Yifei Wang and Ruiwei Wan

DSC180B A03_Group 2

Professor Rajesh Gupta

02/04/2022

Medical Chain Authorization Contract Report

1. Introduction

EHR(Electronic Health Records) was never intended to manage and preserve the complications of cross-institutional and lifelong medical records: Medical information for a patient comes from a variety of places, and different pieces of that information must be put together for clinicians to make efficient healthcare decisions. Because of storage constraints, EHRs frequently store health data at a single location for a few years rather than keeping all-time records for patients. EHR systems used by different hospitals are frequently incompatible. Patients who seek medical treatment at several locations must frequently retype their personal information and request data transfers across these health providers, and they encounter considerable issues accessing their reports, correcting incorrect information, and authorizing medical data.

Another concern in this area is the permission of medical records. To regulate the health industry, patient data protection procedure protocols such as HIPAA and EPHI were established, and different medical information sources have distinct authorization requirements that must be met before patient data can be shared with someone else. Sensitive data, such as the patient's gender, name, residence, zip code, and age, should not be leaked to a third party without authority; similarly, generally non-sensitive medical data should be examined with caution. No information can simply be aired or made available to the general public. Often, a physician will have all of the information they require, as well as others that they may not be aware of but are necessary to care for[2].

2. Literature Review

The distributed ledger technology (DLT) infrastructure of the Blockchain could be used to outperform conventional centralized EHR systems in terms of data access, extension, and security. Due to lower overhead and fewer intermediaries, decentralized systems on blockchain may be more cost-effective, cut transaction times, and be more efficient than the existing centralized systems. In terms of infrastructure expenses, private Blockchains usually have no interaction costs (such as transaction fees), but public Blockchains tend to not be free of charge. However, the simplicity of using a public Blockchain may outweigh the costs of licensing, establishing, and maintaining a private healthcare data exchange infrastructure[4].

We are going to compare our products with three existing healthcare applications using blockchain technology. Guardtime, a blockchain-based platform that has secured over 1 million Estonian patient records, offers an immutable auditing service as well as continuous personal data compliance and overwatch, reducing the need for external audits and including tools to flag bespoke data misuse and data tampering events for a company[3]. Another example is the MedRec project, a collaboration between the MIT Media Lab and Beth Israel Deaconess Medical Center that intends to give patients control over their own data by allowing them to decide who can access it using fine-grained access permissions built on blockchain[1]. Yet Another example is the Gem Health Network (GHN), which is being created by the US startup Gem on the Ethereum blockchain technology. Different healthcare practitioners can access the same data using GHN[2].

Although these products all offer valuable solutions to decentralized EMR, our project differs from Guardtime in that Guardtime collaborates with medical institutions and corporations to access the authorized tokens from patients, so they are essentially private corporate blockchains. However, we offer authorization smart contract solutions to existing blockchains. We also differ from the MedRec blockchain where we add more functionalities to the authorization application. GEM connects the existing systems to blockchain networks, enabling the automation of arbitrary business processes using the data and identities of those existing systems while our application would prioritize patients' needs and build on the EHR smart contracts to also offer health advice for patients.

3. Solution Overview

The current domain is mainly focused on the EHRs systems. Besides a decentralized EHR system on the Ethereum blockchain which reduces the cost of maintaining medical records at different EHR systems and preserving lifelong medical records for the patients, Our product could also offer additional functions: helping patients see multiple doctors online and improving the efficiency for patients by resolving time/location/money/medical resources limitations through this online platform.

We, therefore, propose MedCoin Smart Contract: a novel, decentralized authorization smart contract to handle patient controlled authorization systems for EHRs, using smart contract technology. Our design gives patients a comprehensive, immutable log and easy access to their medical information across providers and treatment sites. Firstly, We use smart contracts to separate sensitive and non-sensitive data when patients log their medical information and we would show legal statements (HIPAA, EPHI) to notify the patients when they are authorizing their private data to a third party. Then, the smart contracts would allow different levels of authorization of access to data. The smart contracts would also allow for the protection of private data while delivering useful medical data to health providers and doctors.

We would also implement inquiry/confirmation smart contracts for both parties during this part, we would alert patients of the possible use of private data and we would ask the doctors

whether more private data is really needed.

4. The Authorization Contract Project

We create a decentralized smart contract application built on Ethereum using solidity programming and Remix. Our product would have a smart contract interface, allowing patients to authorize their medical data for necessary and legally justifiable use and enable patients to manage different levels of authorizations for access to their medical records. We also have an interface powered by smart contracts and Ethereum for the medical stakeholders (researchers, providers, doctors, etc.) to notify when their request for data has been accepted by the patients and allow them to offer medical advice and access to reward research data.

This auditing layer of smart contracts has featured a security design that would prevent data breaches in the medical records and separate sensitive data from non-sensitive data: We separate sensitive and non-sensitive data when patients log their medical information and we would show legal statements (HIPAA, EPHI) to notify the patients when they are authorizing their private data to a third party. Then, the smart contracts would allow different levels of authorization of access to data. The smart contracts would also allow for the protection of private data while delivering useful medical data to health providers and doctors.

This authorization contract would therefore provide the medical record requesters(doctors, researchers, providers) with stratified access to medical information for research use, clinical use, or kept private; Patients could choose different authorization levels for people to access their medical records enabling a distributed system that provides layered and use for info users and info providers. This authorization smart contract would be the core construct in our medical data encryption, authorization stratification, and medical records transfer aggregation pipeline.

For the data acquisition, we plan to obtain medical data from the healthcare system that is authorized for school research use. We will transfer patients' medical records from the healthcare system to our system. Since it would be hard for us to obtain the authentic data, and the data ingestion part would be easier to implement without the smart contract, we therefore assume that the data has been cleaned and fit within this smart contract in a readable format.

By enabling decentralized storage of comprehensive, lifelong, authorized medical records for the patients, we could solve the incompatibility and enhance the interoperability of EHR. The patients could request their relevant medical records to be sent to various institutions according to their needs in a protected and made-easy way so that they no longer need to order and wait for fax when they transfer medical data between different EHR systems. Medical records could be protected from malicious distorted information and attack by the immutable and encrypted nature of blockchain technology. We could also effectively reduce the cost of medical records transfer and improve the encryption and authorization process of sensitive and non-sensitive medical data. Additionally, the smart contracts allow patients to access medical resources online so that they could get proper treatments whenever they needed and they do not have to be restricted by

the location they are at and the limited time they may have. Easy access and affordable healthcare could be guaranteed in this way.

5. Discussion

(will include discussion of strengths and weakness of our project in the end)

6. Conclusion

(will include a more comprehensive conclusion in the end)

7. References

[1] A. Azaria, A. Ekblaw, T. Vieira and A. Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management," 2016 2nd International Conference on Open and Big Data (OBD), 2016, pp. 25-30, doi: 10.1109/OBD.2016.11.

[2] Agbo, Cornelius C., Qusay H. Mahmoud, and J. Mikael Eklund. "Blockchain technology in healthcare: a systematic review." Healthcare. Vol. 7. No. 2. Multidisciplinary Digital Publishing Institute, 2019.

[3] Buldas A., Firsov D., Laanoja R., Lakk H., Truu A. (2019) A New Approach to Constructing Digital Signature Schemes. In: Attrapadung N., Yagi T. (eds) Advances in Information and Computer Security. IWSEC 2019. Lecture Notes in Computer Science, vol 11689. Springer, Cham. https://doi.org/10.1007/978-3-030-26834-3_21

[4] Mayer AH, da Costa CA, Righi RDR. Electronic health records in a Blockchain: A systematic review. Health Informatics J. 2020 Jun;26(2):1273-1288. doi: 10.1177/1460458219866350. Epub 2019 Sep 30. PMID: 31566472.

8. Appendix

Project Proposal

We propose to implement the authorization smart contracts for EHR-related medical blockchains. This auditing layer of medical blockchain has featured a security design that would prevent data breaches in the medical records and separate sensitive data from non-sensitive data: We separate sensitive and non-sensitive data when patients log their medical information and we would show legal statements (HIPAA, EPHI) to notify the patients when they are authorizing their private data to a third party. Then, the smart contracts would allow different levels of authorization of access to data. The smart contracts would also allow for the protection of private data while delivering useful medical data to health providers and doctors.

This authorization contract would therefore provide the medical record requesters(doctors, researchers, providers) with stratified access to medical information for research use, clinical use, or kept private; Patients could choose different authorization levels for people to access their medical records enabling a distributed system that provides layered and use for info users and info providers. This authorization smart contract would be the core construct in our medical data encryption, authorization stratification, and medical records transfer aggregation pipeline.