ISSN 1870-4069

Design of a Blockchain Network Construction Methodology for Maintaining Patient Records based on Analysis and Modeling of Components with Standard ISO/IEC 29110 and UML for Hyperledger Iroha

Arturo I. Mendoza Arvizo, Liliana Avelar Sosa,
José Mejía, Jorge Luis García, Vicente García Jimenez

Universidad Autónoma de Ciudad Juárez,
Mexico

{arturo.arvizo, liliana.avelar, jose.mejia,
jorge.garcia, vicente.jimenez}@uacj.mx

Abstract. The use of blockchain technology is one way to make data more trustworthy in the health domain; blockchain is essentially a distributed database of digital transaction or event logs that are executed and shared between participating parties. Developing a secure and effective system has been suggested to strengthen the health sector supply chain and enable a combination of cost reduction and increased accessibility to information. The approach of this paper is a blockchain network construction methodology to improve health data management and structure a system using the potential of blockchain technology in multiple ways to hold and control access to health data. A mixed-methods methodology was applied: a structured literature search on the topic was conducted in February–May 2021, document review, survey, focus group workshops, observation, and brainstorming. Technology can be part of the development solution, a scenario that focuses on obtaining the most excellent certainty for the correct treatment of the patient; the healthcare plans complex scenarios be seen in the light of this new blockchain technology.

Keywords: Hyperledger, blockchain, iroha, consensus, secure storage.

1 Introduction

The storage of data year after year has become a challenge in information technology; this process does not require only storage but the analysis, reading, and the possibility that the information generates an economic benefit for the company [1]. A current tool that can benefit resource management in hospitals is blockchain technology, considered as an emerging technology; it is a term born in the world of information and communication technologies that have become a general use term, used in various areas

of knowledge, although mainly in economics [2]. The study attempts to answer the following questions:

a) Is it helpful to have the complete medical file of a patient available online with the certainty that the registered operations have not been altered or modified?
b) How could blockchain technology, in conjunction with electronic data capture systems, be applied to automatically aggregate, replicate, and distribute clinical data among medical personnel?
c) What are the relevant variables considered by physicians to better perform patient care and diagnosis?

Blockchain is a distributed database of digital transactions or event logs executed and shared between the participating parties. Each transaction in the blockchain is verified by the consensus of most of the participants in the system, and when added, the information remains until it is required or requested by an agent, client or staff, waiting in advance for authorization [3]. Transactions are grouped into blocks with a timestamp that reflects the instant or time that transaction is created, and these blocks are linked in chronological order. Applying blockchain technology to health data would imply using its principal characteristics from the point of view of information management, which are:

a) First, the data is stored in a chain of immutable transactions that anyone can read.
b) Second, blockchain is implemented in a decentralized network of computer nodes, making it robust against failure and attack.
c) Third, the metadata describing each transaction is available to everyone in the system [4].

2 Literature Review

This paper focuses on the architectural design for blockchain-oriented applications and proposes a construction methodology to improve the performance-based in UML (Unified Modeling Language). Arango et al. [5] consider that the systems development process involves a successive construction of models; that initially describe the application domain until reaching the solutions models, including technical aspects of the chosen implementation platform. For Fuentes et al. [6], a model describes a system in a well-defined language. A well-defined language has precise syntax and semantics that can be interpreted and manipulated by a computer.

Rumbaugh et al. [7] describe models as the entity that allows us to "grasp and exhaustively list the requirements and knowledge domain of a system so that all those involved can understand and agree with them" (p. 13). They also define UML as a visual modeling language used to specify, visualize, build, and document artifacts of a software system (p. 15). The UML is also the language proposed by the OMG (Object Management Group), an international organization whose objective is to standardize information technologies to the specification of computer systems [8].

2.1 Blockchain

The concept and the blockchain technology were created in 2009, and it is a technology that allows data transfer in a completely secure way thanks to sophisticated encryption. Essentially, a blockchain network is just a database that allows new records to be read and written. This technology represents the most critical change in databases since they were developed almost 50 years ago.

Blockchain is a person-to-person public accounting that is maintained through a distributed network of computers, and that does not require any central authority or third parties to act as intermediaries [9].

The basic idea behind blockchain technology is that it allows system actors (called nodes) to make digital transactions of assets using a peer-to-peer (p2p) network that stores these transactions in a distributed way over the network.

The assets' owners and the transactions involved in the change of ownership are recorded in the account book (ledger) through public cryptographic keys and digital signatures [2].

2.2 Blockchain Types

In blockchains, we can differentiate three main types of blockchain: private, public, and consortium [10]. In the private blockchain, only specific parties can read information and perform transactions. In the public blockchain, any user can join the network and access its information; the consortium blockchain is a mix of private and public.

2.3 Consensus Mechanisms

According to Islam et al. [11], a prominent feature of blockchain is the intervention of miners or nodes that validate and group transactions in blocks generated in the chain; this is called a consensus mechanism. Also, the consensus mechanism establishes which user in the blockchain will append the transactions to the chain as a new block.

The most common consensus algorithms in blockchain systems are proof of work, stake, and authority [12]. Consensus protocols allow transactions to be made by blockchain without relying on a third party. Selecting and implementing the correct consensus protocol is one of the most important decisions to be made at the beginning of a blockchain project.

3 Preliminaries

For the choice of the blockchain platform, the search was limited to those that have possibilities to a license with free software that allows you to work directly on the source code and documentation and are in a stable state of development. From this selection, we got the candidates named Hyperledger Iroha and Ethereum.

3.1 Blockchain Platform Chosen

The chosen platform is Hyperledger Iroha; what is Hyperledger? Hyperledger is an open-source project (open source) that was introduced in 2015 by the Linux Foundation for the development of platforms to create private blockchains with tools and programming code for the industry and the community in general; the Linux Foundation created in 2007, is a non-profit consortium dedicated to promoting the use and growth of the operating system for GNU / Linux computer systems and aims to increase its use in education, industry, and government, as well as adaptation and standardization in hardware and software components for this operating system. Sukhwani et al. [13] mention that one of the innovative characteristics of the Hyperledger platform is the consensus mechanism used to validate transactions and create blocks, this protocol is PBFT, and that transactions are controlled by a program code that provides the ability to write and design the applications that interact with the network. Hyperledger Iroha has the option of working both on a private network in permissionless, using thousands of nodes that are part of the Hyperledger Iroha network at the level global.

Additionally, Hyperledger Iroha has a creation time in which bugs found have been corrected, cases of use have been created in production, and more documentation is available to develop applications at an industrial level. Cachin et al. [14] and Valenta et al. [15] consider it a solution for constructing private-type platforms. Dhillon et al. [16] consider that the Hyperledger Iroha platform is designed as a development framework to include mobile device applications in large blockchain projects, as it integrates client libraries for application development on Android and iOS. The design of this platform also includes a domain approach, which allows a comprehensive development of set theory and set algebra and a high-performance, high-grade, fault-tolerant Byzantine consensus algorithm called YAC (Yet Another Consensus).

4 Proposed Scheme

The initial step is to identify the participants or users that interact with an application. First, a comprehensive evaluation is performed to identify actors and processes. These are the defined actors and processes:

- Actors (doctors, nurses, paramedics, administrative staff, relatives).
- Processes (information query, query data record, vital signs data record, right-of-way data records, family data record).

Entity model. The stakeholders in the proposed system can be divided into five groups: patients, patient family, medical staff (physician, caregivers, nurses), medical and administration/management.

Data model. The hospital blockchain links all parties related to hospital service into a whole network structure. The related transactions between parties are recorded and stored in the blockchain. All participants share the whole process information.

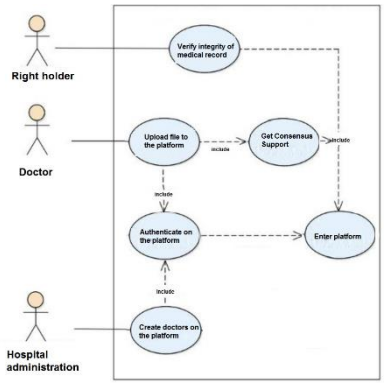

Fig. 1. Use case diagram.

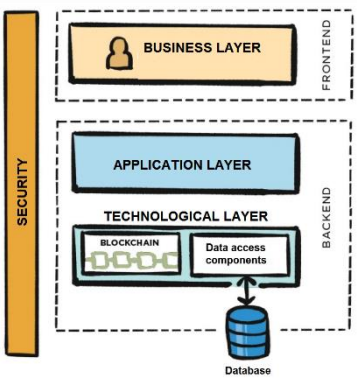

Fig. 2. Architecture.

Use case model. Diaz et al. [17] define the use case model as the model that contains the agents or actors that can interact with the system, where this interaction is shown in the use case form. In this activity, the elements of the use case in the patient care unit and the medical history management processes are identified, and the functions within the system and their relationship with the actors are reflected, as shown in figure 1.

Architecture. The proposed architecture consists of the following layers: business, application, and technology and aims to store medical history data. Figure 2 depicts the architecture of the model.

- Business layer: it is where all the logic of the business network is.
- Application layer: the connection layer contains the necessary infrastructure to receive information from the business and technological layers in real-time.
- Technological layer: this layer is the blockchain operating machine.

The components are explained in the following:

- Transaction Gateway: The transaction gateway is a connection component that

will coordinate the various components that work together to discover and connect with the blockchain endpoint.

- Request Receiver: It is an upfront server that receives the HTTP requests.
- Communication Interface.
- Blockchain Engine: Hyperledger Iroha that it is one of the critical components.
- Functional Interface.

5 System Implementation

This section concerns the implementation and simulation of the blockchain-backed application. The Agile Unified Process (AUP) methodology will be followed, characterized by being directed to use case, focused on architecture, iterative and incremental. This application will assist stakeholders in performing tasks related to the issuance and validation of electronic health records. More specifically:

- Hospital institution.
- Patients.
- Medical Staff.

5.1 ISO / IEC 29110

The ISO / IEC 29110 standard is taken as a reference for developing the architecture because it is a compliance standard that helps ensure and increase the quality of the software product, strengthening the production process and understanding that a product is strongly influenced by the process that develops it. ISO / IEC 29110 contains two approaches:

- Management process.
- Software implementation.

5.2 Tools

The tools and accessories to be used for the development of the architecture are planned considering that the blockchain architecture is based on resources, where a resource is the abstraction of anything that can be conceptualized, as follows:

- Physical structure. As a hardware tool for the proposed system, a computer with Intel Core i5-8500 @ 2.00Ghz CPU, 8 GB of RAM, was used.
- Operating system. Ubuntu Linux (16.04.1 LTS) was installed for the operating system.
- Blockchain operating platform. Hyperledger Iroha.

5.3 Application Functionality

In this section, the installation, configuration, and startup of the technological layer is carried out, which is done from an Ubuntu terminal console and with the CLI of the blockchain platform (Command-line Interface), which is the communication path of the engine (machine) or main engine of blockchain work.

5.4 Installation

As the first step for the installation is the creation of the network.

- sudo docker network create Iroha-network

A workspace is set up.

- sudo docker volume create block store

The latest version of the engine is obtained and installed:

- sudo apt-get install git git clone -b develop https://github.com/hyperledger/iroha–depth = 1

5.5 Initialization

The platform is entered, and the execution begins, with the instructions:

- docker exec -it Iroha / bin/bash

5.6 Access

The controls are accessed to perform operations on the platform and to be able to enter instructions from the platform's CLI.

- Iroha -cli -account name admin@test.

Furthermore, we are shown the menu of operations.

- New transaction (tx).
- New query (qry).
- New transaction status request (st).

6 Conclusion and Future Work

This paper proposes a blockchain solution for managing data privacy, integrity, and process workflow for electronic health records. It also proposes a structure and a methodology for the construction of blockchain architecture. It is intended to expand the study using a cloud service such as AWS or IBM Blockchain to evaluate the proposed methodology in a production environment attached to a patient care unit.

Numerical analysis is also required to study the impact of hardware components, such as memory allocation, disk type and speed, network speed, and CPU. In addition,

it is planned to investigate the impact of the proposed methodology on other new private blockchain platforms.

Acknowledgments. We are grateful for the funding received by CONACYT for the research and writing of the article within the framework of the project: “Design of a Blockchain architecture for the management of medical records in the health sector". Furthermore, the support received from the Autonomous University of Ciudad Juárez through the postgraduate area in the Doctorate in Advanced Engineering Sciences (DOCIA).

References

1. Ocampo, C.: Blockhain la nueva base de SQL en BIG Data (2017)
2. Warburg, B.: How the blockchain will radically transform the economy. TED Summit (2016)
3. Crosby, M., Nachiappan, P. P., Verma, S., Kalyanaraman, V.: Blockchain technology. Sutardja Center for Entrepreneurship and Technology, 1, pp. 2–5 (2015)
4. Engelhardt, M. A.: Hitching healthcare to the chain: An introduction to blockchain technology in the healthcare sector. Technology Innovation Management Review, 7(10) (2017)
5. Arango, F., Gómez, M. C., Zapata, C. M.: Transformación del modelo de clases UML a Oracle9i bajo la directiva MDA: Un caso de estudio, Dyna, 73(149), pp. 166–179 (2006)
6. Fuentes, L., Vallecillo, A.: Una introducción a los perfiles UML, Novatica. 168, pp. 6–11 (2004)
7. Rumbaugh, J., Jacobson, I., Booch, G.: The unified modeling language, Reference manual, Addison Wesley Longman Inc (1999)
8. Hause, M.: The SysML modeling language. In Fifteenth European Systems Engineering Conference, 9, pp. 1–12 (2006)
9. Karp, N.: Tecnología de cadena de bloques (blockchain): la última disrupción en el sistema financiero. BBVA research (2017)
10. López, J., Mora, J. J.: La economía de blockchain: Los modelos de negocio de la nueva web (2016)
11. Islam-Najmul, A. K. M., Mantymaki, M., Turunen, M.: Why do blockchains split? An actor-network perspective on Bitcoin splits Technological Forecasting and Social Change, 148 (2019)
12. Li, X., Wang, Z., Leung, V., Ji, H., Liu, Y., Zhang, H.: Blockchain-empowered Data-driven Networks: A survey and outlook (2021) arXiv preprint arXiv:2101.12375,2021.
13. Sukhwani, H., Wang, N., Trivedi, K., Rindos, A.: Performance modeling of Hyperledger fabric permissioned blockchain network. In: IEEE 17th International Symposium on Network Computing and Applications (NCA), pp. 1–8 (2018)
14. Cachin, C.: Architecture of the Hyperledger blockchain fabric. Workshop on

distributed cryptocurrencies and consensus ledgers, 310(4) (2016)
15. Valenta, M., Sandner, P.: Comparison of ethereum, hyperledger fabric and corda, Frankfurt School Blockchain Center, 8 (2017)
16. Dhillon, V., Metcalf, D., Hooper, M.: Unpacking ethereum, blockchain-enabled applications, pp. 37–72 (2021)
17. Díaz, J. S., Vila, A. A., Pastor, O., Fons, J. J.: Prototipado de interfaces de usuario a partir de escenarios y modelos UML, WER, pp. 126–139 (2000)