Securing Healthcare Book through Public Blockchain and Elliptic Curve Cryptography

Nelson Josias Gbètoho Saho

Securing Healthcare Book through Public Blockchain and Elliptic Curve Cryptography

Nelson Josias G. Saho[1]

[1]Institut de Formation et de Recherche en Informatique, Université d'Abomey-Calavi, BENIN

*E-mail : Nelson SAHO nelson.saho@uac.bj

Abstract

Healthcare systems and services vary from one country to another due to States' policies. The healthcare book, whenever digital or physical is a patient health history record. This record provides sustainable and traceable health pattern for medical doctors in patient examination cases. Unfortunately in most developing countries, such documents are not kept safely by their owners. Moreover, many developing countries do not have digital systems for healthcare management. When healthcare systems exist, data are not stored nor secured to prevent information to be altered. To overcome these problems and to avoid patient data lost, we developed the healthcare digital book by using a public blockchain Ethereum. Due to the medical information criticality, we have added an encryption layer by using elliptic curve cryptography in order to use short key sizes and ensure considerable robustness of the cryptosystem. Thus, we obtain smaller cryptograms and therefore use less Gas fees in comparison with other cryptographic algorithms. Smart contracts are unit-tested to guarantee all functionalities as expected. Due to the benefits of this technology, the digitized healthcare book shall guarantee data integrity, confidentiality and provide secure information to doctors for various medical exams, patients' pathologies and so forth.

Keywords

Blockchain Technology, Smart Contract, Electronic Health Records, Personal Health Records, Digital Healthcare Book

I INTRODUCTION

Healthcare provision and protocol are the main priority of the government who endorsed its safe practicability to ensure the well-being of its citizens. The quality of healthcare systems and services can be considered as one of the crucial factors that define Government activities. Healthcare systems and services vary from one country to another. Health policies are very important to determine the physical and mental well-being of living people.

One of the used documents in healthcare systems and services is the healthcare book. The latter is designed to record the most important data about a patient pathologies and provided treatments. A reliable health record must be established under patient testimony and consent by medical doctors, nurse and health practicing officials Marinič [2]. So, the healthcare book is a practice that allows hospital workers to monitor each patient.

Unfortunately, in developing countries, patients' data are not safely recorded in a way that allows them to be retrieved for future use. In addition to this, recorded data may be altered leading

doctors to wrong diagnostic about patients. In preventing falsification of health data record, we develop a decentralized application that we called a healthcare electronic book (*healthcare e-book*) using the Ethereum blockchain. By implementing it, patient data are secured. Due to the medical information criticality, we have added an encryption layer by using cryptography through elliptic curve. The application front-end allows the different actors to interact with data in a secure mode.

This research work document is organized as follows. In section II we will present the fundamental concepts including the materials and methods used. In Section III we will describe the different results we have achieved by showing the designing process. We will complete this research paper with remarks in Section IV.

II FUNDAMENTAL CONCEPTS

This section reviews the advantages of blockchain in healthcare systems, presents the related works and the materials and methods.

2.1 Benefits to use blockchain technology in healthcare system

Nowadays, the blockchain technology is an interesting research area and many benefits in many areas. For instance, the healthcare industry is expected to benefit immensely from the blockchain technology due to security, privacy, confidentiality and decentralization Shahnaz, Qamar, and Khalid [12]. According to Marko Hölbl et al., blockchain technology research in healthcare is increasing and it is mostly used for data sharing, managing health records and access control Hölbl, Kompara, Kamišalić, and Nemec Zlatolas [7].

The Electronic Health Record (EHR) systems are facing problems such as data security, integrity and management Shahnaz, Qamar, and Khalid [12]. The blockchain technology can be used to transform healthcare book systems and could be a solution to these issues.

Here are the significant advantages that blockchain brings to medical information systems.

- Since blockchain is immutable and traceable, any patient can send recorded data to anyone without fearing data corruption.
- Similarly, a medical record that has been generated and added to the blockchain will be completely secured.
- The patient can have some control over how their medical data are used and shared by institutions.
- Medical data access will be controlled. So, any party looking for the medical data about patients could check with the blockchain to get the necessary access level.
- The patient can be rewarded by tokens for giving their data for clinical trials and research purposes.

Easy access to patients' data would help doctors to treat them without expecting their previous exams' results. Data availability allow hospital workers to create specialized treatment plans on the basis of outcomes and treatment efficacy Vazirani, O'Donoghue, Brindley, and Meinert [14]. Daily health data would also engage more the patient in the monitoring process with improvement of patient compliance Linn and Koo [4]. The capability of personalized medicine would therefore be improved with this interoperability, as a single access point to all real time patients' health data.

In this paper, we opted to use the Ethereum blockchain.

2.2 Related works

Many research papers in the literature addressed the healthcare industries. Petar Franček et al. Franček, Piljić, Dragić, Mlinanć, Kovač, and Gvozdanović [1] created communication adapter in the midst of EHR and PHR systems to share data. Nevertheless, these systems have shown their limitations since they do not guarantee data integrity. In Esposito, De Santis, Tortora, Chang, and Choo [6], Christian Esposito et al. used the blockchain potential to protect data and services in the cloud instead of shifting them into the cloud. Alex Roehrs et al. Roehrs, Costa, Rosa Righi, Silva, Goldim, and Schmidt [11] analyzed the performance of a blockchain-based personal health record implementation and found that the blockchain implemented in their prototype achieved 98% availability. Their performance results indicated that data distributed via a blockchain could be recovered with low average response time with high availability Roehrs, Costa, Rosa Righi, Silva, Goldim, and Schmidt [11]. Bahar Houtan et al. Houtan, Hafid, and Makrakis [17] reviewed the state of the art and provided an analysis of the design trade-offs. They found that the majority of the currently developed use-cases focus on cryptocurrency (BC 1.0) and smart contracts/Dapps (BC 2.0). Hence, blockchain has gained more admiration in the healthcare industry.

Data privacy is important in the context of e-health systems. Although blockchain could provide data integrity, it would perhaps harms data privacy and confidentiality since all the data stored on blockchain are publicly available. Unfortunately, none of the related works mentioned above addressed these aspects. Thus, this paper focuses on such issues.

Chun-Ta Li et al. Li, Shih, Wang, Chen, and Lee [18] have implemented remote medical monitoring and have designed a group authentication mechanism for multiple authorized users (such as patient, doctors, caregivers, family and friends) to freely access patient's personal health records. Mohammad Moussa Madine et al. Madine, Battah, Yaqoob, Salah, Jayaraman, Al-Hammadi, Pesic, and Ellahham [19] proposed Ethereum blockchain-based smart contracts to give patients control over their data. They used trusted reputation-based re-encryption oracles to securely fetch, store, and share patients' medical data. However, these two last works do not guarantee the end-to-end security of patient medical data. This paper is meant to contribute filling that gap.

2.3 Materials and methods

The goal is to store information in a safe mode and easily retrieve them at anytime and anywhere once needed.For its implementation, we refer to blockchain that implements the smart contract Ethereum. Below are the tools we used:

- **Truffle:** Truffle is used to design the *DApp*. It allows the smart contracts' deployment in the local environment and also to test them Truffle [22];
- **Ganache:** this is a blockchain client for Ethereum DApp development, and is now part of the Truffle suite of tools;
- **Solidity compiler (solc):** Solc is a command line compiler for Solidity. Influenced by C++, Python, and JavaScript, Ethereum was designed to target the Ethereum Virtual Machine (EVM) Ethereum [16]. It creates *opcodes* as outputs that EVM can interpret.
- **Chai and chai-as-promised libraries Chai [15]:** they have been used to test the DApp in Truffle testing environment

The developed *DApp* will be accessed through a web browser that communicates with a front-end website written in Hyper Text Markup Language 5, Cascading Style Sheet version 3, and

JavaScript. Instead of communicating to a back-end web server, the website will directly communicate with the blockchain. The latter will essentially be our back-end that hosts all the code and data for the decentralized healthcare book. To achieve this goal, the following tools have been used:

- **Web3.js- Ethereum JavaScript Application Programming Interface:** Web3.js is a collection of libraries allowing to interact with a local or remote Ethereum node using *HTTP, IPC or WebSocket*. However, the Ethereum JavaScript API methods can also be exposed to normal web applications to communicate with Ethereum Virtual Machine Chris [5];
- **MetaMask:** MetaMask comes pre-loaded with fast connections to the Ethereum blockchain and several test networks MetaMask [20]. This allows to get started without synchronizing a full node, while still providing the option to upgrade the security and the use of the chosen blockchain provider.
- **Bootstrap, Lite-server and others** are also used.

III SIMULATION RESULTS: DESIGN PROCESS

After this short overview on the fundamental concepts that underpin this paper, we present in this section the different results achieved. We also present the various smart contracts implemented and the client application allowing us to access the designed DApp.

3.1 Proposed architecture for medical information system with public blockchain

Due to the sensitivity of EHR or PHR data, the architecture of the system is of paramount importance. Indeed, the proposed system should be able to protect each patient data. We pay attention to two fundamental aspects in this architecture namely:

- the adequate blockchain; and
- the data privacy.

3.1.1 The adequate blockchain

Among the types of blockchain, we have the permissionless or public blockchain and the permissioned or private blockchain Yaga, Mell, Roby, and Scarfone [10]. The debates around opting for the cloud or having its own datacenter resurface with respect to the choice between private blockchain and public blockchain. Several reasons influence the choice between one or the other. Among them, we retain the criticality of the data and the implementation cost.

No doubt, the EHR or PHR data are critical. It is obvious that the cost of implementing a private blockchain is much higher than the transaction fee (Gas) of public blockchain for the development of large decentralized applications, in the medium and long term.

To allow patients not to be tied to a private architecture and allow them for easy accesses to data (since they may need them beyond the borders of a country), we recommend for EHR or PHR data the use of public blockchain implementing smart contracts like Ethereum.

3.1.2 Data privacy

It is vital to secure data access mechanisms that can ensure only authorized entities have access to the patients' medical information Ramani, Kumar, Bracken, Liyanage, and Ylianttila [8]. Since we recommended the use of a public blockchain for medical information (EHR or PHR), we closely think about the data security in more details. As a public blockchain being pseudonymous Kosba, Miller, Shi, Wen, and Papamanthou [3], we should not fear a priori about the protection of personal data. To guarantee that data are not used for unwanted purposes, we

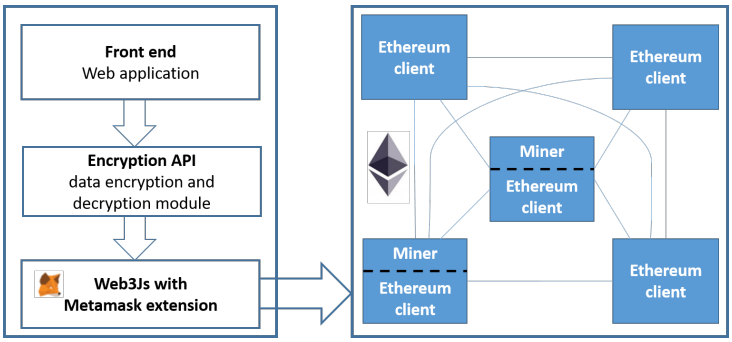

Figure 1: Proposed health record architecture using blockchain

integrated an encryption mechanism to provide end-to-end security.

Considering the different choices, the Fig. 1 represents the general architecture of an EHR or PHR information system using blockchain.

We will not proceed as usual where the client application is directly connected to the blockchain via the Metamask API. An encryption API will be in charge to encrypt the data in case of sending requests or to decrypt data in case of call type requests to the blockchain. This will protect the user. Indeed, without the user's agreement who holds the decryption key, the provided data cannot be monitored.

In our previous paper entitled Survey on Asymmetric Cryptographic Algorithms in Embedded Systems Saho and Ezin [21], we concluded that setting up a robust cryptosystem no longer necessarily involves the use of significant machine resources. We recommended an asymmetric encryption based on the elliptic curves algorithms under the Gas limitation. For an equivalent level of robustness between two RSA and Elliptic Curves cryptosystems, the one based on the elliptic curves uses a shorter key length. Therefore, its cryptogram is the shortest.

3.1.3 Drawbacks of this architecture

Since we integrated an encryption mechanism to guarantee end-to-end security, the data size to be written into the system (blockchain) will increase. This architecture will use more Gas compared to an architecture, which does not integrate an encryption module. Nevertheless, this drawback is minor since Gas is only used when writing into the blockchain.

3.2 Decentralized application process

Figure 2 illustrates the architecture of the DApp showing the different actors. Three actors are in concern namely the owner, the doctor and the patient.

1. **The owner:** he is the deployer of the DApp with the following functionalities or abilities:
   - adding doctors to the system; and
   - providing basic authorization control functions through the *Ownable* contract with the owner address to simplify the implementation of user permissions.
2. **The doctor:** he is the hospital worker with the following abilities:
   - adding a patient;
   - setting non-variable examination values of the patient;
   - prescribing a specific drug to the patient;
   - setting observation during or after the use of the drug by the patient;
   - adding an eventual allergy of the patient;

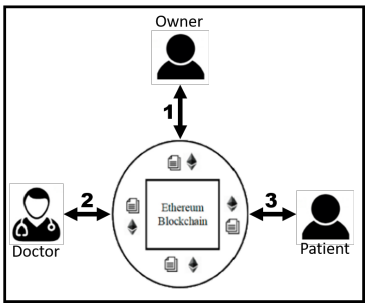

Figure 2: Architecture of the proposed system

- ordering an examination; and
- adding the result and the details of the result of the examination.

3. **The patient:** s/he can access all her/his medical information.

In our previous paper entitled Developing a Digital Healthcare Book based on the blockchain Technology Saho and Ezin [23], we already designed the healthcare e-book by writing smart contracts.

3.3 Healthcare book Dapp

To design the healthcare book DApp and implement all the features, we improved all the smart contracts and used an existing smart (Ownable) contract and a library (SafeMath). The smart contracts are as follows:

- *Doctor:* via this smart contract, the owner can add a doctor in the system. Since medical information is in concern, only doctors are allowed to add patient data to the blockchain;
- *Patient:* this smart contract is critical since it inherits almost all the others. The doctor can first use it to add a patient to the system and then to perform all operations for adding medical information related to a patient;
- *Non variable examination:* through this smart contract, we add data from non-variable biological examinations of a patient like blood typing;
- *Specific medicine:* it is used to add a specialized drug prescribed by the doctor to a patient;
- *Allergy:* this smart contract allows the user to log all the allergies of a patient under treatments or not;
- *Examination:* thanks to this contract, we can register any medical examination prescription made by a doctor to any patient;
- *Result examination:* through this one, the doctor can record the result of a prescribed medical examination;
- *Result examination detail:* this contract is used for the purpose of recording the details of each exam result.

Functions are within an Ethereum smart contract, which were then deployed to the Kovan test network.

The whole project is available online on GitHub (nelson-saho/healthcareBook).

3.4 Client application development process

The user's input was read through a web interface and sent to the Ethereum network via the web3.js API Ranganthan, Dantu, Paul, Mears, and Morozov [9]. This API, *Metamask* MetaMask [20] and the fundamentals of web programming are therefore used for the front-end design process. We coded the back-end that allows us to interact with the developed decentralized application on Ethereum.

The web application (front-end) and the back-end are also available on GitHub in the folder *src/demos/eliteadmin-hospital*.

IV CONCLUSION AND REFERENCES

4.1 Discussion

We have tested all smart contracts and the results obtained (especially compute times) show us that the decentralized application is working correctly. The appended figures present the results of some tests. Our fear was the latency time which could induce data encryption. But the use of elliptic curve cryptography which uses reduced sizes key to guarantee the same robustness as the other algorithms was useful to us.

In short, we were able to use a public blockchain to manage confidential data by leveraging the comparative advantage of elliptic curve cryptography over others.

4.2 Conclusion

With Siyal, Junejo, Zawish, Ahmed, Khalil, and Soursou [13] we can conclude that there has been remarkable interest in using blockchain applications for providing safe and secure management of healthcare data.

In this paper, we developed an architecture for medical information (EHR or PHR) due to their specificity. We retained the use of asymmetric encryption over elliptic curves algorithms in order to have a robust system using less Gas. We digitized the information provided by the health book ensuring that it is not tampered by using Ethereum blockchain.

A real estimate of the ratio between the cost of deploying a private blockchain and the cost of our architecture will elucidate the benefit generated by this one. It will be done in our future work. This blockchain information system also can be extended to other actors covering the healthcare book system such as pharmacists.

REFERENCES

Publications

[1] P. Franček, I. Piljić, L. Dragić, H. Mlinanć, M. Kovač, and D. Gvozdanović. "Overcoming E-health interoperability obstacles: Integrating PHR and EHR using HL7 CCD". In: *2015 57th International Symposium ELMAR (ELMAR)*. IEEE. 2015, pages 73–76.

[2] M. Marinič. "The importance of health records". In: *Health* 7.05 (2015), pages 617–624.

[3] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou. "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts". In: *2016 IEEE symposium on security and privacy (SP)*. IEEE. 2016, pages 839–858.

[4] L. A. Linn and M. B. Koo. "Blockchain For Health Data and Its Potential Use in Health IT and Health Care Related Research". In: *ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST*. 2016, pages 1–10.

[5] D. Chris. "Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners". In: *Apress, New York* (2017).

[6] C. Esposito, A. De Santis, G. Tortora, H. Chang, and K.-K. R. Choo. "Blockchain: A panacea for healthcare cloud-based data security and privacy?" In: *IEEE Cloud Computing* 5.1 (2018), pages 31–37.

[7] M. Hölbl, M. Kompara, A. Kamišalić, and L. Nemec Zlatolas. "A systematic review of the use of blockchain in healthcare". In: *Symmetry* 10.10 (2018), page 470.

[8] V. Ramani, T. Kumar, A. Bracken, M. Liyanage, and M. Ylianttila. "Secure and efficient data accessibility in blockchain based healthcare systems". In: *2018 IEEE Global Communications Conference (GLOBECOM)*. IEEE. 2018, pages 206–212.

[9] V. P. Ranganthan, R. Dantu, A. Paul, P. Mears, and K. Morozov. "A decentralized marketplace application on the ethereum blockchain". In: *2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC)*. IEEE. 2018, pages 90–97.

[10] D. Yaga, P. Mell, N. Roby, and K. Scarfone. *Blockchain Technology Overview. National Institute of Standards and Technology Internal Report 8202, 66 pages*. 2018.

[11] A. Roehrs, C. A. da Costa, R. da Rosa Righi, V. F. da Silva, J. R. Goldim, and D. C. Schmidt. "Analyzing the performance of a blockchain-based personal health record implementation". In: *Journal of biomedical informatics* 92 (2019), page 103140.

[12] A. Shahnaz, U. Qamar, and A. Khalid. "Using blockchain for Electronic Health Records". In: *IEEE Access* 7 (2019), pages 147782–147795.

[13] A. A. Siyal, A. Z. Junejo, M. Zawish, K. Ahmed, A. Khalil, and G. Soursou. "Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives". In: *Cryptography* 3.1 (2019), page 3.

[14] A. A. Vazirani, O. O'Donoghue, D. Brindley, and E. Meinert. "Implementing blockchains for efficient health care: systematic review". In: *Journal of medical Internet research* 21.2 (2019), e12439.

[15] Chai. *Chai Assertion Library*. 2020.

[16] Ethereum. *Solidity*. 2020.

[17] B. Houtan, A. S. Hafid, and D. Makrakis. "A survey on blockchain-based self-sovereign patient identity in healthcare". In: *IEEE Access* 8 (2020), pages 90478–90494.

[18] C.-T. Li, D.-H. Shih, C.-C. Wang, C.-L. Chen, and C.-C. Lee. "A Blockchain Based Data Aggregation and Group Authentication Scheme for Electronic Medical System". In: *IEEE Access* 8 (2020), pages 173904–173917.

[19] M. M. Madine, A. A. Battah, I. Yaqoob, K. Salah, R. Jayaraman, Y. Al-Hammadi, S. Pesic, and S. Ellahham. "Blockchain for giving patients control over their medical records". In: *IEEE Access* 8 (2020), pages 193102–193115.

[20] MetaMask. *MetaMask Docs*. 2020.

[21] N. J. G. Saho and E. C. Ezin. "Survey on Asymmetric Cryptographic Algorithms in Embedded Systems". In: *International Journal of Innovative Science and Research Technology (IJISRT)* 5.12 (2020), pages 544–554.

[22] Truffle. *Truffle suite*. 2020.

[23] N. J. G. Saho and E. C. Ezin. "Developing a Digital Healthcare Book based on the Blockchain Technology". In: *2021 International Symposium on Electrical, Electronics and Information Engineering (ISEEIE 2021)*. ACM, New York. 2021, 6 pages.