Yifei Wang and Ruiwei Wan

DSC180B A03

Professor Rajesh Gupta

03/09/2022

An Exploration on Medical Records using Blockchain Technology

1. Abstract

In this project, we set out to explore the application of blockchain technology to Electronical Health Records systems. As we are prototyping the blockchain applications on the Electronic Medical Records System using our proposed MedCoin application, we encountered several challenges. After careful evaluations and discussions, we decide to turn our project into an exploration of the pros and cons of using blockchain applications in the Electronic Health Records system. We find that the proposed authorization contract could not meet the required authentication and testification functions of EHR, which are the two essential components for EHR, we, therefore, stop in our prototyping and in our report provide a discussion of the advantages and disadvantages of using Blockchain for EHR systems. And due to the privacy issue of medical records, we also find the authorization smart contract proposal infeasible and exhibits a lack of considerations. Our prototyping of smart contract failure could serve as a valuable lesson to why centralized applications could be more proper to Medical Records related system design.

2. Problem Statement

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].

3. MedCoin Prototype 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 to secure over 1 million patients records in Estonia, provides an immutable auditing service and delivers a continuous personal data compliance and overwatch service, reducing the requirements for external audits, and incorporating the tools to flag bespoke data misuse and data tampering events for a company[3]. Another such example is the MedRec project, a project of MIT Media Lab and Beth Israel Deaconess Medical Center, which aims at giving patients agency over their own data, to determine who can access them, through some fine-grained access permissions built on blockchain[1]. The Gem Health Network (GHN) is yet another example, which is developed by the US startup, Gem, using the Ethereum blockchain platform. GHN allows different healthcare practitioners to have shared access to the same data[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.

4. Proposed prototyping: MedCoin Authorization Smart Contract

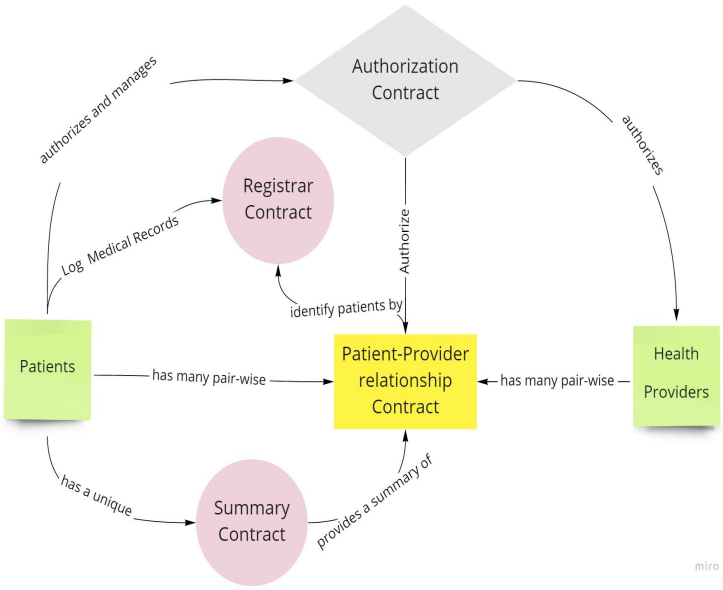

Figure 1: Proposed MedCoin Prototyping Structure

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.

5. Expected Output of Prototyping

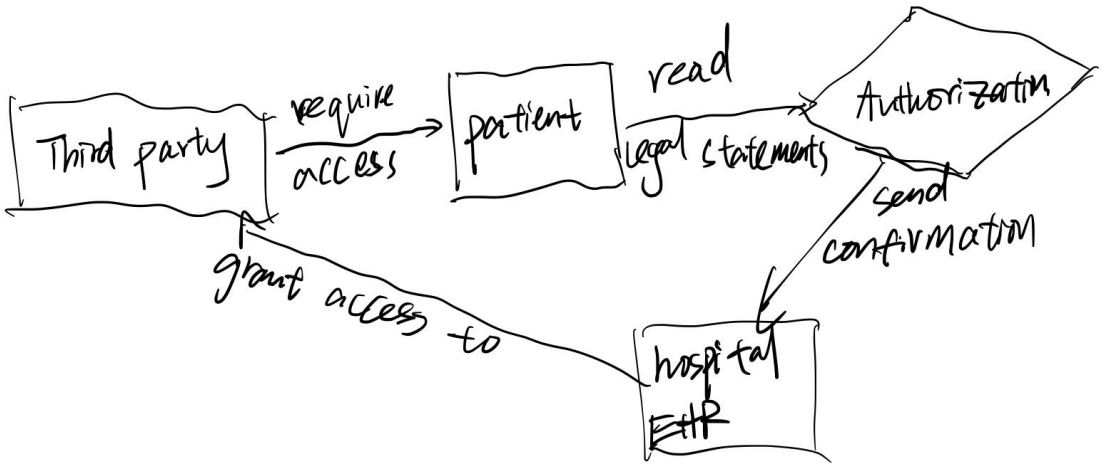

Figure 2: Authorization Contract Action Takers

We will 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 would 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.

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.

6. Actual Implementation Outcome

We originally set out to implement the whole MedCoin BlockChain Ecosystem from scratch, meaning that we would first consider the token mechanism to incentivize the miners to verify the medical data authorization records, then build the network of nodes for the blockchain infrastructure and also the smart contracts that would be automatically executed on the blockchain when input is given. However, with the limited available time of our project, we decided that it would be too ideal to build a blockchain network from scratch. Instead, we focus only on the authorization smart contract implementation, which could serve as an add-on to the existing medical records blockchain. We expect that our authorization smart contract would be patient-centric, designed for the patients, and enable the patients to decide whether they would like to share the medical data to the requesting third parties, instead of the traditionally centralized medical records systems controlled by the health providers.

For our authorization smart contract prototyping, we encountered many challenges. We were first stuck on deciding the format and content of the medical data input. We were unsure about how to align different EHR systems' medical data and automatically separate the medical records into sensitive and non-sensitive data. We realized that privacy is an especially crucial part of authorization smart contracts, if we could not determine how to recognize and protect sensitive data then we could not successfully ensure the encryption of private data and the transparency of records sharing on the blockchain. After discussing with our health blockchain advisers, we decided that we could focus on the authorization part and leave the separation part to other blockchain applications and we would only focus on giving patients the right to grant stratified data access to the requestors.

We finished the patient registry smart contract, where we would allow the patients to connect to the smart contract using a MetaMask account, which is a cryptocurrency wallet that would be essential to the blockchain user interactions. We tested this registry part of our smart contract by setting up a MetaMask account and connecting to the Ropsten test network in

Ethereum and then authorized compiled the smart contract on Remix to interact with our smart contract. We could input the patient's name and the addresses of the patient on the blockchain. We also wrote the test smart contract to test the functionalities related to the patient registry. However, we were not sure how the smart contract could store information for the patient and make the patient-id unique to the patient address on the blockchain. The smart contract has storage limitations and we simply could not store the data on the smart contracts and we have to rely on the blockchain infrastructure to store patient identity, however, as we detailed in previous sections, building blockchain infrastructure would be too complicated for prototyping purposes.

We then experimented with the relationship contract which would record which the third parties required medical records from which patients and what level of access the patients granted to the third parties. Unlike other conventional programming languages, the solidity programming we used for this project is a rather limited programming language, and it does not have as many data structures available as in Python or Java, etc. We quickly find that our relationship management smart contract would also be infeasible because we cannot find a suitable data structure to map the third-party and patient relationship which would be central to the design of the authorization contract.

Another issue is that there are many versions of solidity programming, and the grammar varies between different versions. When we tried to use the scaffold-ETH repository on Github to visualize our smart contract, we found out that the version did not match and we have to rewrite everything from scratch. This situation comes unexpectedly and we stopped our prototyping attempts there.

The deadly blow came as we finally realize that although decentralized blockchain technology is capable of solving many types of problems, for this problem, blockchain was inappropriate, because a centralized authority is required to dispatch patients' records and protect the privacy of the data transfer. Blockchain technology is a double-edged sword, it could be costly to maintain and remember the data transfer records although it does provide encryption and anonymization functions. Blockchain technology fundamentally requires anonymization, while electronic medical records require authentification, permission, and testification. The existing centralized EHR systems would hardly be revolutionalized by the use of blockchain technology because record-keeping for medical data requires more than decentralized applications. Health data is a sensitive and discretion-required topic; because it entails loads of privacy data and life decision records, which in nature provides a sharp contrast with the immature blockchain technology. Even if the above-mentioned issue could be solved, the health providers would be reluctant to provide the blockchain with access to EHR systems, because laws and regulations on patient data are heavy and essential and the decentralization would give rise to a series of new problems that we would later analyze in the disadvantages of blockchain technology part.

7. Summary on Prototyping Attempt

For our authorization smart contract prototyping, we encountered many challenges. We were first stuck on deciding the format and content of the medical data input. We then struggled with the insufficient functions solidity programming language could provide. The intrinsically limited storage space on the smart contract and blockchain node also limits our attempts. We lastly admit that it would be best to continue using the existing centralized EHR systems instead of using decentralized blockchain technology for patient data access management and authorization problem.

We also learned valuable lessons from our exploration of Medical Records using blockchain technology. We familiarized ourselves with the implementation of smart contracts using solidity programming, and we know that the versions of solidity programming must be standardized and stated before the actual implementation begins. We also learned how to use MetaMask to connect to the test network and verify if the smart contracts have the functions we desire. We realized that decentralized and anonymized blockchain technology might not be the panacea for every problem: although blockchain technology could be applied to many areas, the restrictions and nature of health data implies that we best leave the existing centralized EHR systems as they are, and reconsider the use of blockchain technology on whether it is necessary to implement a decentralized solution to a problem.

8. Discussion on Benefits and Disadvantages of Using Blockchain Technology for EHR

There are some benefits of using blockchain technology for EHR systems. Firstly, blockchain technology makes EHR systems secure and private. Cryptographic functions are used by blockchain technology to give security to the nodes linked to its network. The hashes contained on the blocks are hashed using the SHA-256 cryptographic technique. The Secure Hashing Algorithm (SHA) is a set of hashes that provide security to the blockchain by ensuring data integrity. Cryptographic hashes are one-way strong functions that generate checksums for digital data that can't be extracted. As a result, blockchain is a decentralized platform secured by cryptographic technologies, making it a viable solution for protecting the privacy of particular applications [5]. Secondly, All of the patients' data that is spread across several facilities can be integrated in an automated way. Provides healthcare providers with a comprehensive picture of the patient's medical history. A uniform data code is followed by all EHR/EMR stored on the blockchain system. Removes the possibility of data theft or mistreatment. Natural disasters do not pose a threat to health data held on the blockchain. Without having to go to different places, medical companies may readily access all of their patients' data. Provides medical institutions with global access and traceability. Allows auditors to quickly and easily check transactions. Maintains compliance with essential legal standards and regulations for healthcare establishments. It aids in the avoidance of redundant data [6]. Thirdly, blockchain, which supports a sharing and trust mechanism, could be a future option for data sharing, allowing for collaborative clinical decision-making in telemedicine and precision medicine [7].

There are some challenges to using blockchain technology for EHR systems. Firstly, data

storage on the blockchain has two major drawbacks: confidentiality and scalability. The data on the blockchain is available to everyone on the chain, making the data exposed, which is not what a decentralized platform should be. The data kept on the blockchain would include a patient's medical history, records, lab results, X-ray reports, MRI results, and a variety of other reports; all of this copious data would be maintained on the blockchain, putting a strain on the blockchain's storage capacity. Secondly, only a small percentage of the population understands how blockchain technology works. This technology is still in its early stages and is always changing. Furthermore, the transition from trusted EHR systems to blockchain technology will take time, since hospitals and other healthcare institutions will need to totally overhaul their systems [5]. Thirdly, the cost of developing, maintaining, and upgrading a blockchain in healthcare is unknown. Last but not least, It's hard to authenticate the medical data and provide a unique id for each patient to match with the records in the existing EHR. Sharing medical data is a challenge. Insider privacy violations could be encouraged by easy access to medical records.

9. Conclusion for Our Exploration

To further explore how blockchain technology could be applied to EHR systems, we first prototyped an authorization smart contract to enable the patients to manage their medical records and decide the stratified access for the requesting third parties. We proposed to implement the authorization smart contracts for EHR-related medical blockchains. 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.

However, as we finished the patient registry and nearly finished the patient-third parties relationship functions of the authorization smart contract, we found out that the features of the blockchain technology, the untested nature of blockchain infrastructure, and the limited functionality of the solidity programming language limits its application in the medical industry. Although we figured out how to connect our smart contract to the Ropsten test network using MetaMask, and how to test on Remix and using the Scaffold-ETH to implement tests, we could not go any further in our smart contract functionality. We realized that decentralized and anonymized blockchain technology might not be the panacea for every problem: although blockchain technology could be applied to many areas, the restrictions and nature of health data implies that we best leave the existing centralized EHR systems as they are, and reconsider the use of blockchain technology on whether it is necessary to implement a decentralized solution to a problem.

Our exploration shed light on the critical use of blockchain technology in the medical industry. We further provided an analysis of the pros and cons of using blockchain in the medical

industry. We concluded our exploration project by researching the current discussions of blockchain incorporation into the healthcare area. We found out that blockchain technology makes EHR systems secure and private. It would also save lots of time and money when transferring medical records. The use of blockchain technology would also help to share medical data with different doctors and allow for collaborative clinical decision-making in telemedicine and precision medicine. However, there are some challenges in using blockchain in the medical field that still exists. The blockchain has two major drawbacks when it comes to data storage: confidentiality and scalability. There is only a small percentage of the population understands how blockchain technology works. It's hard to find lots of professional people to develop and maintain blockchain technology. The costs for maintaining and developing are also unknown and expensive.

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.

[5] A. Shahnaz, U. Qamar and A. Khalid, "Using Blockchain for Electronic Health Records," in IEEE Access, vol. 7, pp. 147782-147795, 2019, doi: 10.1109/ACCESS.2019.2946373.

[6] Yaqoob, I., Salah, K., Jayaraman, R. et al. Blockchain for healthcare data management: opportunities, challenges, and future recommendations. Neural Comput & Applic (2021). https://doi.org/10.1007/s00521-020-05519-w

[7] Mayer AH, da Costa CA, Righi R da R. Electronic health records in a Blockchain: A systematic review. Health Informatics Journal. June 2020:1273-1288. doi:10.1177/1460458219866350

Appendix

For our originally proposed MedCoin White Paper, please refer MedCoin White Paper