Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 8, July 2021: 4498-4507

Blockchain based healthcare information exchange systems for security of healthcare data

Garima Mathur[a], Anjana Pandey[b], Sachin Goyal[c]

[a]Department of Computer Science and Engineering, UIT, RGPV, Bhopal
[b,c]Department of Information Technology, UIT, RGPV, Bhopal

Abstract

Medical care administrations are changing to empower a patient-driven methodology, blockchain-based medical services frameworks can help in improving the security as well as constancy of patients' information since patients can now have authorized access over their medical care records. With the incredible potential in healthcare system for making data immutable and secure blockchain is gaining importance. Storage of clinical information of patients is significant in medical care. These information's are exceptionally sensitive and in this manner additionally an ideal objective for digital assaults. It is imperative to make sure about all delicate information. Another perspective is command over information which would preferably be overseen by the patient. Thusly, sharing and getting to the control of patients' medical services information is another utilization case which can profit by cutting edge present day innovations. Blockchain innovation is extremely powerful against attacks, and gives various techniques for access control. Consequently, blockchain gives a decent structure to medical care information. Those groups of people who don't trust one another but still want to share data without including a trusted third-party for them blockchain would be most appropriate solution. In this paper it has been surveyed about how blockchain technology can be used to achieve security and privacy in biomedical and healthcare information exchange system.

Keywords: Healthcare, Blockchain, biomedical, Distributed Ledger, FASTA.

1. Introduction

Blockchain is a technology that enables information to be stored and exchanged on a peer-to-peer1 (P2P) basis. Basically, blockchain record can be consulted, shared and secured way to consensus-based algorithms. It is utilized in a disseminate way and expels the requirement for intermediaries, or "trusted third parties".

Trust-enforced security among the numerous estimations of blockchain technology can be considered as the primary one. The algorithm consists of infinite chained block architecture that makes it more secure and hard to infiltrate by attackers.

In the simplest term a blockchain is a sequence of immutable records managed by a group of computers not controlled by any single substance. These blocks of information are kept bounded to one another using cryptographic standard (for example chain).

All in all, what is so extraordinary about it and for what reason would we say we are stating that it has industry-disrupting abilities? There are no central authorities in blockchain network which is the very definition of a democratized framework. The data in it is open for anybody and everybody to see as it is immutable and shared records. Henceforth, those who are involved in blockchain are responsible for their activities and those who are based on it are transparent by its nature.

1.1. Motivation

Picture a spreadsheet that that is copied a huge number of times over a system of PCs. At that point envision that you have a basic knowledge of the blockchain and this system is intended to normally refresh this spreadsheet. In blockchain data exists as a common database which is continually reconciled. Utilizing the system in this way shows clear advantages. The blockchain database isn't stored in any single location; the records are kept open and easily verifiable. The hackers cannot corrupt this information as there is no centralized version of it available. Below are some reasons for blockchain's admirations-

- It is decentralized by its nature as it is not possessed by a single substance.
- It cryptographically store information inside
- It makes data immutable, so that nobody can mess with the information that is inside the blockchain
- The data inside blockchain can be tracked as it is transparent.

Transparency feature of blockchain can be considered as the most fascinating and misjudged idea because some individuals state that blockchain is transparent and other state that it gives you secrecy. For what reason do you believe that occurs?

The identity of a person is represented only by their public address and covered up by means of complex cryptography. Thus, if you somehow happened to look into an individual's transaction history, you will see "0x5eFd6F7c79447eAaCD0c13B4AE17c8F64188ddC5" sent 1 BTC" instead of "Alice sent 1 BTC".

So, even if the individual identity is hidden, we can still observe the transactions that have been made using their public address.

Another most important feature of blockchain technology is immutability, which implies that once something has been gone into the blockchain, it can't be altered. Would you be able to envision how significant this will be for money related establishments? Envision what number of misappropriation cases can be stopped if somehow someone can realize that they can't "work the books" and mess with organization accounts. Only because of cryptographic hash the blockchain gets this property.

1.2. Blockchain technology as a distributed Ledger

Blockchain's are the linked list of records known as block, time-stepped and connected through a cryptographic hash value which are fixed in a protected and unchanging way [1, 2]. It has a continually growing list where every new block will be added at last .Each new block points towards its previous block through cryptographic hash value [3]. Blocks in blockchain are sorted out in a distributed (P2P) network. Every node holds two keys [4]: one is utilized for encoding the messages

(i.e. for encryption) known as public key and other is utilized for unscrambling the messages (i.e. for decryption) known as private key that permits a node to understand it. Only the correct private key can unscramble the messages encoded with the relating private key. In this way the consistency, irreversibility and non-repudiability of a blockchain can be achieved [6].This is known as asymmetric cryptography, further details can be found in [4,5].

Every block of a blockchain are linked together with the help of cryptographic hash that is generated by a cryptographic hash function such as SHA256 .It also guarantees for the anonymity, compactness and immutability of the block [7].

Everytime a node makes a transaction it will be first signed and then communicated to the network for further affirmation. Every transaction is signed by a private-key for ensuring authenticity and integrity of transaction. In the network transactions which are dispersed and have been considered legitimate are first arranged and then packed in a block by some specific nodes, known as miners when the network utilizes explicit agreement systems, for example, proof-of-stake and proof-of-work.

How the miners are picked and what information must be there in the block rely upon the agreement convention Consensus protocol will finally decide about the how miners must be selected and what data should be there. The selected blocks will be then transmitted across the network, the approving nodes then confirm whether this got block contains legitimate transactions as well as verifies that whether it refer to the past block in the chain or not by the use of its corresponding hash. Furthermore if both conditions are satisfied the block will be added to the chain by node otherwise it will discard the node.

The essential work carried out by blockchain nodes are:

- interfacing with the blockchain network
- saving updated ledger
- listen to transaction carried out
- passing on the legitimate transactions into network
- tuning in for recently fixed blocks
- approving recently fixed blocks— affirming transactions
- generating new blocks and passing it

1.3. The need of blockchain in healthcare

Blockchain is considered to have incredible potential in healthcare system [8]. In order to improve medical services the authority must be assigned to administration of information and its ability to connect different systems can increment the precision of electronic health records. This technology can be utilized in drug prescriptions as well as supply chain management, pregnancy and any sensitive information the executives just as to help access control, information sharing and overseeing of a review trail of clinical exercises. Other medical services zones that can profit by blockchain innovation are supplier accreditations, clinical charging, contracting, clinical record trade, clinical preliminaries etc.

Medical care administrations are changing to empower a patient-driven methodology. Blockchain-based medical services frameworks can be helpful in improving secrecy as well dependability of patient's information because now patients can have authority of their medical care records.

Storage of clinical information of patients is significant in medical care. These information's are exceptionally sensitive and in this manner additionally an ideal objective for digital assaults. It is imperative to make sure about all delicate information. Another perspective is command over information which would preferably be overseen by the patient. Thusly, sharing and getting to the control of patients' medical services information is another utilization case which can profit by cutting edge present day innovations. Blockchain innovation is extremely powerful against attacks, and gives various techniques for access control. Consequently, blockchain gives a decent structure to medical care information.

For individual clinical information, it would be more appropriate to use a private blockchain instead of public. Those groups of people who don't trust one another but still want to share data without including a trusted third-party for them blockchain would be most appropriate solution. [9].

2. LITERATURE REVIEW

Prior researches that have been done for the security & privacy of Biomedical and Healthcare Information Exchange Systems based on blockchain technology has been shown below.

[10] Focuses on the security of patient centric data, with no need of central authority, blockchain technology empower a decentralized and distributed environment. Use of cryptographic standards makes transaction secure as well as reliable. Nowadays, blockchain technology has gotten exceptionally popular what's more, infiltrated various areas, generally because of the prevalence of crypto currencies. One field where blockchain technology has huge potential is medical services, because of the requirement for a more patient-centric way to deal with medical care frameworks and to associate different frameworks and also improves the precision of electronic healthcare records (EHRs). The point of this paper is additionally to show the possible utilization of blockchain in medical care and to show the difficulties and likely bearings of blockchain research. in healthcare.

[11] This work proposes a loss free compression algorithm BAQALC which stands for blockchain applied FASTQ and FASTA lossless compression that enables the storage and exchange of vast amount of DNA sequencing data. The proposed BAQALC algorithm not only shows highest compression performance but also makes the DNA data immutable. This paper compares the compression ratio of various compression algorithms for five chronic diseases and the results shows that BAQALC has highest compression ration as well as provide secure storage platform.

[13][14] Depicts the case study of IoT and blockchain powered healthcare. The basic capability that humans need nowadays is health to recognize, feel and act effectively, and as such, it acts as an essential component used in the individual's development, yet in addition of nature people has a place with. While examining the patient, the doctor must write down each and every detail about personal health. Noting this measured data can cause human error. Internet-related tools, which measure the patient's condition, may solve some problems.

Everytime a patient visit to hospital, doctor has to go through his/her previous medical record. By using connected devices, all data is stored directly in his / her HER. Although doctors still need to examine the patient but now it will save their time. with the help of this special devices we can continuously monitor patients condition. Likewise, wearable gadgets can give more important information to specialists and scientist for better understanding of diseases, by checking explicit things all day, every day, so that we can prevent the happening of any event and can save lives.

With the use of a monitoring system and IoT devices, storage of large amounts of data is possible which can also result in updating the patient's electronic health record [14] . The immutability characteristic of blockchain technology, allows the user to keep the patient data immutable as well as provide a fully protected medical history. Users can access to their reports from anywhere at any time using the right credentials and this will not only save time but also reduce the cost of transfer of medical records between institutions.

Another issue is centralized systems because centralized control can have many downsides that make it difficult to collaborate between institutions. On the other hand, blockchain is evolutionary, appreciated and very new technology. Storing this large amount of data on the blockchain is an issue. However, replication of this data still remains the primary concern. Big data technology would be the most appropriate solution to this problem. Using block chain as well as big data makes it more powerful, for example blockchain DB [13] [14].

[15] depicts a case study of medical use case of internet of things and blockchain that intends to give an answer for the issue of unreliable storage of health records, by proposing a blockchain based internet of things model where the ongoing information as for a patient's restorative status is collected by means of a bio-sensor and stores it in the blockchain. Along these lines immutable data storage can be generated. By conveying a smart contract the final medical clinic bill can be determined alongside insurance coverage. This would nullify the need of outsider suppliers and make a straightforward framework (transparent system). The paper additionally proposes the utilization of Inter planetary document framework to save the details of discharged patient records subsequently diminishing the heap on the genuine blockchain. Generally this will definitely profit patients and specialists the same by making a protected and straightforward condition alongside speedy reaction to a patient's need.

[16] This work focuses on the application of blockchain in healthcare. Blockchain has likewise collected excitement as a phase to improve the credibility and straightforwardness of therapeutic administrations data through many use cases, from keeping up consents in electronic health records (EHR) to streamlining claims processing. The author likewise depicts the fundamental of blockchain and shows the present and future utilizations of this innovation inside the healthcare industry.

[17] An immutable DNA sequence data transmission for next generation bioinformatics using blockchain technology has been created after fast growth in the high throughput DNA sequencing technology, and also there is a reduction in the cost of genome-sequencing, that has led to a advances in the genetic industries. However, the reduction in cost and time required for DNA sequencing there is still an issue of managing such large amount of data. Also, the security and transmission of such huge amount of DNA sequence data is still an issue. The idea is to provide a secure storage platform for future generation bioinformatics systems for both researchers and healthcare user. Secure data

sharing strategies, that can permit the healthcare providers along with their secured substances for verifying the accuracy of data, are crucial for ensuring proper medical services. In this paper, it has been surveyed about the applications of blockchain technology for securing healthcare data, where the recorded information is encrypted so that it becomes difficult to penetrate or being removed, as the primary goals of block-chain technology is to make data immutable.

3. Problems identified in managing healthcare data

There is a vast range of applications of blockchain technology in healthcare environment. It can be used for securely exchange of patient's healthcare records, management of the medicinal supply chain and could be very helpful for the healthcare researcher's for unlocking of the genetic code. The blockchain technology is already gaining importance from securely encryption of patient's record to dealing with the flare-up of unsafe infections.

The most well known blockchain's medicinal services application nowadays is to keep our significant clinical information protected and safe because security is considered to be a big issue in the healthcare system. Somewhere in the range of 2009 and 2017, in excess of 176 million patient records were uncovered in information breaks. The culprits took Visa and banking data as well as the healthcare records.

Blockchain has the ability to keep patient's data immutable, decentralized and transparent which makes it an innovation overflowing for security applications. Furthermore, as the blockchain has a contradictory feature i.e it is both transparent as well as private. Here individual's identity is covered with secure and complicated codes that can ensure the safety of clinical information. The decentralized idea of this technology also allows patients, specialists and medical service providers to have a similar data rapidly and securely. Some data security related issues in healthcare are given below

- **Problem 1: Information Security of Clinical Trials**

Clinical trials are used for either approval or rejection of any medicine or we can say it is used to determine effectiveness of particular medicine. Researchers are always interested in collecting and recording information related to results of tests, quality analysis etc. Every researcher is liable for explicit examination, making it hard to control everybody. This information would then be able to be effortlessly altered or covered up to change the entire result of the research performed.

- **Problem 2: Patient Data Management**

The Health Insurance Portability and Accountability Act (HIPAA) strictly regulate the patient's data privacy, and expect that PHI to be absolutely secure. There is, in any case, another issue identified with PHI: some of the time, patients need to impart their clinical records to outsiders (for example with drug stores when they have to purchase explicit meds). So, how can blockchain provide partial access as well as protection of data at same instance?

4. Solution for data security issues in healthcare

- This era lets in everybody to prove the validness of any report which is registered in device. It provides proof-of-existence through adding records within the form of the transaction and

validating the information by all system nodes. As noted above, blockchain records immutable data. It gives evidence of-presence through adding records inside the type of the exchange and approving the data by all framework hubs. As verified above, blockchain records unchanging information. This feature allows clinical trials data to be immutable and makes it difficult to modify. In 2016 an investigation has been made by two specialists from Cambridge University to perceive how blockchain can give evidence of presence to clinical preliminaries. After comparing the code generated by system with the original code they reached to the conclusion whether data has been changed or not. This is the unique feature of SHA 256 that makes a unique hash each time an alteration has been done to the information.

- For each PHI block, blockchain generates a hash along with ID of paitient. By using an API, each and every entity can get the essential data without uncovering a patient's personality. What's more, a patient can conclude whom to give access and whether this entrance will be either full or halfway. Moreover, if the patient was not sure about what he or she was doing they can set explicit outsiders that would need to give their consent for sharing the PHI. Blockchain has a first-rate potential of use in different industries, along with healthcare.

Blockchain can be viewed as a linked list containing data and a pointer where each block will be pointing towards its previous one in a chain like structure. Hash pointer is nothing but a pointer that simply holds the address of its past block as well as the previous block’s hash value. That one little change is the thing that makes blockchains so incredibly dependable and exploring.

Now imagine, if an attacker attempts to change the information contained in block ‘n’, a slight change in nth block will automatically make a drastic change in n-1th block because of the hash function’s property. Similarly change in n-1th block will force n-2th block’s data to be changed and so on, making the chain completely different. This property of blockchain is known as immutability.

Let us see by considering an example of hashing process. For this activity, we are using the SHA-256 (Secure Hashing Algorithm 256).

Table 1. Hashing Process

Input	**Hash**
Hello	185f8db32271fe25f561a6fc938b2e264306ec304eda518007d1764826381969
Bye	128901223aac8df3b89cd75d7ec644f9924ed9dcd01e0c65ae99334a3cf9273a

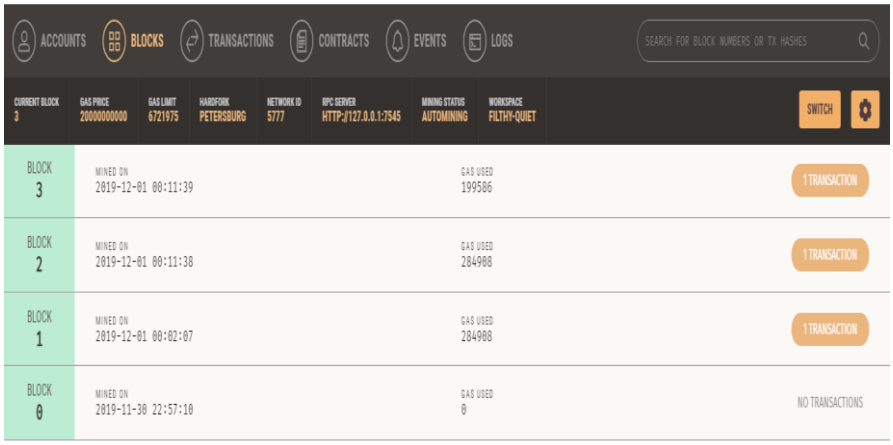
It is clear from the above example that regardless of how enormous or little your information is, we will always have a fixed 256-bits length output. This will become more critical when we have to deal with an immense amount of information. So, remembering the hash instead of input can be easier and also we can keep track of it. One interesting fact about cryptographic hash is that even a small change in input can make a big change in hash value this property is known as Avalanche Effect. Let’s see it by considering an example:

Table 2. Avalanche effect in hashing Process

Input	Hash
Hello	185f8db32271fe25f561a6fc938b2e264306ec304eda518007d1764826381969
hello.	2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824

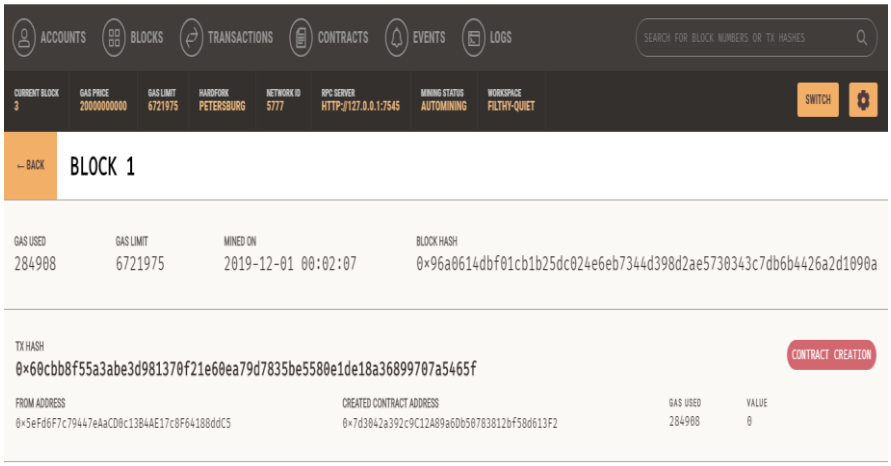
It is clear from the above example that even a small change in input can make a big change in hash value. Figure 1 depicts a linked list like structure of blockchain, where each block contain data and a pointer pointing towards its previous one.

Figure 1. Preview of ethereum exchanges



Complete detail about block 1 is shown in figure 2 like hash value, source address, mined time etc

Figure 2. Detailed preview of ethereum block.



5. Conclusion

As we know that storage of clinical information of patients is significant in medical care. These information's are exceptionally sensitive and in this manner additionally an ideal objective for digital assaults. It is imperative to make sure about all delicate information. Another perspective is command over information which would preferably be overseen by the patient. Thusly, sharing and getting to the control of patients' medical services information is another utilization case which can profit by cutting edge present day innovations. Blockchain innovation is extremely powerful against attacks, and gives various techniques for access control. Consequently, blockchain gives a decent structure to medical care information. Blockchain can be utilized in a situation where numerous gatherings who don't confide in one another need to associate and trade basic information, yet might not want to include a trusted third-party. Therefore, this work comprises of a brief introduction to blockchain technology, security issues in healthcare as well as the applications and need of blockchain in healthcare.

References:

[1] Aste, T.; Tasca, P.; Di Matteo, T. Blockchain Technologies: The Foreseeable Impact on Society and Industry. Computer 2017, 50, 18–28.

[2] Roehrs, A.; da Costa, C.A.; da Rosa Righi, R.; Alex, R.; Costa, C.A.; Righi, R.R. OmniPHR: A distributed architecture model to integrate personal health records. J. Biomed. Inform. 2017, 71, 70–81.

[3] Sleiman, M.D.; Lauf, A.P.; Yampolskiy, R. Bitcoin Message: Data Insertion on a Proof-of-Work Cryptocurrency System. In Proceedings of the 2015 International Conference on Cyberworlds (CW), Visby, Sweden, 7–9 October 2015; pp. 332–336.

[4] Aumasson, J. Serious Cryptography: A Practical Introduction to Modern Encryption; No Starch Press: San Francisco, CA, USA, 2017.

[5] Ferguson, N.; Schneier, B. Practical Cryptography, 1st ed.; John Wiley & Sons, Inc.: New York, NY, USA, 2003.

[6] Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress), Boston, MA, USA, 11–14 December 2017; pp. 557–564.

[7] National Institute of Standards and Technology. Secure Hash Standard (SHS); Federal Information Processing Standards Publication: Gaithersburg, MD, USA, 2012.

[8] European Coordination Committee of the Radiological. Blockchain in Healthcare; Technical report; European Coordination Committee of the Radiological: Brussels, Belgium, 2017.

[9] Wüst, K.; Gervais, A. Do you need a Blockchain? IACR Cryptol. ePrint Arch. 2017, 2017, 375.

[10] Marko Hölbl, Marko Kompara, Aida Kamišali´c and Lili NemecZlatolas. "A Systematic Review of the Use of Blockchain in Healthcare". MDPI, journal, 10 October 2018.

[11] Seo-Joon Lee, Gyoun-Yon Cho, Fumiaki Ikeno and Tae-Ro Lee. "BAQALC: Blockchain Applied Lossless EfficientTransmission of DNA Sequencing Data for NextGeneration Medical Informatics". Appl. Sci. 27 August 2018, 8(9), 1471

[12] LichengWanga, Xiaoying Shen a, Jing Li b, Jun Shao c, Yixian Yang. "Cryptographic primitives in blockchains". Elsevier Journal of Network and Computer Applications 127 (2019) 43–58.

[13] BigchainDB: A Scalable Blockchain Database, T McConaghy, R Marques, A M¨uller, D De Jonghe, T. T McConaghy, G McMullen, R Henderson, S Bellemare, A Granzotto, June 8, 2016, ascribe GmbH, Berlin Germany, https://www.bigchaindb.com/whitepaper/bigchaindb -whitepaper.pdf

[14] BigchainDB features, https://www.bigchaindb.com/features/

[15] Tushar Dey, Shweta Sunderkrishnan, Shaurya Jaiswal, Prof. Neha Katre ," HealthSense: A Medical Use Case of Internet of Things and Blockchain" . Proceedings of the International Conference on Intelligent Sustainable Systems (ICISS 2017) IEEE Xplore Compliant.

[16] Angraal,S.;Krumholz,H.M.;Schulz,W.L. Blockchain Technology: Applications in HealthCare. Circ.Cardiovasc. Qual. Outcomes2017,10,e003800

[17] G. Mathur, A. Pandey and S. Goyal, "Immutable DNA Sequence Data Transmission for Next Generation Bioinformatics Using Blockchain Technology," 2nd International Conference on Data, Engineering and Applications (IDEA), Bhopal, India, 2020, pp. 1-6, doi: 10.1109/IDEA49133.2020.9170715.