ISSN 2007-9737

A Blockchain-based Functional Approach for Geriatric Electronic Health Record

Julio C. Mendoza-Tello*, Alexis I. Males-Anagumbla, Wladimir G. Gualoto-Alvaro

Universidad Central del Ecuador, Facultad de Ingeniería y Ciencias Aplicadas, Quito, Ecuador

{jcmendoza, aimales, wggualoto}@uce.edu.ec

Abstract. An electronic health record (EHR) is a repository that contains the events related to the patient's health, such as preventive tests and disease treatments. These registries play a vital role for health field because they improve patient care and medical prescription, as well as the provision of data for the clinical research field; in this context, the health of the elderly is a priority. The versatility of an EHR depends on aspects related to security, privacy, integrity, and immutability. Privacy and security are necessary requirements for data exchange (between medical service providers and patients) because they prevent data loss and unwanted access in the scheme. In this sense, the patient must have the privilege to share his clinical record with other users. In addition, the integrity must be guaranteed by the immutability of the events recorded over time. Without a doubt, a reliable scheme for EHR management is a must. Facing these challenges, blockchain was designed to store digital assets in a decentralized environment; that is, without the supervision of trusted third parties. This technology can carry digital assets or tokens, such as smart contracts. These contracts automate functional requirements and inherit the immutability feature from blockchain. This ensures strict compliance between the parties sharing information, ensures that the data is not manipulated and prevents data leakage. With these considerations, the aim of paper is to define a blockchain-based functional approach for geriatric electronic health record. For this, this research focuses on four main phases, namely: core concepts review, requirements specification, model development, and functional test. In this context, components were developed (using smart contracts) and implemented on the blockchain; in addition, web forms were used to test our proposal. Conclusions and future work are described at the end of this paper**.**

Keywords. Blockchain, smart contracts, EHR, healthcare**.**

1 Introduction

An electronic health record (EHR) is a digital repository that contains a patient's health information, as well as the history of treatments carried out to determine and improve health status[1]. An EHR plays an important role in the health area because it provides data for both effective medical prescription and future clinical research. An EHR is a private document with legal and ethical implications. Therefore, one of the biggest challenges in healthcare systems is security to share data and prevent user information leakage.

The computer field provides a vital support for these health activities. However, the technology management of EHR suffers from some problems related to privacy, availability, and security to exchange data between users and health providers. Sometimes, these weaknesses are caused because the technological infrastructure management model is centralized; that is, the reliability and availability of the schema is the responsibility of a single entity.

If the central node falls at any time, the service drops, and service availability is affected for an unlimited amount of time. It should be noted that centralized administration delegates responsibility to a specific server, which can suffer denial-of-service attacks that affect the service quality provided to the user. Additionally, centralized storage causes delays in collaborative efforts and decision making. In this context, there is a lack of trust for data sharing due to privacy intrusions, tampering, and plagiarism.

Consequently, data integration is difficult and health care quality decreases. In some cases,

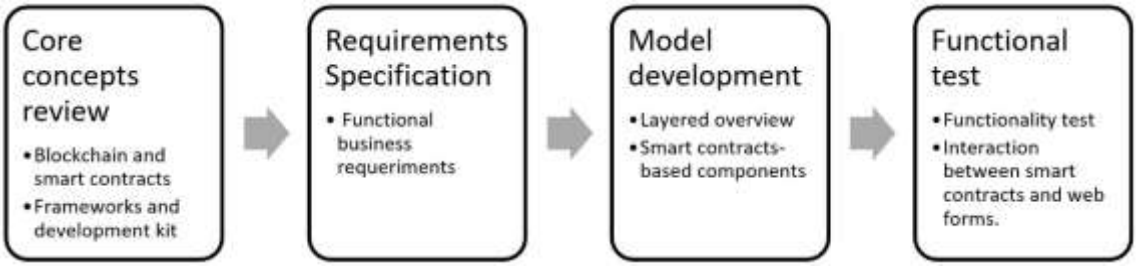

Fig.1. Research phases overview

patients need to repeat laboratory tests, the analysis of which is requested by various health service providers. This is not acceptable especially in the prevention, diagnosis, treatment of diseases and health of older adults.

Faced with these challenges mentioned above, blockchain was designed to transport digital assets without the need for trusted third parties to certify operations performed in the scheme.

That is, the credibility of the blockchain is supported by decentralized consensus mechanisms. Regarding data security, blockchain has the immutability characteristic; that is to say, once the data is registered, it cannot be adulterated; therefore, non-repudiation between participants is guaranteed.

This technology is based on cryptographic algorithms that guarantee the authorization and confidentiality. In addition, the implementation of blockchain on P2P infrastructures is a versatility that avoids single point of failure problems and allows system recovery using any node of the scheme. This implies that operations are protected against denial-of-service attacks.

With these considerations, the aim of paper is to define a blockchain-based functional approach for geriatric electronic health record.

In this context, the paper sections are as follows. Section 2 explains the work methodology. Section 3 describes the materials and theoretical core that support our research proposal. Section 4 details the requirements and development of a web prototype based on blockchain and smart contracts. Finally, section 5 describes the conclusions and future work that arise from this paper.

2 Methodology

This research focuses on four main phases, namely: core concepts review, requirements specification, model development, and functional test. Figure 1 shows a research phases overview carried out.

3 Background

In this section, a brief description of the theoretical concepts, related works and materials are described to support our research objective.

3.1 Blockchain and Smart Contracts

A blockchain is an ordered list of blocks linked chronologically; that is, each subsequent block is linked to a previous block. Each block consists of header and transactions.

Regarding the block header. Each block is identified by a hash, which is a reference to the header of the previous block. That is, within each block header there is an exact copy called previous block header hash. The first block of a blockchain is called genesis and from this, new blocks are added sequentially to the chain.

The amount of blocks added to the chain is called block height. The header occupies 80 bytes, each block contains about 500 transactions, and each transaction occupies 250 bytes. The block header contains three metadata sets. (i) block hash. It is a fingerprint generated by twice applying the SHA-256 algorithm.

Each block header hash is 32 bytes. This operation ensures that any subsequent block

validates the immutability of a previous block. In this way, integrity is ensured because if one bit is altered, the entire chain is invalidated and rejected by the entire network of participants. (ii) Metadata. It is a set of parameters related to mining competition; the following fields are identified: difficulty, nonce and timestamp. (iii) Merkle Tree.

It is a cryptographic procedure that dually groups transactions using hash functions. Any bit that attempts to adulterate is reason for the block to be invalidated. The essential function of the header is to ensure the creation, propagation, validation and stacking of blocks for the chain.

Regarding transactions. A transaction is the most essential and important for the blockchain scheme. A transaction is a data structure consisting of several fields, namely: sending address, receiving address, signature, and digital token. Each transaction is created through the signature of a token owner.

This transaction is propagated through the network. Any node can validate the transaction, and if it is correct, the transaction will be validated and accepted as a confirmed transaction. If the transaction is not correct, any node will invalidate it, sending a rejection message to source.

Blockchain is implemented on decentralized P2P networks; that is, there is no central server that controls the operational flow of the scheme. Any node with processing and storage power can participate; and each node can own a copy of the blockchain.

Although P2P network nodes are similar, they assume different roles according to the following functions: routing, full node, and simplified payment verification for lightweight nodes.

The versatility of the blockchain allows tokens to be transported on top of its upper layer. These tokens are pointers that reference a digital asset, such as virtual currencies and smart contracts. A virtual currency is a medium of exchange between participants, and a smart contract defines the rules for that exchange. A smart contract is a set of self-executing instructions that are executed according to programming conditions.

These conditions are previously agreed by the participants. Each smart contract is implemented through the publication of a transaction and can be invoked by an external user account or by another contract. A contract is defined by the following structure, namely: (a) Turing complete language-based program code, (b) account balance to receive and send virtual currencies, y (c) storage for writing, reading, modifying, and reading data variables.

A smart contract based on blockchain inherits the property immutability; that is, once implemented it is impossible to adulterate its coding and of course, the purpose of it. In this context, a smart contract guarantees strict compliance with a pre-contractual agreement without exception. Figure 2 shows how smart contracts interact with the blockchain.

3.2 Related Works

Previous blockchain-based EHR research has focused mainly on seven considerations: (i) storage, (ii) types of blockchain, (iii) traceability, (iv) latency, (v) cryptography, (vi) ethical aspects, and (vii) user applications.

(i) Storage. The information processed by the blockchain and IPFS (InterPlanetary File System) is distributed between the nodes to store immutable health records [2]. IPFS usage intensifies as the EHR is shared using mobile cloud-based systems [1]. Findings show that the storage cost of blockchain-based EHR is 20% lower compared to existing repositories [3].

(ii) Types of blockchain. Previous research suggests that a private blockchain is suitable for EHR storage, while a consortium blockchain is useful for EHR indices [4]. In this context, EHR management supports the exchange of information between various stakeholders and supports the claim of health insurance [5].

(iii) Traceability. Preserving the integrity of an EHR is a challenge for various healthcare providers. Preserving the integrity of an EHR is a challenge for various health care providers. To do this, the blockchain traceability property generates audit trails that support monitoring user access and behaviors in cloud environments [6]. The idea is to integrate behaviors into the blockchain, so that illegitimate manipulations cannot be executed after an EHR is registered within the blockchain [7].

(iv) Latency. Time is an essential metric to assess the efficiency of decentralized storage [8]. In this context, the findings show that the response time for EHR systems based on blockchain is 50%

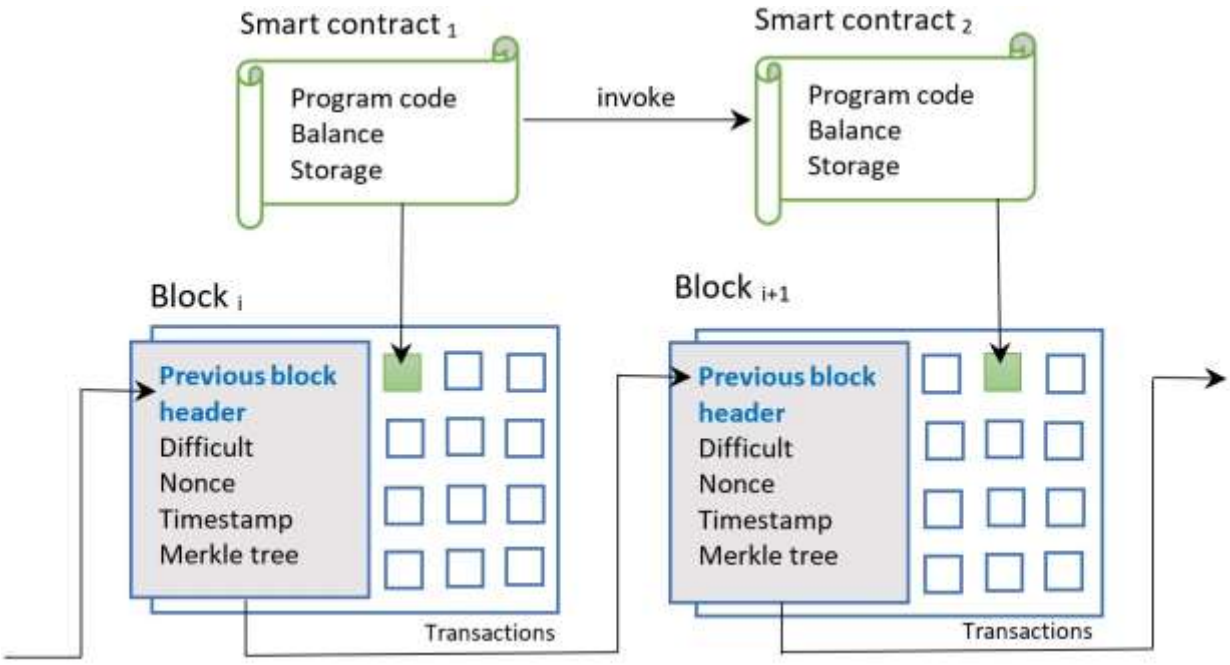

Fig. 2. How do smart contracts interact with blockchain?

less than systems based on conventional techniques. These performance improvements demonstrate that minimal network latency improves levels of data privacy and security [1].

(v) Cryptography. The sharing of EHR requires an authorization model based on strict access control policies. In this context, a blockchain-based multi-hop permission delegation scheme with controllable delegation depth was designed [9]. For this, attribute-based encryption is used to provide access control. In addition, a homomorphic cryptosystem was tested in blockchain schemes, and the results showed high effectiveness against plaintext attack. [10].

Additionally, index-based search encryption techniques can be integrated into smart contracts to support both EHR integrity [11] and the monetary reward that brings sustainability to the scheme. In the same way, a modified Merkle Tree structure is encoded to store an EHR smart contract, which improves data reliability [12].

(vi) Ethics. Blockchain features provide guidelines to preserve privacy according to ethical supervision, and strict legal protection of people's health data [13]. The implementation of EHR on blockchain poses ethical challenges, which were framed within nine parameters, namely: accountability, fairness, privacy, accuracy, right to be forgotten, data access, data ownership, and governance [14].

(vii) Health care apps. Hospitals are adopting IoT devices to monitor rooms and health status of patients. Blood pressure, glucose, and electroencephalography monitors are devices that collect patient information and support decision making. However, these devices are susceptible to security risk when connected to a network. In this context, blockchain guarantees security for the authentication processes of devices that access cloud services [15].

In addition, disease statistics can be tracked without violating patient privacy [2]. Blockchain also has space for the forensic environment. In this regard, blockchain was used to preserve forensic data by comparing antemortem and postmortem dental data. In this way, human remains of missing persons can be identified using an electronic dental and health record system. Thus,

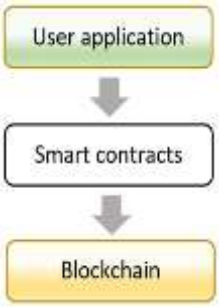

Fig. 3. A layered overview to support the functional model

redundancies, inconsistencies and errors can be detected and protection against data alteration is guaranteed [16].

3.3 Materials

In this research, software and hardware were used to develop the blockchain-based scheme. Regarding hardware, a computer with an Intel Core i7 processor and speeds of up-to 2.4 GHz with 128 MB RAM were used to develop the software. Regarding the software, frameworks and programming languages were used to develop smart contracts and web user interfaces. In this context, the software is as follows:

- Solidity. Turing-complete high-level language used for programming smart contracts. The structure is like JavaScript and supports different types of data such as: boolean, integer, address, and string dynamic array. Both variables and functions are supported by the following access specifiers: public, private, external, and internal.
- JavaScript. Programming language to create dynamic web pages. It is compatible with any browser because the JavaScript code is embedded into the HTML code.
- TypeScript. Microsoft free-source language that works as a JavaScript extension. It incorporates classes, structures, and annotations.
- Truffle. Blockchain-based framework to debug, compile and deploy smart contracts. It supports bytecode to implement transactions on the blockchain. It provides a direct connection interface for smart contracts. The framework installation is done through the NPM package manager.
- React. JavaScript library for developing iOS and Android apps. The library translates React Native code into Objective-C. Furthermore, it establishes an interface for mobile applications using declarative components.
- SAP Power Designer. Tool for business modeling and software design. It supports a variety of development methodologies, modeling languages and variety of extensions (such as pdm, cdm, bpm).
- Ganache. Tool that provides a private Ethereum blockchain for test. It provides 100 ether of test to execute commands. It provides an interface through which it is possible to observe account statements, addresses, transactions, and account balances.
- Metamask. It is a crypto software wallet installed as a web browser extension and used to interact with the Ethereum blockchain. It is an interface to send and receive cryptocurrencies, as well as to store and transmit transactions in decentralized applications. It is compatible with web browsers and mobile apps.
- Web3 JS. Library suite for remote interaction with Ethereum nodes using HTTP, IPC, JSON-RPC specification, and WebSocket.

4 Results: Model Development

In accordance with the methodology, this section designs a model using the following phases: identification of blockchain characteristics, identification of functional requirements, model design, and functional testing.

4.1 Blockchain Characteristics to Support Model

Certainly, Blockchain provides benefits that support the functionality of the model. In this context, four versatilities were identified, namely.

First, shared intelligent. Doctors, stakeholders, and researchers can share an EHR with patient's prior authorization [2]. Thereby, the accuracy of the medical diagnosis is improved because isolation

between different information systems is avoided [4]. Thus, making decisions about a patient's treatment is more agile [5]. Consequently, quality and intelligence of the health care system is improved [8], efficiency is increased, and health care costs are reduced [9].

Second, transparency and immutability. Verification is transparent because the data distribution has a high level of privacy and security [3]. Immutable logs are generated each time a user accesses an EHR. In addition, any attempt to adulterate a previously registered EHR is visible and rejected by the P2P network. Thus, an EHR is immutable; that is, it cannot be adulterated or falsified [13].

Third, automation. Functional requirements, access policies and authentication procedures are implemented through smart contracts. Additionally, auditing mechanisms are provided by the protocol to record any event or request into the ledger. In this way, the use of cryptographic mechanisms annuls repudiation and identity theft [2].

Fourth, decentralization. Intermediation between medical service providers is eliminated. Therefore, storage is decentralized through P2P networks. Consequently, the confidence of the scheme is based on decentralized consensus mechanisms, rather than a central control authority [17]. Therefore, the scheme is reliable and fault tolerant.

```
pragma solidity ^0.8.7;
/* Comments
 * Personal. It defines the personal data structure.
 * dataType. Attribute data type.
 * attribute. Structure attribute.
 * PersonalContract. It defines the personal data contract.
 * putPersonal(). Function to add personal data.
 * getPersonal(). Function to search personal data.
 * sessionContract. Contract Instance Address
 * _id. User Identification
 * _personal. Personal Data structure information
*/

struct Personal {
uint256 id;
dataType attribute2;
dataType attribute3;
dataType attributeN;
}

contract PersonalContract {
mapping (uint256 => Personal[]) PersonalContractFunctionsMap;
constructor ();

function putPersonal(dataType _id, dataType _attribute2,
 dataType _attribute2, dataType _attributeN) }
 internal pure returns (Personal memory) {
 Personal memory _personal;
 _personal.id = _id;
 _personal.attribute2 = _attribute2;
 _personal.attribute3 = _attribute3;
 _personal.attributeN = _attributeN;

 return _personal;
 }

function getPersonal(address sessionContract){
 returns (Personal[] memory)
 }
}
```

Fig. 4. Algorithm for user administration

4.2 Functional Requirements

Two functionalities were identified, namely: user management, and geriatric care management.

First, user management. As a result, it includes the creation of users and access privileges. Three types of users were identified, namely: doctor, patient, and medical service provider. The scheme is focused on the patient, who can grant, and revoke read permissions to other users.

It is necessary to register the following personal information, namely: date of birth, name, gender, marital status, telephone number and contact address; in the case of medical personnel and medical service providers, it is necessary to register the specialty and contact information, such as address and telephone number.

Second, geriatric care management. It considers the clinical aspects of prevention, treatment, prevention, and rehabilitation of the patient, including social and family aspects. Six components were defined, namely:

(i) Physical assessment. Component including the following items, namely: blood pressure, heart rate, respiratory rate, weight, height, body mass index, skin condition, head and neck condition, oral cavity condition, lung condition, cardiovascular system, abdomen condition, urinary and genital organs, digital rectal examination, nervous system, musculoskeletal system, and temperature.

(ii) Biological assessment. Component that includes the following items, namely: urination, bowel movements, appetite, thirst, and sleep.

(iii) Clinical assessment. Component that includes the following items, namely: incontinence, nutrition, mobilization, and patient behavior.

```
pragma solidity ^0.8.7;

/* Comments
* Assessment. It defines the structure according to the
  type of evaluation. In this context, this corresponds to
  the following EHR components: Biological_Assessment,
  Physical_Assessment, Clinical_Assessment,
  Geriatric_Assessment, Sickness_Assessment
  Pathological_Assessment.

* dataType. Attribute data type.
* attribute. Structure attribute.
* AssessmentContract. It defines the contract according to
  the type of assessment.
* getAssessment(). Function to search for information
  according to the type of assessment.
* addAssessment(). Function to add information of an
  evaluation type.
* sessionContract. Contract Instance Address.
* _id. Patient identification.
* _assessment. Assessment structure information.
*/

struct Assessment {
  dataType attribute1;
  dataType attribute2;
  dataType attributeN;
}
contract AssessmentContract {
 mapping (uint256 => Assessment[]) AssessmentContractFunctionsMap;
 uint256 AssessmentContract;
 constructor() { }

function getAssessment (address sessionContract, uint256 _id) {
 return AssessmentContractMap[_id];
}
function addAssessment (address sessionContract, uint 256 _id,
 Assessment memory _assessment) {
 AssessmentContractMap[_id].push(_assessment)
 AssessmentContractMapLength++;
 return AssessmentContractMap[_id];
}
}
```

Fig. 5. Algorithm for geriatric EHR

(iv) Pathological assessment. Component that includes the following items: congenital sickness, childhood and adolescence sickness, surgical interventions, transfusions, allergies, harmful habits, and hospitalizations.

(v) Sickness assessment. Component that includes the following items: diagnosis, signs, symptoms, and sickness treatment, as well as details and assessment results.

(vi) Geriatric assessment. Component that includes the following items: delirium, vertigo, syncope, incontinence, visual deprivation, clinical prostration, insomnia, constipation, falls, prostatism, and chronic pain.

4.3 Blockchain-based Schema Design

In this section, a button-up schema is designed as follow: First, blockchain layer. Blocks are generated via consensus mechanisms. Verification fields are implemented (previous block header, timestamp and Merkle tree). Each block implements transactions using cryptocurrencies and smart contracts. This layer is supported by P2P mining layer (Figure 3).

Second, smart contract layer. Each smart contract is a stand-alone trigger that stores and executes encodings. With respect to user administration, a smart contract was coded using the algorithm shown in figure 4. With respect to EHR components, six smart contracts were coded using the algorithm shown in figure 5. Each smart contract contains classes (structures and functions) to implement a domain model. One or several contracts make up a software component; therefore, functional requirements were implemented within this layer. A total of 7 smart contracts were developed and implemented on the blockchain (Figure 6), namely: user management, physical, biological, clinical, pathological, geriatric, and sickness assessments. This layer is supported by the blockchain layer. Third, user application layer. It contains the web application used to test and interact with the smart contracts. This layer is supported by smart contract layer.

4.4 Functional Testing

Web form-based user interfaces were developed using the described software. Our prototype has two main forms: user management and geriatric medical record management. Regarding user management. Web forms were created for the following events: authentication, authorization, granting of roles and access. A representative functionality is shown in figure 7.

About EHR management. Web forms were created for registration and search of EHR. In this context, frames were embedded inside HTML pages. These frames retained the same cascading style sheets for all EHR components. A representative functionality is shown in figures 8 and 9.

5 Conclusions

This paper explains how the versatility of the blockchain can support EHR management.

ISSN 2007-9737

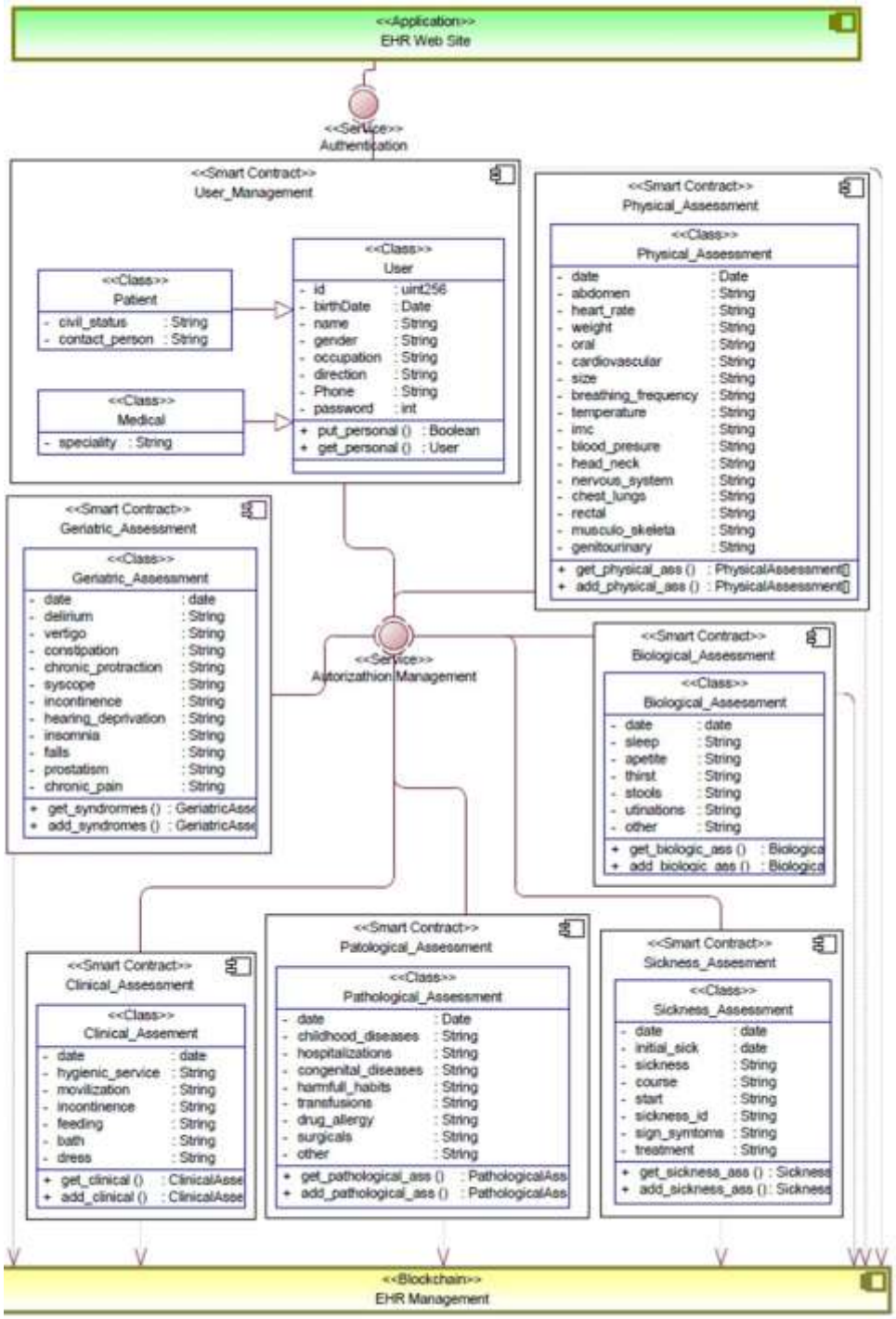

Fig. 6. Component diagram

Fig. 7. User authentication

Fig. 8. EHR Options menu

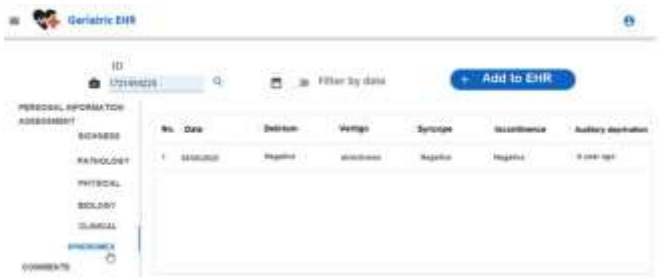

Fig. 9. EHR components

These versatilities bring benefits to the operation of an EHR and allow shared intelligence, transparency, immutability, automation, and decentralization. In this context, this paper proposes contributions, as well as defines future works focused on the results obtained from this research.

5.1 Contributions

This research contributes both to theory and practice. In theory terms. A model is designed using two perspectives. First, a button-up schema to explain how the various layers of the model interact with each other. Second, a UML class model is designed to describe the attributes, operations, and relationships between system objects. Each class abstracts the functionality of the various geriatric assessments that make up an EHR.

This allows the modeling of information related to the health status of an older adult. Consequently, a smart contract-based UML component diagram is designed using the defined classes.

Based on this, seven smart contracts were developed and implemented on the blockchain, namely: user management, physical, biological,

clinical, pathological, geriatric, and sickness assessments.

In practice terms, the proposed model is based on the blockchain characteristics, which ensure that the information is immutable. The developed web application uses components and communication protocols with the blockchain, which allow the correct consumption of the services and functionalities described in the smart contracts.

In addition, the functional tests demonstrate the validity of our proposal. In this context, two main web forms were developed to support the two main requirements: user management and medical records.

5.2 Future Works

According to these considerations, the versatility, and benefits of blockchain are evident. However, there are some challenges that need to be addressed. Security and privacy for cloud-based data sharing are essential to maintaining the integrity of the blockchain scheme.

In this sense, the authentication of IoT devices play an important role for the storage and audit of events in a health information system. Consequently, these issues pose ethical challenges for the processing of sensitive information through mobile devices. Finally, it is necessary to define legal regulations to regulate the use of blockchain and enhance its benefits in health.

References

1. **Nguyen, D. C., Pathirana, P. N., Ding, M., Seneviratne, A. (2019).** Blockchain for secure EHRs sharing of mobile cloud based E-Health systems. IEEE Access, Vol. 7, pp. 66792–66806. DOI:10.1109/ACCESS.2019.2917555.
2. **Sabu, S., Ramalingam, H. M., Vishaka, M., Swapna, H. R., Hegde, S. (2021).** Implementation of a secure and privacy-aware E-Health record and IoT data sharing using blockchain. Global Transitions Proceedings, Vol. 2, No. 2, pp. 429–433. DOI: 10.1016/ j.gltp.2021.08.033.
3. **Nagasubramanian, G., Sakthivel, R. K., Patan, R., Gandomi, A. H., Sankayya, M., Balusamy, B. (2020).** Securing E-Health records using keyless signature infrastructure blockchain technology in the cloud. Neural Computing and Applications, Vol. 32, No. 3, pp. 639–647. DOI: 10.1007/s00521-018-3915- 1.
4. **Shamshad, S., Minahil, Mahmood, K., Kumari, S., Chen, C. M. (2020).** A secure blockchain-based E-Health records storage and sharing scheme. Journal of Information Security and Applications, Vol. 55, p. 102590. DOI: 10.1016/j.jisa.2020.102590.
5. **Jain, M., Pandey, D., Sharma, K. K. (2022).** A blockchain approach on security of health records for children suffering from dyslexia during pandemic COVID-19. Artificial Intelligence, Machine Learning, and Mental Health in Pandemics: A Computational Approach, Elsevier Inc. pp. 343–363. DOI: 10.1016/B978-0-323-91196-2.00004-1.
6. **Huang, H., Sun, X., Xiao, F., Zhu, P., Wang, W. (2021).** Blockchain-based E-Health system for auditable EHRs manipulation in cloud environments. Journal of Parallel and Distributed Computing, Vol. 148, pp. 46–57. DOI: 10.1016/j.jpdc.2020.10.002.
7. **Cao, S., Zhang, G., Liu, P., Zhang, X., Neri, F. (2019).** Cloud-assisted secure E-Health systems for tamper-proofing EHR via blockchain. Information Sciences, Vol. 485, pp. 427–440. DOI: 10.1016/j.ins.2019.02.038.
8. **Rai, B. K. (2023).** PcBEHR: patient-controlled blockchain enabled electronic health records for healthcare 4.0. Health Services and Outcomes Research Methodology, Vol. 23, No. 1, pp. 80-102. DOI: 10.1007/s10742-022-00279-7.
9. **Gao, Y., Zhang, A., Wu, S., Chen, J. (2022).** Blockchain-based multi-hop permission delegation scheme with controllable delegation depth for electronic health record sharing. High-Confidence Computing, Vol. 2, No. 4, p. 100084. DOI: 10.1016/j.hcc.2022. 100084.
10. **Li, F., Liu, K., Zhang, L., Huang, S., Wu, Q. (2022).** EHRChain: A blockchain-based EHR system using attribute-based and

homomorphic cryptosystem. IEEE Transactions on Services Computing, Vol. 15, No. 5, pp. 2755–2765. DOI: 10.1109/TSC.2021.3078119.

11. **Chen, L., Lee, W. K., Chang, C. C., Choo, K. K. R., Zhang, N. (2019).** Blockchain based searchable encryption for electronic health record sharing. Future Generation Computer Systems, Vol. 95, pp. 420–429. DOI: 10.1016/j.future.2019.01.018.
12. **Chelladurai, U., Pandian, S., Ramasamy, K. (2021).** A blockchain based patient centric electronic health record storage and integrity management for E-Health systems. Health Policy and Technology, Vol. 10, No. 4, p. 100513. DOI: 10.1016/j.hlpt.2021.100513.
13. **Gross, M., Miller, R. C. (2021).** Protecting privacy and promoting learning: blockchain and privacy preserving technology should inform new ethical guidelines for health data. Health and Technology, Vol. 11, No. 5, pp. 1165–1169. DOI: 10.1007/s12553-021-00589- 9.
14. **Srivastava, V., Mahara, T., Yadav, P. (2021).** An analysis of the ethical challenges of blockchain-enabled E-healthcare applications in 6G networks. International Journal of Cognitive Computing in Engineering, Vol. 2, pp. 171–179. DOI: 10.1016/j.ijcce.2021.10.002.
15. **Shukla, S., Thakur, S., Hussain, S., Breslin, J. G., Jameel, S. M. (2021).** Identification and authentication in healthcare internet-of-things using integrated fog computing based blockchain model. Internet of Things (Netherlands), Vol. 15, p.100422. DOI: 10.1016/j.iot.2021.100422.
16. **Nuzzolese, E. (2020).** Electronic health record and blockchain architecture: forensic chain hypothesis for human identification. Egyptian Journal of Forensic Sciences, Vol. 10, No. 1. DOI: 10.1186/s41935-020-00209-z.
17. **Mendoza-Tello, J. C., Mendoza-Tello, T., Mora, H. (2021).** Blockchain as a healthcare insurance fraud detection tool. Research and Innovation Forum 2020: Disruptive Technologies in Times of Change Springer International Publishing. pp. 545–552. DOI: 10.1007/978-3-030-62066-0_41.

Article received on 05/02/2023; accepted on 19/08/2024
**Corresponding author is Julio C. Mendoza-Tello.*