International Journal of Scientific Research & Engineering Trends
Volume 6, Issue 5, Sept-Oct-2020, ISSN (Online): 2395-566X

Blockchain-Based Access Control Framework in Patient-Centered Interoperability

Qingsong Zhao, Rodney Thompson
Department of Computer Science
Louisiana State University at Shreveport
Shreveport, LA USA
Qingsong.zhao@lsus.edu, Rodney.Thompson@lsus.edu

***Abstract*-Interoperability is one of the most critical functions in Health Information System (HIS), which is shifting from Hospital-Centered Interoperability (HCI) to Patient-Centered interoperability (PCI). However, in HIS there isn't a framework that supports patient to protect their information's confidentiality and integrity, and to audit data usage. In this paper, we look at Blockchain and Smart Contract technologies and their key features that make blockchain the technology to solve the problem. We then propose a Blockchain-based access control framework in patient-centered interoperability and its implementation.**

***Keywords*-Blockchain, Smart Contract, Access Control Framework, PCI**

I.INTRODUCTION

In Health Information System (HIS), interoperability is the ability of different information systems, devices and applications to access, exchange and integrate health information, within and across hospitals, regional and national boundaries, to provide timely, seamless and efficient patient care. So in HIS, interoperability is all about "sharing health information."

Interoperability provides massive benefits [1]. The key benefits are: improved patient care coordination, greater patient safety, higher productivity, reduced healthcare costs, and more accurate health information. In other words, the benefits are saving more lives, more time and more money [2, 3].

1. Hospital-Centered Interoperability (HCI)

Currently, Interoperability is often focused on data exchange between business entities, for example, multiple hospital systems exchange data through a state-wide Health Information Exchange (HIE). This is called Hospital-centered Interoperability (HCI).

HCI has improved health information exchange in some degree. However, more and more HCI participants are facing several challenges, such as HIE maturity, data quality, data availability, etc.From a cybersecurity standpoint, HCI is vulnerable to a "Single Point of Failure". That means if the HIE fails, the whole system will stop operating.

2. Patient-Centered Interoperability (PCI)

In healthcare systems, patients are always the center of care. All of the systems, providers, and devices are working around the patient.

Correspondingly, in Health information system (HIS), patients are the center of health information.

So in Patient-centered interoperability (PCI), health data exchange is driven by patients, instead of by hospitals.

3. Administrative Support for PCI

21st Century Cures Act was signed by President Obama in 2016, which is pushing the shift from HCI to PCI.

It promotes and supports the research in healthcare, delivering better health services and drug and medical device development.

One of the focuses of this act is patient engagement.

Patient engagement encourages patients to actively participate in their own health care and wellness.

The most commonly used IT strategy to improve patient engagement is to provide patient with patient portals. Patient portals allow patient to complete access to their own health information from both care providers and insurance.

So for patients, the more they participate in managing their health information, the more they need patient-centered Interoperability.

4. Wearable device data

Another reason that patients need PCI is that there is more and more data from patient wearable devices coming into EHR, and this part of data is playing a more and more important role in patient treatment. For example, the MySignals eHealth sensor platform [4] can measure 16 different bio-metric parameters through different sensors, such as blood pressure sensor, airflow sensor, Electrocardiogram sensor (ECG), Electromyography sensor (EMG), snore sensor, body position sensor, and Galvanic Skin response sensor (GSR). The shift towards PCI is an important trend. It brings new opportunities to healthcare, but it brings new challenges to health information security and privacy, as well.

Nowadays, when they go to the hospital, patients are asked to sign consent forms before getting treatment. By signing the form, patients authorize the hospital to share their information among other organizations. Obviously, through consent forms, patients cannot control who can have the access to their data, cannot keep the consistency and accuracy of the shared data, and cannot audit the data usage.

II. BLOCKCHAIN AND SMART CONTRACT

Blockchain was invented by a person (or group of people) using the name Satoshi Nakamoto in 2008 to serve as the public transaction ledger of the cryptocurrency bitcoin [5, 6]. Blockchain technology is currently being actively developed and it is a promising tool for many fields of the economy and business.

1. Blockchain

In a super simple sentence, blockchain is an immutable and decentralized ledger (database). You can think of blockchain as an "append-only" data structure, you can only append new data in the form of a block, then link the block together with previous blocks. All data is permanently stored in blocks and cannot be altered, so it is immutable. The blockchain is duplicated and distributed across many computers (nodes) in blockchain system, so it is decentralized.

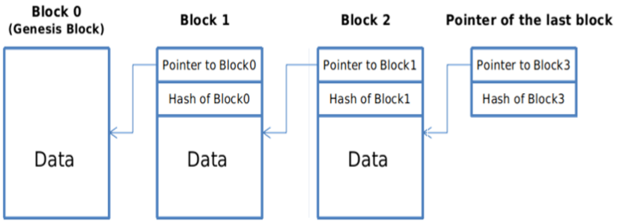


Fig.1 Blockchain.

Hash Pointer is the key data structure of blockchain.
A Hash Pointer is comprised of two parts:

- A Pointer to data is pointing to where the data is stored, which is used to get the data.
- A Hash of data is the Cryptographic hash of that data, and this is used to verify that data hasn't been changed.
- By using hash pointers, blocks are linked to a chain, which is called blockchain.

Please note that the hash stored in the hash pointer is the hash of the whole data of the previous block, which also includes the hash pointer. This makes it impossible to tamper a block in the blockchain without letting others know.

2 Bitcoin

Bitcoin was the first example of blockchain in action. Actually, Blockchain was developed specifically for Bitcoin. Right now Bitcoin is the most widespread and successful cryptocurrency in the world. From a business standpoint, Bitcoin is a decentralized digital currency, or peer-to-peer electronic payment system. Users can anonymously transfer bitcoins without the interference of a third-party authority (like a bank or government). In a Bitcoin block, transaction data is saved in block body, and transaction data hash is saved as a Merkle Tree, the Merkle root is save as in block header. That is, the transaction root is the Merkle Tree root.Merkle tree is a binary tree, the leaves are transaction records, and nodes further up in the tree are the hashes of their respective children.

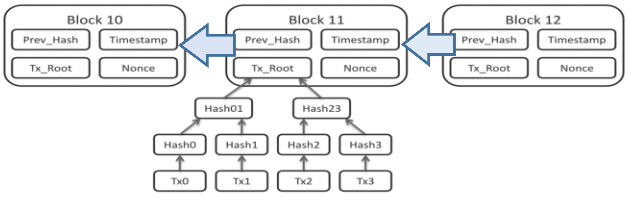


Fig.2 Bitcoin.

3. Smart Contract

Bitcoin is the most widespread business application powered by Blockchain technology, but it is not the only one. Smart Contract is another very successful example.
A smart contract is similar to a contract in the physical world, but it's digital and is represented by a tiny computer program stored inside a blockchain.More specifically, a smart contract is a piece of software that stores the rules to negotiate the terms, automatically verifies fulfilment of the terms, and then enforces the terms.

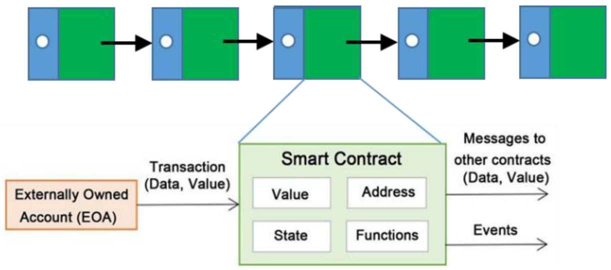


Fig.3 Smart Contract.

4. Key features

Blockchain is an innovative technology; it was born with several significant features.In a blockchain, immutability is achieved through cryptographic hash function. There are many types of hash functions used in Blockchain, the common robust one is called SHA-256 (which stands for Secure Hash Algorithm – 256 bit). As we talked before, transaction data is saved as a Merkle tree in block header.Let's say an attacker wanted to tamper with one transaction, Transaction #a. The attacker changed the content of Transaction #a, because of "collision free" property of the hash function, so now the hash of this modified Transaction #a – Hash #a is also changed.To avoid others noticing the inconsistency, he also needs to change the Hash #a#b, then Hash #a#b#c#d, Now the content of block n+1 is changed, so to make this story consistent, the hash pointer in block n+2 must be changed. Finally, the attacker goes to the hash pointer to the last block of the blockchain.

Immutability can be used to protect the integrity of health information, and protect access log for auditing.

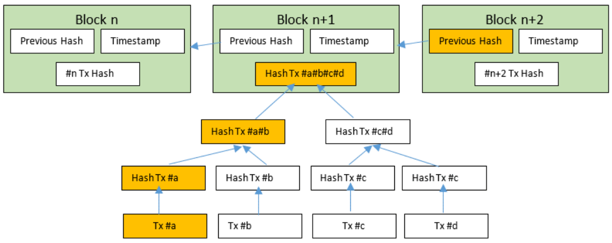


Fig.4 Smart Contract.

Before Bitcoin came along, we were more used to centralized services. An example of a centralized system is the bank.

Centralized systems have treated us well for many years. However, they have several vulnerabilities.

- The central server is an easy target spots for potential hackers.
- Single point of failure.
- A central server upgrade would affect the entire system.

In a blockchain system, data is duplicated and stored in thousands of devices on a distributed network of nodes. Because of this, there is no single point of failure. In fact, everyone in the network owns the information.

The third key feature is that a smart contract is a self-enforcing agreement.Self-enforcing or self-executing, refers to rules in an agreement, which provide that when a given circumstance occurs, certain specific results must automatically follow. In Smart contract, the agreement is embedded in computer code managed by a blockchain.The code contains a set of rules, under which the parties of that smart contract agree to interact with each other. When the predefined rules are met, the agreement is automatically enforced. Like a cryptographic box, it unlocks only if certain conditions are met.

A Vending machine is a simple example. You insert one dollar, you get a Coke, and it doesn't matter if you insert 4 quarters or a dollar bill.Because Blockchain has three key features: immutability, decentralization and Self enforcement, which support creating and enforcing access control rules to protect health information's confidentiality, creating resource hashes to protect health information's integrity and data auditing.

III. BLOCKCHAIN-BASED ACCESS CONTROL FRAMEWORK

This section describes the key components of Blockchain-based access control framework and explain its workflow.

1 Framework Contracts

There are four contracts in the framework, and they are:

- Audit contract, role contract, patient resource contract and user contract.
- In the Healthcare Information System, there are several groups of users accessing patient information, for example, Clinicians, Lab researchers, insurance companies, state agents, pharmaceutical companies, and etc.
- Among all of these users, Clinicians are the largest group. This is an example of an MD user.
- There are two types of attributes, one is static attributes, which will not change during Access Decision-making process.
- The other type is dynamic attributes, also called run-time attributes, which might be changing every time when users request for the access.
- For example, a MD may be a treatment team member for this hospital stay and may be the attending physician for the next time.

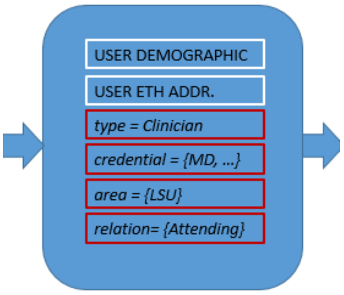


Fig.5 User Contract.

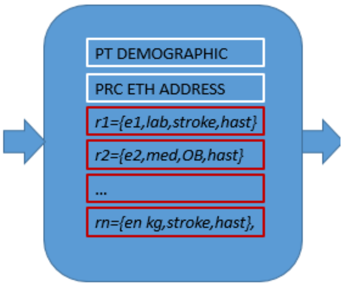


Fig.6 Patient Resource Contract.

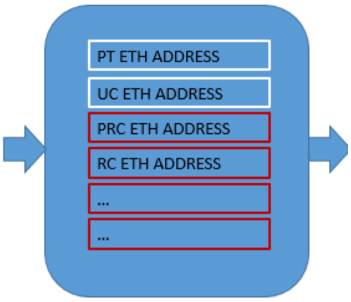


Fig.7 Audit Contract.

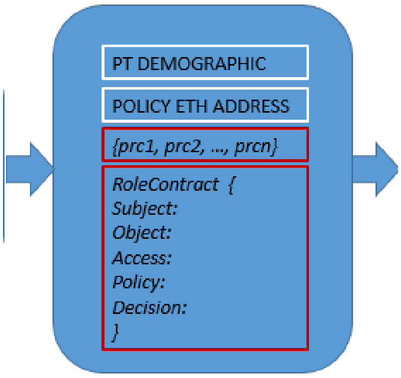
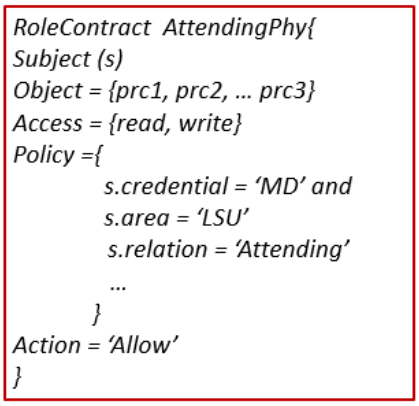


Fig.8 Role Contract.



```
RoleContract  AttendingPhy{
Subject (s)
Object = {prc1, prc2, ... prc3}
Access = {read, write}
Policy ={
            s.credential = 'MD' and
            s.area = 'LSU'
            s.relation = 'Attending'
            ...
          }
Action = 'Allow'
}
```

Fig.9 Role Contract code example.

2 Access control Framework Workflow

Along with the four contracts, EHR database, patient and providers, are the components building up the framework. First of all, through a patient portal, or EHR app, a patient can read from and write to the EHR database, and can also retrieve data from audit contract. Patients also define role contracts on the role contract chain, and set up patient resource contracts on patient resource contract chain.

- Users, or EHR system define user contracts and add them to the user contract chain.
- In the workflow, first, a user initiates the access request. Both the request and user's dynamic attributes are sent to role contract.
- Role contract reaches out to user contract to get user's static attributes.
- By following access policy, the Role contract checks if the user is allowed to access the requested resources. If yes, the role contract calls patient resource contract and get the resource address and the hash value of the resource.
- RC then returns the resource address and the hash value back to the user.
- It doesn't matter that the request is allowed or denied, users information, roles information, and patient resources are saved to audit contract.
- The last step is using the received resource address. The user retrieves the resource from EHR database, which generates the new hash value, and compare it with the hash value saved in patient resource contract.

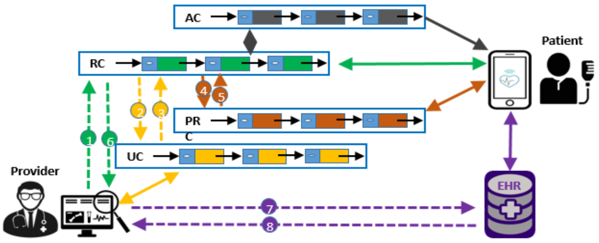


Fig.10 Workflow.

IV. RELATED WORK

Through Meaningful use program (Now it is called Promoting Interoperability) [100], Health Information Technology for Economic and Clinical Health Act (HITECH) incentivized providers and hospitals to adopt Electronic Health Record (HER). More and more hospitals are using EHR systems, as a result, there are more and more health data are sharing between hospitals and patients. Healthcare information sharing is shifting from hospital-driven to patient-driven [7]. Several papers have used Blockchain technology to support better health data sharing [8]. For example, in [9], Yue introduced a "Healthcare Data Gateway" and patients can use it to manage their own healthcare information. Another example is [10], Guo et al. proposed a hybrid architecture to facilitate access control of healthcare data by using both blockchain and edge note. Other related works include [11, 12, 13, 14].

V. CONCLUSION

In this paper, we proposed a blockchain-based access control framework, described the key components of Blockchain-based access control framework and explained its workflow to support sharing patient healthcare information in patient-centered interoperability. We also built up a prototype system using Solidity on Ethereum platform. Our experimental system shows its ability supporting patients to protect their information's confidentiality and integrity, and to audit data usage.

For future work, we will continue developing the system and investigate other possible mechanisms.

REFERENCES

[1] Raina Rajesh "What is DFM & DFY and Why Should I Care?" INTERNATIONAL TEST CONFERENCE 2009

[2] Y. Zhou, J.S. Ancker, M. Upadhye, N.M. McGeorge, T.K. Guarrera, S. Hegde, et al. The impact of interoperability of electronic health records on

ambulatory physician practices: A discrete-event simulation study Inform Prim Care, 21 (2013), pp. 21-29, 10.14236/jhi.v21i1.36

[3] B.A. Stewart, S. Fernandes, E. Rodriguez-Huertas, M. LandzbergA preliminary look at duplicate testing associated with lack of electronic health record interoperability for transferred patients J Am Med Inform Assoc, 17 (2010), pp. 341 - 344, 1 01136/ jamia. 2009. 001750

[4] J. Walker, E. Pan, D. Johnston, J. Adler-Milstein, D.W. Bates, B. MiddletonThe value of health care information exchange and interoperability Health AffProj Hope (2005) Suppl Web Exclusives: W5-10-W5-18

[5] [Online]. Available: http://www.my-signals.com/

[6] C. Catalini, J.S. GansSome simple economics of the Blockchain (2016), 10.2139/ssrn.2874598

[7] Satoshi NakamotoBitcoin: A peer-to-peer electronic cash system (2008)

[8] William J. Gordon and Christian Catalini, “Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability” Computational and Structural Biotechnology Journal 2018, vol. 16, Pages 224-230, April 2018.

[9] W.J. Gordon, A. Wright, A. LandmanBlockchain Technology in Health Care: Decoding the hype NEJM Catal (2017) https://catalyst.nejm.org/decoding-blockchain-technology-health/, Accessed 28th Mar 2018

[10] Yue X, Wang H, Jin D, Li M, Jiang W. Healthcare data gateways: Found healthcare in-telligence on Blockchain with novel privacy risk control. J Med Syst 2016;40:218.https://doi.org/10.1007/s10916-016-0574-6.

[11] H Guo, W Li, M Nejad, CC Shen, " Access control for electronic health records with hybrid blockchain-edge architecture," 2019 2019 IEEE International Conference on Blockchain, 2019. Pages 44-51, June 2019.

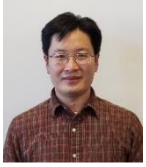
[12] Kuo T-T, Kim H-E, Ohno-Machado L. Blockchain distributed ledger technologies forbiomedical and health care applications. J Am Med Inform Assoc 2017;24:1211–20. https:doi.org/10.1093/jmia/ocx068.

[13] Mettler M. Blockchain technology in healthcare: The revolution starts here. 2016IEEE 18th Int. Conf. E-Health Netw. Appl Serv Heal 2016:1–3. https://doi.org/10.1109/HealthCom.2016.7749510.

[14] [45] Ivan Drew. Moving toward a blockchain-based method for the secure storage of pa-tient records, NIST/ONC; 2016.

[15] Gordon WJ, Landman A. Secure, decentralized, interoperable medication reconcilia-tion using the Blockchain. NIST/ONC; 2016.Wing Chiu Tam and Shawn Blanton “To DFM or Not to DFM” IEEE Asia Pacific Conference on Circuits and Systems, 2006.

Author Profile



Qingsong Zhao

Received his Ph.D. in computer science from Chinese Academy of Science, China in 2003. His research interests include Access Control Models, Operating System security, Blockchain and Electronic Health Record system security.

Rodney Thompson

System and network administration of department computer labs and hands-on classrooms. Designed and configured Cisco Academy lab for Cyber Ops, CCNA security and CCNA Switching/Routing courses. Developed cyber security curriculum and associated courses. Managed graduate assistants and student workers for the CS department. Advisor for independent study of robotics and IoT projects. Worked with department chair on STEM outreach for K-12, business partner advisory council, ABET accreditation and project planning for the Cyber Collaboratory. Developed grant proposals for project funding and helped in most of planning phases of the Collaboratory. Coordinator on group projects for High Altitude Ballooning, data collection using the Raspberry Pi, and data visualization of DNA/RNA motifs.