MedCoin White Paper

Ruiwei Wan
A15650683
r2wan@ucsd.edu

Yifei Wang
A15534370
yiw014@ucsd.edu

Abstract

Medical information for a patient has multiple sources. Multiple pieces of such information need to be assembled together for effective healthcare decision-making by the physician. Different hospitals have different systems of Electronic Health Records/Electronic Medical Records, there is no uniform and complete EHR system in the medical systems due to historical reasons. Due to the lack of money, medical resources, and time, some patients do not have a chance to go to see a doctor in the hospitals. Our product is for the patients who might be in dire need of seeing doctors, or some of them who have difficult miscellaneous diseases. They want to get suggestions from multiple doctors within a short time. To solve these problems, we propose MedCoin: a novel, decentralized record management system to handle EHRs, using blockchain technology:

1. MedCoin is a governance token, voting mechanism, people who have more tokens have more say in implementation decision voting and MedCoin community voting.
2. MedCoin itself has investment value, can be turned into money and be traded.
3. Beneficiaries: patients, doctors, developers
4. Our product is a decentralized medical data storage solution and a ledger for connecting patients with the doctors and allowing patients to authorize their medical records.
5. The process of log medical records will be semi-automated.

1. Introduction

EHRs(Electronic Health Records) were 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 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 to 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).

1.1 Current Problems

We see a number of specific challenges faced by EHR systems users today:

1. Medical information for a patient has multiple sources. Multiple pieces of such information need to be assembled together for effective healthcare decision making by

the physician.

2. Different information sources have different authorization requirements that need to be satisfied before information can be released to someone else.
3. There are multiple EHR systems in use in different medical institutions, it would be costly to summarize all the existing records to form a comprehensive and lifelong medical record for the patients.
4. Oftentimes it would be hard and inefficient for the patients to correct the existing erroneous medical records in the EHR systems.
5. Patients might not have enough time/money/medical resources in the vicinity to get proper treatments.
6. The privacy of patients' medical records was not well guaranteed.

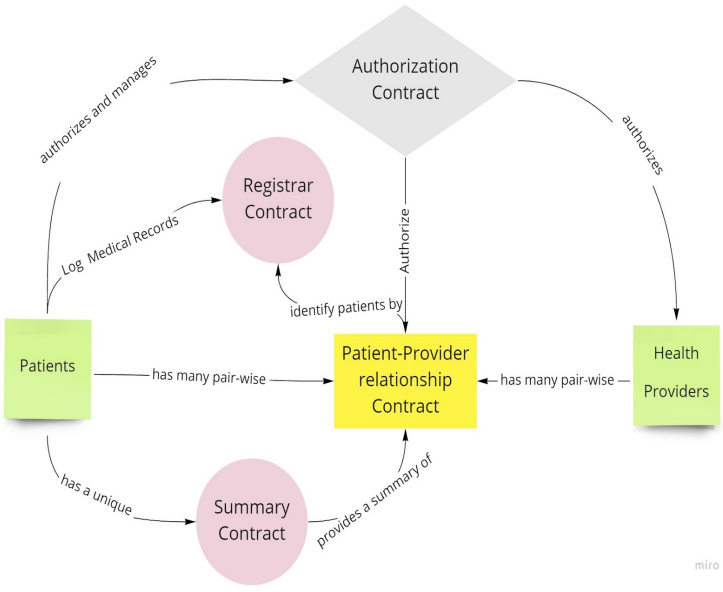
1.2 The MedCoin Project

We propose a MedCoin project as a solution to these problems. We will create a decentralized blockchain application built on Ethereum using solidity programming. Our product would have a smart contract interface, allowing patients to log their medical information, seek medical advice and authorize their medical data for necessary and legally justifiable use. 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. The network of nodes on our MedCoin blockchain would be nodes that store medical information for each patient and the authorized medical research data. The computing power would be contributed by miners that join our network.

Put together, MedCoin creates a protocol where the shared success and prevalence of this decentralized platform directly benefits the participants responsible for its success.

The significance of our product is to build trust in the medical industry. We could improve EHR interoperability by allowing decentralized storage of comprehensive, lifetime medical data for patients. Patients might request secure and easy delivery of their medical records to various institutions, eliminating the need to order and wait for faxes when transferring medical data between EHR systems. Blockchain's immutable and encrypted nature could protect medical data from malicious distorted information and attack. We could also strengthen the encryption and authorization of sensitive and non-sensitive medical data. Also, smart contracts enable patients to access medical resources online, allowing them to receive adequate treatment whenever they need it, regardless of their location or time constraints. This would ensure easy access to affordable healthcare for the good of the community.

The Medcoin smart contracts is detailed in diagram below:



2. Token Model

MedCoin is the name of our currency, which was created to align governance and financial incentives in order to maximize protocol usage and long-term protocol value. Stakeholders can acquire a claim on future issuance by participating in governance as a node operator, patient, or user, motivating value-added actors to enhance protocol adoption and drive demand back to MedCoin.

As a governance Token, MedCoin is closely linked with the voting mechanism of this decentralized blockchain technology. People who have more tokens have more say in implementation decision voting and MedCoin community voting. MedCoin is awarding miners who verify transactions. Developers, investors, and contributors of the MedCoin community can benefit from Medcoin. Any MedCoin staked within the protocol is assigned governance weight, used to shape future iterations of the protocol.

Additionally, MedCoin could be transferred. We are going to put some MedCoin in for circulation first. The first time that the patient uses our system to see a doctor is free. They could gain MedCoin by sharing their medical records. The doctors could gain MedCoin from diagnosing patients. Patients can use Medcoin to see a doctor in our products. The doctors could use MedCoin to trade some scarce data or other medical data. Among the costs of MedCoin, the patients who see doctors in specialty groups will spend more than primary care providers (PCP), and doctors will get more MedCoin from seeing patients in specialty groups.

MedCoin tokens could also be used by researchers and providers to unlock exclusive features and services, mostly anonymous medical research data. Patients could use Medcoin to purchase added services, such as suggestions from doctors. A procedural fee may be generated as transactions were verified by the miners, including patients' authorization to a third party to use their non-sensitive data. At the same time, the intermediate fee for medical treatment will be commissioned to miners of our application.

3. Registrar Contract

The registrar contract connects the identities of participants (patients, providers, and insurers) to their Ethereum addresses (equivalent to a public key). New identity regulation can be written into the contract, guaranteeing that only approved organizations can upload new data to the blockchain. In turn, new information about a patient (such as a new relationship) is only uploaded with the patient's permission. Each identification string has its own blockchain address, which is accessed by a Summary Contract. This raises certain concerns regarding the suitability of a worldwide ID system, which will be addressed later in the privacy discussion.

For this data acquisition smart contract, we plan to obtain medical data from the healthcare system that is authorized for school research use or we could have a smart contract designed to collect patients' self logged and verified medical records. The process will be semi-automated. The patients can choose to log their medical information by themselves or transfer their medical records from the healthcare system to our system. We will pop up a reminder when the patients log their medical records.

4. Patient-Provider Relationship Contract

The patient-provider relationship contract connects two nodes in the system, one of which stores and manages the other's medical records. This relationship can occur between a specific care practitioner and a patient, but it can also be used to describe any paired data stewardship contact.

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. When patients log their medical information, they will be asked to choose a specialty group or consult primary care providers (PCP). Once they select the group, their information will be sent to the corresponding group. If the patients choose to go to the PCP group, the doctor from the PCP group will refer the patients to the proper specialty group when necessary. If the patients choose the wrong specialty group, the doctor from that specialty group will

recommend the patients to the right specialty group.

After the doctor's diagnosis, the diagnosis results, recommendations, and precautions will be returned to the patients. In this program, we use our summary smart contracts to put the sensitive data and non-sensitive data together. the patient needs to verify whether the name is himself and if so, send the diagnosis information to the patient. As a reward, the doctors will get the non-sensitive data authorized by the patients and MedCoin. This modular design integrates with providers' existing, local data storage solutions, facilitating interoperability and making our system convenient and adaptable.

5. Summary Contract

The summary contract acts as a pointer, leading each participant in the system to a summary of their relationships with each other participant. The summary contract encodes a list of references to PatientProvider Relationship contracts, indicating both current and previous interactions with other system nodes. Each relationship also has a status variable that indicates when the relationship was established and whether the patient approved of it. The patient controls the acceptance, rejection, or deletion of relationships, giving them complete control over which records in their history they wish to acknowledge. This MedCoin feature is critical to meeting its usability criterion: pointers to fragmented records are gathered in a single, dedicated location.

This layer of smart contracts would ensure that feedback from the corresponding doctors and health practitioners would be automatically sent to the correct patient. It also provides a comprehensive and panoramic log of the authorization pairs in our decentralized medical records systems.

6. Authorization Contract

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.

7. 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 are public corporate blockchains. We also differ from the MedRec blockchain where we add more functionalities to the decentralized 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.

8. Summary

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.

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.

9. 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.