International Journal of Computer (IJC)

ISSN 2307-4523 (Print & Online)

© Global Society of Scientific Research and Researchers

http://ijcjournal.org/

Review on Blockchain Technology for Healthcare Records

Ekram Ahmed Ali Mirdah[a]*, Sokchoo Ng[b], Khiam Ping Chih[c]

[a]School of Information Technology, SEGi University, Jalan Teknologi, Kota Damansara, Petaling Jaya, 47810, Malaysia

[b]Faculty of Science, Technology, Engineering and Mathematics, International University of Malaya-Wales, Kuala Lumpur, Malaysia

[a]Email: romeeahmed@gmail.com

[b]Email: ashleyng@iumw.edu.my

[c]Email: khiamping@yahoo.com

Abstract

For a long time, the healthcare system has been facing many problems such as incomprehensible doctor's hand-writing, problematic retrieval of patient information and patients are unable to monitor their own data. In addition to that, there are problems afflicting the medical record systems such as how to share the medical data for various purposes without risking data privacy and security. Due to technology advancements, it is now possible to improve the current situations and to minimise these problems by providing more personalised services to the patients. This paper explains the interesting area of blockchain in healthcare, evaluating the blockchain technology from the multiple perspectives around healthcare data and explaining some platforms which could be used for the blockchain system development. Finally, the challenges of implementing the blockchain technology are deliberated.

Keywords: Blockchain ; healthcare ; medical record; privacy; security.

1. Introduction

Distributed ledger technology is a blockchain of records transactions which stores digital data in a cryptographic way in a ledger. Data is organised in blocks and linearly connected while each block develops the hash key from the previous block. Ref [1,2] described the public blockchain as a distributed data repository that allows nodes among the network to share the transaction records while these records are updated and monitored by everyone but owned by no one. Ref [3] perceived blockchain as a stacked data structure, and it has become a social phenomenon for data sharing. The blockchain concept was first proposed by Satoshi Nakamoto in his white paper published in October 2008 [4]. A year later, the open source implementation of Bitcoin based on the blockchain was released. The working principle of the blockchain protocol is allowing different parties which do not need to trust each other to interact and exchange data with each other [5]. Fig.1 shows the structure of a blockchain which is formed by a series of blocks that carries a full list of transaction records as a traditional public ledger [6]. A genesis block is a first block in a blockchain that does not have a parent block. Each block points directly to the next block through a hash value of the prior block called parent block. A block may consist of one or many transactions until the block weight reaches to the limit. It is a part of the block creation, and mining and these transactions can only be confirmed by being inside a block.

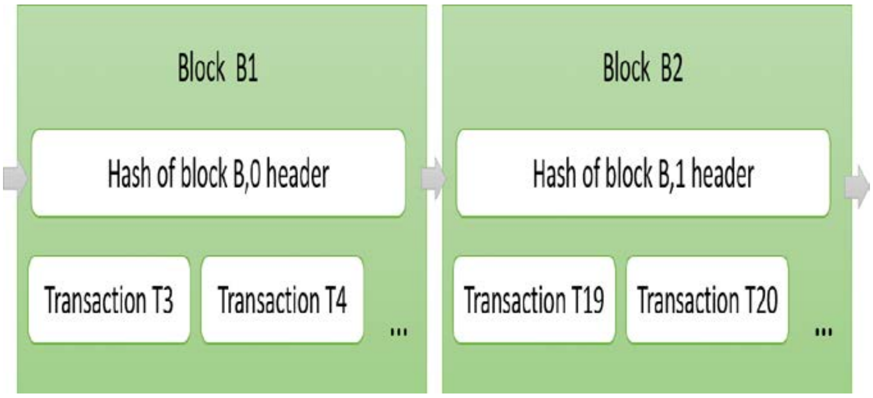
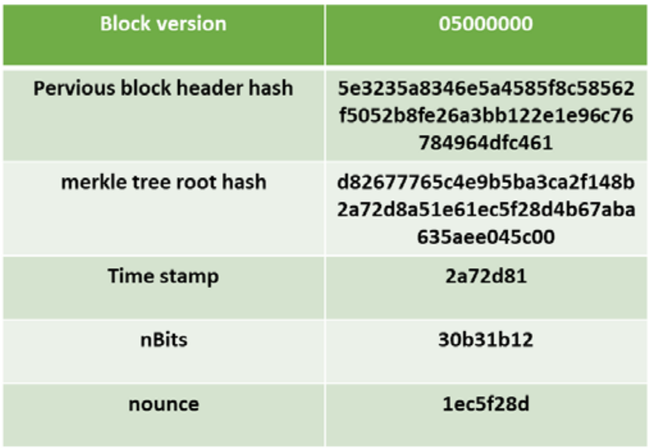


Figure 1: Blockchain structure with genesis and parent blocks

2. Block

Every block consists of a block header and block body Fig.2. The block header consists of six components: block version, previous block hash, Merkle tree root hash, nBits, timestamp, and nonce. The version number refers to the set of rules to validate the data inside the block. The previous block hash is a SHA 256 hash that points to the previous block. The Merkle root stores the hash value of all the transactions. The time stamp demonstrates the transaction time in seconds. The nBits value is the threshold of a valid block hash. During the mining process, the candidate's block hash number must be less than the nBits value so that the block can be added into a blockchain. Miners use a nonce to keep the block hash number below the threshold value. The maximum number of transaction that a block could contain depends on the block and the transaction size.

The body of a block contains the number and group of transactions. A valid transaction consists of two individual parts which are the inputs and outputs. The inputs refer to the unspent transaction outputs (UTXO) in which the underlying block receives from others. Meantime, the outputs which have been used cannot be circulated in the chain anymore. Blockchain applies an asymmetric cryptography technique to confirm the authentication of a transaction as well as to ensure that the integrity of the record is maintained ([7], [8]) . A digital signature based on asymmetric cryptography is particularly an appropriate choice in a distrusted environment.



Block version	05000000
Pervious block header hash	5e3235a8346e5a4585f8c58562f5052b8fe26a3bb122e1e96c76784964dfc461
merkle tree root hash	d82677765c4e9b5ba3ca2f148b2a72d8a51e61ec5f28d4b67aba635aee045c00
Time stamp	2a72d81
nBits	30b31b12
nounce	1ec5f28d

Figure 2: Block structure

3. Cryptography and Hash function

Cryptography plays an important role in a blockchain system for securing the data privacy. Cryptography is a data transformation technique which makes the data unclear to the unwitting receivers. It is the practice of preventing and detecting the disallowed access and usage of data in an illegal way which could harm the actual owner of the data. Data encryption can be categorised into three types: symmetric-key, asymmetric-key and the unkeyed. In symmetric-key algorithms, the same. Key is used for encryption and decryption. Asymmetric-key cryptography uses the public and private key pair for encryption and decryption. The unkeyed cryptography does not use any key to encrypt a message. The asymmetric cryptography or hashing explains the blockchain mechanism and how the data privacy is maintained. In a blockchain system, the records on a blockchain are secured through cryptography. Network participants have their own private keys that are assigned to the transactions they make and act as a personal digital signature. If a record is altered, the signature will become invalid, and the peer network will know right away that something has happened. Early notification is crucial to preventing further damage. A hash is a non-invertible function that transforms an arbitrary length binary string into a fixed-length binary string such that (x) -> y where x and y are both string variables. In other words, hashing procedure converts the arbitrary length string x into a newly fixed length string y. Hashing is a deterministic procedure in which, given the same x value, the hash function will always produce the same y value. In blockchain, the hashing procedure transforms a long string of transaction data into a fixed unique string which later becomes a unique identifier to that transaction. Hashing is also applied to create a unique block id for the mining mechanism. The block hash output length normally ranges from 128 to 512 bits. In the conventional data management infrastructure, all transaction between the parties (individual or organisational) are stored in a repository which is controlled by particular institutions such as government, private agencies, and service providers. This centralised approach causes the integrity of data to highly rely on the data management capability and functionality of the repository. Blockchain instills a new data management paradigm in a way that all the transactions over the network are registered and stored in a peer-to-peer network. Each node in the network maintains an identical copy of the data information in a block format, namely a ledger. The unique structure of blockchain that organises information together by blocks and secures the block using cryptographic hash has made its application available to a wide range of sectors such banking and real estate, and some of the prominent examples are Bitcoin in finance as well as Smart Contract performing as an immutable agreement in the insurance industry. The following section discusses the role of blockchain technology in the healthcare industry. With the development of blockchain technology, there are two different type of options to participate in the validation of the network. Permissioned and permissionless blockchains. A blockchain which exists openly on the internet is called permissionless and classic examples of such are Bitcoin and Ethereum. Also, since the data on the blockchain is open to anyone who wishes to join the network, the data has to be kept completely uncharted [9]. For medical records, it is necessary to keep it private. In some cases, it is not possible to anonymize all the data, or it is simply not desirable that everyone can participate in a network, permissioned blockchains are developed. On the other hand, the idea behind the permissioned blockchains is the control of who is allowed to participate in the network. This can be done by a government or other institutions, either by inviting new members or by predefining a set of criteria. It will increase the privacy and flexibility in adapting the network, in addition to better scalability and faster transactions [3].

4. Blockchain and healthcare

Blockchain technology has gained substantial attention in the healthcare industry. These technology applications have massive opportunities to transform the current practice of health information management and lead the healthcare industry to another level of development [10]. As mentioned earlier, blockchain uses a distributed, peer-to-peer network to make a continuous, growing list of ordered records (blocks) to form a digital ledger. Each transaction is represented by a cryptographically signed block, then validated by the network miners. It improves the authenticity and transparency of healthcare data through many use cases from maintaining permissions in electronic health records (EHR) to streamlining medical claims processing [11]. Besides, the blockchain enhances the privacy and addresses the security of the medical records by creating digital transaction ledgers which can be securely shared among a wide group of stakeholders. Different parties such as hospitals, pharmacies, insurance companied can directly exchange data via a shared ledger by applying the proven public and private key cryptography. Furthermore, blockchain uses a proof-of-work concept among ledger keepers, also known as miners, to validate transactions and ensure a virtual impenetrable and immutable system. The "permissioned" blockchain, in which the key stakeholders (doctors, patients, healthcare institutions management) have verified and have agreed to follow the common policies and procedures, may use a more limited consensus-building process that relies on smaller groups of trusted entities to achieve the proof of work. A few white papers related to the feasibility study of blockchain implementation in healthcare have been published by a group of corporate researchers ([12,13,14]). The Office of the National Coordinator for Health Information Technology (ONC), in their white paper [15], provided an overview of different use cases in interoperability roadmap where blockchain could play a major role to enhance their services for data exchange and protection. The U.S Food & Drug Administration (FDA) has partnered with IBM to explore the potential application of blockchain to securely share patients' data ranging from the medical records to clinical trials using this distributed, time-stamped database with consensus-establishing peers. By using blockchain, the exchange of data in a healthcare organisation will be more secured and flexible for both the patients and the service provider. It is difficult to change the history of each block transaction such as medical and prescription records. The immutability and provenance capability of blockchain provide the basis for tractability of data. The MediLedger Project by Chronicled, Inc. and The LinkLab aspires to move the biopharmaceutical industry forward by adopting a blockchain, specifically the consensus mechanism to track and trace prescription medicines in order to prevent counterfeit medicines from entering the supply chain. Other examples of blockchain application in healthcare are Hashed Health that uses blockchain for medical reports, revenue cycle management and payment reforms while the Health Linkages engages Big Data technology with blockchain to enable healthcare service providers and research institution to trust, protect and exchange medical records. Figure 3 illustrates how the blockchain technology could link all healthcare stakeholders in a high level of security and interoperability of data [16]. The healthcare ecosystem includes patient engagement, health information exchange (HIE), detecting counterfeit drugs, R&D diagnostics, artificial intelligence (AI)-based diagnostics, clinical research patient safety event reporting, adverse event identification, and public health reporting. To develop one blockchain use case, the blockchain network platform such as Ethereum allows the developers to create blocks that hold the crypto assets, write and share smart contracts while Hyperledger and Multi-chain are private open source platforms to develop the Blockchain system. Blockchain has promising potential in medical records systems, the disintermediation of trust would not likely require a middle institution because all the participants could have access to the distributed ledger to maintain a secure exchange without the need to trust. A distributed framework for patient digital identities, which uses private and public identifiers are secured through cryptography, which is a more secure method of protecting a patient’s identity. Shared data enables near real-time updates across the network to all parties. It will also allow a distributed, secure access to a patient’s longitudinal health data across the distributed ledger. Smart contracts create a consistent, rule-based method for accessing patient’s data that can be permissioned to selected health organisation [17].

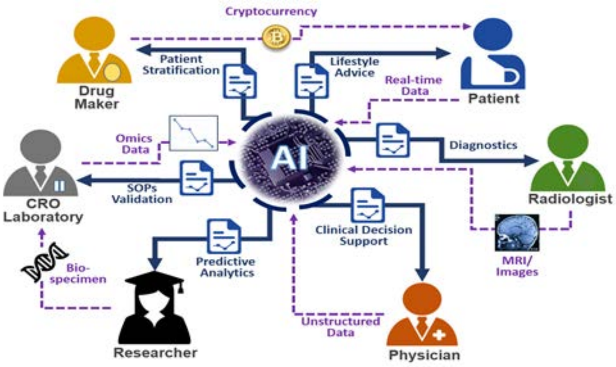


Figure 3: Blockchain technology links all healthcare stakeholders (Schumacher, 2018)

5. Discussion

Blockchain introduces a new data sharing and management model over the traditional centralised database management system in the healthcare industry. The blockchain is peer-to-peer and decentralised data management system in which each node runs independently by following a set of defined protocol. The strength of the distributed data sharing model is in its loose-coupled structure where a breach in one node has no effect on the operation of the whole network. The goal of a loose coupling architecture is to reduce the risk that a change made within one element to avoid it from creating unanticipated changes within the other elements. Limiting interconnections can help isolate problems when things go wrong and simplify testing, maintenance, and troubleshooting procedures. Nevertheless, there are concerns in the blockchain implementation. First, the data within the blockchain can be identified and encrypted especially in relation to sensitive data such as personal profile or medical record where privacy protection is crucial. Patients and healthcare providers in Australia recognise the benefits that could be gained from the sharing of health data, provided there is anonymity. A survey conducted by Research Australia in 2016 revealed over 90% of Australians were willing to share their de-identified health-related information to help advance medical research and improve patient care [18].The blockchain is one technology solution that could be used to allow such data to be securely shared.

Second, the speed and scalability of a completely distributed system would also need to be addressed because concerns have arisen in smaller blockchain-based applications such as Spotify as blocks continue to grow with use, each transaction will need longer time to process. In addition, the cost-effectiveness of the platform that holds a significantly large volume of data has to be proven in real production environments. Many challenges slow down the thorough implementation of blockchain in healthcare which includes the practicability of blockchain to manage the increasing growing data volume as this technology is still at its early phase of development. The heavy regulation of potential user industries and the need for a network to build valuable applications are part of the major consideration prior to putting the blockchain in actual implementation. Blockchain could make a meaningful swift of regulation in many industries in terms of workflow, transaction procedure, and business practice. The General Data Protection Regulation (GDPR) EU has taken a firm stance on data privacy, implementing stringent regulations that have notable implications for blockchain. Nonetheless, healthcare may fall into a grey area where many concerns not yet fully addressed such as data sharing consent from the patient, data aggregation and data coordination especially when a patient moves to another city or country. Furthermore, as blockchain technology works on a network, one cannot do much with the technology in isolation. This makes developing blockchain application difficult in the sense that either a group of users or a number of partners is required [19]. Finally, accustoming the untechnical literate to the complexity of the underlying technologies in a blockchain such as hash functions and cryptography is another hurdle that needed to be overcome by the blockchain developers.

6. Conclusion

Blockchain technology acts as an excellent data sharing facility and management platform for the healthcare industry due to its high level of security and immutability. This paper provides an overview of what the technology has achieved in the healthcare industry. Since working on the implementation will be a continuous development process, questions such as the ownership of data, handling the cost, a new requirement, and the regulation issue will be raised when blockchain becomes another instance of healthcare innovation. In short, a blockchain is suitable for applications which are independently managed because it reduces the need for the middle institution. The scalability of the blockchain system should be properly managed by considering the latency and maintainability in the long run.

References

[1]. Crosby, M., Nachiappan Pattanayak, P., Verma, S. & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. Applied Innovation Review, vol. 2, pp. 6–19.

[2]. Swan, M. (2015). Blockchain: Blueprint for a new economy. Sebastopol, CA: O'Reilly Media.

[3]. Mattila, J. (2016). The blockchain phenomenon – The disruptive potential of distributed consensus architectures. ETLA Working Paper, no. 38.

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

[5]. Ream. J., Chu, Y. & Schatsky, D. (2016). Upgrading blockchains: Smart contract use cases in industry. Deloitte Insights.

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

[7]. Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. Ethereum project yellow paper, vol. 151, pp. 1-32.

[8]. Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. Ieee Access, 4, 2292-2303.

[9]. Ashish.2017.Know which blockchain or DLT platform works well within your usecase:- Comparison of different Blockchain.

[10]. Randall, D., Goel, P. & Abujamra, R. (2017). Blockchain applications and use cases in health information technology. Journal of Health & Medical Informatics, vol. 8, no. 3.

[11]. Angraal, S., Krumholz, H. M. & Schulz, W. L. (2017). Blockchain technology: applications in health care. Circulation: Cardiovascular Quality and Outcomes, vol. 10, no. 9, e003800.

[12]. Kish, L. J., & Topol, E. J. (2015). Unpatients—why patients should own their medical data. Nature biotechnology, vol. 33, no. 9, pp. 921.

[13]. Ekblaw, A., Azaria, A., Halamka, J. D. & Lippman, A. (2016). A case study for blockchain in healthcare: "MedRec" prototype for electronic health records and medical research data. In Proceedings of 2nd IEEE conference on Open & Big data, vol. 13, p. 13.

[14]. Office of the National Coordinator for Health Information Technology. (2015a). Version 1.0. Connecting Health and Care for the Nation: A shared nationwide interoperability roadmap.

[15]. Office of the National Coordinator for Health Information Technology. (2015b). Report to Congress. Report on Health Information Blocking

[16]. Schumacher, A. (2018). Epigenetics of Aging and Longevity: Challenges and Future Directions. In Epigenetics of Aging and Longevity, pp. 499-509.

[17]. Deloitte. (2016). Blockchain: Opportunities for health care.

[18]. Wheelahan.F (2017). Using blockchain to secure and share health data.Corrs Chambers Westgarth.

[19]. Seppälä, J. (2016). The role of trust in understanding the effects of blockchain on business models.