Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 210 (2022) 242–247

Procedia Computer Science

www.elsevier.com/locate/procedia

The 3rd International Workshop on Healthcare Open Data, Intelligence and Interoperability (HODII)
October 26-28, 2022, Leuven, Belgium

Permissioned Blockchain Approach using Open Data in Healthcare

João Cunha[a], Ricardo Duarte[a], Tiago Guimarães[a*], Manuel Filipe Santos[a]

[a]*Algoritmi/LASI research center, University of Minho, Portugal*

Abstract

Digital health records play a key role in the area. However, it is difficult to obtain a unified view of your data, as it is distributed among different providers, spread over several places, and is not integrated. To address these problems, blockchain technology and the openEHR interoperability standard have emerged. Blockchain is a new wave of disruption that has come to redesign interactions that involve any form of exchange of values, with the potential to improve healthcare, bringing a new perspective on security, resilience, and effectiveness of systems. In turn, with the use of openEHR, the standardization of electronic records is guaranteed, offering fine-grained access permissions for stakeholders. In addition to the use of archetypes as a reference to make the templates, where they are integrated to build a module with compatible standards.
Based on an open data framework, OpenEHR, and blockchain technology, this paper has conceptualised a proposed two architectures that will be implemented within a Portuguese hospital, at the ICU, to increase and provide support for clinical decision-making, ensuring interoperability between systems, as well as the veracity, privacy and security of the data being used.

Keywords OpenEHR; Blockchain; Helthcare; Hyperledger Fabric

* Corresponding author.
E-mail address: tiago.guimaraes@algoritmi.uminho.pt

10.1016/j.procs.2022.10.144

1. Introduction

Health is one of the most worrying issues in human society. From early on, Humanity began to be concerned with issues of diseases and health, since these factors accompany our species throughout evolution. In this sense, there is a need to improve the quality of health care provision. For this, it is necessary to guarantee accurate and concrete information so that the decision-making process is useful and provides value to the patient [1].
Nowadays, healthcare institutions manipulate massive amounts of data. Their understanding directly reflects the success of the institution, as a good interpretation of these transforms them into useful information capable of improving its entire environment [2]. These institutions have evolved into more efficient, coordinated and patient-centred systems. This propensity implies more integrated, interoperable, and ubiquitous health services, leading to greater and easier access to information about healthcare, and a more active involvement of patients in this process [3]. However, the management and availability of confidential and sensitive data, that requires special attention and a set of specific rules that guarantee its authenticity, privacy, immutability, and security as the interoperability between all systems. So, to meet these rules it is used the approach of OpenEHR and blockchain technology. The OpenEHR enables the structuring, management, storage, and commutation of patient data in a secure and reliable way between different healthcare organizations. The main idea of this approach is to standardize health-related concepts used in databases or Electronic Health Record (EHR) systems in a set of libraries, called archetype. The Blockchain technology that could be used as a solution to these problems, as it ensures a chronological order of data, as well as its authenticity, privacy, immutability, and security[4]–[6].
The present work is divided into several sections, initiating with a brief introduction. In the sections two and three are presented a literature review about OpenEHR and blockchain, correspondingly. The section four explains a correlation between them, and the architectural conceptualization. Finally, it's presented the final conclusions.

1. OpenEHR

EHR stores a large amount of medical data, data that must be available throughout a patient's life. This information should be understandable regardless of the medical institution accessing it, i.e., ensuring data interoperability. EHRs can have a positive impact on quality of care, patient safety and efficiency. However, without accurate and appropriate content in a usable and accessible format, these benefits will not be achieved, which means that data must be captured, addressing quality issues, so as not to be prone to propagating downstream errors into data warehouses and other data analysis systems. The problem is often not the amount of data available, but the fact that most of the information is composed of free text serving only to record and consulting information [7], [8], [9].
OpenEHR is a non-profit organization that relies on the collaboration of a vast international community, with the aim of creating clinically comprehensive and interoperable EHRs. Its main objective is to guarantee the semantic interoperability of clinical information between EHRs. Semantic interoperability consists of the way it is stored and not the way it is processed, that is, the data does not need to be processed in the same way, but the results must have the same format. It allows the sharing and interpretation of information used by two or more systems [10], [11].
The function of OpenEHR is related to the representation of a generalized information model. That introduces the concept of archetypes related to a specific medical concept, as well as the reference model, which defines the EHR semantics, EHR extract and demographics. The particularity of OpenEHR in relation to other existing EHRs, is that it not only provides the interoperability aspect for the platform, but also an adaptability to the needs of the medical entity in question [12]. In terms of data security, it ensures data resilience by keeping it in the system in a historical and review approach. Each change in the patient's EHR is stored by means of the audit system, which offers high reliability to the structure [11].
The OpenEHR Foundation states that OpenEHR has "multilevel single-source modelling within a service-oriented software architecture where models built by domain experts are in their layer". With this statement, we can conclude that the architecture of OpenEHR is based in two levels that separate information from knowledge [7]. Based on this dual architecture the terms of information and knowledge, aligning technical and clinical knowledge. Clinical information is modelled by means of reference models, while knowledge is simplified by means of Archetype Object Model. This standard is based on its clinical knowledge artifacts, called archetypes, which clinically speaking, represent the basis for defining, discussing, and presenting clinical content [11].

2. Blockchain

Blockchain is not just a change, but a fast-moving phenomenon that is already on the move. It is the new wave of disturbances that has redesigned the way in which any type of exchange of value is carried out [13], bringing a new perspective on the security, resilience and efficiency of systems [14].
Blockchain technology consists of a fully distributed, encrypted system that immutably, securely, and sequentially stores and records data about transactions between nodes on the same network. It also guarantees that this data is stored, updated and verified by the other nodes, providing transparency and reliability of these transactions and consequent network consensus on their legitimacy [15].

1.1. Permissioned (private) blockchain in healthcare

Blockchain technology can be used and categorized in different ways, permissionless or permissioned blockchains [16]. No matter which blockchain is used or applied, both have advantages. In some cases, it is necessary to implement a permissionless blockchain, due to its convenience. In other cases, it is necessary to ensure private control and, as such, permissioned blockchains are the best option [17].
In this case of the study, the preference for permissioned blockchains becomes evident, as they are a better choice to guarantee the privacy and safety of patient's records.
A permissioned blockchain is a system where the identity of the entities is controlled by an identity provider. The latter is responsible to maintain and control network access and user's participation in consensus and block validation [18] . There is an access control mechanism to determine who can join the system, and only those with such permissions can engage with the blockchain. As a result, each node is authenticated, and its identity is known to the other nodes [16], [19]. Hyperledger is one of the most popular private blockchains. In addition to deterministic consensus, another of the important properties is that they support smart contracts that can express highly complex transaction logic [20].

1.2. Hyperledger Fabric

According to Cachin (2016) [21], Hyperledger Fabric is a distributed ledger framework for running smart contracts using blockchain technology, leveraging technologies that are well-known and well-proven, with a modular architecture that allows for pluggable implementations of different functions. It is a blockchain platform aimed for business use and one of the multiple projects currently in development under the Hyperledger Project. It's open-source and standards-based, and it can run user-defined smart contracts. It's also built on a modular architecture with pluggable consensus protocols, and it has solid security and identity features. The fabric's distributed ledger protocol is controlled by peers.
The fabric distinguishes between two kinds of peers, validating peers and non-validating peers. A validating peer is responsible for validating transactions, hence its designation. It also runs consensus. On the other hand, a non-validating peer functions as a proxy to connect clients, distribute transactions, to validating peers. Although a non-validating peer does not perform transactions, it may check them. The fabric it also includes a security framework for authentication and authorization since it implements a permissioned ledger. Enrolment and transaction authorization are supported by public-key certificates, and chain code security is ensured by in-band encryption. Transactions can be public or confidential, depending on the nature of the data stored. As a consensus method, Hyperledger utilizes the Practical Byzantine Fault Tolerant [22].

2. Blockchain and OpenEHR – Architectural Conceptualizations

Integrating Blockchain with OpenEHR comes up to solve the problems related with the idea of standardizing health-related concepts used in databases or EHR systems in an archetype. These problems are the authenticity, privacy, immutability, and security of confidential and sensitive data that fluxes in health care systems which the blockchain technology could be used as a solution.
For our study, we chose to conceptualise two scenarios. First scenario, represented in figure 1, and the second scenario, represented in figure 2.

In the following figure, it is possible to visualize the first scenario. This conceptualization, in addition to maintaining interoperability among all EHRs due to the use of OpenEHR, also ensures the veracity, privacy and security of data due to the use of blockchain technology. Analysing the flow, this starts with the information and records of the users, who can be nurses, doctors and other entities present in the area. These entities generate electronic health records, known as EHRs, which are stored in the existing healthcare services within the hospital. Subsequently, this data will be processed and analysed according to the specifications modelled in OpenEHR in the API's layer, which are present in the gateway. Subsequently, this data will be stored as transactions within the blockchain. The implemented blockchain, will be a permissioned, based on Hyperledger Fabric that will have as consensus method the Practical Byzantine Fault Tolerant. Finally, after validation of the contract, the transactions will be sent to a middleware where they will be treated, organized, and made available according to the needs of the environment, to later be possible to the interested stakeholders, such as doctors, managers, and others, to perform benchmarking, data analysis and audits, in a fast and effective way providing value to the institution.

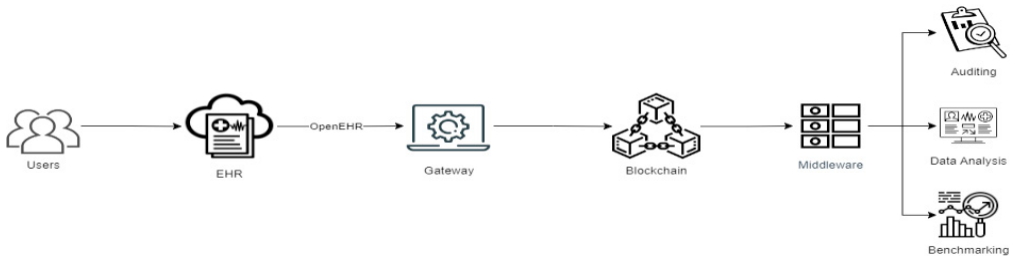

Figure 1. SEQ Figure * ARABIC 1 – First Scenario - Architectural Conceptualization

The following figure presents the second scenario. In this conceptualization, the flow starts the same away as the first scenario, with the information and records of the users, who can be nurses, doctors and other entities present in the area. That create the EHR's of the patient. Later, in the gateway the data will be processed and analysed according to the specifications modelled in OpenEHR in the API's layer. In the gateway, data will be divided and stored in two ways. Following the flow of the upper arrow, the data will be stored in the hospital database, where after passing through the middleware, they will be processed and transformed according to the needs of the hospital stakeholders to be able to perform data analysis, benchmarking, and audits in a fast and efficient way. Following the flow from below, a block hash is created, where the ID of this data is generated and the respective hash. Later, they are inserted in the blockchain with a reference to that line (line ID and hash), here only one hash is stored, and whenever there is an update, this hash is updated. Finally, after validation of the contract, the transactions will be sent to a middleware where they will be treated and analysed to understand if there was any malicious change outside the system.
This way we have the creation of two scenarios. We have scenario 1 which is a more ambitious conceptualisation that spends more resources, however, in terms of security it is better. In scenario 2, we have a lightweight version, where blockchain technology is only used to understand and compare if there has been any malicious change outside the system. This way we achieve a higher form of validation as a layer upon existing systems and not as a replacement.

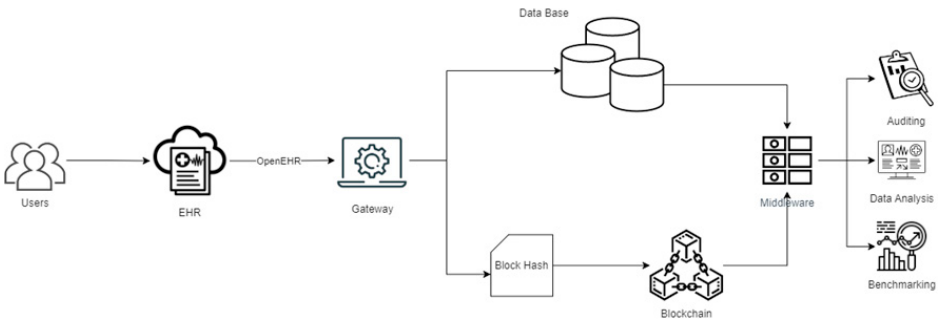

Figure 2. SEQ Figure * ARABIC 2 - Second Scenario - Architectural Conceptualization

3. Conclusion

When developing a platform to augment and provide greater support for clinical decision-making, it is critical to ensure interoperability between systems in addition to the veracity and value of the data being used. In the long term, understanding the data and the ability to obtain correct and reliable methods leads to better functioning of the hospital and more informed, reliable, and secure decisions by the entities involved.

The use of the open data model, openEHR, brings added value as it allows interoperability between the various systems present in this environment. In this way, it becomes possible to transmit the necessary information about a patient to ensure the quality, safety, and efficiency of their data.

The use of blockchain technology implies some benefits for the health area. In particular, the integrity, security, immutability, verifiability, and privacy of sensitive medical data. Such benefits facilitate the process of data management by the various stakeholders present in the area. In this way, accountability for improper consultation of private or confidential patient data can be ensured.

In this paper is presented a conceptualization of two architectures, which uses openEHR and blockchain technology. When we compare the two scenarios, it is possible to see that scenario 2 is more viable to implementation, as it is a more lightweight version. There is less use of resources since the data is stored in conventional databases and in the blockchain only the last hash of the data block is stored, where it only serves to understand if there has been any malicious change outside the system. It is important to note that whenever there is an update to the data, this hash will also be updated. On the other hand, scenario 1, despite being more secure, is also the one that uses the blockchain as a data repository, consequently consuming a lot of resources to the hospital. As future work, in order to understand which one of the two scenarios is more beneficial for the hospital, we will test them and come to new conclusions about them.

Acknowledgements

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

References

[1] J. Cunha, R. Duarte, T. Guimarães, C. Quintas, and M. F. Santos, "Blockchain analytics in healthcare: An Overview," Procedia Computer Science, vol. 201, pp. 708–713, Jan. 2022, doi: 10.1016/j.procs.2022.03.095.

[2] M. Quintal, T. Guimarães, A. Abelha, and M. F. Santos, "Business Analytics for Social Healthcare Institution," in Trends and Innovations in Information Systems and Technologies, Cham, 2020, pp. 503–509.

[3] F. Fernández and G. Pallis, "Opportunities and challenges of the Internet of Things for healthcare: Systems engineering perspective," 2014 4th International Conference on Wireless Mobile Communication and Healthcare - Transforming Healthcare Through Innovations in Mobile and Wireless Technologies (MOBIHEALTH), pp. 263–266, 2014.

[4] S. Angraal, H. M. Krumholz, and W. L. Schulz, "Blockchain technology: applications in health care," Circulation: Cardiovascular quality and outcomes, vol. 10, no. 9, p. e003800, 2017.

[5] M. Prokofieva and S. J. Miah, "Blockchain in healthcare," Australasian Journal of Information Systems, vol. 23, 2019.

[6] T. Ribeiro, S. Oliveira, C. Portela, and M. Santos, "Clinical Workflows based on OpenEHR using BPM.," in ICT4AWE, 2019, pp. 352–358.

[7] F. Hak, D. Oliveira, N. Abreu, P. Leuschner, A. Abelha, and M. Santos, "An OpenEHR Adoption in a Portuguese Healthcare Facility," Procedia Computer Science, vol. 170, pp. 1047–1052, Jan. 2020, doi: 10.1016/j.procs.2020.03.075.

[8] J. Almeida, S. Frade, and R. Cruz-Correia, "Exporting Data from an openEHR Repository to Standard Formats," Procedia Technology, vol. 16, pp. 1391–1396, Jan. 2014, doi: 10.1016/j.protcy.2014.10.157.

[9] D. Oliveira et al., "New Approach to an openEHR Introduction in a Portuguese Healthcare Facility," in Trends and Advances in Information Systems and Technologies, Cham, 2018, pp. 205–211.

[10] L. Cardoso, F. Marins, F. Portela, M. Santos, A. Abelha, and J. Machado, "The Next Generation of Interoperability Agents in Healthcare," IJERPH, vol. 11, no. 5, pp. 5349–5371, May 2014, doi: 10.3390/ijerph110505349.

[11] D. Oliveira et al., "Management of a Pandemic Based on an openEHR approach," Procedia Computer Science, vol. 177, pp. 522–527, Jan. 2020, doi: 10.1016/j.procs.2020.10.072.

[12] F. Khennou, Y. I. Khamlichi, and N. E. H. Chaoui, "Improving the Use of Big Data Analytics within Electronic Health Records: A Case Study based OpenEHR," Procedia Computer Science, vol. 127, pp. 60–68, Jan. 2018, doi: 10.1016/j.procs.2018.01.098.

[13] B. Singhal, G. Dhameja, and P. S. Panda, "Introduction to blockchain," in beginning blockchain, Springer, 2018, pp. 1–29.

[14] T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, and B. Amaba, "Blockchain technology innovations," in 2017 IEEE technology & engineering management conference (TEMSCON), 2017, pp. 137–141.

[15] M. Risius and K. Spohrer, "A Blockchain Research Framework," Business & Information Systems Engineering, vol. 59, no. 6, pp. 385–409, Dec. 2017, doi: 10.1007/s12599-017-0506-0.

[16] R. Beck and C. Müller-Bloch, "Blockchain as radical innovation: a framework for engaging with distributed ledgers as incumbent organization," 2017.

[17] I.-C. Lin and T.-C. Liao, "A survey of blockchain security issues and challenges.," Int. J. Netw. Secur., vol. 19, no. 5, pp. 653–659, 2017.

[18] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, "Secure and trustable electronic medical records sharing using blockchain," in AMIA annual symposium proceedings, 2017, vol. 2017, p. 650.

[19] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in 2017 IEEE International Congress on Big Data (BigData Congress), Jun. 2017, pp. 557–564. doi: 10.1109/BigDataCongress.2017.85.

[20] T. Dinh, R. Liu, M. Zhang, G. Chen, B. Ooi, and J. Wang, "Untangling Blockchain: A Data Processing View of Blockchain Systems," IEEE Transactions on Knowledge & Data Engineering, vol. 30, no. 07, pp. 1366–1385, Jul. 2018, doi: 10.1109/TKDE.2017.2781227.

[21] C. Cachin, "Architecture of the hyperledger blockchain fabric," in Workshop on distributed cryptocurrencies and consensus ledgers, 2016, vol. 310, no. 4, pp. 1–4.

[22] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of Trust: A decentralized blockchain-based authentication system for IoT," Computers & Security, vol. 78, pp. 126–142, 2018.