A Feasibility Study of Improving Healthcare Insurance Management with Blockchain Technology

Kangqi Li

***Abstract*—At present, the identity protection problem gradually aroused peoples attention. Identity data are threatened by both the identity thefts in real life and the cybercriminals in the virtual world. Currently, there are several new technologies that could be the potential solution for this problem, such as biometric screening, face recognition and blockchain technology. Among all of these approaches, one advantage of blockchain technology is it provides a way to protect peoples identity without making the authentication procedure more complicated. Moreover, it is relatively cheap and easy to be implemented when compared with other solutions. Therefore, an identity management system with the blockchain technology is designed and developed as a proof-of-concept. This healthcare ecosystem is a decentralized application (DApp) based on the Ethereum blockchain, which can be used to replace (or in combination with) current medical identity authentication procedure. The robustness of Ethereum blockchain storage helps to reduce the potential risk of cyber attack. Moreover, by introducing the healthcare providers, the insurance provider and the beneficiary into a shared ledger, it also provides a safer approach of the insurance reimbursement procedure.**

***Index Terms*—Blockchain, Ethereum, healthcare insurance, LaTeX, insurance fraud, smart contract.**

I. Introduction

IN resent years, identity fraud is one of the fastest growing crime in many countries. [1]With the gradually adoption of electronic health records (EHR) by physicians, medical identity fraud has become the fastest growing type of identity theft whith a growth of 21.7 percent this year in the United States.[2][3] Moreover, medical identity fraud suffers more costly financial consequences than victims of other kinds of identity frauds. A study of Ponemon Institute shows Sixty-five percent of medical identity theft victims had to pay an average of $13,500 to resolve the crime in the United States.[3]

Medical identity theft, or medical identity fraud, refers to crimes that involve the theft of Personally Identifiable Information (PII) from another individual in order to obtain medical care, buy drugs, or submit fake billings to insurance providers.[4] Unlike financial identity theft, the medical identity fraud is relatively hard to be noticed by victims. Victims can notice happened crimes by the inability to purchase products or the rejection for applying loans as a consequence of financial loss. As for medical identity frauds, in most cases, the insurance provider will afford the financial loss firstly so the beneficiary will not be aware of the frauds until they are notified by the insurance provider. Moreover, the victim's medical identity information is likely to be polluted by the frauds, for example wrong blood type and allergy records. This will put victims in danger once emergency happens and the polluted identity information is in use. The low frequency for people to check and use their medical identity information, the less communication between insurance providers with beneficiaries and the delay of receiving medical billing make it difficult to prevent medical identity frauds.

Medical Identity Fraud Alliance (MIFA) has conducted a survey about the investment willing of healthcare providers towards stragegies against medical identity frauds.[5] The survey suggests that personnel is the most important property with 72% respondents ranking it as the first or second priority, while the IT system is the second one with 57% respondents attaching great importance to it.[5] This shows that current protection methods focus on the prevention of the man-made data breach as well as the malicious cyber attack. The Ponemon Institute also reported that medical identity crimes are mostly caused by sharing identification with family members or friends, responding fake emails or spoofed websites and the data breach of healthcare providers.[3]

In most countries, the relationship between the beneficiary, the healthcare provider and the insurance provider are not as compact as financial identity management system, which limits the effect of current methods against financial identity fraud when they are applied on the medical field.[6] Therefore, a potential solution could be a new medical ecosystem with users, healthcare providers and insurance providers all inside. In this way, it is possible to let these different parties be aware of all the happened events. The Phonemon Institute survey also indicates many victims have a strong willing to be informed about changes of their identity information. About 50% respondents do not know how to check their health information and 60% respondents think the information about their insurace policy coverage and past claims content is the most important imformation they want to know.[3]

Therefore, based on current medical authentication and reimbursement procedure, we developed an application with the Blockchain technology in order to mitigate medical identity frauds. Benefit from the robustness and openness of Ethereum blockchain, this application can provide an efficient way to access user's medical identity information and verify the correctness of existing insurance claims.

II. System Implementation

A. Ethereum Background

Driven by the idea to build a peer-to-peer cryptocurrency and payment system, the blockchain technology is originally designed for financial purpose as a share ledger by Satoshi Nakamoto in 2008 and implemented in the next year as a core component of Bitcoin.[8] Basically, a blockchain is a type of distributed database which is comprised of immutable, digitally recorded data in packages called blocks and shared by multiple nodes.[7] With the generation of new transaction records, blocks are continuously created and added to the previous one. Currently, some existing blockchain implementations have a structure as ”a hashchain inside another hashchain”, for example, Bitcoin and Ethereum. Within this kind of structure, the blocks and the transactions inside the blocks are cryptographically hashed based on their previous transactions and blocks, ensuring the correctness and robustness of the blockchain.

In order to extend the usage of blockchain technology and simplify the development procedure, Ethereum is designed as an alternative protocol for building decentralized applications (DApp). Smart contracts are the core component of decentralized applications that can be executed by the nodes only under specific conditions and can result in ledger updates. Thus, various functions can be achieved by customizing the content of smart contracts.

In Ethereum, there are two types of accounts: externally owned accounts (EOAs) and contract accounts. An EOA is a public key pair that is required when users want to send transactions while the contract accounts are the identifiers for smart contracts.[9] When deploying and interacting with Ethereum blockchain, the hashes of accounts are used to represent users or smart contracts.

In this work, we use Ethereum smart contracts as the backend which provides a safe storage for identity records and a robust algorithm for insurance claim verification.

B. Smart Contracts

This DApp consists of one identity contract and an arbitrary number of insurance policy contracts (IPC).

1) Identity Contract: The ID contract is the ledger with all the identity information of different parties. There are four kinds of identities defined in this contract: users, healthcare providers, insurance providers and issuers. The ID contract stores the relationship between Ethereum addresses with identity information. Once the ownership of an identity is verified in real life, the owner's Ethereum address will be stored and used as the identifier of this identity in our system. Users, healthcare providers and insurance providers represent coresponding identities in real life respectively while the issuer is a special party that can verify other's mundane identity, create new virtual identity and link it with the owner's Ethereum address. Therefore, the issuers should be reliable institutes in real life that have the ability to check mundane identities, for example, the ID cards of users and the facility licenses of healthcare providers.

The ID contract also regulates the accessibility of different types of identities towards different functions. For example, only the issuer can assign new identities, and only the owner can change their customizable information. This is ensured by check the address of the transaction sender.

2) Insurance Policy Contract: Every insurance product is represented by an insurance policy contract (IPC) in this system. The storage of the IPC consists of the information of current covered healthcare products or services for the beneficiary, the addresses of the beneficiary and the insurance provider, all the claims. The claim is a structure type which contains the consumed healthcare providers or services and the corresponding prices, the address of the healthcare provider as the claim creator and the current state of this claim. There are four possible claim states: ”pending” means this claim is created ant not yet be verified, ”Checked by User” means the user has already verified this claim, ”Responded” means the insurance provider has verified this claim and sent the responses to the claim sender, ”Reject by User” means the user refused to approve the content of this claim. Once created, the origin state of the claim will be ”pending”, then only after the user verified the claim and the state was changed into ”Checked by User” can the insurance provider verify this claim and update it to the final state ”Responded”.

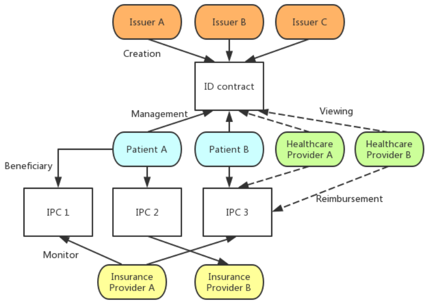


Fig. 1. Smart contracts hierarchy.

Besides providing the information about the related insurance product, this smart contract also helps to ensure the successfulness of claims. IPCs are intended to be designed and deployed by the insurance provider who needs to customize the coverage information based on the insurance product ordered by the beneficiary. In this way, each time a new claim is created, the smart contract will check the claim content. If the contained healthcare products or services are not covered by this insurance product, or the requested amount is beyond the limitation, the Ethereum blockchain will throw out a warning and this claim will not be sent to the smart contract. Furthermore, it also stores the address of the identity contract. Each time when people are interacting with this IPC, it will send transaction to the identity contract in order to check the message sender's identity. Therefore, it regulates that only the registered healthcare providers can create new claim.

3) Application Hierarchy: As 1 shows, there is only one identity contract managed by multiple issuers and all the patients. All the patients are sharing the same contract but they can only modify their own data. Healthcare providers can access and viewing all the shared patient identity information in the identity contract. Insurance Provider Contract (IPC) represents as an insurance product created by the insurance provider and used by the beneficiary. One patient can have multiple IPCs provided by different insurance providers. Only the insurance provider can modify the content of the IPC but healthcare providers and the beneficiary can create or verify claims on it.

III. System Workflow

A. Identity Creation and Authentication

As Fig 2a shows, there are three nodes designed for different parties. All these nodes are independent web interfaces that are connected to the same smart contract on the Ethereum blockchain. All the identity information and permitted issuer addresses are stored in the same smart contract which also contains the inner functions to guarantee the abilities for different addresses. The Issuer Node works between the issuer and the ID contract as a web page. When the contract is accessed through this node, it will search the list of issuers and prevent the executions if the users is not using a permitted address. Issuers are able to create and modify the digital identity stored in the ID contract. Therefore, they are responsible to verify the patients identity in real life. Issuers should be a reliable party that decide the information accuracy in the smart contract.

Before joining in the system, the users need to create their own Ethereum addresses. These addresses will be used in the blockchain that represent their digital identity. Then they need to provide the identifier of their mundane identity, for example, the ID card, and also the address they want to use to an issuer. Once the information is verified by the issuer, the provided Ethereum address will be linked with the patients BSN and stored in the contract. After this registration, the patients can access their information in the contract via the patient node. Patients can prove their ownership of their digital identity in the contract through this node by using their private keys. There are also some additional information that the patients can choose to add on the blockchain for emergency cases, such as their allergies and their trusted people that can provide their identities in case the owner is not capable to do the authentication.

The healthcare provider node is used to read the patients information in the ID contract. After the patient finished the authentication procedure, the healthcare provider can check the corresponding identity information about this patient.

B. Insurance Reimbursement

This system is used to replace the traditional insurance reimbursement procedure which uses the blockchain to record every claim and make the patients aware of every healthcare service claimed by the healthcare provider. Moreover, the policy benefits and previous consumption are stored to simplify the reimbursement procedure. Similarly, there are multiple nodes connected to the policy contract for different purposes.

After the patient requested insurance products, the insurance provider will generate a smart contract that contains the benefits for the patient and the reimbursement history. This contract also has inner algorithm to check if the claims are under coverage before they are sent to the blockchain.

After the patient received medical services, the healthcare provider can use the Healthcare Provider Node (HPN) to make claims. The smart contract will reject the claim if there are services beyond the policy coverage or the amount exceeds the limitation. Once claims are created successfully, they will be recorded in the blockchain as pending events that need verification.

The Patient Node (PN) is for patients to check their policy and created claims. If the patient agrees to the content of a claim, he/she can verify the existence of mentioned services through this node and change the state of this claim in his/her contract.

The Insurance Provider Node (IPN) is for the insurance provider to monitor the status of smart contracts. Once there are claims created by healthcare providers and verified by the patients, this node will notify the insurance provider with all the record about these events in the blockchain. In this way, the healthcare services that are not acknowledged by the patients will never reach the insurance provider. And once the payment is finished, the insurance provider can use the same node to change the claims state and notify the healthcare provider about it.

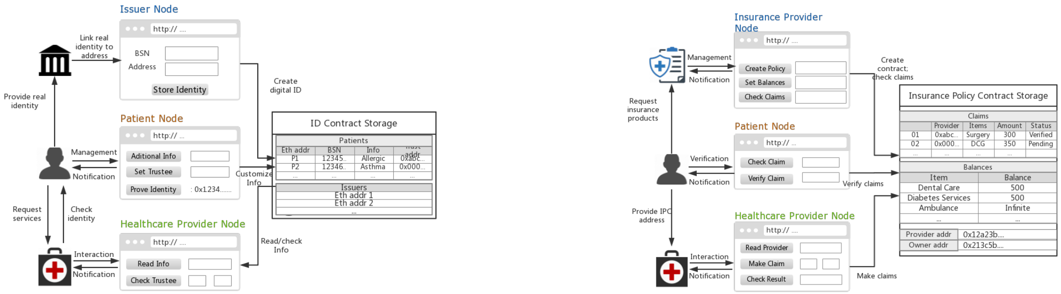
Each insurance product has its own smart contract on Ethereum. But one insurance provider can create multiple smart contracts for different clients. Also, one patient can be the beneficiary of multiple insurance policy constarts. All these contracts are monitored by the same node to interact will the same user.

IV. Medical Fraud Prevention Scheme

On overall, the intent of this healthcare identity management system is to mitigate the healthcare identity fraud from three aspects: to prevent identity frauds from using victim's identity when requesting healthcare products and services, to prevent fake insurance claims for the reimbursement, to reduce the possibility of data breach.

There are several advantages of using Ethereum smart contract to represent identities. A safer yet efficient authentication approach is regarded as the simplest way to prevent medical identity theft [3]. Currently, actual identifiers, like smart cards and radio-frequency identification (RFID), are wildly used for medical authentication. These identifiers are defined as the token-based authentication approach [10]. A typical authentication scheme for these identifiers is the public key infrastructure (PKI). These certificate-based PKI smart cards can generate digital signatures which represent the ownership of the identity [11].

However, this kind of hardware tokens have various drawbacks that limit the security of the authentication procedure. Even for the smart cards with unambiguous identity information, it is also possible to be stolen by the frauds. For example, if emergency happened but the patient cannot provide the token of his/her identity, or there is not a proper verification apparatus, patients are often asked to provide only verbal assertions of their identities. Because the portable card reader is not wildly accepted by the healthcare professionals, it is hard for them to verify patient's identity when they are out of their official workplace. Moreover, patients usually do not know how to distinguish identity criminals who claim they are legal healthcare providers [3]. And it could be very risky to attach the medical card or the identity card to a malicious



(a) Identity contract

(b) Insurance policy contract

Fig. 2. System interfaces and smart contracts.

card reader. This will make personal information exposed to frauds and then result in identity crimes. Therefore, a two-way authentication is also essential for the fraud prevention.

The blockchain technology provides a solution to improve current authentication. In this work, the Ethereum addresses can be used as the software-based or knowledge-based tokens for identities. As Ethereum can be accessed through various devices, it is conveniently to conduct authentication with mobile devices like personal computers and smart phones. Similar with smart cards, Etheruem accounts are also using the public-key cryptography. As described in previous chapters, the two-way authentication is also feasible as the identity information of the healthcare provider is stored in the identity contract. In this way, this system can mitigate the identity fraud by simplifying the verification procedure to avoid unsuccessful authentication, and helping patients to verify the healthcare provider's identity.

The unawareness of medical invoices and claims is another reason for identity crimes as insurance is the most often target of frauds [3]. A lot of people have a strong willing to check their medical invoices and claims but cannot find a convenient approach. The medical billing process is a complicated procedure and varies due to different contexts. In some circumstances, the healthcare provider will send the billing claim directly to the insurance provider and the patient does not participate in this interaction. Traditionally, the assurance of claims need to be investigated by the claim adjustment. Therefore, the patients usually are not always aware of every insurance claim. In our system, the state of the electronic claim can suggests whether it is acknowledged by the beneficiary. This can prevent the payment for healthcare products or services that patients did not receive. In addition, it is also an efficient way for people to monitor their insurance billing claims and detect malicious claims.

The data breach of a centralized database can result from cyber attacks and deliberate behaviour of employees of the database service provider. As a decentralized database, Ethereum blockchain doesn't have a party works as the database administrator and the smart contracts can regulate the updates of data in our system automatically. Therefore, man-made data breaches from the database side can be prevented theoretically. As for the cyber attacks, currently there is a little research about the evaluation of the robustness o Ethereum blockchain and other databases. The security of current database services in use depends highly on the service providers and the protocols. Since the blockchain structure is regarded as extremely fault tolerant, Ethereum smart contracts are expected to have a robuster storage. However, the existence of decentralized autonomous organization (DAO) attacks could probably affect the safety performance of Ethereum.

V. Future Work

VI. Conclusion

In this work, we provide a proof-of-concept system as a potential solution against medical identity frauds. Based on Ethereum smart contracts, this prototype contains various immutable medical information about the registered patients, healthcare providers and insurance providers. It ensures that all these different parties are aware of involved medical activities without replacing current infrastructures. Hence, the medical crimes can be detected by victims efficiently.

Appendix A
Proof of the First Zonklar Equation

Appendix one text goes here.

Appendix B

Appendix two text goes here.

Acknowledgment

The authors would like to thank...

References

[1] E. Harrell and P. W. Daly, *Victims of Identity Theft, 2014*. US Department of Justice Bureau of Justice Statistics Bulletin, September, 2015.

[2] DesRoches, C. M., Campbell, E. G., Rao, *Electronic health records in ambulatory carea national survey of physicians*. New England Journal of Medicine, 2008.

[3] Fifth Annual Study on Medical Identity Theft

[4] Gary R. Gordon, Ed.D. *The Growing Threat of Medical Identity Fraud: A Call to Action*.

[5] *Healthcare Industry Investments to Fight Medical Identity Fraud*.

[6] Nijenhuis, R. G. *Prevention of Dutch fraud cases: a multiple case study on the effectiveness of internal control in the process of financial statement fraud prevention. MS thesis*. University of Twente, 2016.

[7] M. Swan, *Blockchain: Blueprint for a new economy.* "O'Reilly Media, Inc.", 2015.

[8] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008.

[9] G. Wood, *Ethereum: A secure decentralized generalised transaction ledger*. Ethereum Project Yellow Paper, 2014.

[10] K.M. Shelfer, J.D. Procaccino, *Smart card evolution*. Communications of the ACM, 2002.

[11] S. Chokhani, *Toward a National Public Key Infrastructure*. IEEE Communications Magazine, 1994.