such as between patients, physician, hospital, clinic, etc.
Concurrent access	Blockchain is immutable. It secures concurrent analysis of data without the risk of data modification. It provides integrity.
Scalability	Blockchain offers authentication through a consensus algorithm. It verifies each node in the network
Big data(formed from IoT) management	Blockchain creates a secure private network among the nodes. It also provides secure IoT device communication.
Data Access Control and Consistency	Blockchain offers three types of data handling (private, public and user consortium). User can define the regulation for the data.
Cost of Data processing	No third party involvement. Blockchain reduces the data processing and analysis cost
User privacy's	Blockchain handles data secretly and processing is open to all.

Fig. 5. The solution offered by blockchain for the healthcare industry.

5 Conclusion

In conclusion, blockchain offers a solution for some of the challenges faced by the healthcare industry. Blockchain facilitates secure data access and sharing, secure the privacy of the patients, patients can keep track of medical records, etc. In spite of complex design of healthcare system, the blockchain resolves the key challenges of the healthcare industry including data dissemination, concurrent access, a huge amount of data processing, access control, limit the storage of data and cost of data processing. Blockchain not only offers a wide range of application in the healthcare industry but it also offers vast research opportunities on employing blockchain in the healthcare industry.

References

1. Abouelmehdi, K., Beni-Hessane, A., Khaloufi, H.: Big healthcare data: preserving security and privacy. J. Big Data **5**(1), 1–18 (2018). https://doi.org/10.1186/s40537-017-0110-7
2. Mettler, M.: Blockchain technology in healthcare: the revolution starts here. In: IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom) (2016)
3. Zhang, J., Xue, N., Huang, X.: A secure system for pervasive social network-based healthcare. IEEE Access **4**(1), 9239–9250 (2016)
4. Torre, I.: A framework for personal data protection in the IoT. In: 11th International Conference for Internet Technology and Secured Transactions, ICITST (2016)
5. Cai, Y., Zhu, D.: Fraud detections for online businesses: a perspective from blockchain technology. Finan. Innov. **2**(1), 20 (2016). https://doi.org/10.1186/s40854-016-0039-4
6. Kiyomoto, S., Rahman, M.S., Basu, A.: On blockchain-based anonymized dataset distribution platform. In: 2017 IEEE 15th International Conference on Software Engineering Research, Management and Applications (SERA) (2016)
7. Sharmila, Kumar, D., Som, K., Kumar, P., Chaudhary, K.: General outlook of wireless body area sensor networks. In: Singh, M., Gupta, P., Tyagi, V., Flusser, J., Ören, T., Kashyap, R. (eds.) ICACDS 2019. CCIS, vol. 1046, pp. 58–67. Springer, Singapore (2019). https://doi.org/10.1007/978-981-13-9942-8_6
8. Swan, M.: Blockchain: Blueprint for a New Economy. O'Reilly Media Inc., Newton (2015)
9. Zheng, S., Xie, H., Dai, X., Chen, H.: An overview of blockchain technology: architecture, consensus, and future trends. In: 2017 IEEE International Congress on Big Data (BigData Congress), pp. 557–564. IEEE (2017)