Blockchain-Based Healthcare Workflows in Federated Hospital Clouds

Armando Ruggeri[1], Maria Fazio[1,2(✉)], Antonio Celesti[1,3], and Massimo Villari[1]

[1] MIFT Department, University of Messina, Messina, Italy
{armruggeri,mfazio,acelesti,mvillari}@unime.it
[2] IRCCS Centro Neurolesi "Bonino-Pulejo", Messina, Italy
maria.fazio@irccsme.it
[3] INdAM - GNCS Group, Rome, Italy

Abstract. Nowadays, security is one of the biggest concerns against the wide adoption of on-demand Cloud services. Specifically, one of the major challenges in many application domains is the certification of exchanged data. For these reasons, since the advent of bitcoin and smart contracts respectively in 2009 and 2015, healthcare has been one of the major sectors in which Blockchain has been studied. In this paper, by exploiting the intrinsic security feature of the Blockchain technology, we propose a Software as a Service (SaaS) that enables a hospital Cloud to establish a federation with other ones in order to arrange a virtual healthcare team including doctors coming from different federated hospitals that cooperate in order to carry out a healthcare workflow. Experiments conducted in a prototype implemented by means of the Ethereum platform show that the overhead introduced by Blockchain is acceptable considering the obvious gained advantages in terms of security.

Keywords: Blockchain · Smart contract · Healthcare · Cloud · SaaS · Hospital · Federation

1 Introduction

The demographic growth of the last century combined with the increased life expectancy and shortage of specialized medical personnel in Europe [1,2] has made the access to proper medical treatments one of the major concerns of the last decade. The recent advancements brought by the Cloud computing paradigm have been only partially taken in consideration by hospitals and more in general medical centers so far, in spite of a considerable number of scientific initiatives in eHealth [3]. In particular, a crucial aspect that have slowed the "Cloudisation" of hospitals has regarded security of exchanged data. It is essential that shared pieces of healthcare data are certified and their integrity guaranteed in order to prevent that pieces of clinical information are either intentionally or accidentally altered.

In recent years different solutions have been proposed to solve such an issue: among these, the Blockchain technology, thanks to its intrinsic features of data

non-repudiation and immutability, has aroused a great interest in both scientific and industrial communities. Founded in 2009 as the technology behind Bitcoin [4], it has completely revolutionized traditional encryption-based security systems, introducing a new approach able to apply hash-based encryption in which information is saved on blocks and each block is linked to the previous one via a hash coding. One of the major applications of Blockchain regards smart contract, i.e., a computer protocol aimed at to digitally facilitate, verify, and enforce the negotiation of an agreement between subjects without the need of a certification third party.

Blockchain technologies have been increasingly recognized as a technology able to address existing information access problems in different applications domains including healthcare. In fact, it can potentially enhance the perception of safety around medical operators improving access to healthcare services that are guaranteed by a greater transparency, security and privacy, traceability and efficiency.

In this paper, by exploiting the intrinsic security feature of the Blockchain technology, we propose a clinical workflow that:

– enables to create a virtual healthcare team including doctors belonging to different federated hospitals;
– enables to share patients' electronic health records among virtual healthcare team members preserving sensitive data;
– adopts smart contracts in order to make the transactions related to applied therapies trackable and irreversible;
– enables security in electronic medical records when they are accessed by patients and medical professionals;
– guarantees the authenticity of whole federated healthcare workflow.

In general, the proposed solution allows tracking the treatment of patients that can take place in different federated hospitals from the hospitalization to the dismissal, supporting the whole medical personnel in planning treatments. Moreover, we discuss a Software as a Service (SaaS) that allows to apply the workflow.

The remainder of this paper is organized as follows. A brief overview of most recent initiatives about the adoption of Blockchain in healthcare is provided in Sect. 2. Motivations are discussed in Sect. 3. The design of the SaaS is presented in Sect. 4, whereas its implementation adopting Flak, MongoDB and Ethereum is described in Sect. 5. Experiments demonstrating that the overhead introduced by Blockchain is acceptable considering the obvious gained advantages in terms of security are discussed in Sect. 6. In the end, conclusions and light to the future are discussed in Sect. 7.

2   Related Work

In recent years numerous research studies have been conducted in healthcare domain with particular attention to the application of the Blockchain technology [5].

Blockchain can drastically improve the security of hospital information systems as discussed in many recent scientific works [6–9]. However, up to now, most of scientific initiatives are either theoretical or at an early stage and it is not always clear which protocols and frameworks should be used in order to carry out system implementation that can be deployed in real healthcare environments.

Blockchain has been increasingly recognized as a tool able to address existing open information access issues [10]. In fact, it is possible to improve access to health services by using the Blockchain technology in order to achieve greater transparency, security and privacy, traceability and efficiency. In this regard, a solution adopting Blockchain with the purpose to guarantee authorized access to the patients' medical information is discussed in [11]. In particular, mechanisms to preserve both patient's identity and the integrity of his/her clinical history is proposed.

Another application of Blockchain regards the supply chain in the pharmaceutical sector and the development of measures against counterfeit drugs. While the development of new drugs involves substantial costs related to studies in order to evaluate the safety and updating of the drug, the use of smart contracts guarantees informed consent procedures and allows in certifying the quality of data [12].

Differently from the above mentioned most recent scientific initiatives, this paper describes a practical implementation of how Blockchain can be used to improve medical analysis treatments empowering collaboration among a group of federated hospitals.

3   Motivation

This paper aims at recommending new approaches able to harmonize health procedures with new technologies in order to guarantee patients' safety and therapeutic certification, verifying that every doctor's choice is immutably recorded, with the purpose to guarantee and track that all hospital protocols have been scrupulously followed. Furthermore, the proposed system was designed and implemented in order support a virtual healthcare team including a selected group of doctors in order to make a clear picture about the patient's clinical status especially in a critical condition. The anonymized patient's health data and clinical analyses are shared among doctors participating in the federation of hospitals while the patient's data are never shared.

Figure 1 describes a scenario where patient's clinical data is shared across participants to a federation of hospitals for cooperation and knowledge sharing, and the data exchanged is certified on a private Blockchain where all participants are known and trusted.

Specifically, the proposed healthcare workflow adopted in the proposed system includes the following phases:

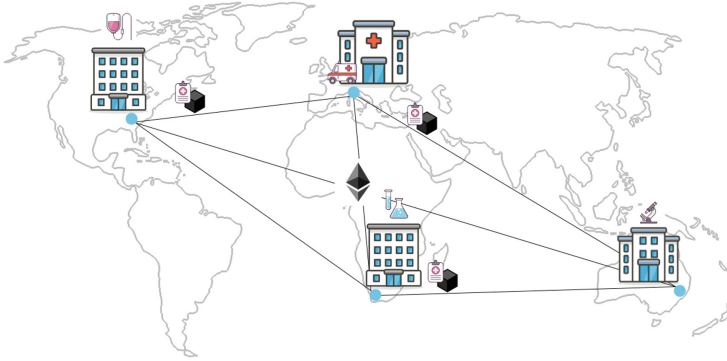1. **Hospitalization**: patient reaches the hospital and personal details, date and type of visit are recorded;

Fig. 1. Federation of hospitals: clinical data is shared across participants for cooperation

2. **Analysis**: patient follows the procedures to ascertain the nature of the disease (e.g., blood tests, clinical examinations, possible CT scans, RX laboratory tests, etc) and the results of the analyzes are saved on a Cloud storage space inside the hospital Cloud managed on a dedicated directory for the patient identified by a visit identification code;
3. **MD evaluation**: doctor analyzes the results of clinical analysis and prepares a report with the therapy to be followed;
4. **Federated teleconference**: a selected pool of doctors belonging to the hospital federation is invited to participate to a virtual healthcare team in a teleconference in order to clarify the patient's clinical situation. The patient's health data and clinical analysis are shared with the other doctors belonging to the virtual healthcare team; patient's details are never shared;
5. **Drug administration**: the hospitalized patient is constantly monitored by nurses who apply treatments based on therapeutic indications; each treatment is recorded.

4   System Design

Once the virtual healthcare team has identified the disease, it writes a prescription for the treatment indicating the disease itself to cure and a drug description including dosage and mode of use. It is important to guarantee that only authorized doctors are allowed to create a new prescription or to update an existing one because a wrong diagnosis can lead to a worsening of clinical condition or death and so it becomes mandatory to know who created a new electronic health record.

The system was designed as a Software as a Service (SaaS) in order to store: (i) patient's electronic health records; (ii) treatments for specific diseases resulting from medical examinations. The objective of the whole system is to harmonize health procedures by means of the following technologies:

– **Blockchain engine**: to use the features of a decentralized and distributed certification system with the technology offered by the development and coding of smart contract;
– **Cloud storage**: to use an open-source and open-architecture file hosting service for file sharing managed with authorizations to archive all the files required to support the analysis of the nature of the disease such as blood tests, CT scans and laboratory tests;
– **NoSQL database**: to exploit the potential of a document-oriented database to store and manage patient data and diseases through tags for a fast and efficient search and to store blockchain transaction hashes and links to files stored in Cloud Storage.

5   Implementation

The SaaS was designed in order in order to apply the previously described healthcare workflow supporting a virtual healthcare team whose members are doctors belonging to different federated hospitals. Figure 2 shows the main software components used to implement the SaaS.
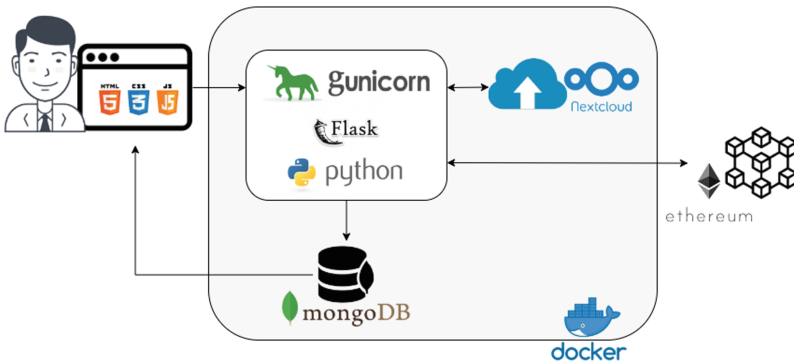

Fig. 2. SaaS software components.

A graphical web interface implemented with HTML5, CSS and JavaScript serves as an entry point of the SaaS. All requests coming from patients and doctors flow through such an interface and are elaborated by a server built in Python3 leveraging Flask as Web Server Gateway Interface (WSGI) and Gunicorn to handle multiple requests with a production-ready setup. All the components are configured as Docker containers in order to take the advantages of the virtualizaiton technology allowing service portability, resiliency and automatic updates that are typical of a Cloud Infrastructure as a Service (IaaS).

The Python web server provides a front-end that allows retrieving all existing patients' information (such as personal details, disease and pharmaceutic codes,

links to documentation and Blockchain hash verification); adding new patients; and submit new treatments specifying all the required pieces of information. Specifically, a web page is dedicated to register a new patient, saving his/her primary personal information, and a separate web page is dedicated to the registration of a new treatment. It is possible to select the medical examination date, patient and doctor who does the registration to be chosen from the patients already registered and available in the database.

Since patients' sensitive data must be anonymized and health records and treatments must be trackable and irreversible, related pieces of information where stored combining a NoSQL DataBase Management System (DBMS) with a Blockchain system. Therefore, all pieces of information are stored in the MongoDB NoSQL DBMS and in the Ethereum private network through a smart contract developed in solidity. It has been chosen to use Ethereum with a private network installation considering what has been reported in Blockbench [13] highlighting the impossibility for Hyperledger Fabric, i.e., an alternative Blockchain platform, to scale above 16 nodes, which results in an important limitation for the scope of this scientific work which aims at creating a trusted and federated network among multiple hospital Clouds, and considering that Ethereum is more mature in terms of its code-base, user-base and developer community.

The smart contract accepts the input parameters such as anonymized patient id and doctor id, disease and pharmaceutic codes and stores these pieces of information in a simple data structure. The hash code resulting from the mining of each transaction is stored in the MongoDB database and can be used for verification using services like etherscan.io.

All the clinical documentation produced is uploaded in a local instance of NextCloud storage using a folder per treatment which does not contain any patient's personal data rather than the patient's anonymized identification number in order to be compliant with the General Data Protection Regulation (GDPR). Every change in the files or content of the folder will be tracked making it possible to keep a history of the documentation and its modifications.

This service is capable of detecting any modification occurred to files or folder using a listener called *External script*. It is then possible to store the fingerprint and timestamp of each modification in the database thus making it possible to track the history of the treatment. This is important to guarantee the system overall anti-tampering feature.

6   Performance Assessment

Experiments were focused on Blockchain mechanism of our SaaS implementation in order to asses the performance of the certified treatment prescription system. In particular, the system assessment has been conducted analysing the total execution time required to perform a varying number of transactions, i.e., treatment registrations through Ethereum in combination with a varying number of accounts of doctors. The testbed was arranged considering a server with following hardware/software configuration: Intel® Xeon® E3-12xx v2 @ 2.7GHz, 4 core CPU, 4 GB RAM running Ubuntu Server 18.04.

All analyses have been performed by sending transactions to the server varying the number of total and simultaneous requests. Specifically, each request invokes a new treatment registration and an Ethereum transaction mining for that. Experiments were conducted considering 100, 250 and 500 transactions and 25, 50 and 100 accounts. Each test has been repeated 30 times considering 95% confidence intervals.

To simulate a real private instance of Ethereum Blockchain, all tests have been performed using Ropsten Ethereum public test network, leveraging 300+ available nodes with a real server load status. It must be considered that Ethereum Blockchain Ropsten environment is based on Proof of Work (PoW) consensus protocol which makes difficult to obtain scalability and system speed.

Figure 3(a) describes a new treatment registration request without sending transactions to Ethereum Blockchain. This demonstrates how the server scales as the execution time is consistent for simultaneous requests (25, 50, 100) in spite of the total number of requests. Figure 3(b) shows an expected degradation of the system as compared to the requests made without Ethereum Blockchain mining and to the total number of sent transactions. This is the worst-case scenario based on the number of accounts as one account can only send one transaction at a time due to the nonce preventing replay attacks.
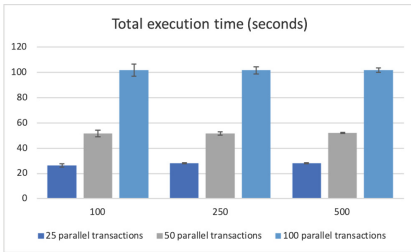
(a) Test execution without Blockchain mining.
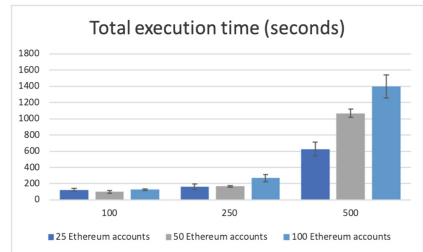
(b) Test execution with Blockchain mining.

Fig. 3. Total execution time variation.

7 Conclusion and Future Work

This project demonstrates how Blockchain can be used in the healthcare environment to improve hospital workflow guaranteeing the authenticity of stored data. Experimental results highlight that the performance of the certified treatment prescription system introduce an acceptable overhead in terms of response time considering the obvious advantages introduced by the Blockchain technology.

Definitely, the Blockchain technology is destined to evolve in the near future improving system capabilities and robustness, and public test instances with

different consensus protocols will be made available with benefits on performance and scalability.

In future developments, this work can be extended integrating a comprehensive healthcare scenario with different involved organizations, such as pharmaceutical companies registering in the Blockchain all the phases of drug production until sealing of final package and shipment, Thus, when patient buys a prescribed medicine it is possible to link the patient with the medicine box, which would mean an important step towards the end of drugs' falsification and an important assurance for the end-user who can be identified in case a specific drug package has been recalled.

References

1. Hassenteufel, P., Schweyer, F.X., Gerlinger, T., Henkel, R., Lückenbach, C., Reiter, R.: The role of professional groups in policy change: Physician's organizations and the issue of local medical provision shortages in France and Germany. European Policy Analysis (2019)
2. Dubas-Jakóbczyk, K., Domagała, A., Mikos, M.: Impact of the doctor deficit on hospital management in Poland: a mixed-method study. Int. J. Health Plann. Manag. **34**, 187–195 (2019)
3. Jha, A.K., et al.: How common are electronic health records in the United States? A summary of the evidence. Health Aff. **25**, W496–W507 (2006). PMID: 17035341
4. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system (2009)
5. Griggs, K., Ossipova, O., Kohlios, C., Baccarini, A., Howson, E., Hayajneh, T.: Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. J. Med. Syst. **42**(7), 130 (2018)
6. Chakraborty, S., Aich, S., Kim, H.: A secure healthcare system design framework using blockchain technology. In: 2019 21st International Conference on Advanced Communication Technology (ICACT), pp. 260–264 (2019)
7. Dasaklis, T.K., Casino, F., Patsakis, C.: Blockchain meets smart health: towards next generation healthcare services. In: 2018 9th International Conference on Information, Intelligence, Systems and Applications (IISA), pp. 1–8 (2018)
8. Srivastava, G., Crichigno, J., Dhar, S.: A light and secure healthcare blockchain for IoT medical devices. In: 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE), pp. 1–5 (2019)
9. Hossein, K.M., Esmaeili, M.E., Dargahi, T., khonsari, A.: Blockchain-based privacy-preserving healthcare architecture. In: 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE), pp. 1–4 (2019)
10. Zhang, P., White, J., Schmidt, D., Lenz, G., Rosenbloom, S.: FHIRchain: applying blockchain to securely and scalably share clinical data. Comput. Struct. Biotechnol. J. **16**, 267–278 (2018)
11. Ramani, V., Kumar, T., Bracken, A., Liyanage, M., Ylianttila, M.: Secure and efficient data accessibility in blockchain based healthcare systems. In: 2018 IEEE Global Communications Conference (GLOBECOM), pp. 206–212 (2018)

12. Razak, O.: Revolutionizing pharma – one blockchain use case at a time (2018)
13. Dinh, T.T.A., Wang, J., Chen, G., Liu, R., Ooi, B.C., Tan, K.L.: BLOCKBENCH: a framework for analyzing private blockchains. In: Proceedings of the 2017 ACM International Conference on Management of Data, Association for Computing Machinery, pp. 1085–1100 (2017)