IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 28 June 2022, accepted 28 July 2022, date of publication 31 August 2022, date of current version 9 September 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3203193

RESEARCH ARTICLE

A System for the Promotion of Traceability and Ownership of Health Data Using Blockchain

RUI P. PINTO[1], BRUNO M. C. SILVA[1,2], (Member, IEEE), AND PEDRO R. M. INÁCIO[1,2], (Senior Member, IEEE)
[1]Department of Informatics, University of Beira Interior, 6201-001 Covilhã, Portugal
[2]Institute of Telecommunications, University of Beira Interior, 6201-001 Covilhã, Portugal

Corresponding author: Bruno M. C. Silva (bruno.silva@it.ubi.pt)

This work was supported by FCT/MCTES through the National Funds and when applicable co-funded EU Funds under Project UIDB/50008/2020.

ABSTRACT The advent of wireless technologies and the development of more and better globally connected mobile devices, leverage real time health monitoring. Mobile health (m-health) promise to deliver health services anytime and anywhere, improving user convenience and enabling faster diagnoses without the need to travel to healthcare facilities. The use of m-health applications on mobile devices with the support of cloud computing is nowadays a technology trend that has many advantages, but also poses several challenges, especially on the data storage and privacy. Blockchain technology is an exponentially growing technology used in various research areas from finance, voting mechanisms, production chains, among others. This technology provides important characteristics such as immutability, non-repudiation, transparency, and reducing the need for intermediaries. Hence, this paper presents a novel approach for blockchain technology applied to m-health systems. This proposal allows an easy and fast integration with other health systems or applications, allowing a patient-user to access their electronic health record in a more secure way. The data is traceable throughout the system, however, maintaining the necessary anonymity. Hence, a prototype for a blockchain-based solution using *Hyperledger Fabric* was developed. This implementation enables the creation of a chronologically organized and immutable health data record. To create an anonymous storage system, the proposed system uses two separate database components that maintain data traceability through sets of *IDs* stored in the blockchain. Furthermore, the development of the proposed system was evaluated in terms of performance and network configurations of the *Hyperledger Fabric*.

INDEX TERMS Blockchain, traceability, data, electronic health record, Internet of Things, mobile health.

I. INTRODUCTION

The continuous increase of the number of mobile devices all around the world in conjunction with significant improvements with wireless connectivity and mobile devices capabilities enabled the real-time monitoring of health-related events, transforming m-health in a hot research and development topic. Mobile devices, at the moment, are capable of much more than just share data. These are equipped with multiple sensors, allowing them to work as a fully-fledged monitoring device. Due to this technological evolution, health records can be transferred and updated, almost in real-time, between patients, healthcare professionals, and other authorized entities. M-health promotes the importance of self-care [1] by the user, allowing patients to become in control of their health records and reliably self-diagnose their symptoms [2]. Furthermore, m-health offers monitoring capabilities, in real-time, of various biometric information, improving the patient's convenience and allowing for a faster diagnosis and treatment without the need for constant travel to a medical care facilities [2]. The use of cloud computing in mobile applications is a very popular approach, however it poses several security challenges that can be mitigated with a correct implementation of blockchain technology [3]. Blockchain technology adoption is growing at an exponential rate, being used in a wide area of studies beyond financial

The associate editor coordinating the review of this manuscript and approving it for publication was Xiaolong Li.

uses (popularized by the application on Bitcoin), such as vote mechanisms, supply chain monitoring, Internet of Things (IoT), data security, and others. Blockchain introduced a decentralized way to implement secure transactions between nodes in an untrustworthy network through a consensus algorithm validating the transactions for all the nodes of the network. It offers important characteristics such as accessibility, immutability, and non-repudiation, creating transparent systems saving money and time by reducing the need for intermediaries. m-health can benefit significantly with the integration of blockchain technology. Any access, insertion, or modification of the data in the system is saved as an event in the blockchain granting immutability and non-repudiation to the system. However, the implementation of blockchain in healthcare systems must address some predominant problems. In a blockchain, usually, transactions are public, creating an incompatibility with the privacy needed in healthcare systems. Furthermore, in this type of implementation, where all the users are anonymous, it may be arduous to identify a specific registered user.

This article presents a novel blockchain-based approach for m-health solutions, for a secure patient-user access and traceability of electronic health records. This implementation enables the creation chronologically organized and immutable health data records traceable throughout the system yet, maintaining the necessary anonymity. To create this anonymous storage system, the proposed system implements two separate database components (personal data and health data) that assures data traceability through sets of IDs stored in the blockchain module.

Scenarios where chains of events are part of the business logic are immediate application scenarios for blockchain, leveraging the immutability and rastreability properties to provide strict assurances of where a process is at a given chain. In this work, we use blockchain as part of a system to keep an immutable track of the interactions between patients and doctors (e.g., consultations, prognosis or prescriptions) or, more generally, between patients and the healthcare system. This particular scenario has additional security requirements, since patient data is sensitive and needs to be stored off the blockchain. Per se, the blockchain only stores the records of the interactions, with apparently random links to sensitive data. Using the proposed system in the context of, e.g., manufacturing chains of products, would be possible, though the data structures would need to be adapted.

This work also presents a proof-of-concept to demonstrate and validate the proposed solution. The evaluation of the system is performed through the evaluation of the performance and network configuration of the blockchain (latency and throughput). The study of the quantity of extra storage needed for the proposed system and, the way that it communicates with other components in the environment. Therefore, the main contributions of this article are as follows:

- A review of the state of the art on m-health solutions integrated with Blockchain.
- A novel Blockchain-based m-health solution where anonymous health data is traceable thought the system.
- The performance evaluation and analysis of the presented proposal.

The remainder of the article is organized as follows. Section II presents a literature review about Blockchain based m-health solutions. Section III describes the proposed system, including the necessary security requirements, explaining the components for the proposed implementation. Section IV discusses the viability of the system and how the proposed system should operate in a real-world environment. The evaluation of the system and the analysis of the results are considered in section V, while section VI-A presents the conclusions and suggests future research work.

II. BACKGROUND

This section provides an overview of the key concepts related to health systems using Blockchain technology and how the integration of this novel technology manages to untangle some security issues related to m-health systems in addition to overview some leading work concerning the use of Blockchain technology embedded in a m-health system to provide traceability, immutability, and non-repudiation.

A. MOBILE HEALTH

As a result of the widespread usage of smart mobile devices and the evolution of wireless connectivity, mobile devices became able to do much more than just transfer information but also receive, store and directly process data [4]. From this development in the use and quality of mobile telecommunications technologies, together with the need for a more personalized health system where patients are allowed to control and monitoring their health data, emerged a novel area of studies known as m-health. A m-health system differs from traditional health systems by granting the patient personalized information about the current health record of the patient in a readable format available anytime and anywhere, without the need of a patient displacement to a medical facility assuring their privacy. Furthermore, the information is shared with the patient, increasing the transparency and the trust in the system by the user. Another advantage of a m-health system is the real-time monitorization, all the time, providing extra information about the health condition of the patient allowing the medical professionals to realize a faster and better diagnosis [5].This method of real-time monitoring and recording is particularly important in critical groups of patients like chronic patients, elderly patients, patients with disabilities and young patients [1]. For example, elderly patients are the group of patients most affected by isolation, chronic diseases and mobility impeachment, therefore the monitorization provided by a m-health system allows not only a better awareness of possible health problems preventing further problems, in addition to a potentially crucial reduction of the need for the elderly patient to physically travel to a medical facility [6]. However, these new technologies become very difficult to implement on a system already established without being completely ready to integrate these new technologies. Firstly, a m-health system needs to improve patient engagement since it is a vital part of the system. These m-health systems need to provide personalized guidance, enlightening the patients about the importance of caring about their health, providing alerts, and enabling support on-demand with medical staff. For this to happen, there might be a need for some organizational changes, varying from training medical staff to implement fully-fledged Information Technology (IT) departments to support the technical part of the system. This requires investment in a developing technology that can be seen as a negative point for full integration. From a technical viewpoint, the handling of healthcare information because of its delicate constitution must be made, so the privacy of the patient is never at risk, for that reason security and privacy must assume a dominant role in the system. Most of the challenges related to the handling of healthcare information stand on communication and storage issues based on where the information is stored, how it is stored, and how it can be accessed [7], [8]. Apart from data storage and communication, more requirements need to be fulfilled on a m-health system. Firstly, the system needs to abide by the regulations made by the countries to protect patients' privacy and security integrating to national and international standards and must be responsible for any problem that may occur [9]. The system must also be in continuous evolution regarding privacy, safety, and security with the implementation of new and better cryptography mechanisms when necessary. Despite all of these security requirements, it must be kept in mind that mobile devices can be easily stolen and damaged and that cannot jeopardize the security of the system [10]. Another important challenges that m-health, like any other system, needs to solve, are the human interactions with the system [11]. The system must be user-friendly and guarantee the usability and human-system interaction concepts presented in ISO 9241 [12]. The level of patient engagement is intrinsically associated with the usability of the system [11], [13], [14]. Another important aspect is the simplicity of the system, a simpler system for the user promotes the learnability of the system, reducing the need for more staff training and helps the patients to adapt to the system by themselves. A simpler system is, most of the time, more trustworthy for the user [15].

B. BLOCKCHAIN

Since the 80s and 90s, there were various researches on creating Byzantine-fault-tolerant consensus systems involving various computers that may be unreliable. The problem was that in an anonymous setting, these model systems were unable to deal with sybil attacks, where an attacker can create nodes until reaching the majority share of the system (51% attack). In 2008, the pseudonym Satoshi Nakamoto proposed a version of electronic cash using a peer-to-peer network that prevents double-spending without a trusted third party but also solves the problem of sybil attacks, called Bitcoin [16]. The innovation with bitcoin is the use of a decentralized consensus protocol using Proof of Work (PoW) as the way a node can interact with the system [17]. However, this technology called Blockchain enables Bitcoin electronic cash system but can be used for more than just electronic money, becoming the enabling force for commercial and academic purposes [1], [18]. Blockchain protocol is an immutable digital transaction ledger shared through a distributed network of nodes based on peer-to-peer. Each of these nodes maintains a copy of the ledger and works together to validate and certifying transactions, adding them to the ledger. If the transaction is considered valid, it is grouped in a block that contains a hash binding each block with the previous block [19]. In 2015, Ethereum, a public blockchain like Bitcoin first described in 2013 by Buterin in [17], surged, changing the focus of blockchain protocol from cryptocurrencies to decentralized applications due to the implementation of smart contracts built on the efforts of Szabo in [20], marking the second generation of the Blockchain protocol also called Blockchain 2.0. Smart Contracts are self-executing contracts inserted into the blockchain written into lines of code that automatically execute when a pre-specified set of rules between nodes are met. The use of smart contacts with Decentralized Applications (DApps) working on top of a blockchain originated a new generation of blockchain known as Blockchain 3.0. Based on a study of the potential for the use of blockchain technology in healthcare systems conducted by Kuo *et al.* in [21], there are five potential benefits for the use of blockchains compared with a traditional healthcare Database Management System (DBMS):

1) Allows the decentralization of the system, enabling the collaboration between healthcare facilities, healthcare professionals, and patients without an intermediary;
2) Provides immutable events suitable for evaluation or auditing;
3) Enables data traceability and ownership of data;
4) Ensures the preservation and availability of data;
5) Increasing the privacy and security of data.

When used in a correct manner, the use of Blockchain technology in m-health applications creates controlled access to critical health information using access control systems through advanced encryption and digital signatures to verify the identity of the user who owns the information. All the accesses and modifications to information are stored in an immutable history, preserving this information for any evaluation or auditing. Ultimately, blockchain technology grants credibility, immutability, and reliability to the data used by m-health applications, allowing m-health to be trusted and a valid alternative to traditional health systems. A traditional health system or even a cloud-based mobile health system has several advantages, but also several disadvantages, including a single centralized point of failure. I.e., cloud or a single server, where all the data sent/received is processed poses as an attractive target for attackers, being subdued to security and privacy threats on health data [22]. Health data can be susceptible to various threats, as clearly demonstrated by the increasing number of security threats and attacks on cloud-based systems and patient data since the first period of the COVID-19 crisis, including data breaches, tampering, and identity theft. A mobile health system could integrate the benefits of blockchain technology to provide: (i) a distributed ledger without a single point of failure [23]; (ii) privacy assurances by being possible to share data via transactions unreadable by other parties, and (iii) confidentiality, integrity, and availability, inherent to the distributed nature of the blockchain technology, with signed blocks linked to each other via hashes.

We decided to implement the system using a consortium blockchain since it performs better than public blockchains. The consortium blockchain platform chosen was Hyperledger Fabric because, on the one hand, it is completely open-source and, on the other, it is more modular than other consortium blockchains such as Corda or Quorum.

C. RELATED WORKS

In the work done by Motohash *et al.* [24] a m-health system using Blockchain was proposed. Blockchain technology intrinsic characteristics are perfectly fit for providing reliability and immutability to m-health data without any third-party contributor. However, the mobile devices used by the patients need to be authenticated and validated to avoid impersonation attacks to ensure the reliability of the data. The system purposed uses a client hash chain created in the patient mobile device and registered in the blockchain network. It was utilized Hyperledger Fabric v1.0 [19] to implement the blockchain network. A private blockchain network was chosen for the management of medical data because of the node control of the stakeholders and since it is a private network it is possible to use different consensus protocols other than PoW allowing for the processing of more transactions. The authors tested this system in a m-health for insomnia treatment, where medical data was successfully registered and simulated illegal data was correctly identified.

Nguyen *et al.* [25] propose a novel Electronic Health Record (EHR) sharing framework combining blockchain and decentralized InterPlanetary File System (IPFS) on a mobile cloud platform. EHR on mobile cloud environments enables high flexibility and availability, facilitating medical data exchanges between patients and healthcare providers. Nevertheless, this flexibility and availability come with concerns about network security and data privacy. The objective of the work of the author was to guarantee high-security levels in the mobile cloud used to share EHR. For the implementation, it was deployed a private Ethereum blockchain network on Amazon Web Services (AWS) where various virtual machines were used as admin, as miners, and EHR manager. Since it is impossible to share and store large portions of data on a blockchain, causing scalability problems, a decentralized peer-to-peer IPFS was used to build a file system sharing platform in the blockchain network.

For handling protected health information generated by IoT devices, Griggs *et al.* [26] proposed the use of blockchain-based smart contracts for the management of medical sensors securely. To that end, a system using a private blockchain based on Ethereum was created, where the IoT sensors communicate with a smart device to execute smart contracts saving records of all events on the blockchain. The blockchain doesn't store confidential medical information, only storing the records that an event occurred. Medical data is stored in an EHR database, adding a new transaction to the blockchain stating the processing of the data.

Zhang and Lin [27] presented a blockchain-based secure and privacy-preserving Protected Health Information (PHI) sharing scheme to be used to improve diagnosis in e-health systems. This implementation uses two different types of blockchain, private and consortium blockchain owned by a group of entities. The private blockchain was used to store, PHI while the consortium blockchain was used to secure the indexes of the PHI. The block generators are required proof of conformance to add a new block to the blockchain that is, the verifier needs to verify the block, checking if the PHI is generated by an authorized doctor.

To protect medical data from tampering, deletion, and theft, Li *et al.* [28] proposed a novel system based on blockchain technology applied to the data preservation of medical data. The blockchain framework together with cryptographic algorithms enables the protection and immutability of the protected storage data. This system was implemented on the public Ethereum platform. According to the authors, the system displays effectiveness and efficiency during testing yet, there are still some storage optimization problems since each transaction contains a small amount of content, wasting some usable space. To write on the blockchain is invoked the *writeInBlockchain()* program working in different ways if the data is text type or various multimedia files. If the data is a text file, it is used the SHA-256 algorithm to calculate the hash of the original data combined with the encryption of the original text using the AES cipher algorithm and then is written in the blockchain directly. On the other hand, if the data are multimedia files, the data encrypted in conjunction with the hash of the original data along with the encrypted index of the file's location is written in the blockchain.

Ichikawa *et al.* [29] developed a m-health system for cognitive behavioral therapy for insomnia using a smartphone app. The objective of this system was to evaluate the tamper resistance of data against inconsistencies caused by artificial faults in a m-health system using blockchain technology. This system used a private Hyperledger Fabric network so that every electronic health record sent to the network was capable to resist tampering and revision. The network was composed of four validating peers controlling the blockchain, and one membership service authenticating the client and the validating peers. To reach consensus among the validating peers, the system used the Practical Byzantine Fault Tolerance (PBFT) algorithm. In the study, the system was successful to prevent tampering and revision yet, the authors raise two limitations with the system. Firstly, the implementation around the blockchain technology is vulnerable and can be attacked. Second, the PBFT algorithm used to obtain consensus is vulnerable if (N-1)/3 of the validating peers are attacked at the same time, disabling the blockchain.

Brogan *et al.* [30] proposed a new system to use a tamper-proof distributed ledger to share, store, and securely retrieve encrypted data. To tackle this challenge, the Masked Authenticated Messaging extension module of the IOTA protocol was used. The IOTA protocol is an open-source distributed ledger created to record and execute transactions between devices and machines in an IoT ecosystem. IOTA, by not using the concept of mining and miners, reduces the latency and fees required on most of the blockchain-based distributed ledgers. As previously mentioned, the IOTA's Masked Authenticated Messaging extension was also used, allowing the encryption and authenticating of data streams transmitted through the network as zero-value transactions that are transactions without the need for IOTA tokens. Masked Authenticated Messaging also allows post-quantum cryptography and forward transaction linking.

In the paper [31], Mallick and Sharma proposed an IoMT framework featuring Blockchain technology. The framework named Electronic Medical Record Infrastructure (EMRI) makes use of smart contracts for privacy preservation of the information of patients, allowing for scalable and secure communication. The introduction of smart contracts enables the privacy of information without the need for a trusted third party as in traditional centralized IoMT architectures. To reach consensus and block validation the proposed framework utilizes Proof-of-Work (PoW) avoiding that the failure of a single node manages to compromise the entire network while also allowing for better scalability. Although the use of PoW allows for better scalability and security, the use of this consensus algorithm is of high consumption of time and computational power making this an implementation with high latency, not ideal for IoMT solutions.

Gao *et al.* [32] proposed a framework employed with Hyperledger Fabric and Intel SGX (Software Guard Extension) in order to utilize blockchain technology for authentication of IoMT devices and cloud service providers and for providing an access policy management mechanism for health data. In this work, the software guard extension technology is integrated with edge computing, ensuring the integrity and confidentiality of IoMT data. For the authentication of the IoMT devices the proposed system utilizes the Certificate of Authority of the Hyperledger Fabric Network and utilizes the smart contracts of the Hyperledger Fabric Network to manage all the data and accesses policies of the IoT devices.

To develop Personal Health Records capable of being shared without having their security compromised and privacy leaked, Wang *et al.* presented in [33] a blockchain-based PHR management and sharing system using a consortium blockchain (Hyperledger Fabric) and InterPlanetary File system technology. The IPFS technology is used to store the PHR encrypted information of the IoMT. Smart contracts are utilized to reach secure search, access control, and preservation of privacy. To achieve anonymity in storage without divulging the patient's privacy, the system utilizes zero-knowledge proof and attribute-based encryption.

Table 1 shows a short overview of the studies referenced in section II-C. Even though there are various implementations of blockchain in m-health systems and healthcare, none of the solutions found are completely similar to the proposed implementation.

III. SYSTEM REQUIREMENTS AND CONCEPT

This section presents the system requirements and concept. Namely, an m-health system integrated with blockchain technology. This system brings benefits regarding information ownership, data traceability, and anonymity while enabling interoperability and integration with existing systems. The proposed system architecture is established by three crucial modules: a blockchain module where all the new interventions events are stored, the database component where personal information and healthcare information is stored, and finally, the application and Application Programming Interface (API) where the users can communicate with the after-mentioned modules.

A. SYSTEM REQUIREMENTS

Several requirements can be identified by being crucial for a m-health system. These requirements serve as a guideline during the implementation of the system, and the fulfillment of them is fundamental for the implementation m-health system.

Table 2 lists and describes some non-functional and security requirements necessary for a blockchain assisted m-health system. The first requirement listed on the table is Anonymity, in other words, the health information must not have any identifiable element related to the personal information of the patient. Secondly, confidentiality is of extreme importance when handling personal information and medical information, so keeping this data secure and secret from any other identity is critical. Following this, it is listed the requirements of interoperability and link-ability. These requirements are important to the system by the sheer need for integration with other systems with minimal alterations. Another needed requirement is the implementation of non-repudiation and logging. These requirements can be met by utilizing blockchain technology, enabling the preservation and privacy of data while guaranteeing the non-repudiation of data inserted by a user. The system must also be designed with performance and availability in mind. The integration with blockchain technology must not bring noticeable performance and availability downgrades for the end-user. Ultimately, all the users in the system must be authenticated, where access to any data in the system must only be possible by authentication. The proposed system should integrate and comply with the previously described requirements in order to be considered suitable.

TABLE 1. Review of the studies introduced in section II-C and the proposed system.

Name	Published Year	Problem	Solution	Blockchain Network	Consensus
Daisuke Ichikawa et al. [29]	2017	Evaluate the tamper resistance of data against inconsistencies caused by artificial faults.	Blockchain supported system with four validating peers controlling the blockchain and one membership service authenticating the client and the validating peers.	Hyperledger Fabric	PBFT
Kristen Griggs et al. [26]	2018	Handling protected health information generated by IoT devices.	Sensors communicate with smart devices calling smart contracts supporting monitoring, send notifications, and maintain a secure record.	Private Ethereum	PBFT
Aiqing Zhang et al. [27]	2018	Improve diagnosis in e-health systems.	Using private blockchain of a medical service provider to store patient's encrypted PHI and a consortium blockchain keeping record of secure indexes.	Juzhen	Proof of Conformance
Hongyu Li et al. [28]	2018	Protect medical data from tampering, deletion and theft.	Blockchain-based data perservation system.	Ethereum	PoW
James Brogan et al. [30]	2018	Develop a tamper-proof distributed ledger system to share, store, and retrieve encrypted data securely.	Masked Authenticated Messaging extension module of the IOTA protocol	IOTA Tangle	-
Dinh C. Nguyen et al. [25]	2019	Guarantee high security levels in the mobile cloud used to share EHR.	Used a decentralized P2P IPFS to build afile system sharing platform in the blockchain network.	Private Ethereum	PoW
Tomomitsu Motohashi et al. [24]	2019	Avoid impersonation attacks on patient's mobile devices.	Client hash chain created in the patient mobile device and registered in the blockchain network.	Hyperledger Fabric	PBFT
S. R. Mallick et al. [31]	2021	Privacy preservation, without the need of a trusted third party, enabling scalable and secure communication.	Makes use of smart contracts for privacy of information preservation without the need of a trusted third party.	Ethereum	PoW
Y. Gao et al. [32]	2021	Authentication of IoMT devices and cloud service providers and, access policy management mechanism for health data.	Utilizes the Certificate of Authority of the Hyperledger Network to manage data accesses policies of the IoT devices. To ensure the integrity and confidentiality of data, a junction of Intel SGX and edge computing is used.	Hyperledger Fabric	RAFT
Y. Wang et al. [33]	2021	The data sharing process of PHRs leads to privacy leakage and security compromises.	Utilizes IPFS and Blockchain technology in junction with cryptographic primitives and smart contracts to achieve secure search, privacy and access control.	Hyperledger Fabric	PBFT
Proposed System	2022	EHR system allowing for integration with other applications while having data traceability yet maintains anonymity throughout the system.	Utilizes blockchain technology injunction with databases in order to create an immutable health data record, maintaining anonymous storage through sets of random IDs stored in blockchain transactions.	Hyperledger Fabric	RAFT

B. SYSTEM PROPOSAL

The proposed model consists of three major components, namely:

1) **Blockchain Module** - encapsulates all the components of a Hyperledger Fabric network. Provided a blockchain solution to store intervention

TABLE 2. Requirements for the blockchain assisted m-health system proposed.

Requirements	Description
Anonymity.	Personal information and medical records connected to a user of the system must be anonymous.
Confidentiality.	The m-health system must ensure the confidentiality of the stored data encompassing personal information and medical records.
Interoperability & Link-ability.	The system must be capable of linking with other systems, guaranteeing the ability to exchange data and communicate with other systems.
Logging for evaluation or auditing.	Events should be stored, preserving the integrity and privacy of data.
Non-repudiation.	After recording the data in the system by a user, the user cannot deny the insertion of the data.
Performance.	High transaction throughput performance & low latency of transaction.
Preservation and availability of data.	Data must remain unaltered and be available to the users when needed.
User authentication.	All users of the system must be identified.

events and utilize some capabilities of blockchain technology;

2) **Database Module** - encapsulate all the databases utilized to store personal data and health care data separately. This module was implemented using a SQL solution with MariaDB;
3) **Application and API** - encapsulate all the applications and API utilized, allowing the users to communicate to the blockchain module and the database module. NodeJS was used to create the API by handling concurrent requests in an efficient and lightweight way.

Figure 1 illustrates the proposed system using a UML component diagram. The first component on the application of the patient and medical staff is the Authentication component that needs to be implemented to guarantee that any access to data from the system is made by an authenticated user. During the register phase of a new system user, the application receives data that will be sent to the specific API. That data is then used to generate X.509 digital certificates to implement wallets to interact with the blockchain module.

Another important component inside the application of the user is the possibility to view health data records. Furthermore, the application of the medical user allows for the access of health records from various patients if the medical staff is in charge of any treatment or diagnosis. The system can and will be integrated with already developed mobile device applications for the user (patient) and a web application for the medical professional user.

The data is sent to an API, which will deal with the data, creating events in the blockchain and saving data in a medical record database. The application is able to communicate to the API via Hyper Text Transfer Protocol Secure (HTTPS) and as aforementioned, the Backend component communicates with the blockchain module ledger by invoking the smart contracts.

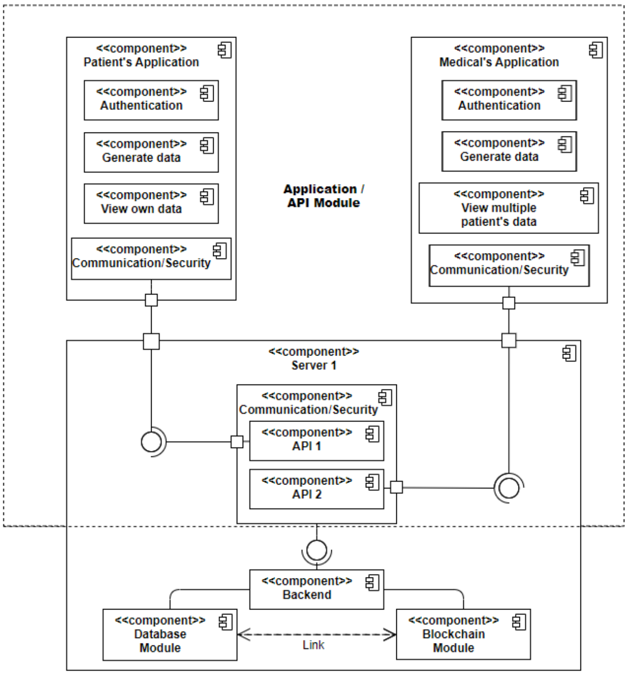

FIGURE 1. Component diagram of the proposed system.

1) BLOCKCHAIN MODULE

The Blockchain component of the system is responsible for the storage of an event with a proper classification (named intervention event), an identifier for both users partaking in the event (medical professional and patient), and a link to a EHR database that stores the data received during the intervention. The data collected is stored outside the blockchain to resolve problems of scalability associated. Furthermore, every query to the blockchain will also be stored as an event in the ledger.

To create the blockchain component, the blockchain framework known as Hyperledger Fabric was used. This decision was made based upon the analysis of the popularity and broad acceptance of this framework combined with the scalability and performance capabilities provided [34], [35]. It is also a modular system purposefully created to develop distributed applications [19] without needing to write Smart Contracts with a native programming language and without the need for paying transaction fees with a native cryptocurrency [35].

For the implementation of the blockchain module, Hyperledger Fabric v2.3.1., released on February 2021, was used. All the components needed for the Hyperledger Fabric implementation execute in Docker containers communicating via RPC. To create all the chaincode, the Go programming language was utilized. With it, it was created chaincode capable to integrate with the API module allowing the use of two key functions:

1) `CreateIntervention` - inserts an intervention on the blockchain referencing two users, the type of intervention, and a link between the blockchain module and the database module.
2) `GetInterventionbyID` - fetch all the data from an event based on a unique ID given.

The chaincode was installed onto the peer nodes and instantiated on the channel where all the peers are members. For the deployment of this concept and to study the capabilities of the Hyperledger Fabric framework, it was implemented a network topology with three peer organizations and one orderer organization. Each organization has an endorsing peer and a separate Certificate of Authority responsible for the creation of X.509 digital certificates for peers, users and administrators, determining the permissions and access that these actors have in the blockchain network. Each one of the peers has a current state database implemented in couchDB (NoSQL solution) isolated in a Docker container.

2) DATABASE MODULE

As aforementioned, storing all the data in the blockchain module is unachievable by facing various scalability problems. The implementation of the database module tries to solve this problem by recording the healthcare information on a EHR database and using a link on a blockchain transaction, recorded on the blockchain, to access this information.

Figure 2 illustrates a Relational Model, with the crucial tables chosen to guarantee the basic functionalities of the system and the data traceability needed. This model also allows the removal of the identifiable personal information from the healthcare information recorded in the EHR. The connection between the blockchain module and the database module is also depicted in figure 2. This connection is possible by storing, on the blockchain, an identifier for each user in the transaction and recording the unique ID working as a link between the transaction and the EHR.

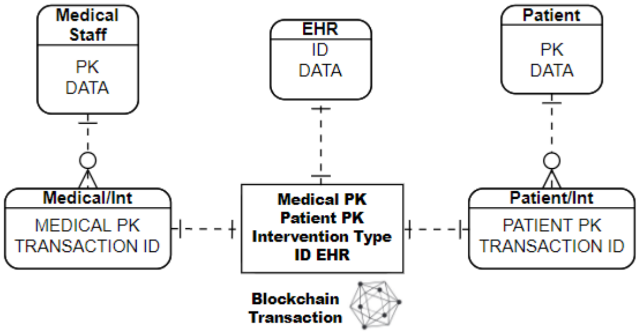

FIGURE 2. Relational Model defining the intercommunication between the parts of the system (though, the blockchain component uses different technology).

This separation, dividing the database module in two parts, by the blockchain model, was made with the intent of not having a direct connection between half of the database module that stores personal information and the other half of the database module that stores medical information. Having this separation, not only allows for the decentralization of the database module yet also solves the problem of having the anonymity of medical information whilst maintaining data traceability in the system by the blockchain module.

The healthcare data and personal data separation provided by this system model can aid in the requirement to guarantee the confidentiality of medical records and individual information. Furthermore, the separation of identifiable personal information from the healthcare records guarantees anonymity, enabling the use of real healthcare information in medical research and studies.

We fulfill the privacy requirement by keeping the private data in a database with access control mechanisms, to then leverage the blockchain properties (such as immutability and incremental nature) to maintain the records of the data insertion, modification or erasure. Using this approach, we use the best of both worlds (legacy structured databases and blockchain). The blockchain is used to preserve the artifacts of data transactions, and keeping links to the private data inside of the controlled database. These links are randomly generated, included in the several blocks, and they can be followed only by the truthful owners of the data, while being untraceable and unmeaningful to other users. These can be understood as the signing of healthcare records.

3) APPLICATION AND API MODULE

The API and application module is the set of applications and APIs utilized in this system, allowing the end users to communicate with the other modules of the system. The applications used by the system can be divided in two different types of applications. Firstly, there is the patient application, capable of receiving data from patients collected by IoT sensors. The other type of application, planned, is a web application to be access by a health service providers to access healthcare records from various patients. The interoperability needed in this system is guaranteed by the implementation of a API used primarily to facilitate the communication between the applications and the blockchain module.

This API is implemented in order to submit a transaction to the ledger of the blockchain module and to store data in the database module. To do so, the API follows the steps necessary to submit a transaction to the ledger, defined in the Hyperledger Fabric documentation. First, locates the wallet, containing the X.509 digital certificates of the user, in the file system, used to access the Hyperledger Fabric network. In second place, connects to a gateway, identifying the peers that provides access to the network. After having access to the network, it is possible to create transactions requests for a smart contract to be submitted to the network. After the submission, the API handles the response, communicating a successfully or not submission of the smart contract. To communicate between the API and applications, it is used a Hyper Text Transfer Protocol (HTTP) request link facilitating the integration of the applications to the system, with the goal of enabling CRUD operations on the system.

IV. SYSTEM ASSESSMENT ON A REAL LIFE SCENARIO

This section serves the purpose of discussing the possible implementation of the system in a real environment. This will also allow a better understanding of how the proposed system concept can meet the requirements previously defined. Although the system could not be integrated with a real testbed environment, the system as a whole was tested using a pre-defined set of possible test values included in common Personal Health Record collections.

A. PROOF-OF-CONCEPT

In this section, the functionality and the *modus operandi* of the proposed system, in a real environment, are explained in detail. To aid in this task, Figure 3 illustrates an activity diagram depicting the integration between the different modules of the proposed system.

In the first place, a health care provider employing medical devices or a patient using a m-health device needs to gather medical data about the patient. This medical data could fall into various categories as Patient/Disease registries, health surveys, or even more complex data like fully-fledged EHR. Before connecting to the proposed system, there needs to be a robust authentication and communication system to support the proposed system. To validate the system and guarantee security, privacy and the identity of the user, this authentication and communication system must implement several SOTA cryptography techniques based on elliptic curve cryptography, public-key cryptography, SSL and several key exchange protocols. The gathered data is sent to the API module that stores the data in a database module and generates a link to connect the blockchain module to the health record database and stores the transaction identifier on another database implementation.

The blockchain transaction is created by invoking the chaincode function `CreateIntervention` containing an identifier for the transaction, an identifier for the wallet of the medical provider, an identifier for the wallet of the patient, and a link to the database module containing the health record data.

If a medical provider needs to verify the health care data of a patient, firstly they need to successfully authenticate, while accessing an application for the purpose of querying the database module and select the identifier of the transaction intervention needed. With this identifier, connecting with the API enables the medical provider to invoke the chaincode function `GetInterventionByID`, keeping a record of the access and returning the transaction containing the link to the database row with the health care records needed.

The process of accessing own health records by a patient is really similar to the method explained for the medical provider. First, the patient must authenticate with success and connect to the personal record database via an external application. After this, it is necessary to query the database until the intervention transaction identifier is found. Using this identifier and invoking the chaincode function `GetInterventionByID`, the transaction is returned with the link for the database row containing the health care records needed.

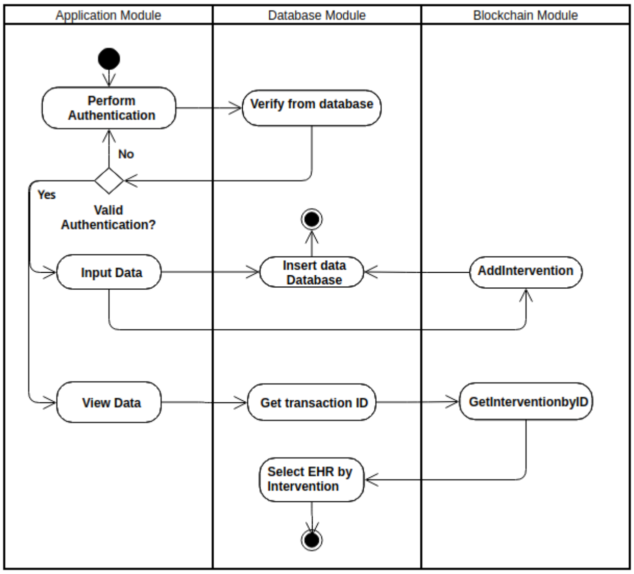

FIGURE 3. Activity Diagram depicting the flow and the integration between the three modules of the system: Application, Database, and Blockchain.

The possibility of having the availability of personal health records grants the patient more information and more ownership of the health records. In the case of auditing, a user with admin privileges on a peer can access and gather all the transaction records from the blockchain, working as an immutable log. In this case, the auditor cannot access any health care information, but can collect access records and intervention records with the identifiers of the users in the system.

For the purpose of scientific research, since there is a separation of the data by the system (medical records and personal records are completely separated by the system unless accessing the blockchain module) it is possible to give access to the database storing the medical records without putting the personal records at risk. In such a manner, the described implementation of the proposed system allows the traceability of the data while keeping anonymity, enabling the possibility of implementing applications to promote the ownership of health records by the patient.

B. SYSTEM VIABILITY AND VALIDATION

For the proposed system to be considered viable, it must be able to fulfill the requirements provided in Table 2, in section III, needed for a blockchain m-health system. To validate and test the viability of the proposed system, a full-fledged prototype was implemented. In such a scenario, validation is a mixed exercise of testing the prototype and intellectually analyzing how the security requirements are met by the combination of the employed technologies. The prototype was implemented by combining a consortium blockchain solution (Hyperledger Fabric) with a database module, and several practical and functional tests were performed to assess viability. The prototype proves that the system is viable and highly scalable, since it decouples private or sensitive data from rastreable data, and allows for different parts of the system to work in different machines or containers. The proposed and prototyped system fulfills the security requirements in the following manner:

The first requirement defined was the anonymity of medical data in the system, particularly the separation between the personal information and the medical records associated with a patient. As aforementioned, the system utilizes two separate databases, one to store personal information and the other to store medical records. These databases do not have any connector between them in the database module, being necessary to connect to the blockchain module to query the health care database with data derived from the personal record database.

Another requirement was the concept of ensuring the confidentiality of the data stored data (personal and medical records). On that account, it is necessary the implementation of SOTA cryptographic techniques for the communication between the applications and the API and blockchain modules in order to protect information from unauthorized access. It will also be necessary to separate and protect organizations and correspondent peers in order to minimize the risk of potential successful attacks.

An additional requirement established was the necessity for the proposed system to be interoperable and linkable with other applications and exchange data with another system. This type of implementation is possible on the proposed system for two different reasons. First, the blockchain module of the proposed system is implemented using a Hyperledger Fabric network. Hyperledger Fabric is a modular technology with the possibility to scale and connect new organizations and peers to already established channels. Secondly, the API module allows communications with other applications and systems with a simple REST request.

Auditing and logging of information are essential in healthcare services, or to any public service for that matter. The implementation of blockchain technology in a m-health system brings various major factors to facilitate and secure auditing and logging. Firstly, a blockchain implementation can establish a repository of audit logs for each organization present in the channel, making the collection of data simpler. Second, due to the immutable characteristics of the blockchain, the audit log data is ensured to be unaltered preserving the necessary information. Finally, the use of smart contracts in the blockchain creates a predefined structure for every transaction, standardizing the audit log.

To fulfill the requirement defined as non-repudiation, the Hyperledger Network, which composes the blockchain module of the proposed system, employs a PKI certificate system with the characteristics necessary to guarantee the non-repudiation of the data inserted.

Regarding performance, the proposed system utilizes a private blockchain that greatly improves the throughput and latency compared to a public solution. The chaincode invoked is also simple with reduced data without the need for substantial computational power. Another important factor achieved by an implementation with Hyperledger Network is the separation between the ordering service (service responsible for a consistent and final blockchain state) and the peers, providing many advantages in terms of performance and scalability. The performance of the proposed system in a test environment was evaluated and is analyzed deeper in section IV.

To guarantee the preservation of the data and immutability, the system utilizes a blockchain module that stores any invocation of the chaincode. Blockchain technology, by working as an append-only log of transactions grouped into immutable blocks by the cryptographic hash of the previous block, creates a structure where data cannot be altered.

V. PERFORMANCE EVALUATION

In this chapter, the performance of the proposed system and the Hyperledger Fabric network are evaluated. This performance evaluation was composed of various tests in order to test the configuration of the Hyperledger Network and the entire system. To guarantee the reproducibility of the data acquired during the system testing, all environment parameters of the test network utilized will be listed. These considerations were made based on the white paper by the Hyperledger Performance and Scale Working Group [36]. This test network was implemented on a remote virtual server with 4 GB of RAM, 2 cores, and a processor clock speed of 3000 MHz running an installation of Ubuntu 20.04.2 LTS. Hence, it can be stated that referring to the geographic distribution of the nodes utilized in the test environment, all the nodes in the system are located in the same machine. In relation to the network model, a simple network with three organizations was utilized, each one with one node (three nodes total) on which all the transactions are broadcasted in between. The consensus protocol chosen was RAFT by being the easiest to implement and the only one fully supported by the documentation of Hyperledger Fabric. Concerning the peer state database utilized, CouchDB state database was utilized, to execute complex queries using data values instead of keys. As explained in previous chapters, the system also uses a database component using MySQL, creating a SQL connection for each transaction executed.

As for the characteristics of the transactions, a simple chaincode with two functions was created, one capable of creating a new transaction and inserting new data based on the data received and a function capable of retrieving JSON data based on previously inserted data by receiving an ID value. In the beginning of the evaluation, the size of the block in the set test model was of a maximum size of 99 MB per block but with a preference for blocks of 512 KB of size with a maximum of ten transactions per block. To generate the test load, a Python script capable of inserting large quantities of data was utilized in junction with the software Postman to test the API capabilities to receive and send data from the blockchain by a HTTP POST request.

Finally, Hyperledger Caliper was installed, to be used as a blockchain benchmark tool for the Hyperledger Fabric network. With this tool it was possible to test and evaluate performance indicators such as throughput, latency and scalability.

A. HYPERLEDGER FABRIC EVALUATION

Performance was evaluated by gauging the ramifications of changing the block size and the number of transactions per block. To better grasp these changes, two types of metrics were used: Latency (Amount of time from the point that the transaction is submitted to the point that the result is available to the network [36]) and Throughput (Rate at which valid transactions are committed in a defined time. Measured in TPS [36]). In such case, the chaincode functions, `CreateIntervention` (used as a write operation to create an event) and `GetInterventionByID` (used as a read operation, returning an event) were tested. The tests were performed using Hyperledger Caliper, sending 1000 transactions at a rate of 100 per second. The fields in the events were generated randomly based on groups of possible real data values.

Figures 4 and 5 illustrate the results acquired for each function while changing the size of the blocks. In the case of the test of throughput (Figure 4), all the data gathered indicates a very similar TPS values across all the block sizes, with an average of 35,60 TPS when using the chaincode function `GetInterventionByID` and 31.14 when using the chaincode function `CreateIntervention`, both with a small deviation of less than 0,4. The values gathered in the test of latency (Figure 5) indicates a similar behavior to the throughput test, with very similar values across all the changes in the size of the block. In this case, there is an average latency of 15,17 seconds while using the chaincode function `CreateIntervention` and an average latency of 12,65 using the `GetInterventionById`, with a small deviation below 0,24.

In each of the plots, the average latency and the throughput measured remained stable, without any real peak or any substantial change. This stability can be attributed to the test environment utilized. In this test environment, the nodes are geographically deployed on the same machine, causing a low propagation time across the network, leading to unnoticeable changes when altering the block size.

Figures 6 and 7 illustrate the results obtained for the functions while modifying the number of transactions per block. From the results presented in figure 6, it is observable that increasing the number of transactions possible within a block, increases the throughput. This behavior was expected and is in line with various other Hyperledger Fabric TPS evaluations [34]. In this case, the maximum TPS was achieved at 150 transactions per block during writing operations (`CreateIntervention`) with 46,7 TPS and at 175 transactions per block during the read operation (`GetInterventionByID`) with 55,4 TPS.

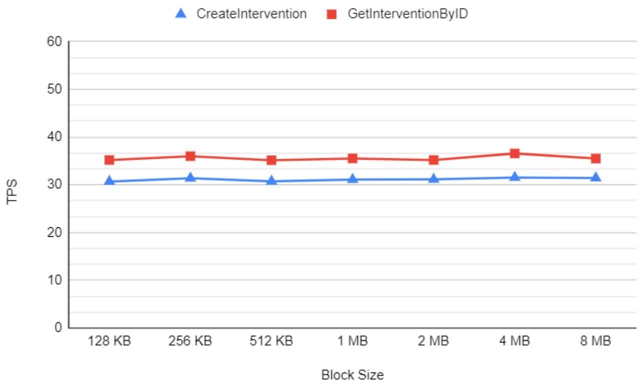

FIGURE 4. Results of throughput (measured in TPS) of the Hyperledger Fabric network and chaincode functions used, while varying the block size (using 10 transactions per block).

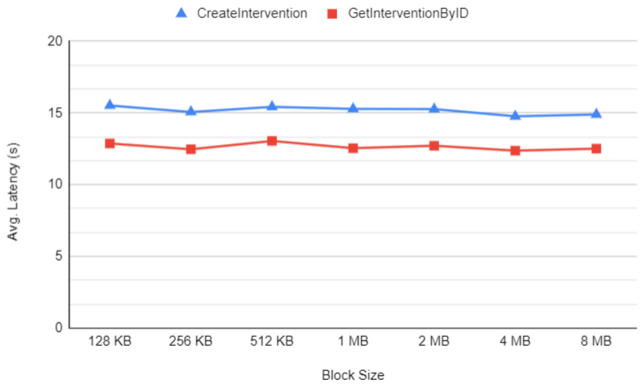

FIGURE 5. Results of latency (measured in seconds) of the Hyperledger Fabric network and chaincode functions used, while varying the block size (using 10 transactions per block).

Regarding latency, there is a drop in latency while increasing the number of transactions per block until a certain point. After reaching 50 transactions per block, the values of latency reach a plateau, with no significant change.

It is important to remind that the evaluation of a Hyperledger Network is intrinsically connected to the test environment used for the System Under Test (SUT). In this case, some hardware choices are not ideal to test this system, creating evaluation results that may differ from a real implementation. Any change in the hardware running the network could then achieve completely different test results without changing the network model.

The performance results obtained are similar to the results other implementations achieved [34]. However, it is important to analyze that the structure of the network and the hardware specifications of the test environment are different from system to system and these two factors have a great deal of importance in performance variance, therefore, comparing performance results from different test environments might be ineffective.

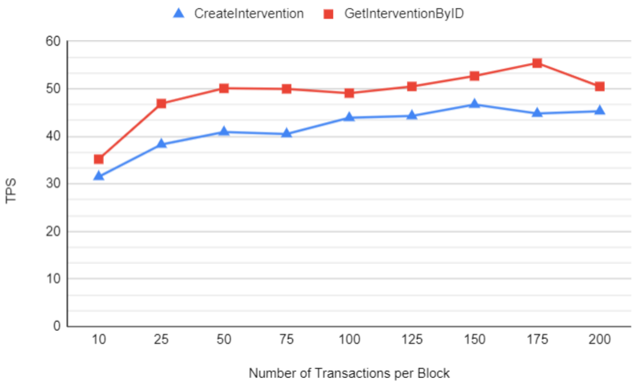

FIGURE 6. Results of throughput (measured in TPS) of the Hyperledger Fabric network and chaincode functions used, while varying the number of transactions per block (using a block size of 2 MB).

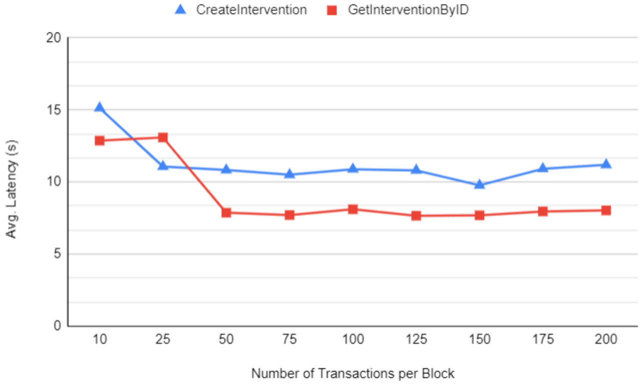

FIGURE 7. Results of latency (measured in seconds) of the Hyperledger Fabric network and chaincode functions used, while varying the number of transactions per block (using a block size of 2 MB).

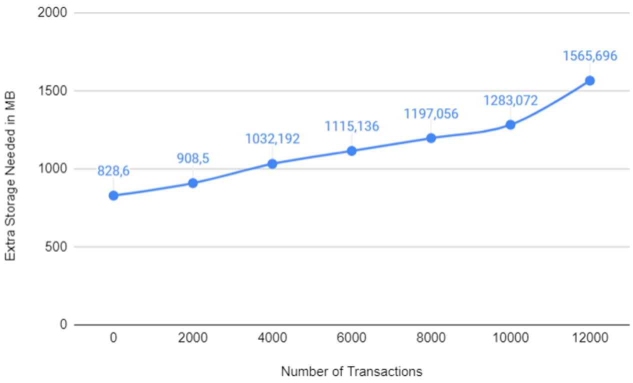

FIGURE 8. Extra storage necessary to implement blockchain technology to traditional healthcare records.

B. EXTRA STORAGE EVALUATION

To test the extra storage necessary to implement the proposed system, numerous transactions were created in the Hyperledger Network and after each batch of insertion, the amount of disk space used was observed and noted. For that purpose, Hyperledger Caliper was, once again, used to create the various transactions. After each 2000 transaction group, the amount of disk space used by the Docker containers and the local volumes containing the components of the blockchain was recorded. Figure 8 illustrates the amount of disk space used in each group of transactions.

According to the collected data, there is an average increase of 11% for each group of 2000 transactions created. It is important to keep in mind that these evaluation results are based on the test environment described in section IV with a Hyperledger Fabric network with 3 organizations, each with 1 peer, hosting ledgers, and smart contracts.

The assessment of the fundamental properties of blockchain applied to healthcare information compared to the amount of storage necessary to apply this type of technology is an underlying step for the implementation of any type of blockchain in a healthcare system. Ultimately, it is important to bear in mind that the confidentiality, integrity, and immutability capabilities of the blockchain comes with the cost of increasing the storage needed in any system.

VI. CONCLUSION AND FUTURE WORK

A. CONCLUSION

In this work, the main objective was to grasp the possibility of implementing a system integrating m-health with blockchain technology with methods for health data traceability while keeping anonymity and enabling the promotion of health data ownership. To accomplish the defined objectives, an analysis of the mechanisms and systems that use an integration of blockchain with m-health systems or that attempt to improve EHR systems using blockchain was conducted [1], [24], [25], [26], [27], [28], [29], [30], [31], [32], [33]. Based on this analysis, it was clear enough that the proposed system should have a database component, to store off-chain data impossible to store in the blockchain itself, a blockchain component, to use the advantageous capabilities of blockchain for immutable transactions control and an Application/API to enabling the communication between the user and both of the other components. The proposed method demonstrates that not only the integration of blockchain with m-health is possible but also beneficial, providing a secure way to store transactions (interventions or data collection in this case) and providing an immutable and auditable append-only log of transactions shared by the participants of the network. The system submitted also enables the separation of personal data from health data, as a result of the separation of the system in an on-chain module and an off-chain module. This separation allows for anonymity of the health data while allowing the traceability of the data across the complete system.

In conclusion, the integration of blockchain with IoT and m-health systems is still in its infancy, yet the advantages gained by having an immutable distributed log of transactions are undeniable. With the constant evolution of blockchain implementations, with fewer costs and simpler deployment, and with the creation of new and improved methods for off-chain storage, IoT system integrated with blockchain technology will surely become the standard for m-health implementations. Therefore, the two major findings of this work are 1) traceability of health data (EHR) through blockchain is feasible and proved by the evaluation results presented in the paper; and 2) Privacy can be achieved by using the combination of off-chain storage technology with blockchain, to cope with privacy requirements in an efficient manner.

B. FUTURE WORK

With the increasing number of entities (organizations, peers, and users) participating in the network, it is necessary to ensure the performance levels remain at a defined level to guarantee to keep the quality of the services of the system for all the entities in the system. To improve possible scalability issues (increased latency) with the increasing number of transactions per second and the increased block size, it could be implemented a sharding protocol for permissioned blockchains [37]. However, the implementation of sharding mechanisms is not a simple and definitive solution for all scalability issues, which is out of the scope of this paper.

REFERENCES

[1] J. Santos, P. Silva, and B. Inácio, *A Blockchain System for Mobile Health Applications and Services*. Covilhã, Portugal: Universidade da Beira Interior, 2019.

[2] S. Steinhubl, E. Muse, and E. Topol, "Can mobile health technologies transform health care," *Jama*, vol. 310, pp. 2395–2396, Dec. 2013.

[3] D. D. Taralunga and B. C. Florea, "A blockchain-enabled framework for mHealth systems," *Sensors*, vol. 21, no. 8, p. 2828, Apr. 2021. [Online]. Available: https://www.mdpi.com/1424-8220/21/8/2828

[4] S. Kumar, W. Nilsen, M. Pavel, and M. Srivastava, "Mobile health: Revolutionizing healthcare through transdisciplinary research," *Computer*, vol. 46, no. 1, pp. 28–35, Jan. 2013, doi: 10.1109/MC.2012.392.

[5] B. M. Silva, I. M. Lopes, J. J. Rodrigues, and P. Ray, "Sapo fitness: A mobile health application for dietary evaluation," in *Proc. IEEE 13th Int. Conf. EHealth Netw., Appl. Services*, vol. 310, Jun. 2011, pp. 375–380.

[6] A. Lorenz and R. Oppermann, "Mobile health monitoring for the elderly: Designing for diversity," *Pervas. Mobile Comput.*, vol. 5, no. 5, pp. 478–495, Oct. 2009.

[7] W. Wilkowska and M. Ziefle, "Privacy and data security in E-health: Requirements from the user's perspective," *Health Informat. J.*, vol. 18, no. 3, pp. 191–201, Sep. 2012.

[8] D. D. Luxton, R. A. Kayl, and M. C. Mishkind, "MHealth data security: The need for HIPAA-compliant standardization," *Telemed. e-Health*, vol. 18, no. 4, pp. 284–288, May 2012.

[9] K. Bennett, A. J. Bennett, and K. M. Griffiths, "Security considerations for E-mental health interventions," *J. Med. Internet Res.*, vol. 12, p. e61, Dec. 2010, doi: 10.2196/jmir.1468.

[10] K. Nagaty, "Mobile health care on a secured hybrid cloud," *Cyber J. Multidisciplinary J. Sci. Technol. J. Sel. Areas Health Informat.*, vol. 4, no. 2, pp. 1–9, 2014.

[11] V. Gurupur and T. Wan. (Mar. 2017). *Challenges in Implementing mHealth Interventions: A Technical Perspective*. MHealth. [Online]. Available: https://mhealth.amegroups.com/article/view/16006

[12] *Ergonomics of Human-System Interaction—Part 11: Usability: Definitions and Concepts*, document ISO 9241-11:2018(en), International Organization for Standardization, 2018.

[13] M. Kamana, *Investigating Usability Issues of mHealth Apps for Elderly People: A Case Study Approach*. Karlskrona, Sweden: Faculty of Computing Blekinge Institute of Technology,2016.

[14] G. Novak, *Developing a Usability Method for Assessment of M-Commerce Systems: A Case Study at Ericsson*. Karlskrona, Sweden: Faculty of Computing Blekinge Institute of Technology, 2014.

[15] K. Karvonen, "The beauty of simplicity," in *Proc. Conf. On Universal Usability*, 2000, pp. 85–90, doi: 10.1145/355460.355478.

[16] S. Nakamoto. (2009). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: http://www.bitcoin.org/bitcoin.pdf

[17] V. Buterin. (2015). *A Next-Generation Smart Contract and Decentralized Application Platform*. [Online]. Available: https://ethereum.org/en/whitepaper/

[18] V. Lopes and L. A. Alexandre, "An overview of blockchain integration with robotics and artificial intelligence," 2018, *arXiv:1810.00329*.

[19] *Hyperledger Fabric—A Blockchain Platform for the Enterprise*. Hyperledger. Accessed: Dec. 2021. [Online]. Available: https://www.hyperledger.org/

[20] N. Szabo, "Formalizing and securing relationships on public networks," *First Monday*, vol. 2, no. 9, Sep. 1997. https://journals.uic.edu/ojs/index.php/fm/article/view/548

[21] T.-T. Kuo, H.-E. Kim, and L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and health care applications," *J. Amer. Med. Inform. Assoc.*, vol. 24, no. 6, pp. 1211–1220, Nov. 2017.

[22] H. Xiong, C. Jin, M. Alazab, K.-H. Yeh, H. Wang, T. R. Gadekallu, W. Wang, and C. Su, "On the design of blockchain-based ECDSA with fault-tolerant batch verification protocol for blockchain-enabled IoMT," *IEEE J. Biomed. Health Informat.*, vol. 26, no. 5, pp. 1977–1986, May 2022.

[23] H.-N. Dai, M. Imran, and N. Haider, "Blockchain-enabled internet of medical things to combat COVID-19," *IEEE Internet Things Mag.*, vol. 3, no. 3, pp. 52–57, Sep. 2020.

[24] T. Motohashi, T. Hirano, K. Okumura, M. Kashiyama, D. Ichikawa, and T. Ueno, "Secure and scalable mHealth data management using blockchain combined with client hashchain: System design and validation," *J. Med. Internet Res.*, vol. 21, no. 5, May 2019, Art. no. e13385. [Online]. Available: https://www.ncbi.nlm.nih.gov/pubmed/31099337

[25] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for secure EHRs sharing of mobile cloud based E-health systems," *IEEE Access*, vol. 7, pp. 66792–66806, 2019.

[26] K. Griggs, O. Ossipova, C. Kohlios, A. Baccarini, E. Howson, and T. Hayajneh, "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring," *J. Med. Syst.*, vol. 42, no. 7, pp. 1–7, 2018.

[27] A. Zhang and X. Lin, "Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain," *J. Med. Syst.*, vol. 42, no. 8, pp. 1–18, Aug. 2018.

[28] H. Li, L. Zhu, M. Shen, F. Gao, X. Tao, and S. Liu, "Blockchain-based data preservation system for medical data," *J. Med. Syst.*, vol. 42, no. 8, pp. 1–13, Aug. 2018.

[29] D. Ichikawa, M. Kashiyama, and T. Ueno, "Tamper-resistant mobile health using blockchain technology," *JMIR mHealth uHealth*, vol. 5, no. 7, p. e111, Jul. 2017. [Online]. Available: http://www.ncbi.nlm.nih.gov/pubmed/28747296

[30] J. Brogan, I. Baskaran, and N. Ramachandran, "Authenticating health activity data using distributed ledger technologies," *Comput. Struct. Biotechnol. J.*, vol. 16, pp. 257–266, Jan. 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2001037018300345

[31] S. Mallick and S. Sharma, "EMRI: A scalable and secure blockchain-based IoMT framework for healthcare data transaction," in *Proc. 19th OITS Int. Conf. Inf. Technol. (OCIT)*, 2021, pp. 261–266.

[32] Y. Gao, H. Lin, Y. Chen, and Y. Liu, "Blockchain and SGX-enabled edge-computing-empowered secure IoMT data analysis," *IEEE Internet Things J.*, vol. 8, no. 21, pp. 15785–15795, Nov. 2021.

[33] Y. Wang, A. Zhang, P. Zhang, Y. Qu, and S. Yu, "Security-aware and privacy-preserving personal health record sharing using consortium blockchain," *IEEE Internet Things J.*, vol. 9, no. 14, pp. 12014–12028, Jul. 2021.

[34] G. Mendes, D. Chen, B. Silva, C. Serr ao, and J. Casal, "A novel reputation system for mobile app stores using blockchain," *Computer*, vol. 54, no. 2, pp. 39–49, Feb. 2021, doi: 10.1109/MC.2020.3016205.

[35] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, C. A. De, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, S. Muralidharan, C. Murthy, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukolić, S. J. Cocco, and J. Yellick, "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proc. 13th EuroSys Conf.*, Apr. 2018, pp. 1–15, doi: 10.1145/3190508.3190538.

[36] H. Performance and S. Group. (Oct. 2018). *Hyperledger Blockchain Performance Metrics*. Hyperledger. [Online]. Available: https://www.hyperledger.org/learn/publications/blockchain-performance-metrics

[37] C. Mao and W. Golab, "Sharding techniques in the era of blockchain," in *Proc. 40th Int. Symp. Reliable Distrib. Syst. (SRDS)*, Sep. 2021, pp. 343–344.

RUI P. PINTO received the B.Sc. and M.Sc. degrees in informatics engineering from the University of Beira Interior, in 2019 and 2022, respectively. His research interests include cloud computing, information security, the Internet of Things, and ubiquitous computing.

BRUNO M. C. SILVA (Member, IEEE) received the B.Sc., M.Sc., and Ph.D. degrees in informatics engineering from the University of Beira Interior, in 2008, 2010, and 2015, respectively. He is currently an Assistant Professor with the Department of Informatics, University of Beira Interior. He is also a Researcher with the Institute of Telecommunications, Portugal. He has authored or coauthored several international conference papers and international journal publications. His research interests include delay tolerant networks, vehicular networks, mobile computing, ubiquitous computing, but especially e-Health, mobile health, the Internet of Things, and cooperation mechanisms. He is a member of many international TPCs. He has participated in several international conferences organization.

PEDRO R. M. INÁCIO (Senior Member, IEEE) received the B.Sc. degree in mathematics and computer science and the Ph.D. degree in computer science and engineering from the University of Beira Interior (UBI), Portugal, in 2005 and 2009, respectively. His Ph.D. work was performed in the enterprise environment of Nokia Siemens Networks Portugal, S.A., through the Ph.D. grant from the Portuguese Foundation for Science and Technology. He has been a Professor of computer science with UBI, since 2010, where he teaches subjects related to information assurance and security, and computer-based simulation, for graduate and undergraduate courses, namely to the B.Sc., M.Sc., and Ph.D. courses in computer science and engineering. He is currently an Instructor with UBI Cisco Academy. He is also a Researcher with the Instituto de Telecomunicações.