Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 177 (2020) 546–551

Procedia Computer Science

www.elsevier.com/locate/procedia

International Workshop on Healthcare Open Data, Intelligence and Interoperability (HODII)
November 2-5, 2020, Madeira, Portugal

ICU Data Management - A Permissioned Blockchain Approach

Tiago Guimarães[a]*, Ailton Moreira[a], Hugo Peixoto[a], Manuel Santos[a]

[a] *Algoritmi Center/University of Minho*

Abstract

Since its origin in finance, blockchain have been revolutionizing data storage and sharing in many other sensitive areas. Being the focus of Permissioned Blockchains around privacy, confidentiality, immutability, interoperability and reliability, it fits perfectly within the data requisites of healthcare. Even more, with the surge of new iterations of more recent implementations based on smart-contracts/chaincode that has its focus on increasing efficiency and usability and ease of implementation.

Intensive Medicine an area with such high data complexity and throughput, and high incidence of medical error and patient injury. As such, it's imperative the continuous research and implementation of new technologies that can make pertinent knowledge available through reliable and accurate data, thus providing appropriate problem-solving skills to physicians.

This paper presents a solution, as part of the Intelligence Decision Support Systems for Intensive Medicine (ICDS4IM) project, which objective is to increase accuracy, confidentiality and value to data from vital sensors and monitors by assuring its immutability and controlled oversee.

Keywords: Blockchain; Healthcare; Hyperledger Fabric; Permissioned; Intensive Medicine

* Corresponding author. Tel.: +35918608484
E-mail address: tsg@dsi.uminho.com

10.1016/j.procs.2020.10.076

1. Blockchain in Healthcare

Data in healthcare is, in its essence, highly diverse and complex, sensitive and private. This information can, however, be shared between peers such as software providers, health insurance companies, patients' families, among others. It's imperative to keep track of the data after being shared between multiple entities, maintaining access control through numerous consents. For many cases, a log is needed to keep a record of the treatment process history of the patient since this information may prove to be crucial for his treatment [1] [2].

Hospitals require a constant communication through an exchange of health information for managing and treating patients. However, a wide available interoperability brings new challenges and requirements regarding security and privacy, technology and governance. Part of the problem consists in solving these challenges, which are still not solved for traditional interoperability, in which blockchain can provide an important role.

Simply putting, Blockchain is an immutable and distributed ledger maintained within a distributed network of peer nodes. These nodes each maintain a copy of the ledger by applying transactions that have been validated by a consensus protocol. [2]

In the context of this paper, a transaction can be the creation, update and sharing of patients' medical data between intervenients (clients, applications, etc). A ledger records all these transactions and represents the state of the network.

2. Permissionless/Permissioned Blockchain

Blockchain networks can be divided in two broad categories, permissionless and permissioned or, as often referred to in literature, respectively public and private blockchains.

In a permissionless blockchain, anybody can participate, and every participant is anonymous. In contrast to a private blockchain or a permissioned blockchain, in a permissionless blockchain there is neither a restriction on the ability to read from the blockchain (this ensures public verifiability) nor a requirement for pre-established identities for write access to the blockchain. In the most popular blockchains like Bitcoin or Ethereum, the consensus is achieved by a proof-of-work mechanism, which is attained by "mining". [2] [3]

Permissioned blockchains, on the other hand, operate a blockchain amongst a set of known and identified participants that have a common goal. However, while the participants may not fully trust each other, a network can be operated under a governance model that is built off of what trust does exist between participants, such as a legal agreement or framework for handling disputes.

By relying on the identities of the participants, a permissioned blockchain can use more traditional crash fault tolerant (CFT) or byzantine fault tolerant (BFT) consensus protocols that do not require costly mining. [1] [2]

A solution using a Permissioned blockchain, namely with Hyperledger Fabric, will be presented. Therefore, both permissioned blockchain and Hyperledger Fabric will be discussed with further detail throughout the paper.

3. Hyperledger Fabric (HLF)

HLF is an open source enterprise-grade permissioned open-source distributed ledger technology (DLT) platform, maintained by IBM and Linux Foundation, designed for use in enterprise contexts. Has a highly modular and configurable architecture, enabling innovation, versatility and optimization for a broad range of industry use cases including, as the purpose of this article, healthcare. [4] [5]

Fabric is the first distributed ledger platform to support smart contracts authored in general-purpose programming languages such as Java, Go and Node.js, rather than constrained domain-specific languages (DSL).

Fabric can leverage consensus protocols that do not require a native cryptocurrency to incent costly mining or to fuel smart contract execution. The absence of cryptographic mining operations means that the platform can be deployed with roughly the same operational cost as any other distributed system. [5]

The HLF is structured upon some main nodes/components and core concepts relevant to this work: Submitting-client, Peer, Orderer, Certificate Authority (CA), Chaincode and Consensus. [5]

Client, represents the entity that acts on behalf of an end-user and has the control to submit transaction-invocation to the endorsers and broadcasts transaction-proposals to the ordering service. [5] [6][7]

Peer, a node that commits transactions and maintains the state and a copy of the ledger. A peer receives ordered state updates in the form of blocks from the ordering service and maintain the state and the ledger. Peers can additionally take up a special role of an endorser. The special function of an endorser occurs with respect to a particular chaincode and consists in endorsing a transaction before it is committed. [5]

Orderer or Ordering Service Nodes, are the nodes that collectively form the ordering service. It provides a shared communication channel to clients and peers, offering a broadcast service for messages containing transactions. Clients connect to the channel and may broadcast messages on the channel which are then delivered to all peers. The communicated messages are the candidate transactions for inclusion in the blockchain state. Orderers are entirely unaware of the application state, and do not participate in the execution nor in the validation of transactions. This design choice renders consensus in Fabric as modular as possible and simplifies replacement of consensus protocols in Fabric. [5][7]

Hyperledger Fabric CA, is the default Certificate Authority component, which issues PKI-based certificates to network member organizations and their users. The CA issues one root certificate to each member and one enrollment certificate to each authorized user. [5]

Chaincode, is the business logic of a blockchain application and functions as a trusted distributed application that bases its trust from the blockchain and the underlying consensus among the peers. A chaincode implements the application logic and runs during the execution phase. [7]

Consensus implies a process in which the members of a blockchain network agrees whether a transaction is valid or not and to keep consistency in ledger synchronization, lowering the risk of malicious transactions.

HLF presents a pluggable consensus approach. The ordering of transactions is delegated to a modular component (ordering service) for consensus that is logically decoupled from the peers that execute transactions and maintain the ledger. Since consensus is modular, its implementation can be tailored to the trust assumption of a particular deployment or solution.

There are many consensus algorithms such as Proof-of-work (PoW), Proof-of-stake (PoS), Practical Byzantine Fault Tolerance (pBFT), among others. The modular architecture presented by HLF allows the platform to rely on well-established toolkits for CFT (crash fault-tolerant) or BFT (byzantine fault-tolerant) ordering and can have multiple ordering services supporting different applications or application requirements. [5] [8]

4. Privacy and Confidentiality

In many public, permissionless blockchain networks, every transaction, and the code that implements it, is visible to every node in the network. This lack of confidentiality and control can be challenging for many enterprise solutions where not all data is desirable to be viewed by everyone. [7]

Data can be encrypted in order to provide confidentiality; however, given enough time and computational resource, the encryption could be broken. For many enterprise use cases, the idea that their information could be accessible or leaked is unacceptable. [5]

HLF, enables confidentiality through its channel architecture and private data feature. In channels, participants on a Fabric network establish a sub-network where every member has visibility to a particular set of transactions. Thus, only those nodes that participate in a channel have access to the chaincode and data transacted, preserving the privacy and confidentiality of both. [5] [7]

5. Interoperability with AIDA for Intensive Medicine

Healthcare institutions face a scenario where data is spread across a multitude of places and systems. Each system has its own database and data dictionary making information share a difficult task. Several steps have been taken to establish some interoperability rules among health data, namely the usage of standards, such as HL7, and ontologies such as SNOMED, LOINC, among others. These tools have made data sharing a less complex task, and some platforms have taken these standard to a next level, acting as central communication point between all the actors among the patient flow inside the healthcare facility, namely AIDA (Agency for Interoperation, Diffusion and Archive of Clinical Information) AIDA is a multi-agent system that uses HL7 as communication gateway and supports its actions in other standards, such as OpenEHR and SNOMED. This behavior empowers data and information flow, not only inside the institution, but also breaking walls in pear-to-pear communication between institutions. Acting as central point in the communication system, AIDA as a complex but rewarding task, being able to ensure GDPR compliance, but most important information quality. [9] [10]

Intensive Care professionals rely an important part of their decisions in a huge amount of data and information. Therefore, real-time data that emerges from all sort of sources, for example, from medical equipment's such as ventilators, and all the registers from the Electronic Health Record available online; and decision support systems are of great value. Decisions are made in a fraction of a second and their competence count on accurate data, pertinent knowledge, and appropriate problem-solving skills. All the collected data must be stored in a proper way to ensure availability and trust in it whenever professionals need it and needs to be provided with enough efficiency and throughput so it won't become more inconvenient than prolific. [11] [12] [13]

5.1. Blockchain in Intensive Medicine

Assuring the value and reliability of information in critical areas such as the Intensive Care is vital. Private blockchain presents here a solution that not only assures the value and veracity of data within this context but also grants privacy and confidentiality between its users, making it possible to provide administrators and auditors with private and secure access to medical information. [2] [14]

HLF consists of two very convenient and distinct parts: world state and blockchain. The first is a distributed database (CouchDB), that maintains the current values of the attributes of an object. This world state allows programs to directly access the value of an object without having to navigate the entire blockchain to calculate it. The second is the blockchain transaction log which stores all the history of changes that led to the most recent value in the world state collected in blocks. [15]

These components not only allow this solution to be more efficient on the retrieval of the latest state of a patient, but also the full historic of data changes for each patient.

The data stored in the ledger and considered for this implementation is separated into two parts: a static one where we have the identifier for the patient (admission id), room and bed; and a dynamic that is based upon what is being gathered by each monitor at that time. The latter is the part that is constantly being updated for the patient within the blockchain. Noting that, for this implementation, no demographic data of the patient is stored or considered.

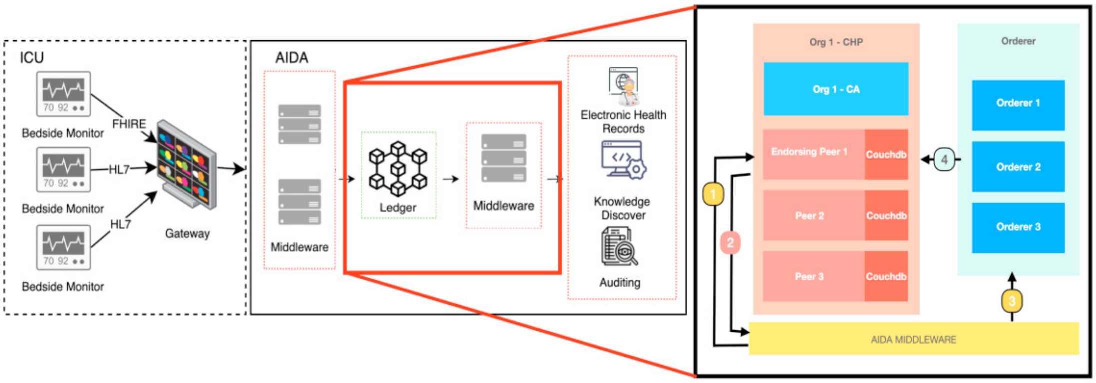

Figure 1 – ICD4SIM Architecture with blockchain

In figure 1, the general architecture for the ICD4SIM is presented, focusing on the components of the Ledger and Middleware that communicates with it.

The transaction flow of information between these two parts goes as follow:

1. Client A initiates a transaction (insertion of a new patient, monitor data update, etc);
2. Endorsing peers verify signature & execute the transaction. Each of these peers checks if: the proposal is well structured, the application is not trying to duplicate a transaction that already exists, the signature of the issuer is valid and if the issuer is allowed to perform the proposed operation. Then, each endorser executes the chaincode individually and generates a transaction response based on the execution results, and then it signs the response. Finally, the signed transaction proposal response is sent back to the application. Depending on the number of endorsing peers defined in the endorsement policy, the client waits until it receives a certain number of endorsements. [4] [6]
3. The client sends the endorsed transaction proposal responses to the orderers. Upon that, the orderers package the authorized transactions into a block in a strict order. The orderer does not bother itself looking into the content of the transactions, unless it is a configuration block. [4] [6]
4. The ordering service delivers a transaction to the peers connected to it, peers that are not connected to the orderer will eventually receive the block by gossiping. Each peer on the channel will validate the transactions in the block separately but in a deterministic way, since all the peers validate the block in the same way, each peer will have an identical copy of the ledger. [4] [6]

6. Conclusion

The constant evolution for data management solutions makes possible the constant growth not only on efficiency and reliability but also confidentiality and privacy of patients' data.

For vital areas such as intensive care medicine, being able to understand data when also respecting the patients' privacy and data being used will lead to a more sustainable and truthful practice.

Blockchain technology, gathers all that integrity, verifiability and resistance to violations of sensitive medical data making it an adequate solution worth researching and improve upon, in this context.

Maintaining not only the ledger with all the transaction historic data but also a database containing the current state of the data, HLF, is a practical blockchain solution that facilitates the data management process, for the different stakeholders present in the health area, and also for data prevision and clinical decision-making support systems.

Also, with its growing documentation, present evolution and contribution, and for its support of smart contracts authored in general-purpose programming languages such as Java, Go and Node.js, the learning curve for its implementation reduces drastically compared with other solutions.

Acknowledgements

The work has been supported by FCT – Fundação para a Ciência e Tecnologia within the Projects Scope: DSAIPA/DS/0084/2018.

References

[1] Dubovitskaya A.; Xu Z. ; Ryu S. ; Schumacher M. & Wang F. (2017). Secure and Trustable Electronic Medical Records Sharing using Blockchain. Retrieved November 23, 2019, from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5977675/

[2] Guimarães, T., Silva, H., Peixoto, H., & Santos, M. (2020). Modular Blockchain Implementation in Intensive Medicine. Procedia Computer Science, 170, 1059-1064.

[3] T. Neudecker and H. Hartenstein, "Network Layer Aspects of Permissionless Blockchains," in IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 838-857, Firstquarter 2019, doi: 10.1109/COMST.2018.2852480.

[4] S. Shalaby, A. A. Abdellatif, A. Al-Ali, A. Mohamed, A. Erbad and M. Guizani, "Performance Evaluation of Hyperledger Fabric," 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), Doha, Qatar, 2020, pp. 608-613, doi: 10.1109/ICIoT48696.2020.9089614.

[5] Hyperledger (2020) Hyperledger Fabric Docs release 2.2. Retrieved August 19, 2020, from https://hyperledger-fabric.readthedocs.io/en/release-2.2/.

[6] J. Sousa, A. Bessani and M. Vukolic, "A Byzantine Fault-Tolerant Ordering Service for the Hyperledger Fabric Blockchain Platform," 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Luxembourg City, 2018, pp. 51-58, doi: 10.1109/DSN.2018.00018.

[7] Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., ... & Muralidharan, S. (2018, April). Hyperledger fabric: a distributed operating system for permissioned blockchains. In Proceedings of the thirteenth EuroSys conference (pp. 1-15).

[8] Nguyen, G. & Kim, K. (2018). A Survey about Consensus Algorithms Used in Blockchain. Journal of Information Processing Systems, Vol.14, No.1, (pp.101-128). Retreived December 1, 2019, from http://myweb.jnu.ac.kr/~kbkim/papers/%5B2018%20JIPS%5DA%20Survey%20about%20Consensus%20Algorithms%20Used%20in%20Blockchain.pdf

[9] Gordon W. J. & Catalini C. (2018) Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability. Retrieved November 23, 2019, from https://www.sciencedirect.com/science/article/pii/S200103701830028X#bb0030.

[10] Peixoto, H., Santos, M., Abelha, A., & Machado, J. (2012, December). Intelligence in Interoperability with AIDA. In International Symposium on Methodologies for Intelligent Systems (pp. 264-273). Springer, Berlin, Heidelberg.

[11] M. A. Musen, B. Middleton, and R. A. Greenes, "Clinical decision-support systems," in Biomedical informatics, ed: Springer, 2014, pp. 643-674.

[12] Peixoto, H., Guimarães, T., & Santos, M. F. (2020). A New Architecture for Intelligent Clinical Decision Support for Intensive Medicine. Procedia Computer Science, 170, 1035-1040.

[13] Gorenflo, C., Lee, S., Golab, L., & Keshav, S. (2019, May). Fastfabric: Scaling hyperledger fabric to 20,000 transactions per second. In 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) (pp. 455-463). IEEE.

[14] T. K. Bucknall, "Medical error and decision making: learning from the past and present in intensive care," Australian critical care, vol. 23, pp. 150-156, 2010.

[15] Foschini, L., Gavagna, A., Martuscelli, G., & Montanari, R. (2020, June). Hyperledger Fabric Blockchain: Chaincode Performance Analysis. In ICC 2020-2020 IEEE International Conference on Communications (ICC) (pp. 1-6). IEEE.