# A Comprehensive Blockchain-Based Architecture for Healthcare Systems

José Victor Marques dos Reis Melo, Inaldo Capistrano Costa[a], Juliana de Melo Bezerra[b]
and Celso Massaki Hirata[c]

*Department of Computing Science, Instituto Tecnológico de Aeronáutica (ITA), São José dos Campos, Brazil*

Keywords: Blockchain, Healthcare Systems, Software Architecture, Smart Contract, Medical Records.

Abstract: Blockchain technology has emerged as a versatile solution with wide-ranging applications across various industries, including healthcare. The increasing number of breaches in medical records in health systems highlights the imperative for innovative solutions. This paper delves into the potential of blockchain to improve information management in healthcare systems, considering data privacy, cybersecurity, and reliability concerns. We propose a blockchain-based architecture that takes into account key entities of healthcare systems, such as patients, physicians, diagnostic centers, and pharmacies, and facilitates their transactions through the use of blockchain technology. Through comprehensive sequence diagrams, we illustrate the orchestrated interactions among selected entities. The paper presents a proof of concept implementation, providing details on application development, smart contract specifications facilitating seamless information sharing, and the tests conducted. The implementation of the blockchain-based architecture and sequence diagrams was successfully tested. We conclude that the proposed architecture enables the improvement of the data privacy of entities, the cybersecurity of data sharing among diverse entities, and the reliability of transactions within healthcare systems.

## 1 INTRODUCTION

From the evolution of enabling technologies for various industries over the years (Mubarok, 2020), blockchain has emerged as a versatile technique with wide-ranging applications across different sectors (Javaid et al., 2021), including the healthcare domain, educational services, logistics and transport, and government domain. The focus of blockchain technology has been on fostering innovation within these domains.

Nowadays, healthcare systems face various challenges, particularly addressing concerns related to cybersecurity, data privacy, and reliability. The escalating number of breaches in medical records over the years (HIIPA Journal, 2021) underscores the imperative for health organizations to address these concerns with heightened responsibility.

Numerous scandals have unfolded involving the leakage of healthcare data. In 2018, there was a personal data breach affecting 1.5 million patients in Singapore (Davis, 2019b). In 2021, patient data from multiple providers was illicitly obtained and subsequently leaked on the data repository GitHub (Davis, 2021). Notably, only a small percentage of healthcare data breaches compromise sensitive medical data, such as diagnoses, while the majority (almost 70%) exposes patients to the risk of identity theft and fraud by hackers (Davis, 2019a).

The issue of privacy becomes increasingly relevant, given the growing market demand for access and sharing of personal data (Pauletto, 2021). This often occurs without the data owner having full control over their information, as the mechanisms for data sharing and handling are currently not transparent. Consequently, data subjects frequently find themselves in a vulnerable situation.

The concern for data protection has been heightened in recent years with the enactment of laws that restrict the use and sharing of data by organizations, exemplified by the General Data Protection Regulation (GDPR) in European countries and the General Personal Data Protection Law (LGPD) in Brazil. These laws grant greater autonomy and control to the data owner, imposing sanctions for inappropriate use and sharing by organizations. Despite the existence of such laws, many organizations disregard these measures (Magalhaes and Oliveira, 2021).

[a] https://orcid.org/0000-0002-0141-0736
[b] https://orcid.org/0000-0003-4456-8565
[c] https://orcid.org/0000-0002-9746-7605

Melo, J., Costa, I., Bezerra, J. and Hirata, C.
A Comprehensive Blockchain-Based Architecture for Healthcare Systems.
DOI: 10.5220/0012616400003690

In *Proceedings of the 26th International Conference on Enterprise Information Systems (ICEIS 2024) - Volume 1*, pages 250-257
ISBN: 978-989-758-692-7; ISSN: 2184-4992

Moreover, there are challenges in the relationships among the various entities involved in healthcare. With numerous entities participating and limited data sharing among them or their respective organizations, challenges arise, such as facilitating the efficient and secure collection of a patient's medical data by other healthcare entities or enhancing the communication of data between physicians and patients, as discussed in the article (Shen et al., 2019). Aligning the need for data sharing between different healthcare entities with patients' demands for data protection is a notable challenge.

We propose a blockchain-based architecture that orchestrates interactions among the key entities in healthcare systems. We delineate these interactions through sequence diagrams, elucidating the role of blockchain. The fundamental idea is to ensure the cybersecurity and data privacy of the patient's medical data while simultaneously guaranteeing authorized entities access to records. An additional benefit of integrating the patient's medical history into the blockchain is to ensure that physicians can access more comprehensive data, thereby contributing to a detailed and reliable diagnosis. Subsequently, we develop a proof of concept by implementing smart contracts to manage medical records.

The paper is organized as follows. Section 2 provides the background of the work, including an exploration of the main concepts related to the theme and a literature review. Section 3 delineates our proposal, featuring the general architecture with entities and interactions involved in managing medical records. Section 4 introduces a proof of concept, detailing the technologies utilized in developing the application, specifications of the smart contract, and an overview of the conducted tests. In the final section, we conclude and indicate future work.

## 2 BACKGROUND

Blockchain is defined as a decentralized and distributed digital ledger, serving to facilitate record management and traceability (Javaid et al., 2021). Its characteristic of decentralization is realized through a peer-to-peer (P2P) network, where each node possesses a copy of the blockchain, ensuring heightened security through the consensus algorithm. An advantageous feature of blockchain is the elimination of intermediaries, as it allows direct interaction with data without the need for intermediaries (Onik et al., 2019).

The chain structure is essentially a linked list of blocks, where each block includes the hash of the current block, the hash of the previous block, and the data field. Tampering with a block would necessitate changing the hash values of subsequent blocks and gaining control of at least 50% of the network to effect this alteration. Given the computational expense involved, this process is deemed unfeasible, contributing to the characterization of blockchain as a mechanism that stores information in an immutable way (Ali et al., 2019).

Smart contracts are programs that execute on the blockchain and are uniquely identified. These contracts encompass key properties, including functions and state variables. Additionally, these functions are activated by specific input logic and execute when transactions are requested. Programmers have the flexibility to write smart contracts in various languages, with the choice contingent on the programmer's preferences and the platform selected for implementing these contracts. For instance, on the Ethereum platform, the Solidity language is commonly employed (Ali et al., 2019).

The application of blockchain in the healthcare sector has gained significant attention in academic circles, particularly driven by concerns about cybersecurity, reliability, and data privacy scandals. These issues, coupled with the challenge of enhancing interoperability of medical data across different healthcare entities, have spurred research in this area.

A decentralized approach (Madine et al., 2020) is proposed to give patients control over their data, involving entities such as insurance companies, patients, physicians, regulatory agencies, and hospitals. The regulatory agency oversees patient and physician records, with authorization and deauthorization schemes between physicians and patients. We extend the focus of the approach (Madine et al., 2020) to include greater data interoperability and involve additional entities beyond the patient-physician relationship.

Inspired by the work in (Carniel et al., 2021), which describes a reliable approach to managing population vaccination data on a blockchain, our proposal delves into entity details and relationships, emphasizing a broad consideration of patients' medical data. In the work of (Shen et al., 2019), a decentralized patient-oriented network connects patients, physicians, and healthcare providers to securely and privately share data using blockchain technology. Our proposal builds upon their work by incorporating new entities, storing a wider variety of information, and seeking to streamline the implementation process with the use of smart contracts.

The work in (Shahnaz et al., 2019) discusses applying blockchain technology to Electronic Health

Record (EHR) systems, focusing on an access control schema for improved security. The system involves only the administrator and user entities, with the administrator defining user roles (physician or patient) and users making requests to validate themselves before any execution. In our work, we explore interactions among various healthcare entities and detail data exchange using blockchain to support a comprehensive solution.

In what follows, we present our proposal of the blockchain-based architecture.

## 3 A BLOCKCHAIN-BASED ARCHITECTURE FOR HEALTHCARE SYSTEMS

The proposal aims to harness the capabilities of blockchain technology, specifically through smart contracts, to create an innovative medical records management application. The utilization of blockchain offers a robust solution to meet the stringent requirements of cybersecurity, reliability, and data privacy. Moreover, the integration of smart contracts within the framework enhances the interoperability of patient medical data, facilitating seamless data sharing among various stakeholders in the healthcare systems.

In Figure 1, we present a typical diagram showcasing the roles of each class of entities and their interactions within the blockchain in Brazil's healthcare system. The responsibilities of each class of entity are described below.

- **Patients.** They are responsible for managing access, authorizing necessary entities, and verifying records.
- **Physicians.** They are responsible for updating patient records and checking patient histories.
- **Regulators.** They manage and monitor the blockchain, by updating (registration, suspension, reactivation) entities and monitoring their transactions.
- **Research Institutes.** They access data from the blockchain for research purposes.
- **Pharmacies.** They are responsible for checking entity records and registering the drug acquisitions to patients.
- **Diagnostic Centers.** They check the records of patients to perform exams and store the results in the blockchain.
- **Insurance Companies.** They are responsible for checking the data and authorizing the release of tests.
- **Hospital Staff.** They are responsible for authorizing a medical appointment and assisting physicians.

For a more detailed description of the interactions among classes, we have selected five representative classes: Patients, Physicians, Regulators, Pharmacies, and Diagnostic Centers. The selection of Patients, Physicians, and Regulators is justified by the significance of Physician-Patient interactions during appointments and the Regulator's role in creating these entities and assigning initial credentials. Additionally, the choice of Pharmacies and Diagnostic Centers aims to showcase common flows and activities in the healthcare system.

To describe the interactions among the selected classes of entities in different scenarios, sequence diagrams are employed. Each sequence diagram outlines a flow of interactions between entities. In the sequence diagrams, we describe the interactions between single entities. For clarity, we employ "patient" to refer to a single entity within the "Patients" class. Similarly, this naming convention is applied to other single entities and classes.

In Figure 2, the regulator entity, often represented by the Government, assumes the responsibility of registering new entities to the system. During the registration process, an identifier and a temporary password are assigned for the entity under analysis. Subsequently, this information is stored in the blockchain. Furthermore, the regulator is granted the authorization to access patients' medical records for management and monitoring purposes.

In Figure 3, the interactions between a patient and a physician during a medical consultation become explicit through the sequence diagram. Initially, both the physician and the patient possess known identifiers from a previous step. Consequently, the patient can authorize access to the physician using the physician's identifier. Once authorized by the patient, the physician can review the patient's records and, based on clinical analysis, create a new record on the blockchain. Consequently, the patient can access the new record at any time. Records can be associated with a prescription for necessary medication or the requisition of additional medical exams.

In Figure 4, the sequence diagram between the patient and the diagnostic center is shown. Initially, the patient must authorize the diagnostic center based on the available identifier. Subsequently, the diagnostic center reviews the patient's medical records to validate the examination request specified by the patient.

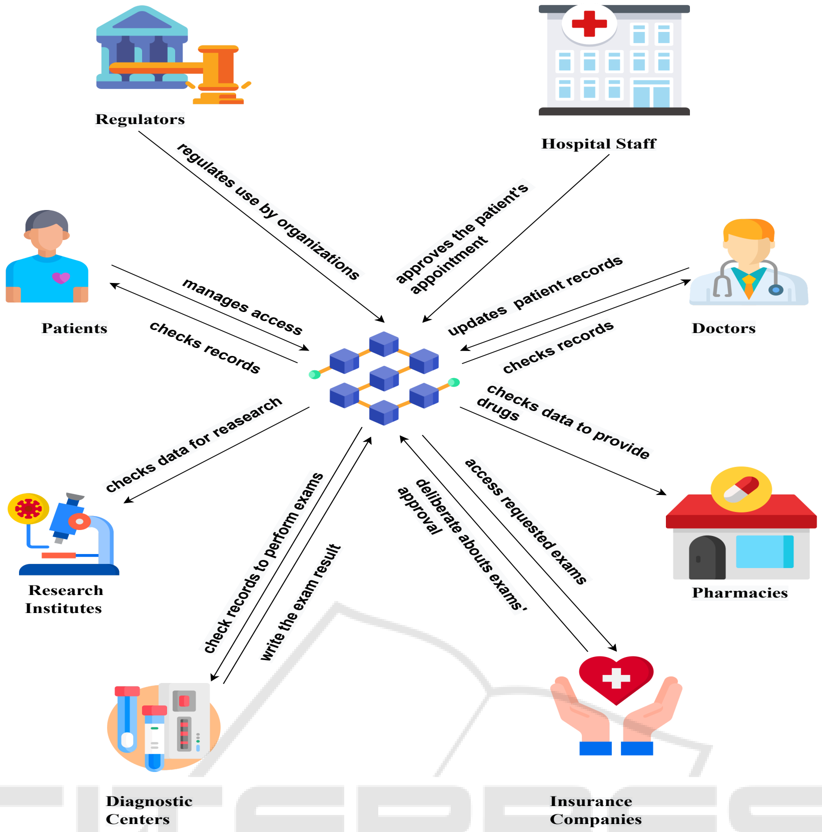

Figure 1: Blockchain-based architecture for a healthcare system.

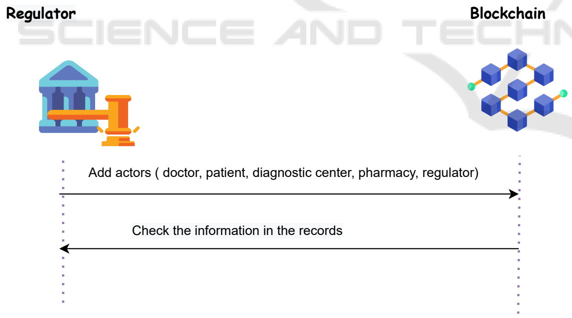
Regulator
Blockchain
Add actors ( doctor, patient, diagnostic center, pharmacy, regulator)
Check the information in the records

Figure 2: Sequence diagram of regulation.

Upon confirming the request's existence, the diagnostic center authorizes the examination. Following the completion of the process, the diagnostic center enters the examination result into the patient's record information. Finally, the patient can review the examination results at any instant.

In Figure 5, the sequence diagram between the patient and the pharmacy is outlined. Initially, the patient must authorize the pharmacy entity to access their records, considering that the patient knows the pharmacy's identifier. Subsequently, the pharmacy reviews the patient's records to verify the availability of the requested medicine. If the prescribed medicine for the patient is available, the pharmacy can effect the acquisition and record it. This recording serves to prevent the patient from acquiring any medication twice if the medication is under control.

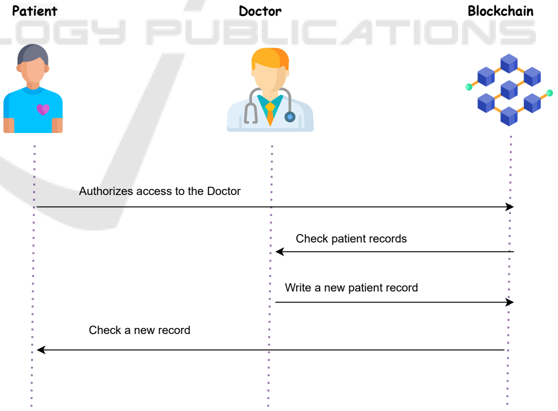

Figure 3: Sequence diagram of medical consultation.

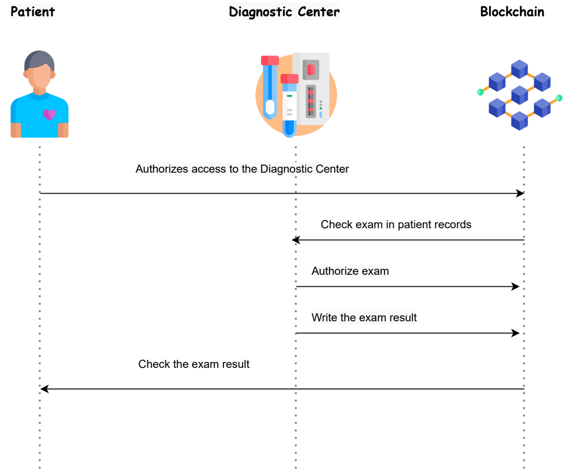

Figure 4: Sequence diagram of exam.

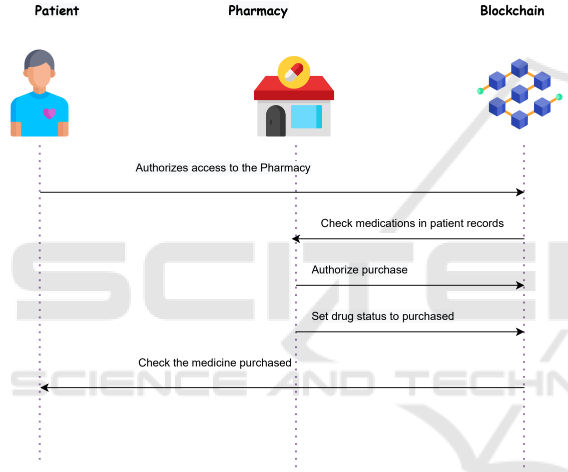
Patient
Pharmacy
Blockchain
Authorizes access to the Pharmacy
Check medications in patient records
Authorize purchase
Set drug status to purchased
Check the medicine purchased

Figure 5: Sequence diagram of medicine acquisition.

## 4 A PROOF OF CONCEPT

In this section, we present a proof of concept for the proposed blockchain-based architecture designed for healthcare management. By illustrating interactions among different entities in the healthcare system, the proof of concept showcases how the proposed architecture enhances patient-centric care, facilitates data sharing among entities, and ensures the integrity and privacy of medical records.

Figure 6 demonstrates the integration between some tools in the implementation of the proof of concept. Truffle is used to compile and deploy the smart contract (written in the Solidity language). We connect to the Ethereum blockchain (Goerli testnet) via the Infura API. There is the bidirectional connection of the DApp with the blockchain network using Infura. This connection incorporates a set of useful tools on the front-end, such as the Browser (in this case represented by Chrome), Metamask, React App, and Web3. The code is available at (Marques, 2022).

To select the front-end tools, we opted for ReactJS for creating the application's user interface, Web3 for interacting with Ethereum nodes, and Heroku for deploying the platform on the web. The decision to use the ReactJS library stems from its ability to facilitate extensive component reuse in the code (Technostacks, 2023). The adoption of Web3 is driven by its status as a JavaScript API that interfaces with blockchain nodes. Lastly, the choice of Heroku is motivated by its standing as a cloud application platform, ensuring straightforward and rapid hosting of projects on the web, along with simplified scalability in any application.

For the blockchain technology, Ethereum is selected as the platform for contract development. Despite being hosted on a public network, access control is ensured through patient login, authorization mechanisms, and regulatory oversight, safeguarding the integrity of blockchain information. Opting for Ethereum on a public network enhances public acceptance compared to a private network. The Goerli test network was chosen for the developed project due to its accessibility and cost-free availability of faucets for testing, coupled with integration with Infura. However, it is important to note that this network's drawback is its usage by many applications, which may result in slower transactions.

The use of Infura is imperative for DApps (Decentralized Applications). In essence, Infura is a blockchain infrastructure-as-a-service (IaaS) provider that offers developers simplified access to blockchain networks. It acts as a middleware service, abstracting the complexities associated with running and maintaining a node on a blockchain network. Infura provides a convenient and reliable way for developers to interact with blockchain networks without the need to manage their nodes (Macedo, 2020).

Truffle is selected due to its status as an Ethereum blockchain development environment for DApps. It provides an all-encompassing solution with built-in support for building, testing, deploying, and binding smart contracts. Additionally, it offers an interactive console for communication with these contracts and network management for both public and private networks.In terms of complementary tools, Metamask (as a digital wallet) and Git (as code versioning system) were utilized.

In a way to organize the smart contract, we divided it into the following classes: structures, mappings, counters, constructors, and functions. Below,

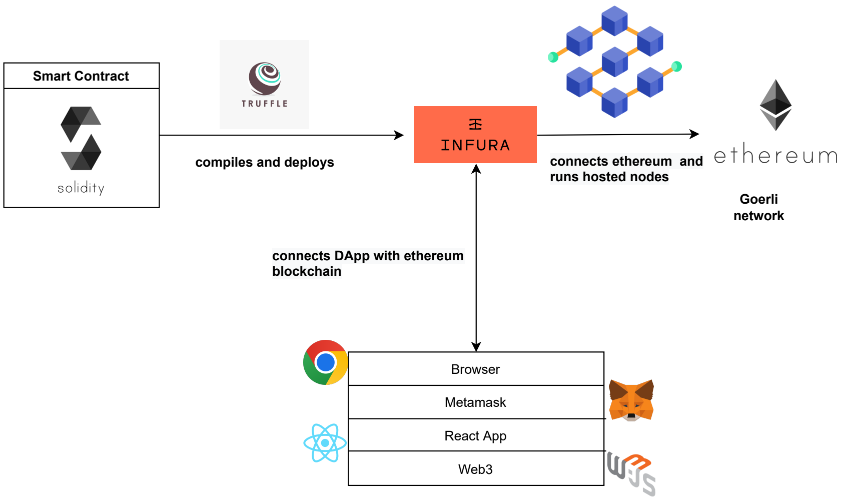

Figure 6: Technological tools used in the proof of concept.

each of these classes and their applications are presented.

- The **structures** contain the declaration of entities that are members of the classes of entities (Patients, Physicians, Regulators, Pharmacies, Diagnostic Centers), as well as entities that support the interactions. These latter entities are members of the classes Diagnoses, Exams, and Medicines.
- Regarding the **mappings**, there exists a key-value relationship to form vectors and matrices for the aforementioned structures, as well as vectors related to access authorizations for the Medical, Pharmacy, and Diagnostic Center entities.
- The **counters** are utilized to define numbers of elements of entity classes, making this information public so that the limits to the mappings are known by the functions.
- The use of **constructors** defines the initial entities of the platform.
- The use of **functions** is what triggers transactions and writes some information to the blockchain. These functions play an essential role in the overall functionality of the smart contract.

To exemplify how the contract is specified in code, we can consider a specific scenario of the interaction between a patient and a physician during the consultation (as presented in Figure 3). As structures, we have Diagnosis, Patient, and Physician. Firstly, the Diagnosis structure includes the 'diagnosis code' field, which will be inserted according to the value presented in the ICD table (International Classification of Diseases) (Harrison et al., 2021); the 'exam code' field, based on the TUSS table (Unified Terminology of Supplementary Health) for the classification of procedures in Brazil (ANS, 2019); and the prescriptions for medicines using the 'medicine code', based on the medication number present in the open data made available by the Brazilian government (ANVISA, 2020). The Diagnosis structure also includes the time of consultation, the physician's ID, the physician's observation, and the prescriptions for exams.

In the Patient structure, the patient's ID and password fields are used in the patient's login; the number-of-appointments field is used to control the number of consultations that the patient had; the token field is used to perform user verification more securely when entering the platform; and the name field is used to describe the patient. As for the Physician structure, it follows the same pattern as the Patient structure but adds the fields of CRM (physician's certification in the regional council of medicine) and the physician's specialty.

Considering the scenario of consultation in Figure 3, the mappings of the smart contract contain information in the form of a key-value, for instance, a list of physicians, a list of patients, a list of authorized physicians by patients, and list of diagnoses by patients. Regarding the counters in the smart contract, we defined the following: number of patients, number of physicians, number of regulators, quantity of pharmacies, and quantity of diagnosis centers. We add only one constructor in this case, to create a regulator, which in turn allows the creation of other entities for test purposes. Two functions are specified to manage the interactions between patients and physicians: the authorization function of any entity (physician, pharmacy, or diagnosis center) and the code about patient consultation (which allows the creation of new medical records for the patient).

In a way to test the developed application, we analyze the flow of interactions through a real-life scenario. In this scenario, a patient is unwell and seeks a physician for appropriate treatment. The idea is to outline a comprehensive sequence of interactions as the patient engages with the medical, pharmacy, and diagnostic center entities while utilizing the developed platform to manage his records.

Here is a breakdown of the key steps in the scenario. The patient initiates the platform login and decides whether to authorize the physician (using the screen in Figure 7). If the authorization is granted, the physician accesses the patient's records and adds a new entry (using the screen in Figure 8). If not, the interaction is terminated.

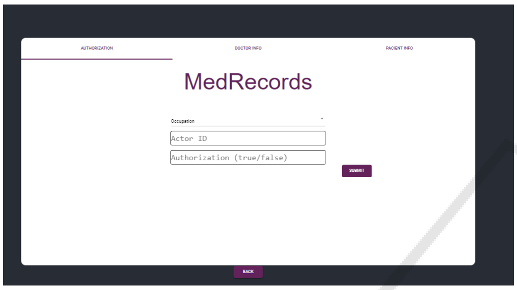

Figure 7: Patient authorization screen.

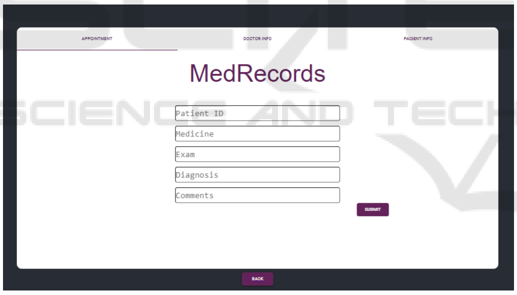

Figure 8: Screen for the physician to add appointment information.

The patient checks whether the physician has prescribed any medication. If so, the patient proceeds to request the acquisition of the prescribed drug from a pharmacy. Authorization must be granted to the pharmacy entity for this transaction to proceed; otherwise, the interaction ends. If authorization is granted, a pharmacy staff member reviews the records and approves the acquisition in the system, concluding the interaction between these entities.

The patient checks whether the physician has prescribed any diagnostic tests. If there are test requests, the patient contacts the diagnostic center to schedule the examination. To initiate this process, the patient must authorize the diagnostic center to access their records. Once authorized, the diagnostic center reviews the requested test and conducts the examination. Finally, the diagnostic center records the test results in the patient's medical records.

Upon completing these steps, the interactions within this scenario terminate. It is worth noting that this sequence of procedures can be repeated for subsequent appointments. We tested all these sequence diagrams with the implementation of our proof of concept. All the tests were executed with success.

## 5 CONCLUSIONS

The proposed architecture consists of entities and their interactions involved in the healthcare system using the blockchain technology. Each entity, including patients, healthcare providers, regulators, and others, plays an essential role in contributing to a comprehensive and collaborative healthcare system. The architecture serves as a blueprint for understanding the flow of information, transactions, and permissions within the application. It highlights the seamless interaction between entities and the blockchain. Blockchain, with proper controls, ensures that entity data is not only secure but also accessible and shareable.

The decentralized and immutable nature of the blockchain ensures a tamper-resistant environment, instilling trust in the integrity of patient data. The cornerstone of our application lies in the implementation of smart contracts. These self-executing contracts operate on the blockchain, fostering a secure and automated environment. Notably, the smart contract framework enhances the interoperability of patient medical data, enabling efficient and secure data sharing among diverse entities in healthcare systems.

Through the proof of concept implementation, we aimed to validate the viability and effectiveness of the proposed solution. The proof of concept provided insights into the seamless coordination between patients, physicians, regulatory entities, pharmacies, diagnostic centers, and other stakeholders within the blockchain-based framework. It is important to note that the patient is the rightful owner of their data and has the authority to grant access to specific entities for their transactions. This feature aligns with the principles of data protection outlined in GDPR and LGPD.

Our proposal contributes to enhancing the reliability of the physician's diagnosis process by providing access to the complete patient history, including medications and exam results. Furthermore, it ensures a more dependable medication control system, allowing pharmacies to prevent irregular acquisitions. Regulatory entities benefit from broad access to the medical data of the population, empowering the formulation of comprehensive public health policies.

As part of our future work, we aim to integrate additional entities outlined in our proposal, for instance, the health research institutes, pharmaceutical and biotechnology companies, and health insurance providers. The sequence diagrams could be enhanced with supplementary interactions to better reflect the complexity of the problem at hand. Conducting tests with real users is also crucial. Another issue that deserves some care is the application's usability, mainly for the patients, since they may have health restrictions to interact with the system.

On the implementation front, considering the costs associated with Ethereum transactions, we need to explore the possibility of replacing it with non-monetary blockchain platforms. The scalability of blockchain solutions refers to the system's ability to handle a growing amount of work, transactions, or users effectively without compromising performance. Scalability is a critical consideration for blockchain networks. We view it as a relevant concern that merits further investigation.

This work signifies an endeavor to harness the power of blockchain and smart contracts for the enhancement of healthcare systems, tackling challenges related to cybersecurity, reliability, and data privacy. Moving ahead, the proposed architecture has the potential to elevate patient care, streamline healthcare processes, and promote a more interconnected and collaborative healthcare landscape.

## REFERENCES

Ali, A., Rahouti, M., Latif, S., Kanhere, S., Singh, J., Janjua, U., Mian, A. N., Qadir, J., Crowcroft, J., et al. (2019). Blockchain and the future of the internet: A comprehensive review. *arXiv preprint arXiv:1904.00733*.

ANS (2019). Terminologia unificada da saude suplementar. https://dados.gov.br/dados/conjuntos-dados/terminologia-unificada-da-saude-suplementar-tuss Accessed on 2023-12-29. *In Portuguese*.

ANVISA (2020). Medicamentos registrados no brasil. https://dados.gov.br/dataset/medicamentos-registrados-no-brasil Accessed on 2023-12-29. *In Portuguese*.

Carniel, A., Leme, G., Bezerra, J., and Hirata, C. (2021). A blockchain approach to support vaccination process in a country. In *Proceedings of the 23rd International Conference on Enterprise Information Systems*, pages 343–350. SciTePress.

Davis, J. (2019a). 70% of data involved in healthcare breaches increases risk of fraud. https://healthitsecurity.com/news/70-of-data-involved-in-healthcare-breaches-increases-risk-of-fraud. Accessed on 2023-12-29.

Davis, J. (2019b). Massive singhealth data breach caused by lack of basic security. https://healthitsecurity.com/news/massive-singhealth-data-breach-caused-by-lack-of-basic-security. Accessed on 2023-12-29.

Davis, J. (2021). Patient data from multiple providers leaked in third-party github incident. https://healthitsecurity.com/news/patient-data-from-multiple-providers-leaked-in-third-party-github-incident. Accessed on 2023-12-29.

Harrison, J. E., Weber, S., Jakob, R., and Chute, C. G. (2021). Icd-11: an international classification of diseases for the twenty-first century. *BMC medical informatics and decision making*, 21(6):1–10.

HIIPA Journal (2021). Healthcare data breach statistics. https://www.hipaajournal.com/healthcare-data-breach-statistics/ Accessed on 2023-12-29.

Javaid, M., Haleem, A., Singh, R. P., Khan, S., and Suman, R. (2021). Blockchain technology applications for industry 4.0: A literature-based review. *Blockchain: Research and Applications*, page 100027.

Macedo, R. (2020). Deploy dapp - end to end. https://medium.com/@rcbm539/deploy-dapp-end-to-end-a5aae2f6f2a6/ Accessed on 2023-12-29. *In Portuguese*.

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

Magalhaes, R. A. and Oliveira, E. C. R. N. (2021). O direito À privacidade na era digital. *Revista Jurídica da FA7*, 18(1):55–70.

Marques, J. V. (2022). Dapp truffle github repository. https://github.com/JoseVictorMarques/dapp-truffle. Accessed on 2023-12-29.

Mubarok, K. (2020). Redefining industry 4.0 and its enabling technologies. *Journal of Physics: Conference Series*, 1569:032025.

Onik, M. M. H., Kim, C.-S., Lee, N.-Y., and Yang, J. (2019). Privacy-aware blockchain for personal data sharing and tracking. *Open Computer Science*, 9(1):80–91.

Pauletto, C. (2021). Options towards a global standard for the protection of individuals with regard to the processing of personal data. *Computer Law & Security Review*, 40:105433.

Shahnaz, A., Qamar, U., and Khalid, A. (2019). Using blockchain for electronic health records. *IEEE Access*, 7:147782–147795.

Shen, B., Guo, J., and Yang, Y. (2019). Medchain: Efficient healthcare data sharing via blockchain. *Applied Sciences*, 9(6).

Technostacks (2023). 10 best frontend frameworks. https://technostacks.com/blog/best-frontend-frameworks/ Accessed on 2023-12-29.