EPiC Series in Computing
Volume 63, 2019, Pages 34–42
Proceedings of 32nd International Conference on
Computer Applications in Industry and Engineering

Blockchain Technology applied to Electronic Health Records

Suboh M Alkhushyni , Du'a M Alzaleq, and Nadine L Gadjou Kengne
Suboh.alkhushayni@mnsu.edu, daa.al-zaleq@mnsu.edu, gadjoun@uwplatt.edu

Abstract

Blockchain technology is on the cusp of revolutionizing the way we handle healthcare data, in term of storage and utilization. The main goal is to empower patients to be the center of their own health record so that, the patient doesn't have to rely on different institutions or hospitals they might visit. Blockchain technology and smart contracts provide an interesting and innovative way to keep track of Electronic Health Records (EHRs). This technology could help the patients to have better control of their own data. Health professionals and institutions, such as hospitals, could have access to patient's data owned by other institutions. In the present article, we discuss how blockchain technologies can be used to handle EHR while improving the efficiency of operations through streamlining processes and transparency. We propose an architecture to manage and share healthcare data among different organizations. The proposed work could significantly reduce the time needed to share patient data among different health organizations and reduce the overall cost.

1 Introduction

In today world we carry our photos, video, emails, and event banking services in our mobile device. But we are still unable to hold on to our medical records. As life events take patients away from one provider's data record into another, they leave data dispersed across various health institution. The healthcare ecosystem is increasingly complex, with multiple stakeholders involved in complex and sensitive data interactions. This can lead to privacy challenges, data insecurity, and operational inefficiencies. Ownership and trusted access to medical data and administrative data is a critical process that must be made simpler, fast, and less costly. Thus, the problem of Data Health Interoperability remains open.

The main question is how to put patients at the center of their healthcare data and share medical data with known and unknown stakeholders while ensuring the protection of patient privacy, data integrity, and avoiding data misusage. In this article, we explore how blockchain and smart contracts can be applied to improve the way electronic health record (EHR) are handled across various health institutions. To do that, we will first present the blockchain methodology used to handle electronic health record then, we will propose an architecture that is able to improve the current EHR systems, we will discuss and analyze the usability of our software implementation for EHR using blockchain, and finally we will discuss some implementation challenges.

2 Related Work

We have seen a dramatic rise in the adoption of EHR technology. Today, many companies are getting acquainted with the blockchain technology to revolutionize the way they handle patient data. Blockchain technology was first import into the design of a healthcare system by Yue et al. They have proposed the architecture of a healthcare data gateway application for easy and secure control and sharing of medical data between different entities that may use patient data, without any security or privacy evaluation. Jenkins et al. proposed to use blockchain for a multifactor authentication in a specific research scenario such as medical large data analysis with functional biomarkers. This involves biometric and biomedical data. for instance, the MedRec prototype has been proposed. It is based on permissionless blockchain implementation. It uses Ethereum smart contracts for an intelligent representation of existing medical records that are stored within individual nodes on the network. Some blockchain projects currently working to innovate the EHR space includes Medibloc, Medicalchain, and Patientory. Apple is also working on bringing healthcare records to the iPhone.

3 Blockchain Methodologies for Electronic Health Record

This section first discusses some nontechnical aspects that make health data sensible and how blockchain can enable data interoperability and privacy. Then, describes the process flow used by blockchain to handle medical data, discuss and analyze the usability of our software implementation and finally discuss some implementations challenges.

3.1 Limitation of current HER and Blockchain Solutions

The state of health care records is currently unconnected due to lack of common architectures and standards that would allow the safe transfer of sensitive information among stakeholders [1]. Patient access permissions to the current EHRs are very limited, and patients are typically unable to easily share their data with researchers or providers. Despite all the advances in medicine, different EHR systems do not communicate effectively. The primary means of transferring healthcare data from one health institution to another are still through fax machines and snail mail. Each health care institution provides services, tracks, and updates the patient’s clinical information set each time a medical service is provided. This information includes personal data, such as the patient’s gender and date of birth, as well as information on the specific service provided, such as the procedure performed, the care plan. Those information’s are usually stored in a database within the organization or within a defined network of health care stakeholders. This flow of information originating from the patient through the health care organization each time a service is performed should not stop at the individual organizational level or at the health care network only. Instead, that information representing each patient interaction should be directed into a nationwide blockchain transaction layer. Thus, information stored on the blockchain could be universally available to a specific individual through the blockchain private key. The private key enables patients to share their information with different health care organizations more seamlessly. Health care information's are sensible data that must be kept in secret. Thus, each health organization’s EHR system must implement privacy policies in order to ensure that only the patient and the healthcare agents, who have explicitly granted permission by the patient, can have access to personal health records. In addition, all health care organizations connected to the blockchain should maintain and updated their own copy of the health care ledger. To help improves security and help limit the risk of malicious activities, any changes made on the blockchain are immediately broadcast to the network. The distributed ledgers provide safeguard copies against harmful hacks. In the next section, we discuss the process flow used by the blockchain technology to handle and share patient's data among different health organization.

3.2 Process Flow

The process flow of a blockchain transaction can be summarized in four main steps as shown in figure 1.

- **The health organization store information on the blockchain:**
  Health organization provides services to a patient and stored the patient's data (the doctor could write a note, or a pharmacist could dispense medicine) into an existing health IT system. Then, the data fields and a patient's public ID are redirected to the blockchain via APIs.
- **The transaction is completed and uniquely identified:**
  Each transaction is encrypted and given an identity that is stored on the blockchain, containing the patient's public (non-identifiable) ID [2].
- **Health organizations and institutions can directly query the blockchain:**
  To request the data, health organizations and institutions submit their queries via APIs and use the patient's public ID on the blockchain to retrieve the encrypted data. Patient's information's such as (e.g. age, gender, illness, physician) are now viewable and can be analyzed to uncover new insights.
- **Patients can specifically authorize any individual to access their medical information:**
  The patient's private key links their identity to blockchain data. This private key can be shared with new health organizations, which can use it to decrypt the patient's data. Thus, data remains non-identifiable to those without the key.

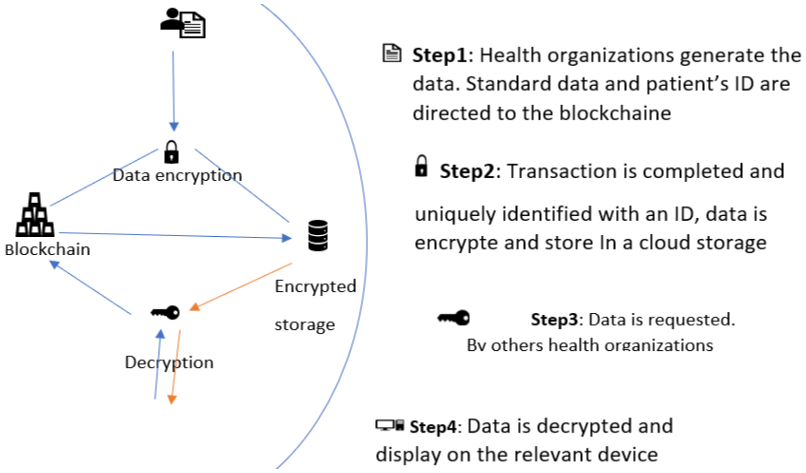
Data encryption
Blockchain
Encrypted
storage
Decryption
Step1: Health organizations generate the data. Standard data and patient's ID are directed to the blockchaine
Step2: Transaction is completed and uniquely identified with an ID, data is encrypte and store In a cloud storage
Step3: Data is requested. Bv others health organizations
Step4: Data is decrypted and display on the relevant device

Figure 1: Basic Blockchain's process flow

3.3 System Implementation

2.3.1 Background

At its core, a blockchain is a distributed system that record and stores transaction. More specifically, it is a shared and immutable record of peer-to-peer transactions built from linked transaction blocks and stored in a digital ledger [3]. Record are linked together and can provide the entire history or provenance of an asset. A transaction is added to the blockchain only after it has been validated with a consensus protocol, which ensures that it is the only version of the truth. Each record is also encrypted to provide an extra layer of security.

Blockchain was originally intended to timestamp digital document so it is not possible to backdate them. However, it went by mostly unused until it was adapted by Satoshi Nakamoto to create a digital cryptocurrency bitcoin [4] for peer-to-peer electronic cash that would allow online payments to be sent directly from one party to another without going through a financial institution. The transaction consists of moving specific amounts of Bitcoin from one account to another. Anyone in the blockchain can verify which account a Bitcoin belongs using appropriate software tools to examine the transactions on the public blockchain. In a healthcare context, transactions would consist of the documentation of specific healthcare services provided. The healthcare providers and patients would encrypt the data, which would reference a patient ID, to a public blockchain.

Blockchain uses an established cryptographic technique to allow each participant in a network to interact (e.g. store, exchange, and view information), without preexisting trust between the parties. Blockchain system does not provide central authority; instead, transaction records are saved and distributed across all network participants. The interactions with the blockchain become known to all participants and require verification by the network before new information is added. This enables trustless collaboration between network participants while recording an immutable audit trail of all interactions [1].

2.3.2 System Architecture

Blockchain technology utilizes computer science technique such as (linked lists, distributed networking) as well as cryptographic primitives such as (hashing, digital signatures, public/private keys) mixed with financial concepts such as ledgers [3]. In the blockchain technology, the centralized infrastructure is replaced with a distributed one. Blockchain software runs on thousands of nodes distributed across the entire network. When a new transaction arrives, it is distributed to all the network nodes, when all the nodes have reached a consensus to accept the new transaction into the common ledger, the transaction is added to the ledger. As the name indicates, a blockchain is a chain of blocks that contain information. It contains:

A hash: used to uniquely identify a block. Even the smallest change of input (e.g., a single bit) will result in a completely different output [3]. The blockchain technology takes a list of transactions and creates a hash "fingerprint" for the list. Anyone with the same list of transactions will generate the exact same fingerprint. If a single value in a transaction within the list changes, the fingerprint for that block changes. A block also contains the hash of the previous block.

A transaction: It is a recording of an assets (consist of documentation of specific healthcare services provided) [5]. An ID or a hash is generated for that specific transaction as a unique identifier. To validate the transaction, it is signed with a public/private key pair. Each transaction is assigned a block that cannot be altered unless the other blocks in the chain are altered. The transaction should include a digital signature of the contributor to trace the provenance of data. After the documents are stored in the blockchain, the patient would use a web-based or mobile application to view their blockchain contents and to grant or revoke access to specific parties.

*Asymmetric-key cryptography***:** (also referred to as public/private key cryptography). They are mathematically related to each other. The public key may be made public without reducing the security of the process. It is used by Health organizations and institutions on the blockchain to retrieve the encrypted data, but the private key must remain secret to retain its cryptographic protection of the data [3].

Address: It is a short, alphanumeric string derived from the user's public key. It uses a hash function, along with some additional data. Addresses are not secret and are shorter than the public keys. They are used to send and receive digital assets [3]. They are generated by taking a public key, hashing it, and converting the hash to text. Addresses represent the public-facing "identity" on a blockchain for a user. When a transaction is added to the blockchain, it is assigned an address. Users or Health organizations must prove possession of the address's corresponding private key. Thus, when a transaction is digitally signed with the private key, the transaction can be verified with the public key on the blockchain.

*Private Key Storage***:** It is stored on an external software commonly called a wallet. The wallet is a basic interface and method of access to the system. It can store private keys, public keys, and associated addresses. The wallet software can also calculate the total number of transactions a user may have. It contains the patient's identification to a blockchain. It could be a web-based or mobile application used by the patient to view their blockchain contents and to grant or revoke access to specific stakeholder [5].

Figure 2 shows the EHRs system in the blockchain. Every patient owns this chain by himself, after of specific episode of healthcare services are provided in one hospital, all the pieces of information related to the patient are encapsulated in one block.

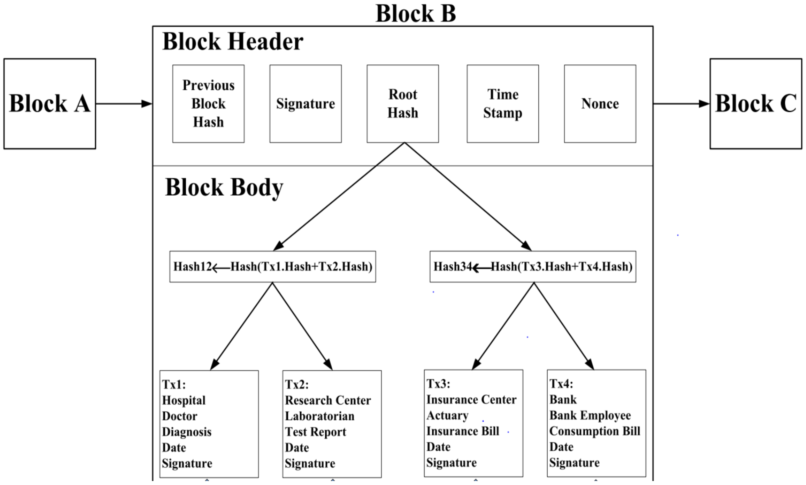
Block B
Block Header
Block A
Previous Block Hash
Signature
Root Hash
Time Stamp
Nonce
Block C
Block Body
Hash12⟵Hash(Tx1.Hash+Tx2.Hash)
Hash34⟵Hash(Tx3.Hash+Tx4.Hash)
Tx1: Hospital Doctor Diagnosis Date Signature
Tx2: Research Center Laboratorian Test Report Date Signature
Tx3: Insurance Center Actuary Insurance Bill Date Signature
Tx4: Bank Bank Employee Consumption Bill Date Signature

Figure 2: EHR ledger architecture in blockchain **[9]**

A ledger is a collection of transactions. In a healthcare context, transactions would consist of documentation of specific healthcare services provided. Healthcare providers, payers, and patients would encrypt the data. This information would be stored in the blockchain and could only be decrypted by parties who have the patient's private key. Thus, a ledger is a linked list of blocks where each block contains the patient's public key, the pointer to the previous transaction (hash of the previous block), the encrypted data(hash), and the provider's cryptographic signature. The blockchain ledger will be copied and distributed amongst every node within the network system.

A node is a computer in the healthcare network system. There is no central entity determining which node publishes the next block on the blockchain. Each node maintains a copy of the blockchain and may propose a new block to the other mining nodes. When a new transaction is submitted to a node, there is a mechanism (smart contract) to alert the rest of the network that a new transaction has arrived. The transaction will be added after the require consensus method have been met. This new block will be distributed across the system and all ledgers will be updated to include the new transaction. Invalid blocks will be detected and rejected. Whenever new users join the system, they receive a full copy of the blockchain, making loss or destruction of the ledger difficult.

To automate and track certain state transitions such as (changing the viewership rights or creating a new record in the system), the blockchain technology uses "smart contracts. A smart contract is a computer program that is stored in the blockchain and can be executed in a virtual machine [5] more specifically it is a computerized transaction protocol that executes the terms of a contract [6]. It is activated automatically when a trigger event occurs." some examples include; the execution of a new transaction, the regulation of conflicts between transactions.

3.4 Implementation Analysis and Usability

Blockchain technology is a distributed system and should, therefore, involve many participants. To use blockchain technology in healthcare industry, the health organization and other record keeping systems would encrypt the data and send them into the public healthcare blockchain as one transaction (containing patient care data, encounter notes, prescriptions, family histories, etc.). After the documents are stored on the blockchain, the patients would use a web-based or mobile application generally call wallets to view their blockchain contents and to grant or revoke access to specific parties. this technique will facilitate the process of collecting old patient data and reduce the cost of transactions.

To ensure security and trusted access to the patient's data, the ledger component could be implemented using the Ethereum platform. Ethereum uses the proof of work consensus algorithm and its peer-to-peer protocol to secure the state-machine and transition logic from tamping and to share information with all nodes participating in the system. Ethereum is a decentralized platform that runs smart contracts [7]. Smart contracts are programs written in solidity and stored in the blockchain ledgers and can be executed in a virtual machine. They are responsible to store a new transaction in the ledger, to receive and process requests to access, and to grant. Figure 3 shows a basic task performed by each actor in the system. Its development should minimize the possibilities of exposure of sensitive data. The users must create or have an Ethereum account prior to any transaction. Our basic smart contract implementation will define the following types of methods

New Record: Used to create and store a new record containing the patient's information including his address. This address will be used to retrieve the data

Request access: Create by the institution to request the content owned by a patient

Granted access: Create by a patient in response to the request access

Modify record: Create by the institution to update a patient's record

Our implemented system currently running on the test Network, allows a doctor to store new patient's information on the blockchain, allow a doctor to see or update patient's information stored on the blockchain, give or revoke access to any doctor who wishes to access patients' information. Figure 4 shows a basic interface that can be used by a patient to grant access to a doctor with an Ethereum account. and figure 6 shows a basic interface that can be used by a doctor to retrieve the patient's data. the doctor must first check if he has access before doing any further action on a patient's record.

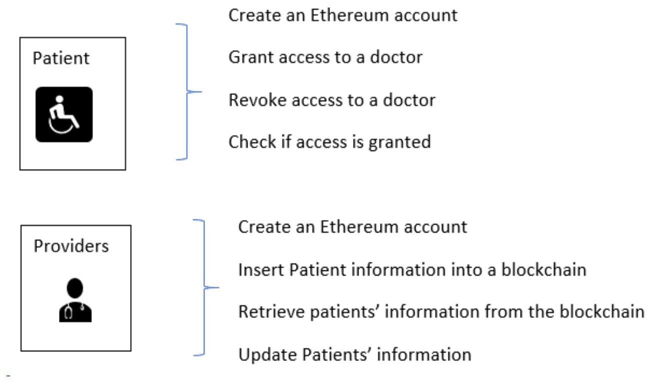
Patient
Create an Ethereum account
Grant access to a doctor
Revoke access to a doctor
Check if access is granted
Providers
Create an Ethereum account
Insert Patient information into a blockchain
Retrieve patients' information from the blockchain
Update Patients' information

Figure 3: Tasks performed by the patient and provider in the system.

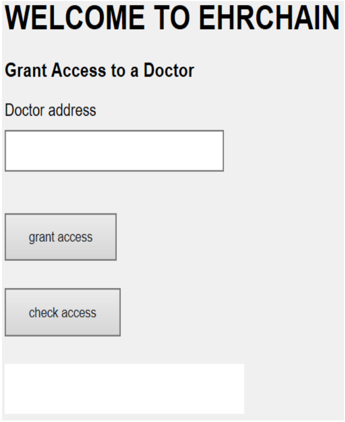

Figure 5: interface to give access to a doctor

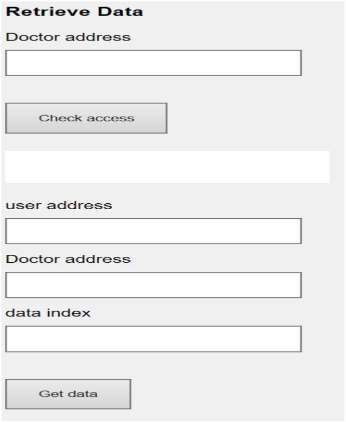

Figure 4: interface use to retrieve patient information

3.5 Implementation Challenges

Despite the numerous opportunities offered by blockchain to improve the current EHR system management, there are also concerns about it that are still preventing its widespread adoption. Several technics and organization challenges must be addressed before it can be adopted by health care organization nationwide.

Scalability constraints: Compromises between transaction volume and available computing power. In the case of Permissioned blockchains, they can expedite the transaction processing times, but they may face computing power constraints due to reduced participation in the network. For example, In the health care landscape where the United States Department of Health and Human Services (HHS) operates, The HHS could supply the computing power necessary to process all blockchain transactions on one permissioned network for select participants; however, this would result in HHS being the relative owner of the blockchain. A nationwide blockchain, with many health care participants, would make the system not only more interoperable, but it would also make it more secure [1]

Data standardization and scope: Organizations must consider what information is stored in or out of the blockchain. For health care blockchain, the most immediate concern is the size of information stored on the blockchain. A form submission of data to the blockchain, such as doctor notes, could create unnecessarily large transaction sizes that could adversely impact the performance of the blockchain. The blockchain can be efficiently operable with a specific and confined set of data, such as demographic information, medical history, and codes for services rendered. Thus, to standardize data stored on the blockchain, organizations should align on a framework for defining what data, size, and format can be submitted. Participants can also privatize the blockchain to restrict access.

Costs of operating blockchain technology***:*** While blockchain technology enables faster, near-real-time transactions, the cost of operating such a system are still unclear. Health institutions spend a lot of time and money to set up and manage traditional information systems and data exchanges. This requires resources to continuously troubleshoot issues, update field parameters, perform backup and recovery measures [1]. Blockchain's open-source technology and its distributed nature can help reduce the cost of these operations. Once the blockchain and its smart contracts are configured, the parameters become absolute and reduce the need for frequent updates and troubleshooting. Moreover, the blockchain's transparent information structure could reduce many data exchange integration points and time-consuming reporting activities.

Integration with Legacy Systems: In order to make the move to a blockchain-based system, the organization must either completely overhaul their previous system or find a way to integrate their existing system with the blockchain solution. However, it may be difficult for blockchain solutions to handle all functions needed by organizations, making it difficult to completely eradicate legacy systems. Therefore, considerable changes must be made to the existing systems in order to facilitate a smooth transition. This process may take a significant amount of time, funds and human expertise.

4 Conclusion and Future works

In this paper, we discuss how blockchain technology can be used to handle EHR (Electronic Health Record) and we propose an architecture that could be used to improve the current EHR, as well as the challenges behind its widespread adoption. We chose the Ethereum framework to implement the ledger of the proposed scenarios. It is clear from these analyses That, a medical record is the most comprehensive record about the identity of a person and must be handle in a secure manner. Because blockchain encrypted information cannot be modified or deleted, it ensures complete integrity and security of medical records from day one of its use. Thus, to enable trusted access to medical data, patients would be place at the center of their healthcare data and could grant or revoke access to any other institution who needs to access their information. The blockchain and distributed infrastructure technology are exciting developments that show promise in the healthcare industry. It should be a part of the strategic design for the business process modernization of an institution who worried about issues of security, interoperability, and privacy. Therefore,as medical information is comprised of medical records, images, documents and lab reports which require a significant amount of storage space. Conceptually, every member included in the chain would have a complete copy of the full medical record of every individual and this volume could potentially exceed the storage capacity of current blockchain technology. In the future, we plan to further strengthen the design of the interface application with login access to allow easy and trusted user interaction, add pointer to get patient's data from the provider database, deploy on the main Ethereum and investigate on the storage capability of the blockchain.

References

RJ Krawiec, Dan Housman, Mark White, Mariya Filipova, Florian Quarre, Dan Barr, Allen Nesbitt, te Fedosova, Jason Killmeyer, Adam Israel, Lindsay Tsai;, "Blockchain: Opportunities for Health re," Deloitte, 2016.

"Medicalchain: A blockchain for electronic health records," 22 February 2019. [Online]. Available: ps://medium.com/crypt-bytes-tech/medicalchain-a-blockchain-for-electronic-health-records-181ed14c2 . [Accessed 22 February 2019].

Dylan Yaga, Nik Roby, Karen Scarfone, "Blockchain Technology Overview," National Institute of ndards and Technology, 2018.

RUI GUO, HUIXIAN SHI, QINGLAN ZHAO, AND DONG ZHENG, "Secure Attribute-Based nature Scheme With Multiple Authorities for Blockchain in Electronic Health Records Systems," EE Access, 2018.

Ariel Ekblaw, Asaph Azaria, John D. Halamka, MD, Andrew Lippman, ""MedRec" Prototype for ctronic health record and medical reseach data," White paper, 2016.

"Ethereum For Beginners. Ethereum Oxford LJC Hack. The Tower - June 11

G. Wood, ""Ethereum: A secure decentralised generalised transaction ledger." Ethereum Project," llow Paper, 2014.

S. Nakamoto, "Bitcoin A Peer-to-peer Electronic Cash System," 2019.

D. S. Raymond Cheng, "Smart Contract," 2018.