Electronic Health Record Sharing System Using Smart Contract

K. C. Suhas Holla[1], Shraddha S. Varekar[2]

[1,2]UG Scholar, Department of Computer Science, JSS Academy of Technical Education, Bangalore, India

Abstract*: Due to enhancement of the information technology all over the world, electronic health records (EHRs) have become a general method to store the patients' health record in hospital databases. When a patient visits a hospital, the health record is stored in that hospital database. If the same patient visits another hospital, that health record from the previous hospital is not accessible by the present hospital. Thus, sharing of sensitive information of patients among healthcare providers while maintaining the integrity of the data and protecting patient privacy has become a key issue for the healthcare industry nowadays. And, it is very tiresome and tedious task to construct a consolidated health record for a patient by collecting records from different hospital databases due to the security and privacy concerns. In healthcare Industry currently, involving patient at every stage of treatment and diagnosis, thereby building a coordinated care system is gaining attention. The patient health record must be accessible at each step of medications and multiple parties should be granted access to view, edit, and share records while preserving the precision and updation of records timely and securely. We know that, the personal health data is very sensitive and estimable. Thus, to address the key challenges faced by healthcare industry today, it is ideal to use blockchain technology for sharing health record. A blockchain Electronic Health Record sharing system utilizes smart contract to grant access to the medical records and it improves data sharing quality and maintains the privacy of records. In this paper, we will realize the true supremacy of using blockchain for sharing EHR involving patient at every step.

Keywords*: Healthcare Industry, Blockchain, EHR, Privacy, coordinated care.

1. Introduction

A blockchain is a distributed decentralised ledger to record transactions between parties.[1] Beyond financial industry, where much of the initial development is taking place, blockchain also has the power to revolutionize the healthcare industry.[2] By providing hospitals, patients, researchers, clinical trial practitioners and other healthcare professionals with a mechanism for the controlled exchange of sensitive, permissioned data, blockchain technology can improve data sharing and interoperability between data systems. Healthcare organization that takes part in a blockchain confederation can share medical information, without worrying about their native electronic health record systems. Blockchain also helps healthcare organizations to deliver more efficacious medications and diagnoses through increased provider data sharing, and potentially secure and more powerful clinical trials through research methods. Smart contracts are self-executing contracts with the terms of the agreement between interested parties. They are written in the form of program codes that prevails across a distributed, decentralized blockchain network. Smart contracts allow transactions to be conducted between anonymous or untrusted parties without the need for a central authority [2].

In this paper we propose a system on how health records could be shared among stakeholders while still taking in consideration of the patient privacy and data integrity by using blockchain technology.

2. Related Work

As we progress to the new edges of technology in today's decade, blockchain [3, 4] has been advancing a lot in the domain of healthcare to solve issues pertaining to security, privacy and authenticity of medical records. One of its most effective and powerful characteristics is its decentralized server configuration. Storing the medical records on a centralized server may be receptive to attacks from malicious third parties, and thereby failure of an important system will cause service failure which affects the organisation in critical ways. However, a decentralization based system has high probability to keep this issue away and enable continuous service. One more favourable factor of blockchain is that, due to the privacy guaranteed by the hash functions [5] and the proof-of-work [6], it is difficult to play with the transactions that exists in the blocks. As far as we are aware of, there are very few research results in health record sharing system using blockchain that takes patient at each level of medication. In [7], a technique for patient information exchange network is proffered. There are two main contributions. First, it advises on solving the issue related to interoperability by EHR linguistics and pattern checking to ensure that all EHRs in the blockchain network have the same pattern. Secondly, it has preferred an algorithmic solution to randomly select the next miner to preserve computational power and system resources. And, [7] suggests involving blockchain encryption, privacy maintaining keyword searches and smart contracts to provide personal security and anonymity, but there is no detailed method incorporated. The medical system MedRec submitted in [8] is based on smart contract for easy administration of EHRs. Parties identification characters

International Journal of Research in Engineering, Science and Management
Volume-2, Issue-12, December-2019
www.ijresm.com | ISSN (Online): 2581-5792

607

are matched to their Ethereum addresses in registrar contracts (RCs) to keep parties anonymous. However, [8] does not provide any elaborated techniques to solve issues such as how patients' EHRs are encrypted and accessed by authorized personnel, how parties are authenticated and how to maintain a log about EHRs' access. In [9], a blockchain based Application Healthcare Data Gateway (HGD) is built to provide patients an easy way to control and manage their health records. All data are stored in the blockchain cloud and administered through the data management layer. Only the authorized personnel can access patients' data, the copy of which may be destroyed when the authorized session is over. [10] focuses on discussing about the main prospects of health records, and the pros and cons of using blockchain on the storage and retrieval of health records.

3. Proposed System

We propose a health record sharing system using blockchain technology [11] based on the work done in [12]. The system we propose is secure and allows patients to administrate control over their own health records while still granting other stakeholders to have an easy access to the records with right permissions (see Figure 1).
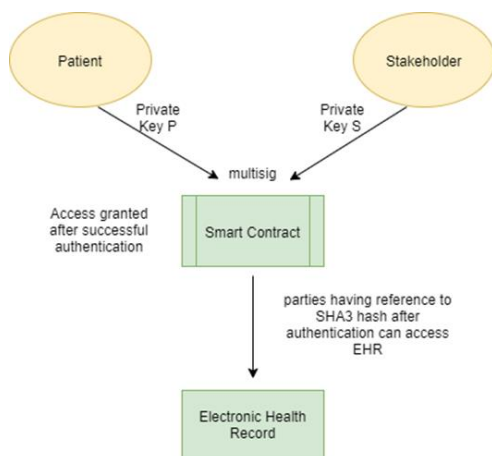

Fig. 1. Overview of Health Record Sharing System with multi signature

We deploy our EHR model based on the Ethereum service, which is a decentralized platform that allows us to run applications on a custom built blockchain. As blockchains do not innately provide enough storage space, we store the actual health records on a decentralized [13] cloud storage known as Ethereum Swarm (ES), a native base layer service of the Ethereum web3 stack that functions as a distributed storage platform and content distribution system. Each medical record will have a unique swarm hash, basically a regular hash function (in our case SHA3), which combined with the decryption key, makes the root chunk. The basic unit of hashing is known a chunk. Only those with the pointer to the root chunk can access the electronic health records. Thus, the root chunk is safely stored in SC's with the help of blockchain and are granted access only under certain specific scenario if certain

conditions are met.

To evade the problem of data ownership and control of accessibility, we use multi-signature contracts. Multi-signature contract needs multiple user, in our case the patient and the stakeholders, to both use their secure private keys to sign a transaction for validating authentication. With the help of this technique, the record owner will not be able to alter them without permission of the hospital, but she still can control which all entities can access her medical record. A new SHA3 hash (Swarm hash) must be generated on each iteration after the record has been accessed previously as the old hash will be known now, Thus, we also add a "previously accessed" timestamp (TS). The change in the actual data will spontaneously change the hash, which can then be secured once again till it receives the grant for access through smart contract. This system not only provides the security and inflexibility offered by the blockchain, but it also includes a multi-signature contract to solve the data control and accessibility problem.

4. Future Scope

Analyzing the outcomes that were obtained from the literature review and our proposed system, we assert that Blockchain technology might be a future suitable solution for all the key problems in the healthcare industry, such as EHR interoperability, sharing trust among healthcare providers, privacy and security concerns, and granting of health data access control by patients, which would in turn provide them the power to choose with whom to share their electronic medical records. However, further analysis and research, clinical trials, and experiments must be conducted to ensure that a secure and conservable data sharing system is implemented prior to using Blockchain technology on a large scale in healthcare industry, since a patient's health data are very personal, highly estimable, very sensitive, and is critical information.

5. Conclusion

As blockchain maximizes security and interoperability, the same technology can be used in many different areas of the healthcare industry, such as for storing and sharing health records and insurance information both in healthcare domains and in mobile applications, and for clinical trials. Research about blockchain's applications to healthcare is currently qualified, but more research becomes available each day. Blockchain is one of the most active and blooming areas of research presently, and it can change the dimensional hierarchy of the entire healthcare industry by giving control over medical records and health data to the very own patient. This transmission of control may in turn lead to an overall shift in the healthcare industry toward patient centered care; the blockchain movement for patients is just the beginning of what it can do.

References

[1] Shuai Wang, Yong Yuan, Xiao Wang, Juanjuan Li, Rui Qin and Fei-Yue Wang, "An Overview of Smart Contract: Architecture, Applications, and Future Trends," in *2018 IEEE Intelligent Vehicles Symposium (IV)*.

[2] D. Tapscott, and A. Tapscott, "Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World," *London: Portfolio,* 2016.

[3] R. Dennis, G. Owenson, and B. Aziz, "A temporal blockchain: A formal analysis," in *2016 International Conference on Collaboration Technologies and Systems (CTS)*, pp. 430–437, Oct 2016.

[4] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *2015 IEEE Security and Privacy Workshops*, pages 180–184, May 2015.

[5] Bart Preneel, "Universal One-Way Hash Functions," *Springer US, Boston, MA,* 2005, pages 643–644.

[6] Ning Shi, "A new proof-of-work mechanism for bitcoin," in *Financial Innovation,* 2(1):31, 2016.

[7] Kevin Peterson, Rammohan Deeduvanu, Pradip Kanjamala, and Kelly Bole, "A blockchain-based approach to health information exchange," 2016.

[8] Asaph Azaria, Ariel Ekblaw, Thiago Vieira, and Andrew Lippman, "Medrec: Using blockchain for medical data access and permission management," in *2016 2nd International Conference on Open and Big Data (OBD)*, 2016.

[9] Xiao Yue, Huiju Wang, Dawei Jin, Mingqiang Li, and Wei Jiang, "Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control," in *Journal of Medical Systems*, 40(10):1–8, October 2016.

[10] Paul Tak Shing Liu, "Medical Record System Using Blockchain, Big Data and Tokenization," pages 254 – 261 in *Springer International Publishing*, Cham, 2016.

[11] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).

[12] Hannah S Chen, Juliet T Jarrell, Kristy A Carpenter, David S Cohen, Xudong Huang, "Blockchain in Healthcare: A Patient Centered Model".

[13] Roehrs A, da Costa CA and da Rosa Righi R, "OmniPHR: A distributed architecture model to integrate personal health records," J Biomed Inform 71: 70–81. 2017.