applied sciences

MDPI

Article

Beneficiary Contracts on a Lightweight Blockchain Architecture Using Smart Contracts: A Smart Healthcare System for Medical Records

Arturo I. Mendoza Arvizo [1], Liliana Avelar Sosa [2,*], Jorge Luis García Alcaraz [2] and Oliverio Cruz-Mejía [3]

[1] Doctorate Program in Advanced Engineering Sciences, Institute of Engineering and Technology, Universidad Autónoma de Ciudad Juárez, Ciudad Juárez 32310, Chihuahua, Mexico; arturo.arvizo@uacj.mx

[2] Department of Industrial Engineering and Manufacturing, Institute of Engineering and Technology, Universidad Autónoma de Ciudad Juárez, Ciudad Juárez 32310, Chihuahua, Mexico; jorge.garcia@uacj.mx

[3] Department of Industrial Engineering, Universidad Nacional Autónoma de Mexico, FES Aragon, Mexico City 57171, Estado de México, Mexico

[*] Correspondence: liliana.avelar@uacj.mx

Abstract: The effective management of medical records is essential in the ordinary and emergency operations of healthcare providers. This work uses blockchain to develop a smart contract algorithm for users of a medical record platform. This algorithm provides immutable execution and addresses authentication and reliability issues to control access to healthcare platforms. An executable distributed code is used to build the smart contract algorithm. In the proposed algorithm, management operations of the clinical history are carried out and integrated in an automated way in a distributed environment. Solidity is the programming language used to create the algorithm for a private and permissioned architecture with a proposed consensus algorithm requiring significantly less computational power using a 22% faster hash function.

Keywords: health systems; medical records; blockchain applications; healthcare supply chain

check for updates

Citation: Mendoza Arvizo, A.I.; Avelar Sosa, L.; García Alcaraz, J.L.; Cruz-Mejía, O. Beneficiary Contracts on a Lightweight Blockchain Architecture Using Smart Contracts: A Smart Healthcare System for Medical Records. *Appl. Sci.* **2023**, *13*, 6694. https://doi.org/10.3390/app13116694

Academic Editor: Gianluca Lax

Received: 27 April 2023
Revised: 24 May 2023
Accepted: 26 May 2023
Published: 31 May 2023

Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Hospital facilities provide valuable information for healthcare staff and patients. Such facilities preserve patient rights and accurate medical information that must be collected, kept, and used during diagnosis and treatment operations [1]. However, in some cases, this information is not kept in a secure system and, unfortunately, the number and severity of cyber attacks on medical record files are increasing. As safe and trustworthy health data transfer does not have systematic infrastructure support, much of this data sharing is still conducted manually or by fax or mail. This limited information resource affects sensitivity and secrecy, causing a delay in the provision of medical care [2]. Between 2009 and 2021, the United States Department of Health and Human Services reported more than 4419 cases of medical record breaches resulting in the exposure of 314,063,189 medical records [3–5]. Access control is an essential component of information systems and establishes security by verifying whether a user has the necessary rights to access the services they request. Current access control schemes face a lack of privacy, validation, and operation by third-party entities. One technological tool that can benefit hospital resource management is the emerging blockchain technology. Blockchains offer consistency and decentralization that improve data security and integrity and alter entire sectors [6]. Since blockchains are secure, unchangeable, and decentralized, they can provide adequate data storage and access management. Blockchain technology can be a valuable tool for creating a smart healthcare network [7]. Owing to the properties of this technology, it can safeguard patient privacy and maintain and manage access to huge quantities of anonymous health data, thus allowing new studies and insights [8]. One of the most well-known and often-used aspects of blockchain-based systems is the usage of smart contracts [9]. Smart contracts are a means to make the blockchain programmable in the context of blockchain and cryptocurrency.

1.1. Smart Contracts

Smart contracts can define, enforce, and manage access permission. According to Buterin [9], a smart contract is a piece of machine-readable code that simplifies, confirms, and enforces the negotiation or performance of a contract. Szabo [10] introduced smart contracts as "a computer-based transaction protocol that executes the terms of a contract to satisfy common contractual conditions, minimizing exceptions without the need for trusted intermediaries." Traditionally, contracts are external to the system they regulate and are prescriptive rather than descriptive. They do not define what is possible but what is permitted as well as the consequences of breaching the prescriptions. By contrast, smart contracts define how entities can transact and execute them automatically. Morabito [11] described how organizations can leverage smart contracts to automate transactions and reduce operating costs. Smart contracts are an efficient way of gaining a competitive advantage. Swan and Magazine [12] proposed a solution to execute smart contracts under optimal time conditions. This condition is directly implemented in the code of the contract for automatic execution. Peer-to-peer (P2P) cooperation can be governed by well-defined protocols that smart contracts add to blockchains [13]. Generally, the main goal is to use the blockchain to digitally enable and enforce verifiable contract conversations between two participating parties [9].

1.2. Blockchain in the Health Sector

Hathaliya and Tanwar [14] stated that data integrity and the privacy of medical records information are two of the primary issues facing the healthcare industry worldwide and are essential factors in considering blockchain as a feasible technology. Gordon and Catalini [15] determined that data exchange is the main reason blockchain should be used in healthcare because of the security and immutability this technology provides. Among the best-known applications of blockchain architectures implemented in the medical sector is the Estonian government's Guardtime System. Guardtime is the first blockchain-based healthcare system at the national level that creates a framework for validating patient identities by employing smart cards that link different government institutions with the healthcare sector. This method creates links or bridges between entities, thus ensuring the flow of information, but its scope needs to reach the operational bases of the system [16]. Another well-known application is MedRec, a project developed by MIT Media Lab and Beth Israel Deaconess Medical Center. This public blockchain network type uses pointers and creates bridges between hospital service providers, patients, and hospitals. Its weakness is security, as it assumes that its administrators ensure the integrity of the databases of participating entities [17]. Peterson et al. [18] developed the Mayo application, which strengthens semantic and syntactic interoperability by pushing nodes to produce proof to reach network consensus that the data referenced by a transaction can be meaningfully interpreted. It develops a consensus called interoperability. This application is designed for clinical service providers and presents difficulties in identifying patients in institutional nodes.

The present work proposes a secure, private, and immutable medical record architecture using blockchain-based smart contracts that provide a secure execution and storage environment for smart contracts. The proposed algorithm has distribution, storage, consensus, and encryption technology. It connects patients and healthcare personnel to medical records, allowing them to consult with a high degree of privacy. The primary contributions of the algorithm are as follows:

1. We provide a dynamic, distributed access control system for effective, reliable, and authoritative data sharing for users in a healthcare system. The registration contract covers the entire medical system scenario by using smart contracts for user authentication. It comprises three entities: patients, hospitals, and some current regulatory frameworks.

2. The consensus protocols allow transactions to be made by utilizing blockchain without an outside party. To avoid congestion and reduce overhead in the blockchain network, we modify the original consensus protocol of the blockchain, namely, proof of work (PoW). We choose to formalize an alternative to using a lightweight PoW algorithm. This algorithm consumes low energy when used in the medical history. The design goal is summarized as compact, fast, and optimized for lightweight applications.

The remaining sections of this document are structured as follows. In Section 2, we present related works. Next, in Section 3, we discuss the materials and methods used in the study, the recommended structure, and the implementation. In Section 4 we talk about the performance and outcomes, respectively. The paper is concluded in Section 5.

2. Related Works

We discuss recent academic research on smart contracts and medical record management and provide a critical overview of the current initiatives. A blockchain-based system for managing vaccination registration, storage, and delivery was developed by Rotbi et al. [19]. This method includes the registration of citizens, immunization, and vaccination control. Pham et al. [20] presented a blockchain-based medical platform that employs smart contracts to manage patient records and equipment that are useful or available for use in therapy. A prototype that uses smart contracts to control access rights and data exchange between patients and doctors was defined by Dubovitskaya et al. [21]. In the prototype, there are three sorts of schemas in smart contracts:

1. This prototype system enables patients to actively communicate their data without relying simply on the data supplied by the healthcare facility where patient-defined permissions are located.
2. The location of all the data required to access files is kept outside the blockchain.
3. Patient-provided private information that is directly attached to the blockchain.

Khatoon [22] used blockchain technology based on smart contracts and showed how decentralization principles might be applied to massive data processing for auditability purposes. Dagher et al. [23] suggested six smart contracts as access constraints for exchanging medical records between healthcare providers. The first contract reads operations and registers the user. The second divides users into third parties, providers, and patients. The third defines the relationship between the users, while the fourth describes the characteristics of medical records. The fifth contract describes the rights of access to those documents, and the final one discusses encryption.

In their prototype for electronic medical records, Azaria et al. [17] implemented various smart contracts, such as: (1) registration contracts, which provide social security numbers, public signing keys, and patient names to be utilized in blockchain, as well as rules for identity formation and updating; (2) contracts between patients and healthcare providers which let patients alter their access to specific providers. Additionally, some contracts include data pointers that the providers may use.

Smart contracts used in the work of Xia et al. [24] share medical data with healthcare and research companies in the cloud. The three main uses of smart contracts are the encryption of medical reports, tracking actions concerning submitted data, and revoking access to violating data. Ahram et al. [25] developed smart contracts to guarantee that just one patient is registered at the initial visit to a hospital and the original version of their medical record is created. The second kind of smart contract ensures that a provider will update or transmit patient records. Smart contracts were utilized by Saravanan et al. [26] to allow doctors to access health information gathered by sensors. Medical records and access logs are included in the contracts. In order to guarantee the transparency and integrity of clinical trials and medical studies, Benchoufi et al. [27] suggested utilizing two contracts. Under these contracts, public institutions could track a study's development and progress and confirm its authenticity. Two contracts were suggested by Nugent et al. [28] as a way to increase the openness data from clinical studies. McFarlane et al. [29] focused on billing and providing emergency medical access.

3. Materials and Methods

The system architecture of the proposed scheme considers two main design objectives:

1. Privilege-based access: Information is distributed in a hierarchy according to user privileges. Data users with more privileges have access to more sensitive information than users with lesser privileges.
2. Data privacy: All parties are entirely safeguarded according to the type of user and the data for which they have privileges. Data users have the right to access the levels their data is located in and any levels below them concerning their own data.

3.1. Proposed Scheme

Throughout the procedure, a patient in a medical facility communicates with healthcare professionals. Healthcare workers may request access to patients' prior medical records in order to treat patients effectively. The same care unit may have produced these records, or they may have come from a separate location, such as the emergency room, lab, or pharmacy. Accessing such information ensures the quality of patient care and saves time and resources. However, it is essential to maintain patient privacy and only have access to and share this information with authorized personnel, where smart contracts are viewed as "black boxes" that consent to receiving transaction messages from outside and may carry out calculations based on such messages.

3.2. Identity Authentication

Blockchain-based identity authentication has the characteristics of decentralized authentication, where each node in the network possesses two keys: a private key used to decode the content and enable a node to identify the sender and a public key used to encrypt transactions. Encoding the original communication into one that cannot be deciphered as the original message is known as encryption. Decryption entails modifying the message as it was originally encoded.

The identity information of the network nodes is stored in the blockchain; therefore, it is complicated to manipulate, and the use of smart contracts to perform addition, deletion modification, and verification operations streamlines the process. In the health sector, in the medical record management process, the recommended identity assignments to the actors are:

1. User-beneficiary node: The primary function of the user is to check the data and request access. They can add authorized information and authorize other people to check their medical information.
2. User-physician node: The primary function of the physician user is to add, delete, modify, and check data, allowing physicians to add medical records to patients.
3. User administrator node: Manages accounts, passwords, and permissions of users participating in the network, password recovery, and links public and private keys.

The recommended identity assignment overview in a patient care unit and the medical record management process are shown in Figure 1.

3.3. Architecture of the System

This section discusses the privacy levels of medical records and the access permissions used to develop the proposed framework. The framework has three elements or modules, as seen in Figure 1. These modules would keep the system running when coupled. The following section also explains the access rights for specific entities or modules.

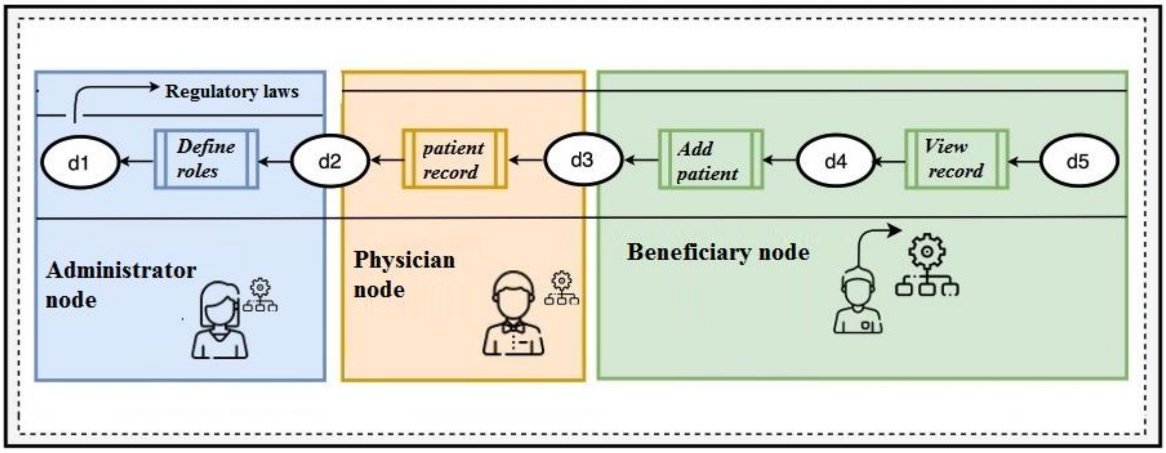

Figure 1. Identity assignments.

3.3.1. Levels of Privacy of Medical Records

We take into account the following factors based on access rights' degrees of security and data privacy:

- The citizen registry is only visible to governmental institutions, according to regulations.
- Medical records are only visible to administrative staff.
- Medical records are only visible to administrative and health personnel.
- Medical records are only visible to administrative staff, healthcare personnel, and patients or family members.

The access structure is based on privileges and divides the users into levels. An access policy is linked to each level. A set of stated rules and the attributes that abide by those rules are specified in an access policy. Data users who meet the requirements of an access policy and have the proper qualities are members of a particular level.

3.3.2. System Components

Some actors and entities were considered in the system's components, such as:

1. Patients/rightsholders: Patients who received treatment or required it out of necessity from a medical institution.
2. Health personnel: Access to the previous medical records of a visiting patient is necessary for the medical staff to provide better care. Each employee has a set of qualities (A) that can be used to divide them into categories of comparable traits and order them in a hierarchy.
3. Administrator.
4. A governmental body, public or private institution.
5. Family members (entitled).

3.3.3. Functions of Each Entity

- Access instance, government, public or private institution: Health service providers and managers within the Mexican data protection laws covering all medical record data.
- Patient: The patient visited the hospital for a medical check-up. He is a data user.
- Physician: The physician is responsible for generating the patients' medical records and extracting keywords for integration into the file. In this scheme, the physician is assumed to be honest and not transacting for illegal gain.
- Data user: The data user will use the information, for example, internal departments of the institution or patients' families who can obtain the relevant records as long as their attributes comply with the corresponding access policy.
- Blockchain mechanism: The blockchain mechanism is the backbone of the architecture and performs operations based on smart contracts.

3.3.4. System Modeling

Our design is centered on a blockchain with a proof-of-work consensus mechanism.

The problem was formalized according to Coperneec [30]. Under this scheme, the PoW can be interpreted as

$$H\Big(H(B^{prev}) \oplus R^{H}(B) \oplus timestamp(t) \oplus b \oplus nonce\Big) \leq target \tag{1}$$

where:

H is the hash function, which is a deterministic function that transforms data of arbitrary size into fixed sizes.
B^{prev} is the last accepted block in the blockchain.
t is the transaction time; $timestamp(\bullet)$ obtains the current time of the transaction.
R^{H} Merkle root of the transactions of the block to be mined.
nonce is a scalar, meaning "number used only once", which solves the proof-of-work.
b number expressing the degree of difficulty of the algorithm.

Furthermore, we contemplated the activities performed by health personnel users in a hospital center which, as a first step, we intend to log in to the platform. Then we ensured authenticity and requested authorization to upload, modify, or make any changes to the medical records. Modeling will help us structure the operation algorithms of the entities or users when entering the architecture.

3.3.5. Smart Contracts

The smart contract is a component of computer code that executes when users transmit transactions on the blockchain to carry out a specific activity [31,32]. Smart contracts are a contractual relationship between physicians and patient administration users. Actions or events that will result in specific conditions depending on the user's role or those agreed upon in the contract will be established. To model the interaction of miners in the framework, we first consider a process in which primary users, patients, doctors, and medical service providers establish a smart contract with a reward. The reward is considered a favorable remuneration or payment amount, depending on how the smart contract is established. Miners can use the reward to obtain medical resources, such as medicines or appointments with specialists on the blockchain platform.

3.3.6. Requirements for Smart Contracts

It should be noted that several requirements are necessary for a fully functioning system; therefore, the following requirements are necessary to create a secure medical record storage and exchange system to be considered in smart contracts.

- Requirement 1: Registration capabilities in compliance with current regulations.
- Requirement 2: Patients must have access to their registers.
- Requirement 3: Dependents must be able to request access to patients' records.
- Requirement 4: Records must be able to be uploaded based on access for healthcare providers.
- Requirement 5: Records must be accessible to providers and patients for download based on the access.
- Requirement 6: Each record that is uploaded must be encrypted.

3.4. Implementation

We outline the detailed algorithms which direct the execution of the proposed smart contracts. Smart contracts operate so that only "then" creates specific actions "if" particular conditions (coded in the smart code) are met [1].

Smart Contract Design

In this stage, the structure of the smart contracts algorithm was developed, where the activities performed by health personnel users in a hospital center were considered. As an initial step, the intention is to enter the platform, ensure authenticity, and request authorization to upload, modify, or make any changes to the medical record.

First, the contract parties are created and controlled by the government body or public or private institution, and then by the administrator to supervise the transaction operations in the blockchain infrastructure, where the contracts mainly provide operation functions. Algorithm 1 illustrates the principle of interaction.

Algorithm 1: Hospital node incorporation

```
Input: Hospital ID, city, name
Output: Hospital node
if msg.sender == Health Sector ADMIN then//Health Sector Gov. Admin.
        if a hospital address node exists in hospital mapping then
                Abort function and output Error
            else
            create a hospital node with input data
            add the public key to hospital mapping
else
   Abort function and output Error
```

In our proposal, five fundamental operations—adding, viewing, modifying, and removing records—interact with these algorithms to create their respective roles. The administrator and other system users use these functions. Table 1 shows the functions, their dimensions, and the recipient's user.

Table 1. Functions based on medical record.

Author	Function	Dimension	User
[33,34]	*Define roles*	Define roles	Administrator
[17,35]	*Add patient record*	Add medical records	Physician
[34,36]	*View patient record*	View medical records	Administrator, physician, and patient
[37,38]	*Update patient record*	Update medical records	Physician
[34,38]	*Delete patient record*	Delete medical records	Physician

The first function establishes the roles. The administrator is in charge of it, and it has two inputs: the figure to be represented and the account, which will be used to add a new role and account, respectively. The attribution of duties to physicians and patients is shown in Algorithms 2 and 3.

Algorithm 2: Medical node incorporation

```
Input: Public key, specialty
Output: Medical node
if msg.sender == hospital ADMIN then
        if a medical node address exists in medical mapping then
                Abort function and output Error
            else
            create a medical node with input data
            add the public key to medical mapping
else
 Abort function and output Error
```

Algorithm 3: Patient node incorporation

Input: Public key, gender
Output: Patient node

```
if $msg.sender$ == $hospital\ ADMIN$ then
    if the patient node address exists in patient mapping then
        Abort function and output Error
    else
        create a patient node with input data
        add the public key to patient mapping
else
    Abort function and output Error
```

Algorithm 4 shows the assignment of patients to physicians for care. This function maintains a task check of the physician's authenticated account using the term "msg.sender" to identify the user's address. After this check, the physician added the patients' records.

Algorithm 4: Assign physician to patient node

Input: Public key medical
Output: Physician assigned to a patient

```
if $msg.sender$ == $hospital\ ADMIN$ then
    if a Public key exists in patient attention list mapping then
        Abort function and output Error
    else
        add the public key to the patient attention list mapping
else
    Abort function and output Error
```

The doctor, who has to be registered by the administrator, performs the second function: adding patient records. Viewing patient records is the third function, which calls for looking for patient records using the patient ID variable. Since only medical professionals are qualified to carry out these procedures, checking the duties that the patient or doctor has been assigned is another aspect of the task at hand. The patient's medical history is updated using the fourth function, which is used to alter or update information in the patient's history. The fifth function is the deletion of data about patients, and its operation entails taking the patient's identifier as the input, verifying that a health worker is carrying out the function, and then deleting the data. Algorithm 5 illustrates the interaction principle.

Algorithm 5: Integrate medical records to file

Input: Public key patient
Output: Integrating register

```
if $msg.sender$ == $doctor$ then
    if Public key does not exist in patient attention list mapping then
        Abort function and output Error
    else
        open lists of medicalrecords where $R_m \leftarrow Public\ key$
        record $R_m \leftarrow tx_{n,k}$
        $tx_{n,k} \in Q$
else
    Abort function and output Error
```

Role-based access prevents unauthorized access to the architecture; only authorized users can access the system, and only authenticated users can access the correct processes.

4. Results

We evaluated our architecture against the design criteria shown in Table 2 and the first comparison was made according to the simulation scenarios, platforms, and tools used. In Alharby and van Moorsel [39], simulations were used to predict and describe the impact of different configurations, targets, and scenarios on the system behavior. Thus, simulation can answer questions such as, "What would happen if experimenting with new designs and policies without the need for the system's operation?" [40]. When designing and deploying blockchain solutions, many performance-impacting configuration choices must be made [24,39,41].

Table 2. Platforms and tools used.

Model	Target	Tools for Development	Platform	Environments of Simulation
Access administration system [42]	IoT access control	Remix IDE	Ethereum, raspberry	Javascript
System for controlling access [43]	Cross-chain-based access control in the IoT	-	IOTA and Tangle	Ubuntu 16.04
Access administration system [44]	Access control with IoT-related key management	-	Multiple public blockchains	OMNeT++ 5.4.1
Safeguard data exchange [45]	Deep learning is used to share data	Go	Ethereum	Python
Secure data exchanges	Data sharing with A.I.	-	Hyperledger fabric	-
The proposed model includes access control, record sharing, and management	Access control, data exchange, and management.	Remix IDE, Solidity	Hyperledger, separate modules	Remix IDE, python, JavaScript

The smart contract is made up with Solidity in the proposed design and compiled and tested using Remix IDE. Solidity is a sophisticated high-level programming language to create intelligent contracts; it lets users create decentralized programs so that miners may run and test and debug Solidity code in its environment [8,46,47]. Conversely, Table 3 displays the functional attributes of blockchain architectures for medical record management and data exchange. An implementation comparison was made to highlight the usefulness and feasibility of the proposed design, in which the authentication of users and the safeguarding of information under the attributes of reliability or data structure are performed, authorized, and access is authenticated with validation and decentralized supervision, in addition to compliance within the country's legal framework, where the medical record is considered as a set of documents of any kind, in which health personnel must record, annotate, and certify their interventions.

Table 3. Comparison of parameters with other works.

Systems	Reliability	Authorization	Authentication	Validation	Decentralized	Regulations
Access administration system [42]	Yes	No	No	Yes	Yes	No
Access administration system [43]	No	No	No	No	Yes	No
Access administration system [44]	No	Yes	No	No	Yes	Yes
Data sharing system [45]	No	No	Yes	Yes	Yes	Yes
Data sharing system [48]	Yes	No	No	No	Yes	No
Proposed data sharing and access control system	Yes	Yes	Yes	Yes	Yes	Yes

Ortiz [49] mentions that Mexican information protection laws cover all the data in the medical record to be protected and prevent unauthorized personnel from using this information. Medical records are defined and regulated legal standards focus on the parameters of medical information integration and on technical regulation. The safety of the proposed design was consistent with that of the theorem.

Theorem 1. *Suppose an unauthorized user can access the medical record management system without the authorization of the network administrator, such an attacker may find it very difficult to retrieve and read medical records.*

Test: In our design, all entities, administrators, doctors, and patients participating in the network are encrypted with a public key, and to retrieve the data, any applicant must be in access lists where it is essential to know the private key of the patient to decrypt the packet of information. Considering that this private key is unique and only the assigned user knows it, the probability that the attacker can obtain or guess the private key to decrypt and obtain data in the network is almost zero.

Moreover, within this study, it is suggested to employ an H64 algorithm for the computation of the hash and the verification of the transactions associated with each block. Consequently, an experiment was conducted to compare the duration required for computing the hash of three blocks, utilizing distinct algorithm types (SHA256, MD5, SHA1, H128, and H64). The resultant temporal curves are visually presented in Figure 2. The fluctuations observed in each curve are attributable to the random variability in block sizes generated during each cycle. The obtained outcomes reveal that the transaction validation period using the hash64 method has exhibited an average acceleration of 22% when compared to SHA256. Consequently, in our implementation of smart contracts, there exists a substantially diminished necessity for computational resources when employing the proposed hash64 approach.

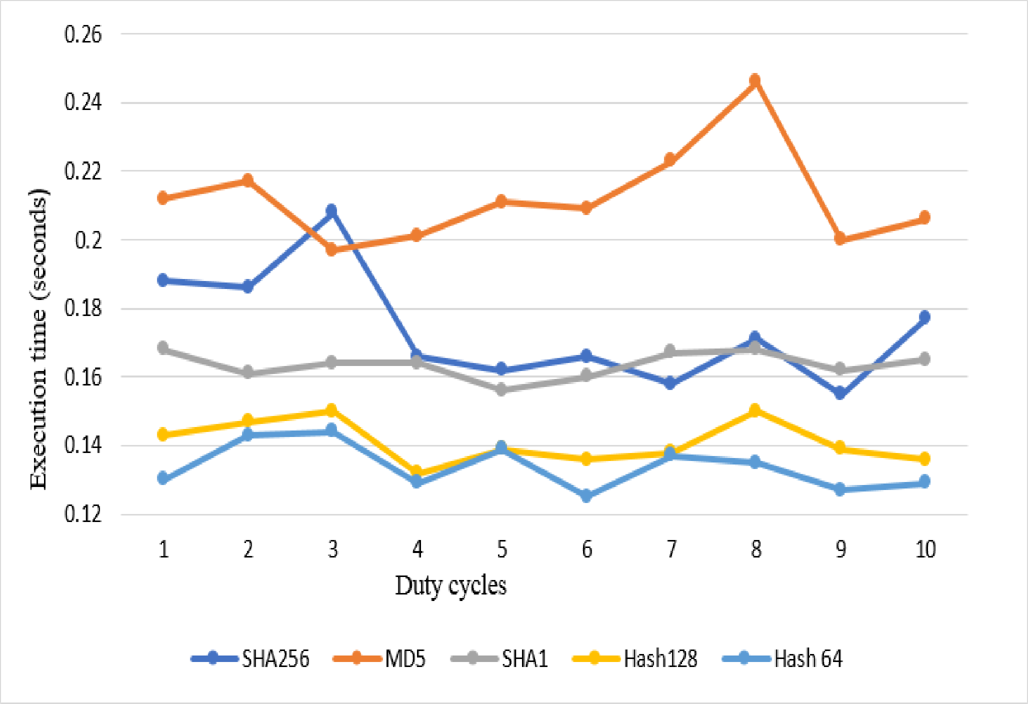

Figure 2. Consensus performance test.

The execution time data of the smart contracts (SC) developed for the proposed system is compared with the data extracted from smart contracts mentioned in the literature review (SC_LIT) [46,50,51]. The implementation of SC_LIT considers the metrics investigated by Hegedűs [52], which include the following:

SLOC: source lines of code;
LLOC: logical lines of code;
CLOC: comment-only lines of code;
NF: number of functions;
McCC: McCabe's cyclomatic complexity of the functions.

To analyze the SCs and extract metrics from the object-oriented (OO) programming paradigm, we utilized the SolMet tool implemented in Java, as provided by Hegedűs [52]. The obtained results are illustrated in Figure 3, displaying two curves. The orange line represents the time required to execute the SCs using the proposed method, while the other curve represents the SC_LIT method. It is evident that the execution times increase with an increase in the number of source code lines. This growth is nearly linear, with an execution time observed in the SC_LIT being 7.5 s for a contract with 15 SLOC, as compared to our proposed method which achieved 6.0 s. On the other hand, the maximum execution time with the SC_LIT method is 23.5 s for a contract with 71 SLOC, whereas the proposed method achieved 18.33 s. Overall, our proposal demonstrates an average reduction of 14% in the execution time of smart contracts.

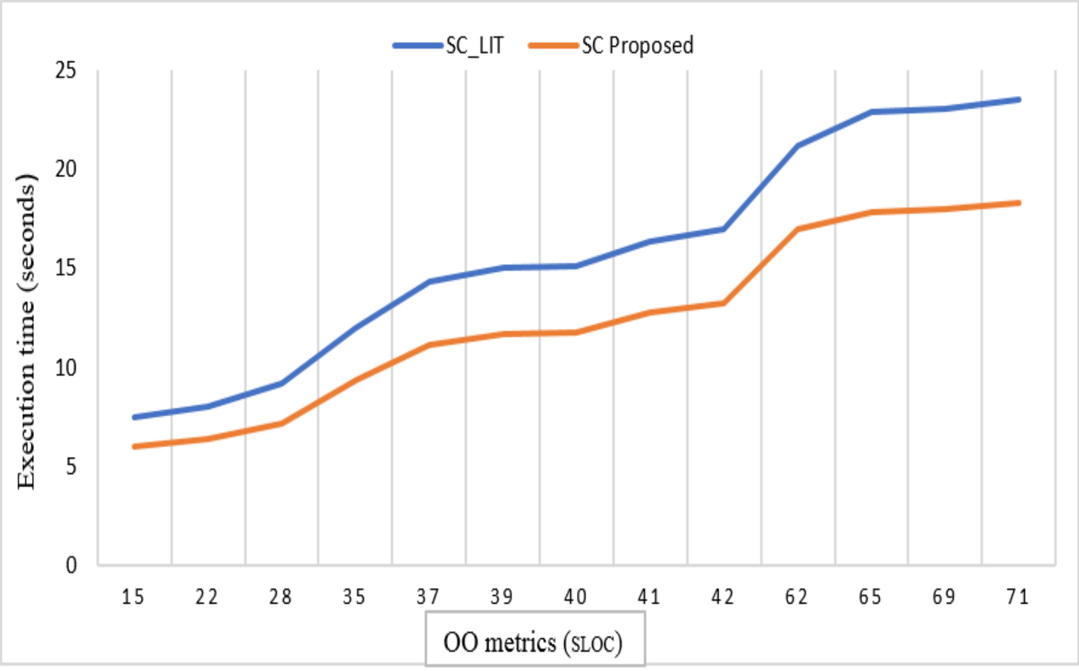

Figure 3. Analysis of smart contract execution times.

5. Discussion and Conclusions

This article outlines the advantages and difficulties of applying blockchain technology and smart contracts to the health industry, specifically in medical records, and presents some examples of use cases. In addition to summarizing the operation of blockchain, the article also discusses its importance in the development of systems for the health sector in Mexico that comply with current regulations and takes a step forward in the coverage of the fundamental axes of medical records, such as those listed below:

1. Privacy of information: Given the nature of the type of data—personal, diagnostic, and treatment—the actors will have the protection of the right to privacy regarding the records as well as the operations carried out on them and on the entities that execute them.
2. Immutability: Given that each block contains a previous block hash, any change in a medical record will result in different data in the block identification. In this way, a modification is identified, which avoids the alteration of the data.
3. Identity of the actors: Access to data must be performed only by authorized entities, and the system must be able to manage the different operations according to the type of user or node.
4. Data traceability: Data access must always be recorded. Writing, reading, and modifying data should be accessible to authorized actors on the blockchain without restrictions.

We demonstrated how the process of providing access rights may be conducted in a decentralized manner and without the involvement of a wholly untrusted third party by using a blockchain and smart contracts. To implement our suggested method, new medical knowledge will need to be updated on the blockchain, which calls for proper smart-contract lifecycle management.

Author Contributions: Conceptualization, A.I.M.A. and L.A.S.; methodology, J.L.G.A.; software, A.I.M.A.; validation, O.C.-M., J.L.G.A. and L.A.S.; formal analysis, L.A.S.; investigation, A.I.M.A.; resources, A.I.M.A.; data curation, A.I.M.A.; writing—original draft preparation, A.I.M.A. and L.A.S.; writing—review and editing, L.A.S.; visualization, J.L.G.A.; supervision, L.A.S.; project administration, A.I.M.A.; funding acquisition, L.A.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by CONACYT, grant number 1033480.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data sharing does not apply to this article as no new data were created or analyzed in this study.

Acknowledgments: We are grateful for the support of the Ph.D. program in Advanced Engineering Sciences (DOCIA) at the Universidad Autónoma de Ciudad Juárez.

Conflicts of Interest: The authors declare that they have no competing interests. The study's design, data collection, analysis, or interpretation; the preparation of the paper; and the choice to publish the findings were all made independently of the funders.

References

1. Georgiev, S.; Priftis, S.; Grigorov, E. Blockchain in the Logistics of Health Technologies. In Proceedings of the Information Systems and Grid Technologies, Online, 28–29 May 2021; pp. 189–202.
2. Haddad, A.; Habaebi, M.H.; Suliman, F.E.M.; Elsheikh, E.A.; Islam, M.R.; Zabidi, S.A. Generic Patient-Centered Blockchain-Based EHR Management System. *Appl. Sci.* **2023**, *13*, 1761. [CrossRef]
3. Kelly, B.; Quinn, C.; Lawlor, A.; Killeen, R.; Burrell, J. Cybersecurity in Healthcare. In *Trends of Artificial Intelligence and Big Data for E-Health*; Springer: Berlin/Heidelberg, Germany, 2023; pp. 213–231.
4. Thakur, A. Market Determinants Impacting Distributed Ledger Technology, and AI-Based Architectures in the Healthcare Industry. *Int. J. Bus. Anal. Intell.* **2022**, *10*, 10.
5. Lehto, M. Cyber-attacks against critical infrastructure. In *Cyber Security: Critical Infrastructure Protection*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 3–42.
6. Haque, A.B.; Muniat, A.; Ullah, P.R.; Mushsharat, S. An automated approach towards smart healthcare with blockchain and smart contracts. In Proceedings of the 2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), Greater Noida, India, 19–20 February 2021; pp. 250–255.
7. Abutaleb, R.A.; Alqahtany, S.S.; Syed, T.A. Integrity and Privacy-Aware, Patient-Centric Health Record Access Control Framework Using a Blockchain. *Appl. Sci.* **2023**, *13*, 1028. [CrossRef]
8. Amir Latif, R.M.; Hussain, K.; Jhanjhi, N.Z.; Nayyar, A.; Rizwan, O. A remix IDE: Smart contract-based framework for the healthcare sector by using Blockchain technology. *Multimed. Tools Appl.* **2020**, 1–24. [CrossRef]
9. Zaghloul, E.; Li, T.; Ren, J. Security and privacy of electronic health records: Decentralized and hierarchical data sharing using smart contracts. In Proceedings of the 2019 International Conference on Computing, Networking and Communications (ICNC), Honolulu, HI, USA, 18–21 February 2019; pp. 375–379.
10. Szabo, N. Formalizing and Securing Relationships on Public Networks. *First Monday* **1997**, *2*. [CrossRef]
11. Morabito, V. *Business Innovation through Blockchain*; Springer: Berlin/Heidelberg, Germany, 2017; Volume 2021, pp. 1–188.
12. Swan, M. Blockchain thinking: The brain as a decentralized autonomous corporation [commentary]. *IEEE Technol. Soc. Mag.* **2015**, *34*, 41–52. [CrossRef]
13. Kormiltsyn, A.; Udokwu, C.; Karu, K.; Thangalimodzi, K.; Norta, A. Improving healthcare processes with smart contracts. In Proceedings of the International Conference on Business Information Systems, Seville, Spain, 26–28 June 2019; pp. 500–513.
14. Hathaliya, J.J.; Tanwar, S. An exhaustive survey on security and privacy issues in Healthcare 4.0. *Comput. Commun.* **2020**, *153*, 311–335. [CrossRef]
15. Gordon, W.J.; Catalini, C. Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability. *Comput. Struct. Biotechnol. J.* **2018**, *16*, 224–230. [CrossRef]

16. Mettler, M. Blockchain technology in healthcare: The revolution starts here. In Proceedings of the 2016 IEEE 18th International Conference on E-Health Networking, Applications and Services (Healthcom), Munich, Germany, 14–17 September 2016; pp. 1–3.
17. Azaria, A.; Ekblaw, A.; Vieira, T.; Lippman, A. Medrec: Using blockchain for medical data access and permission management. In Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD), Vienna, Austria, 22–24 August 2016; pp. 25–30.
18. Peterson, K.; Deeduvanu, R.; Kanjamala, P.; Boles, K. A blockchain-based approach to health information exchange networks. In Proceedings of the NIST Workshop Blockchain Healthcare, Gaithersburg, MD, USA, 26–27 September 2016; pp. 1–10.
19. Rotbi, M.F.; Motahhir, S.; Ghzizal, A.E. Blockchain technology for a safe and transparent covid-19 vaccination. *arXiv* **2021**, arXiv:2104.05428. [CrossRef]
20. Pham, H.L.; Tran, T.H.; Nakashima, Y. A secure remote healthcare system for hospital using blockchain smart contract. In Proceedings of the 2018 IEEE Globecom Workshops (GC Wkshps), Abu Dhabi, United Arab Emirates, 9–13 December 2018; pp. 1–6.
21. Dubovitskaya, A.; Xu, Z.; Ryu, S.; Schumacher, M.; Wang, F. Secure and trustable electronic medical records sharing using blockchain. In Proceedings of the AMIA Annual Symposium Proceedings, Washington, DC, USA, 6–8 November 2017; p. 650.
22. Khatoon, A.J. A blockchain-based smart contract system for healthcare management. *Electronics* **2020**, *9*, 94. [CrossRef]
23. Dagher, G.G.; Mohler, J.; Milojkovic, M.; Marella, P.B. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustain. Cities Soc.* **2018**, *39*, 283–297. [CrossRef]
24. Xia, Q.; Sifah, E.B.; Asamoah, K.O.; Gao, J.; Du, X.; Guizani, M. MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. *IEEE Access* **2017**, *5*, 14757–14767. [CrossRef]
25. Ahram, T.; Sargolzaei, A.; Sargolzaei, S.; Daniels, J.; Amaba, B. Blockchain technology innovations. In Proceedings of the 2017 IEEE Technology & Engineering Management Conference (TEMSCON), Santa Clara, CA, USA, 8–10 June 2017; pp. 137–141.
26. Saravanan, M.; Shubha, R.; Marks, A.M.; Iyer, V. SMEAD: A secured mobile enabled assisting device for diabetics monitoring. In Proceedings of the 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Odisha, India, 17–20 December 2017; pp. 1–6.
27. Benchoufi, M.; Ravaud, P. Blockchain technology for improving clinical research quality. *Trials* **2017**, *18*, 335. [CrossRef] [PubMed]
28. Nugent, T.; Upton, D.; Cimpoesu, M. Improving data transparency in clinical trials using blockchain smart contracts. *F1000Research* **2016**, *5*, 2541. [CrossRef]
29. McFarlane, C.; Beer, M.; Brown, J.; Prendergast, N. *Patientory: A Healthcare Peer-to-Peer Emr Storage Network v1*; Entrust Inc.: Addison, TX, USA, 2017; Volume 3, p. 19.
30. Coperneec. "How to represent a blockchain through a mathematical model?". Available online: https://canopee-group.com/wp-content/uploads/2020/05/ (accessed on 26 April 2023).
31. Lande, S.; Zunino, R. SoK: Unraveling Bitcoin smart contracts. In *Principles of Security and Trust LNCS*; Springer: Berlin/Heidelberg, Germany, 2018; Volume 10804, p. 217. [CrossRef]
32. Shahnaz, A.; Qamar, U.; Khalid, A. Using blockchain for electronic health records. *IEEE Access* **2019**, *7*, 147782–147795. [CrossRef]
33. Mercenne, L.; Brousmiche, K.-L.; Hamida, E.B. Blockchain studio: A role-based business workflows management system. In Proceedings of the 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 1–3 November 2018; pp. 1215–1220.
34. Bhavin, M.; Tanwar, S.; Sharma, N.; Tyagi, S.; Kumar, N. Blockchain and quantum blind signature-based hybrid scheme for healthcare 5.0 applications. *J. Inf. Secur. Appl.* **2021**, *56*, 102673. [CrossRef]
35. Alexaki, S.; Alexandris, G.; Katos, V.; Petroulakis, N.E. Blockchain-based electronic patient records for regulated circular healthcare jurisdictions. In Proceedings of the 2018 IEEE 23rd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Barcelona, Spain, 17–19 September 2018; pp. 1–6.
36. Liu, P.T.S. Medical record system using blockchain, big data and tokenization. In Proceedings of the Information and Communications Security: 18th International Conference, ICICS 2016, Singapore, 29 November–2 December 2016; pp. 254–261.
37. Tith, D.; Lee, J.S.; Suzuki, H.; Wijesundara, W.M.A.B.; Taira, N.; Obi, T.; Ohyama, N. Patient consent management by a purpose-based consent model for electronic health record based on blockchain technology. *Healthc. Inform. Res.* **2020**, *26*, 265–273. [CrossRef]
38. Sharma, R.; Kumar, A. Electronic Health Records Using Blockchain. Available online: www.ir.juit.ac.in (accessed on 15 November 2022).
39. Alharby, M.; van Moorsel, A. Blocksim: An extensible simulation tool for blockchain systems. *Front. Blockchain* **2020**, *3*, 28. [CrossRef]
40. Banks, J. *Discrete Event System Simulation*, 4th ed.; Pearson Education India: Delhi, India, 2005.
41. Wang, Q.; Qin, S. A Hyperledger Fabric-Based System Framework for Healthcare Data Management. *Appl. Sci.* **2021**, *11*, 11693. [CrossRef]
42. Zhang, Y.; Kasahara, S.; Shen, Y.; Jiang, X.; Wan, J. Smart contract-based access control for the internet of things. *IEEE Internet Things J.* **2018**, *6*, 1594–1605. [CrossRef]
43. Jiang, Y.; Wang, C.; Wang, Y.; Gao, L. A cross-chain solution to integrating multiple blockchains for IoT data management. *Sensors* **2019**, *19*, 2042. [CrossRef]

44. Ma, M.; Shi, G.; Li, F. Privacy-oriented blockchain-based distributed key management architecture for hierarchical access control in the IoT scenario. *IEEE Access* **2019**, *7*, 34045–34059. [CrossRef]
45. Liu, C.H.; Lin, Q.; Wen, S. Blockchain-enabled data collection and sharing for industrial IoT with deep reinforcement learning. *IEEE Trans. Ind. Inform.* **2018**, *15*, 3516–3526. [CrossRef]
46. Omar, I.A.; Jayaraman, R.; Debe, M.S.; Salah, K.; Yaqoob, I.; Omar, M. Automating procurement contracts in the healthcare supply chain using blockchain smart contracts. *IEEE Access* **2021**, *9*, 37397–37409. [CrossRef]
47. Yadav, A.K.; Bajpai, R.K. KYC optimization using blockchain smart contract technology. *Int. J. Innov. Res. Appl. Sci. Eng.* **2020**, *4*, 669–674. [CrossRef]
48. Zhang, G.; Li, T.; Li, Y.; Hui, P.; Jin, D. Blockchain-based data sharing system for ai-powered network operations. *J. Commun. Inf. Netw.* **2018**, *3*, 1–8. [CrossRef]
49. Valeriano Ortiz, O. Development of a Web System for Records Management in ICB's Nutrition Clinic in Compliance with Federal Regulation NOM-024-SSA3-2010. Available online: http://hdl.handle.net/20.500.11961/2911 (accessed on 5 November 2022).
50. Gupta, R.; Shukla, A.; Tanwar, S. Aayush: A smart contract-based telesurgery system for healthcare 4.0. In Proceedings of the 2020 IEEE International Conference on Communications Workshops (ICC Workshops), Virtual, 7–11 June 2020; pp. 1–6.
51. Musamih, A.; Salah, K.; Jayaraman, R.; Arshad, J.; Debe, M.; Al-Hammadi, Y.; Ellahham, S. A blockchain-based approach for drug traceability in healthcare supply chain. *IEEE Access* **2021**, *9*, 9728–9743. [CrossRef]
52. Hegedűs, P. Towards analyzing the complexity landscape of solidity based ethereum smart contracts. In Proceedings of the 1st International Workshop on Emerging Trends in Software Engineering for Blockchain, Gothenburg, Sweden, 27 May 2018; pp. 35–39.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.