UNIVERSIDADE
BEIRA INTERIOR

Engenharia

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

Rui Pedro de Oliveira Pinto

Dissertação para obtenção do Grau de Mestre em
Engenharia Informática
(2.º ciclo de estudos)

Orientador: Professor Doutor Bruno Silva
Coorientador: Professor Doutor Pedro Inácio

Covilhã, janeiro de 2022

Resumo

O desenvolvimento de mais e melhores dispositivos móveis interligados globalmente devido ao progresso das ligações móveis sem fios, tornou possível utilizar as capacidades destes dispositivos para monitorizar eventos relacionados com a saúde em tempo real tornando Mobile Health (m-health) ou Tecnologias Móveis para a Saúde, numa tecnologia mais apelativa e funcional. A m-health permite a monitorização de vários dados de saúde, melhorando a conveniência do seu utilizador e permitindo diagnósticos mais rápidos sem a necessidade de deslocação para instalações de saúde.

A tecnologia *Blockchain* é também uma área tecnológica em crescimento exponencial utilizado em várias áreas de investigação desde a área financeira, mecanismos de voto, cadeias de produção e até para controlo de eventos de Internet of Things (IoT) (Internet das Coisas). Uma *Blockchain* pode ser descrita como um conjunto de registos organizados em blocos, em que cada bloco está ligado ao anterior de uma forma criptográfica. A utilização destes registos de transações agrupados em bloco permitem que a informação não possa ser alterada, devido a ser assegurada pela *hash* criptográfica do bloco anterior. Esta tecnologia fornece características importantes desde imutabilidade, não repúdio, transparência e reduzindo a necessidade de intermediários.

Estas características fornecidas pela tecnologia *Blockchain* garantem vantagens enormes a sistemas *m-health*. Um sistema de *m-health* integrado com *blockchain* permite, por exemplo, que cada acesso e transação seja armazenado na *blockchain* fornecendo assim imutabilidade e não repudio a estas transações aumentando a confiança no sistema de *m-health*.

Esta dissertação visa o estudo da tecnologia *blockchain* em junção com sistema de *m-health* capaz de ser facilmente integrado com outros sistemas ou aplicações que permitam que um utilizador paciente possa aceder ao seu registo de saúde eletrónico e onde os dados possam ser rastreáveis ao longo do sistema, mas mantendo o seu anonimato. Para isso, foi desenvolvimento um protótipo para uma solução baseada em *blockchain*, utilizando *Hyperledger Fabric*, para ser aplicado neste caso.

Esta implementação permite a criação de um registo de dados de saúde, cronologicamente organizado e imutável. Para criar um sistema de armazenamento anónimo, o sistema proposto utiliza dois componentes de base de dados separados que mantém a rastreabilidade dos dados através de conjuntos de *IDs* armazenados na *blockchain*. Após, o desenvolvimento do sistema proposto, o sistema foi avaliado em termos de desempenho e de configurações de rede do *Hyperledger Fabric*.

Com este trabalho, foi mostrado como a tecnologia *Blockchain* pode ser utilizada em junção com dados de saúde recolhidos por dispositivos móveis de uma forma benéfica em contextos onde a segurança, a anonimidade e a imutabilidade dos dados são aspetos cruciais.

Palavras-chave

Armazenamento de Dados, Bases de Dados, Blockchain, Hyperledger Fabric, Internet das Coisas, Registo de Eventos, Registo de Saúde Eletrónico, Segurança.

Resumo alargado

Introdução e Motivação

Com o desenvolvimento de mais e melhores dispositivos móveis interligados globalmente devido ao progresso das ligações móveis sem fios, tornou possível utilizar as capacidades destes dispositivos para monitorizar eventos relacionados com a saúde em tempo real tornando m-health numa tecnologia mais apelativa e funcional. A m-health permite a monitorização de vários dados de saúde, melhorando a conveniência do seu utilizador e permitindo diagnósticos mais rápidos sem a necessidade de deslocação para instalações de saúde.

A tecnologia *Blockchain* é também uma área tecnológica em crescimento exponencial utilizado em várias áreas de investigação desde a área financeira, mecanismos de voto, cadeias de produção e até para controlo de eventos de IoT. Uma *Blockchain* pode ser descrita como um conjunto de registos organizados em blocos, em que cada bloco está ligado ao anterior de uma forma criptográfica. A utilização destes registos de transações agrupados em bloco permitem que a informação não possa ser alterada, devido a ser assegurada pela *hash* criptográfica do bloco anterior. Esta tecnologia fornece características importantes desde imutabilidade, não repúdio, transparência e reduzindo a necessidade de intermediários.

Estas características fornecidas pela tecnologia *Blockchain* garantem vantagens enormes a sistemas m-health. Um sistema de m-health integrado com *blockchain* permite, por exemplo, que cada acesso e transação seja armazenado na *blockchain* fornecendo assim imutabilidade e não repudio a estas transações aumentando a confiança no sistema de m-health.

A motivação por trás do trabalho que esta dissertação reflete está no estudo e desenvolvimento de um sistema de m-health integrado com tecnologia *Blockchain*.

Objetivos

Como principal objetivo para o trabalho que esta dissertação reflete está o desenvolvimento de um sistema de m-health com integração de tecnologia *Blockchain* Ademais, para este objetivo ser cumprido, será necessário o estudo das tecnologias (m-health e *blockchain*), mitigar potenciais problemas de uma implementação com *blockchain* e a avaliação do sistema proposto.

Organização da Dissertação

Conceitos Fundamentais e Trabalhos Relacionados

O capítulo 2 divide-se em duas secções fundamentais usados como fundação do trabalho elaborado. A primeira secção, Trabalhos Relacionados, analisa implementações da tecnologia *Blockchain* em sistemas de m-health. A comparação entre os fatores essenciais presentes nas várias implementações permitiu a criação de uma ideia mais consolidada dos componentes que deveriam incorporar o sistema.

A segunda secção introduz os conceitos e tecnologias fundamentais para a realização da dissertação. Consequentemente, esta análise permitiu ainda a identificação com detalhe destas tecnologias e como a estas várias tecnologias se podem integrar de uma forma benéficial, tornando um sistema tradicional num sistema robusto e capaz. Para isso, o conceito de m-health foi primeiro introduzido, enquadrando-o no mundo atual, identificando a sua funcionalidade e as suas características fundamentais que o destacam comparativamente a sistemas tradicionais de saúde. Ademais, os desafios que esta tecnologia enfrenta para se tornar numa tecnologia mais difundida e utilizada também foram identificados e analisados. A identificação destes desafios, permitiu compreender os aspetos em que a integração com a tecnologia *Blockchain* pode ser beneficial.

Da mesma forma foi necessário compreender os conceitos que formam a tecnologia Blockchain. Para facilitar a usa compreensão foi feito um pequeno enquadramento histórico sobre o desenvolvimento e evolução da tecnologia. Além disso, é feita uma análise da estrutura básica da *Blockchain* e dos seus componentes bem como a identificação das várias diferenças entre as várias categorias de *Blockchain* existentes. Desta forma, foi possível identificar como as características da *Blockchain* podem ser aplicadas como vantagens para a integração de um sistema de m-health.

Requisitos do Sistema e Conceito do Sistema

O capítulo 3 apresenta o sistema de m-health proposto com integração de tecnologia *Blockchain*. Este capítulo divide-se, por isso, em duas secções para apresentar o modelo do sistema.

Na primeira secção, a discussão sobre os requisitos críticos de um sistema de m-health será aprofundada, de modo a identificar os requisitos fundamentais, funcionando como uma diretriz durante o desenvolvimento prático do sistema. As questões de viabilidade e de aplicação do sistema em modelos reais vão sempre referir esta secção onde os requisitos foram primeiramente definidos.

Na segunda secção, será feito a apresentação do sistema proposto, dividindo-o em três módulos fundamentais: 1) Módulo de Blockchain, que encapsula todos os componentes de uma rede *Hyperledger Network* para guardar eventos de intervenções e utilizar capacidades da *Blockchain*, 2) módulo de base de dados, utilizado para encapsular as bases de dados utilizadas para armazenar os dados pessoais e os dados de saúde separadamente utilizando uma solução Structured Query Language (SQL) com *MariaDB*, 3) Módulo de aplicações e Application Programming Interface (API) que permite a comunicação entre os módulos de base de dados e os módulos de *Blockchain* permitindo também responder a pedidos por aplicações que possam ser implementadas. Após a apresentação dos módulos, cada um deles será explicado ao pormenor de forma a dar a entender a estrutura do sistema. Para facilitar esta explicação são apresentados também vários diagramas definindo as comunicações e os componentes utilizados.

Desenvolvimento e Viabilidade do Sistema num Cenário Real

Este capítulo aprofunda a discussão de como o sistema proposto seria implementado na realidade. Este capítulo está dividido em três secções designados por Prova de Conceito, Viabilidade do Sistema e Discussão sobre as possíveis Vantagens e Desvantagens de uma implementação como esta.

Na secção Prova de Conceito será explicado como a implementação funcionaria num ambiente real. Para isso, após serem identificados as atividades a ser realizadas por cada categoria de utilizador, será explicado como o sistema vai agir de modo a responder a estas necessidades. Na secção Viabilidade do Sistema, o sistema proposto será analisado para ser considerado uma opção viável para um uso futuro. Assim, deverá preencher todos os requisitos definidos no capítulo anterior para garantir a sua viabilidade.

Por fim, a última secção inicia uma discussão sobre as vantagens e desvantagens possivelmente encontradas durante uma implementação deste sistema proposto num ambiente real. O objetivo desta discussão será mais uma vez a reflexão sobre a viabilidade de um sistema como este.

Avaliação do Sistema

No capítulo 5, o sistema proposto vai ser avaliado no âmbito de desempenho principalmente no módulo de *Blockchain*. Estes testes de desempenho que se focam no teste das várias configurações da rede *Hyperledger Fabric*.

Para desenvolver estes testes de desempenho, primeiramente, será necessário definir o ambiente de testes utilizado para obter estes resultados. Desta forma será possível garantir a reprodutibilidade dos dados conseguidos durante o teste do sistema. Esta definição do ambiente de teste será feita logo após a secção de Introdução do capítulo. O ambiente de testes não será só fundamental para a reprodutibilidade dos dados mas também será o fator mais importante para os resultados alcançados nos testes de desempenho.

Com a descrição do ambiente de testes, poderá se dar início à avaliação das configurações de *Hyperledger* propostas, focando-se em desempenho e na medição da capacidade de armazenamento extra, necessário, comparativamente a um sistema sem *Blockchain*. Para realizar esta avaliação no sistema em teste será utilizado o *Hyperledger Caliper* que funcionará como uma ferramenta de *benchmark* de *Blockchain*, capaz de gerar várias transações por segundo para a rede *blockchain* utilizando o *chaincode* implementado (`CreateIntervention`, `GetInterventionByID`). Para avaliar a junção dos módulos *Blockchain*, Base de Dados e

API foi desenvolvido um pequeno programa na linguagem de programação *Python* para comunicar com a API enviando depois a informação para os módulos corretos.

Conclusão e Trabalho Futuro

No capítulo 6, a conclusão da dissertação será apresentada, com algumas sugestões de integrações com outros projetos ou sugestões de investigação para trabalho futuro.

Na primeira secção do capítulo, os objetivos inicialmente apresentados são novamente apresentados para concluir o que foi feito ao longo do desenvolvimento do trabalho. Esta discussão passa também por referir os passos tomados para que os objetivos tenham sido cumpridos e para que o sistema proposto fosse construido.

Na segunda e última secção, serão fornecidas várias sugestões de investigação futura e integração do sistema proposto com outros sistemas construidos. A aplicação destas sugestões permitia o desenvolvimento de um sistema muito mais robusto capaz de ser utilizado num ambiente real.

Abstract

With the development of more and better globally connected mobile devices and thanks to improvements in wireless connectivity, it became possible to utilize the capabilities of mobile devices to monitor health-related events in real-time, making m-health a technology more appealing and functional. m-health enables the monitoring of health data, improving user convenience and enabling faster diagnoses without the need to travel to healthcare facilities.

Blockchain technology is also an exponentially growing technology used in various research areas from finance, voting mechanisms, production chains, and even for IoT event control. A Blockchain can be described as a group of recorded transactions organized into blocks, where each block is linked to the previous block cryptographically. The use of these records of transactions grouped into blocks does not allow the modification of the stored information due to being secured by the cryptographic hash of the previous block. This technology provides important characteristics as immutability, non-repudiation, transparency, and reducing the need for intermediaries.

These features provided by Blockchain technology grant huge advantages to m-health systems. A m-health system integrated with blockchain allows each access and transaction to be stored in the blockchain thus providing immutability and non-repudiation to these transactions increasing the trust in the m-health system.

This dissertation aims to study the blockchain technology in conjunction with m-health system, capable of being easily integrated with other systems or applications allowing a patient-user to access his electronic health record. The data should be traceable throughout the system but maintain the necessary anonymity. For this end, a prototype for a blockchain based solution using *Hyperledger Fabric* was developed to be applied in this case.

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. After, the development of the proposed system, the system was evaluated in terms of performance and network configurations of the *Hyperledger Fabric*.

This work shows how the *Blockchain* can be used in junction with health data collected by mobile devices, in an advantageous manner, in contexts where security, anonymity, and immutability of data are crucial aspects.

Keywords

Blockchain, Databases, Data Storage, Eletronic Health Record, Event Registration, Hyperledger Fabric, Internet-of-Things, Mobile Health, Security.

Contents

List of Figures

List of Tables

Acronyms List

ACM	Association for Computing Machinery
AES	Advanced Encryption Standard
API	Application Programming Interface
AWS	Amazon Web Services
CA	Certificate Authority
CCS	Computing Classification System
CFT	Crash Fault Tolerant
CRUD	Create Read Update Delete
DApps	Decentralized Applications
DBMS	Database Management System
DDoS	Distributed Denial-of-Service
EHR	Electronic Health Record
EHS	Electronic Health System
GB	Gigabyte
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IaaS	Infrastructure-as-a-Service
ID	Identifier
IPFS	InterPlanetary File System
IoT	Internet of Things
IT	Information Technology
JSON	JavaScript Object Notation
KB	KiloByte
LTS	Long Term Support
MB	MegaByte
m-health	Mobile Health
MHz	Megahertz
MSP	Membership Service Provider
P2P	Peer-to-Peer
PaaS	Platform-as-a-Service
PBFT	Practical Byzantine Fault Tolerance
PHI	Personal Health Information

PHR	Personal Health Record
PKI	Public Key Infrastructure
POC	Proof-of-Concept
PoW	Proof-of-Work
RAM	Random access memory
REST	Representational State Transfer
RM	Relational Model
RPC	Remote Procedure Calls
SaaS	Software-as-a-Service
SHA	Secure Hash Algorithm
SQL	Structured Query Language
SOTA	State Of The Art
SSL	Secure Socket Layer
SUT	System Under Test
TLS	Transport Layer Security
TPS	Transactions per second
UML	Unified Modeling Language

Chapter 1

Introduction

1.1 Scope and Motivation

The motivation behind the project leading to this dissertation is the study and development of the integration of blockchain technology in an m-health system. 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 made it possible to monitor health-related events in real-time, making m-health a much more appealing field. Mobile devices, at the moment, are capable of much more than just share data, are equipped with multiple sensors, allowing them to work as a fully-fledged monitoring device. Due to this technological evolution, health records can be communicated and updated, almost in real-time, between patients, medical care professionals, and other authorized entities. m-health promotes the importance of self-care [SSI19] by the user, allows that the patients become in control of their health records and reliably self-diagnose their symptoms [SMT13]. 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 dislocations to a medical care facility [SMT13].

Similarly, blockchain technology is a technology growing at an exponential rate, being used in a wide area of studies beyond financial uses (popularized by the application on Bitcoin), such as vote mechanisms, supply chain monitoring, IoT and securely share medical data. Blockchain introduced a decentralized way to securely implement transactions between nodes in an untrustworthy network through a consensus algorithm validating the transactions for all the nodes of the network. Blockchain brings 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 in a system. First, 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.

Following the 2012 version of the Association for Computing Machinery (ACM) Computing

Classification System (CCS) the scope of the master's project is defined by the ensuing categories:

- **Applied computing - Life and medical sciences - Health care information systems;**

- **Computer systems organization - Distributed architectures - Cloud computing;**

- *Security and privacy - Cryptography - Key management;*

- *Security and privacy - Cryptography - Public key (asymmetric) techniques - Digital signatures;*

- *Security and privacy - Cryptography - Public key (asymmetric) techniques - Public key encryption;*

- **Security and privacy - Cryptography - Symmetric cryptography and hash functions - Hash functions and message authentication codes;**

- *Security and privacy - Security services - Authentication;*

- **Security and privacy - Security services - Access control;**

- **Security and privacy - Systems security - Distributed systems security.**

1.2 Objectives

The main objective behind this dissertation is the development of an m-health system integrated with blockchain technology with methods of promoting health data ownership and traceability. To realize this main objective, the ensuing secondary objectives must also be achieved:

1. Study how blockchain technology can be used with health care information and how decentralized health system should operate;

2. Develop methods for promoting health data traceability;

3. Mitigate potential issues that arise from the implementation of blockchain;

4. Test the proposed methods and prototype appraising costs of implementation, costs of storage, and the number of transactions per second.

1.3 Document Organization

The dissertation is composed of five chapters summarily organized as follows:

1. Chapter 1 – **Introduction** - on which this section is included, presenting the scope and motivation of the dissertation;
2. Chapter 2 - **Background and Related Work** - discusses works and implementations of blockchain on m-health systems. It also provides background about m-health providing important advantages and challenges of the technology. This chapter also offers background for Blockchain technology and the importance of data traceability on m-health systems;
3. Chapter 3 - **System Requirements and System Concept** - presents the necessary requirements for a m-health system and the proposed system. It also provides discussion related to the technologies utilized to create the various modules of the system;
4. Chapter 4 - **Deployment and Viability of the System in a Real Scenario** - discusses the viability and how the proposed system should operate in a real-world environment;
5. Chapter 5 - **System Evaluation** - Provides analysis on the performance of the Hyperledger Network using Hyperledger Caliper. The extra storage necessary for blockchain integration is also discussed;
6. Chapter 6 - **Conclusions and Future Work** - presentation of the final thought about the dissertation and outline of possible future work.

Chapter 2

Background and Related Work

2.1 Introduction

This chapter provides an overview of the key concepts related to decentralized health systems using Blockchain technology, how can the integration of this novel technology untangle some security issues related to m-health systems, in addition to some leading work concerning the use of Blockchain technology embedded in a m-health system to provide traceability, immutability, and non-repudiation. Section 2.3 reviews m-health systems that incorporate Blockchain technology and does an analysis comparing essential factors of the implementations. Section 2.2 is subdivided into different subsections, each of them describing a different topic, providing the necessary foundation for the thesis. Thereby, subsection 2.2.1 introduces the concept of m-health and some enabling technologies used in m-health. Subsection 2.2.2 focuses on some security challenges a m-health system faces and how integration with Blockchain technologies can solve them. Subsection 2.2.3 addresses the Blockchain technology, presenting the benefits of using a system with this technology compared with traditional healthcare database management. 2.2.4 introduces the concept of data traceability and how it can be applied to Blockchain technology. Ultimately, Section 2.4 encapsulates the conclusions of the chapter.

2.2 Background

2.2.1 m-health

The continuous growth and evolution of wireless connectivity acquired primarily by the widespread usage of smart mobile devices allows much more than a bidirectional transfer of information but also receive data, store data and directly process this data [KNPS13]. 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 emerging a novel area of studies are known as m-health.

Today, most health care systems, difficult the access to health records making this a lengthy and even tedious process for the patient. Contrarily, on a m-health system, the patients are empowered, allowing them to be more involved with their current health state enabling a way for a better and more reliable self-diagnoses of their symptoms. Through m-health is also possible to monitoring and send various information about the patient health (e.g., blood pressure, glucose level, heart rate, oxygen levels) collected by the mobile device or sensors of the patient enabling a remote and fast analysis of the condition of the patient, while increasing the engagement in their care [SMT13].

An 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 an 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 [SLRR11].

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 [SSI19]. 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 [LO09].

2.2.2 m-health Challenges

As discussed above, the flexible and personalized nature of a m-health system brings a lot of advantages comparing to a traditional health system, but the implementation of one of these novel systems also creates various challenges that must be carefully approached to fully implement these systems [SSI19]. Furthermore, these new technologies become very difficult to implement on a system already established without being completely ready to integrate these new technologies.

These challenges vary from a vast plethora of problems but can be divided into two categories: social/economic challenges and technical challenges. 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 [WZ12] [LKM12].

Nowadays, cloud storage is the most predominant storage technology used to store data originated from m-health devices. Remote cloud storage brings storage flexibility, reliability, and accessibility in a possibly more secure way, reducing the security costs and maintenance costs of a physical hardware server. However, cloud storage still has some security problems that need to be resolved related to ownership of data and access control to the data allowed [Top16].

Another challenge related to cloud services/storage is choosing the right cloud computing offer for the right system, comparing the way they work and how the services are deployed. Cloud services can change according to the deployment model used from Public Cloud, Hybrid Cloud, and Private Cloud, offering different types of services such as Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), or Software-as-a-Service (SaaS), that constitute different security challenges for each case. As referenced before, cloud data storage needs to control access to information. For the user to access any data in the cloud storage, the system must verify that the user the rightful owner of the data or has permission to access the data requested. The aforementioned is even more critical in health data cases where only the patient and the right health service provider, may have access to the information.

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 [BBG10]. The patient must know and be in control of what data is being shared and stored in the system, guarantying full transparency from the system to the user. Furthermore, on an m-health any event saved in the system must be authenticated as being from a user already in the system recording who introduced it in the system, these events must also stay immutable being valid for any valuation or auditing. 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 [Nag14]. Another important challenges that m-health, like any other system, needs to solve, are the human interactions with the system [GW17]. The system must be user-friendly and guarantee the usability and human-system interaction concepts presented in ISO 9241 [fS18]. The level of patient engagement is intrinsically associated with the usability of the system [GW17] [Kam16] [Nov14].

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 [Kar00]. Finally, m-health systems use low-resources IoT devices and mobile devices sensors that need to be reliable to realize their core function.

Sometimes evaluating and quantifying the reliability of these devices is a critical and arduous task however, it needs to be made to guarantee the security and precision of the data generated.

2.2.3 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 [Nak09]. 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 [But15]. 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 [SSI19] [LA18]. 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 [Hyp].

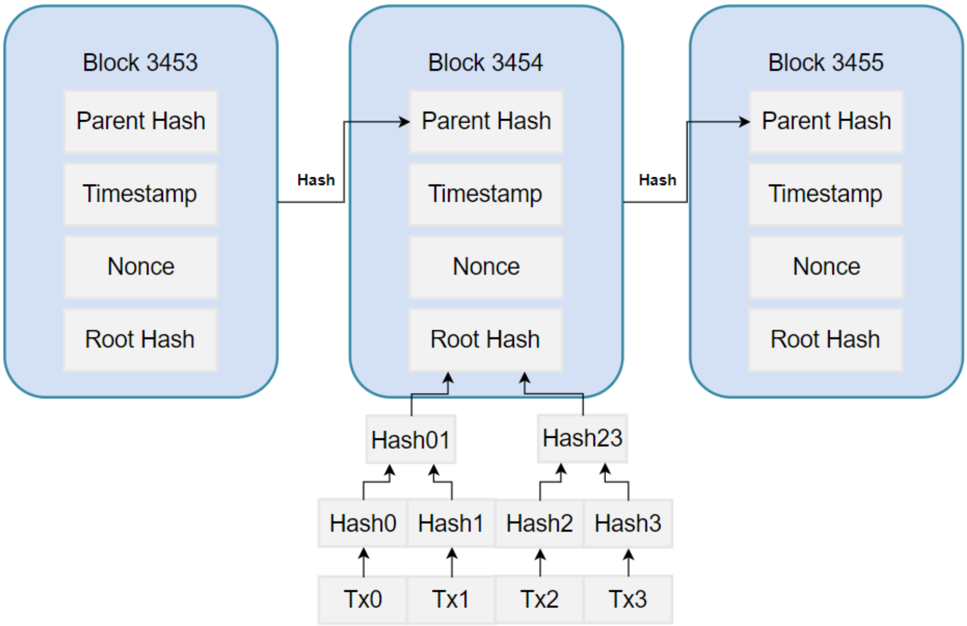


Figure 2.1: Bitcoin's Blockchain structure [Nak09].

Figure 2.1 illustrates Bitcoin's Blockchain structure, where three blocks are linked together by the hash of the header of the previous block. These blocks contain a parent block hash that is the hash correspondent to the previous block, a timestamp representing the time the block was validated, a nonce incremented to achieve the value of hash needed to complete the cryptographic puzzle of the PoW consensus mechanism, and the hash of the root of a Merkle Tree representing all the transactions in the block. A Merkle tree is a binary tree used to store all the transactions in the block. It is organized by leaf nodes at the bottom of the tree containing the data of the transactions, intermedium nodes created by the hash of its two children, and lastly the root node also composed by the hash of its two children being the only part of the Merkle tree in the block header. The Merkle Tree allows a node of the blockchain system to download just the needed part of the tree and the header of the block and verify that the data is correct, even from different sources.

In 2015, Ethereum, a public blockchain like Bitcoin first described in 2013 by Vitalik Buterin in [But15], surged, changing the focus of blockchain protocol from cryptocurrencies to decentralized applications due to the implementation of smart contracts built on the efforts of Nick Szabo in [Sza97], 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.

Both Bitcoin and Ethereum are examples of what is known as public and permissionless blockchains, where everyone is authorized to make and process transactions. This isn't the case with most of the industrial or corporate blockchains used. A private and permissioned blockchain is implemented when some characteristics or levels of performance cannot be met using a public counterpart. Firstly, every participant allowed in the private blockchain system is known and can be identifiable at any time [Hyp]. Second, a private blockchain can achieve higher transaction throughput and lower latency of transaction confirmation using different consensus algorithms, like Proof of Authority, because there is no need to be resilient against Sybil and Distributed Denial-of-Service (DDoS) attacks and maintain anonymity in a closed network. Lastly, access to data can be controlled, restricting access to the network, or using private transactions. However, private blockchains offer less transparency, less interoperability with other applications, and less security if the majority of the nodes are compromised, with extra cost with development and maintenance. Some of the most popular frameworks of private blockchain are Corda, Hyperledger Fabric, Quorum, and Private Ethereum [Hyp].

Based on a study of the potential for the use of blockchain technology in healthcare systems conducted by Tsung-Ting Kuo et al. in [KKOM17], there are five potential benefits for the use 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.

2.2.4 Data Traceability

Data traceability is the process of analyzing the lifecycle of data, tracking all access and changes to the data that may occur. In a health system environment, data traceability can be described as the accurate identification of the patient, the relationship between patient and healthcare professional, and all the other data of the patient(medication, medical diagnosis, medical care history) [PDG18].

In an Electronic Health System (EHS), tracing the data used and stored in the system is essential to guarantee transparency, compliance to regulations and rights, the privacy of medical data, and verify the data as it is being requested by the various phases of a process. Implementing measures for data provenance allows a system to be capable to easily collect information about what, when, and how an error occurred, or a system was compromised.

The intrinsic properties of a blockchain supported by IoT technologies are suited for providing trust in all transactions gathered by the system since blockchain technology provides immutability, and any eventual change needed is registered as an event. However, the storage of all the information related to a patient in a blockchain is not feasible as the increasing number of patient records would generate problems of scalability related to storage and network requirements to replicate all the information for the nodes in the distributed ledger. Nevertheless, an implementation of a system allowing traceability assisted by blockchain technology might be a great solution for these traceability challenges.

2.3 Related Work on Blockchain Based Solutions for m-health

In the work done by Tomomitsu Motohash et al. [MHO^{+}19] 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 [Hyp] 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.

Dinh C. Nguyen et al. [NPDS19] 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 authorwas 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, Kristen Griggs et al. [GOK$^+$18] 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.

Aiqing Zhang et al. [ZL18] presented a blockchain-based secure and privacy-preserving Personal 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, Hongyu Li et al. [LZS$^+$18] 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 Secure Hash Algorithm (SHA)-256 algorithm to calculate the hash of the original data combined with the encryption of the original text using the Advanced Encryption Standard (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.

Daisuke Ichikawa et al. [IKU17] 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.

James Brogan et al. [BBR18] 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.

Table 2.1: Review of the studies introduced in section 2.3.

Name	Year	**Problem**	**Solution**	**Blockchain Network**	**Consensus**
Tomomitsu Motohashi et al.[MHO+19]	2019	Avoid impersonation attacks on patient's mobile devices.	Client hash chain created in the patient mobile device and registered in the blockchain network.	Hyper-ledger Fabric	PBFT
Dinh C. Nguyen et al.[NPDS19]	2019	Guarantee high security levels in the mobile cloud used to share EHR.	Used a decentralized Peer-to-Peer (P2P) IPFS to build a file system sharing platform in the blockchain network.	Private Ethereum	PoW
Kristen Griggs et al.[GOK+18]	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.[ZL18]	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.[LZS+18]	2018	Protect medical data from tampering, deletion and theft.	Blockchain-based data perservation system.	Ethreum	PoW
Daisuke Ichikawa et al.[IKU17]	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.	Hyper-ledger Fabric	PBFT
James Brogan et al.[BBR18]	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	-

Table 2.1 shows a short overview of the studies referenced in section 2.3. From the solutions presented in this section it is possible to see that [NPDS19] and [IKU17] have similar architectures to the planned implementation for this project. The paper [NPDS19] proposes a EHR method using mobile cloud computing and blockchain, proposing a real prototype implementation. The main difference between this paper implementation and the proposed implementation is the use of and IPFS for decentralized storage.

In [IKU17], an implementation of an m-health system for cognitive behavioral therapy for insomnia integrating blockchain technology was described. This solution applies blockchain to an important area of m-health but the system architecture is different and is not referenced in the ownership of data by the patients. Therefore, even though there are various implementations of blockchain in m-health systems and healthcare, none of the solutions found are completely similar to the planned implementation.

2.4 Conclusion

An overview of key concepts related to the initial focus of the dissertation was made in this chapter, focusing on: advantages and challenges of m-health, the blockchain protocol and the integration of this technology with m-health systems, and the importance of data traceability and ownership of data in this type of system. In the section *Related Work*, it was made a review of some methods that integrate blockchain technology in m-health systems implemented in different platforms. Finally, in the section Background, the key concepts of the dissertation were established to serve as an important introduction to technology discussed in ensuing chapters.

Chapter 3

System Requirements and System Concept

3.1 Introduction

An m-health system integrated with blockchain technology is proposed is this chapter. 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 API where the users can communicate with the after-mentioned modules.

Section 3.2 indicates and describes the essential requirements to the system. Section 3.3 provides an overview of the system, identifying the major system components. Subsection 3.3.1 focuses on the blockchain module, pinpointing the network technologies implemented and the network topology utilized. Subsection 3.3.2 addresses the database model applied, and the methods used to store and guarantee separation of personal data and healthcare data. Subsection 3.3.3 introduces the application and API module that encapsulates all the components used to communicate with the previous modules and integrate with other systems. Finally, section 3.4 abridges the conclusions of the chapter.

3.2 System Requirements

Deriving from the discussion presented in section 2.2.2 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 3.1 lists and describes some of the 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 3.1: 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.

3.3 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 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;

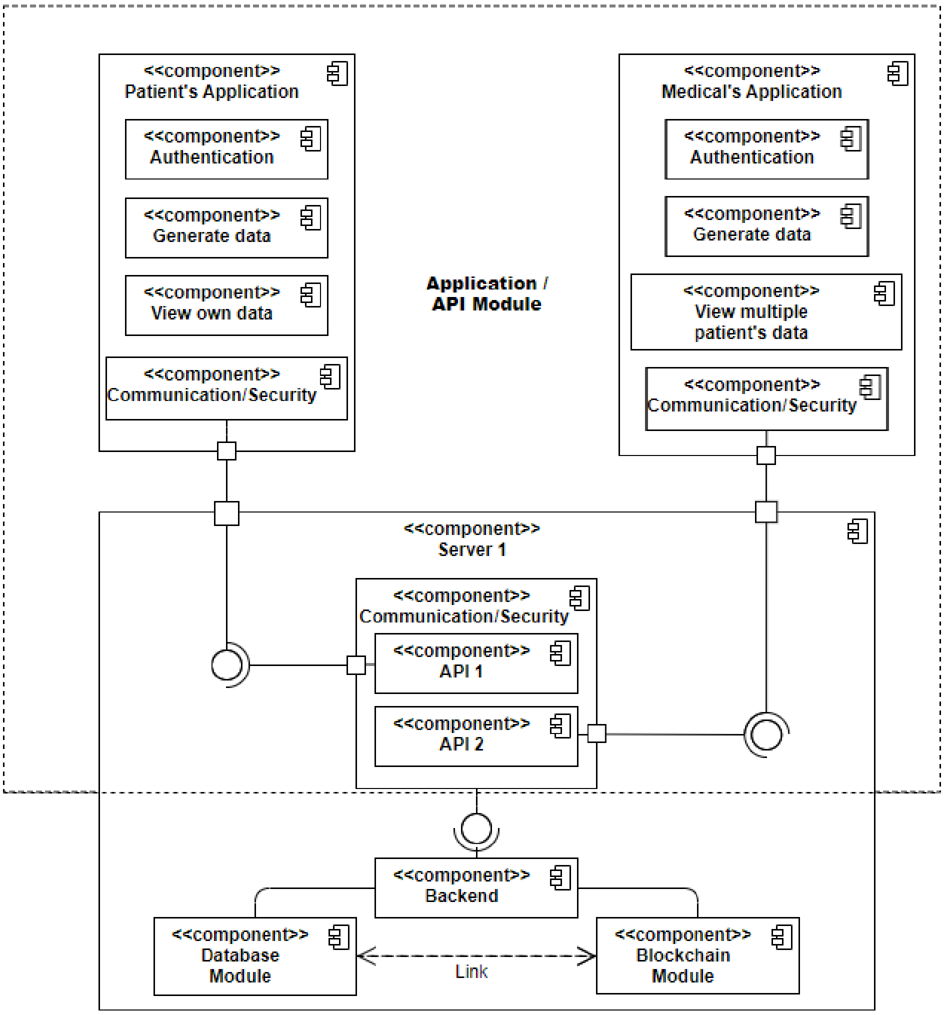
3. **Application and API** - encapsulate all the applications and API utilized, allowing the users to communicate to the blockchain module and the database module. NodeJS was used to create the API by handling concurrent requests in an efficient and lightweight way.

Figure 3.1 illustrates the proposed system using a Unified Modeling Language (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.

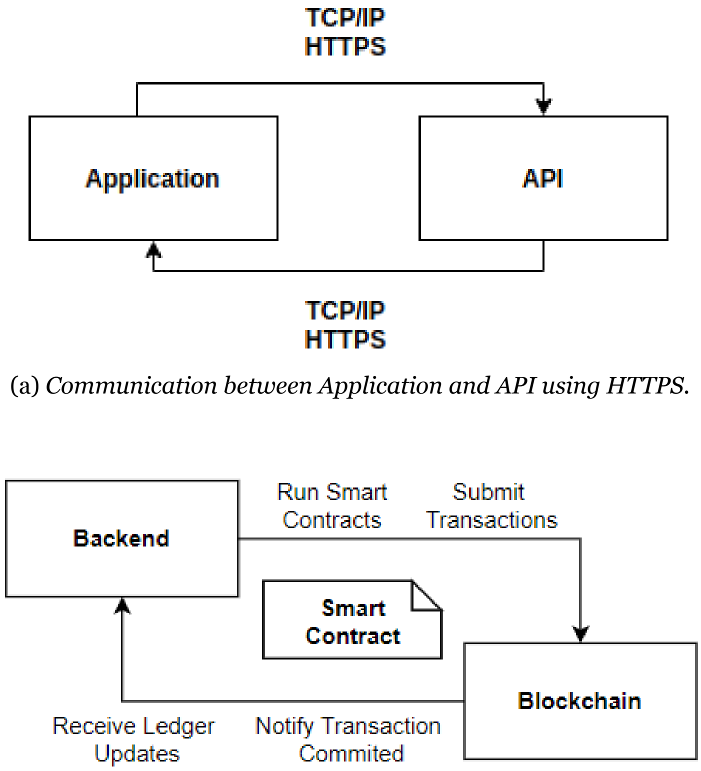
Another important component inside the application of the user is the possibility to view health data records. Furthermore, the application of the medical user allows for the access of health records from various patients if the medical staff is in charge of any treatment or diagnosis. The system can 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. Figure 3.2 illustrates the communication between the modules, presented in diagram 3.1. The application is able to communicate to the API via HyperText Transfer Protocol Secure (HTTPS) and as aforementioned, the Backend component communicates with the blockchain module ledger by invoking the smart contracts.



<<component>> Patient's Application
<<component>> Authentication
<<component>> Generate data
<<component>> View own data
<<component>> Communication/Security
Application / API Module
<<component>> Medical's Application
<<component>> Authentication
<<component>> Generate data
<<component>> View multiple patient's data
<<component>> Communication/Security
<<component>> Server 1
<<component>> Communication/Security
<<component>> API 1
<<component>> API 2
<<component>> Backend
<<component>> Database Module
Link
<<component>> Blockchain Module

Figure 3.1: Component diagram of the proposed system.



(a) *Communication between Application and API using HTTPS.*

(b) *Communication between API and Blockchain by invonking a smart contract*

Figure 3.2: Communication between modules of the system.

3.3.1 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 [MCS+21][ABB+18]. It is also a modular system purposefully created to develop distributed applications [Hyp] without needing to write Smart Contracts with a native programming language and without the need for paying transaction fees with a native cryptocurrency [ABB+18].

According to the documentation of the Hyperledger Fabric, a Hyperledger Network contains the following components:

- **Ledger** - consists of a blockchain (immutable ledger) and a world state database containing the up-to-date value of sets of key-value pairs that were added, changed, or deleted by transactions validated and committed in the blockchain. Currently, the supported databases are couchDB and levelDB;

- **Smart Contract or Chaincode** - a Smart Contract or chaincode (as referred to in Hyperledger Fabric) is a code, installed on peers, that can be invoked by a client application capable of modifying pairs in the world state. For isolation motives, each Smart Contract is executed within an isolated Docker container environment;
- **Peer nodes** - maintain an append-only blockchain and allows the member of a peer to execute read/write operations by running the Smart Contract containers;
- **Ordering service** - broadcasts state updates to all the peers, ordering the transactions into a block. Fabric uses deterministic consensus algorithms, so any block validated is final without the need to create forks to rearrange itself. There are three different ordering services:
  - Solo, currently deprecated;
  - Kafka, currently deprecated;
  - Raft.
- **Channel** - is a ledger shared across authenticated peers in a specific channel. Channels allow data isolation and confidentiality inside a consortium blockchain;
- **Fabric Certificate Authorities** - issues Public Key Infrastructure (PKI)-based certificates to network organizations and their users.

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 Remote Procedure Calls (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

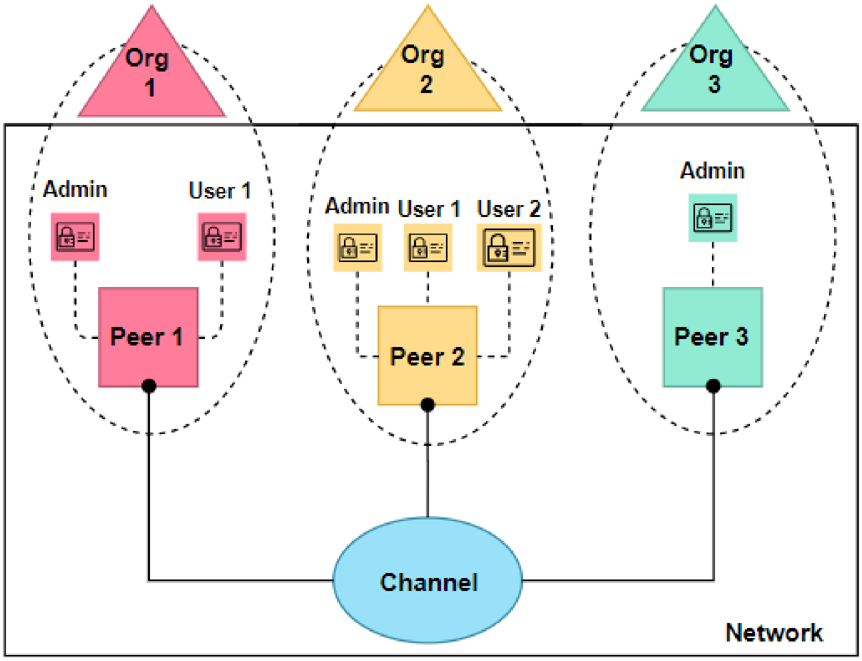


Figure 3.3: Simplified topology of the Hyperledger Fabric network implemented.

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. Figure 3.3 illustrates this topology in a simplified way with a structure inspired by the documentation of the Hyperledger Fabric.

The Raft algorithm was chosen and implemented in the scope of this work. Hyperledger Fabric version 1.4.1. (January 2019) introduced this Crash Fault Tolerant (CFT) ordering service based on Raft. Raft is a consensus algorithm that abides by a ”leader and follower” model, in which a channel dynamically elects a leader node that will replicate the order decisions to all the other nodes [OO14]. A Raft ordering service is said to be CFT by allowing the system to continue to perform if the majority of the ordering nodes remain active (even if the failed node is a leader node) [OO14]. For the Hyperledger Fabric implementation, it was necessary to download and install samples, binaries and Docker images provided by the documentation of Hyperledger Fabric [Hyp].

Ensuing this installation, it was necessary to set up a Fabric Certificate Authority (CA) for each of the organizations (three peer organizations and one orderer organization). A Docker image was deployed to carry out this task, hyperledger/fabric-ca (provided by Hyperledger Fabric) to initiate an instance of the Fabric CA server. The listing 3.1 illustrates the structure of a Docker service utilized to deploy a Fabric CA used by one of the organizations.

Listing 3.1: Docker service to launch a Fabric CA container.

```
ca_org1:
    container_name: ca.org1
    image: hyperledger/fabric-ca
    command: sh -c 'fabric-ca-server start -b admin:adminpw -d'
    environment:
      - FABRIC_CA_HOME=/etc/hyperledger/fabric-ca-server
      - FABRIC_CA_SERVER_CA_NAME=ca.org1
      - FABRIC_CA_SERVER_TLS_ENABLED=true
      - FABRIC_CA_SERVER_PORT=7054
    volumes:
      - ./fabric-ca/org1:/etc/hyperledger/fabric-ca-server
    networks:
      - test-network
    ports:
      - "7054:7054"
```

Second, the Fabric CA, created in the previous step, was used to create the cryptographic material for the organizations. This setup is necessary before starting up a peer, to enroll identities of the peers with the CA to get the local peer Membership Service Provider (MSP) to be used by the peer. To do this, it is necessary to enroll the CA admin and register all the identities of the Org 1. In the implemented model, the registered identities are the following:

- Peer - (peer0);
- Admin - (org1admin);
- End user - (user1).

After this, following the documentation of Hyperledger Fabric, it can be generated a MSP for each of the identities (peer, admin, and user). These steps are repeated for the orderer organization, yet without the need of implementing an end-user.

Following this, the system Genesis block, the channel configuration transaction, and anchoring peer transactions, one for each org were generated. To accomplish this, it was used the binary configtxgen to create the genesis block (genesis.block) and the channel configuration transaction (channel.tx). The genesis block is a configuration block used to start the ordering service, containing the MSP IDs partaking in the consortium with a trusted certificate for each of them. The channel configuration transaction, in turn, is the first block of the network storing the name of the channel and all the peers allowed to make use of the channel.

The interaction between the users of the applications of the system and the blockchain ledger is possible by allowing the users to invoke smart contracts deployed to a channel. In Hyperledger Fabric, the procedure of deployment of a smart contract to a channel is known as Fabric chaincode lifecycle. The Fabric chaincode lifecycle requests the agreement, from the channel members to parameters that define the chaincode, ranging from name to endorsement policy. To reach this agreement, the Fabric chaincode lifecycle is divided into four steps:

1. Package chaincode;
2. Install chaincode;
3. Approve chaincode definition;
4. Commit chaincode definition.

After deploying the Hyperledger Fabric network and creating a channel with various organizations, successfully, it is possible to begin the first step of the Fabric chaincode lifecycle, the packaging of the smart contract necessary to install the smart contract in the organization peer. The smart contracts utilized by this system were written using Go language and as with any other language utilized to write smart contracts is necessary to install all the chaincode dependencies. The listing 3.2 illustrates the commands used to create the `go.mod` file used to list the dependencies of the chaincode, importing the Fabric contract API toward the packaging of the chaincode.

Listing 3.2: Commands used to create a `go.mod` file with the dependancies of a smart contract written in the file `test.go`.

```
go mod init test.go #Creates a go.mod file
go mod tidy #Removes unnecessary dependencies
```

This Fabric contract API is then used to define a smart contract structure used to provide the functions necessary to operate the assets, creating the transaction context capable of enabling the query of data in the ledger. The listing 3.3 illustrates how to define this structure according to Hyperledger Fabric documentation and an example of a chaincode function implementation using Go. This function, when invoked, is capable of receiving data from an intervention, via an application, and create a transaction with the data storing it in the blockchain ledger.

Listing 3.3: Go code used to define a SmartContract struct using Fabric API and a chaincode function example

```
type SmartContract struct {
    contractapi.Contract
}

func (s *SmartContract) CreateIntervention(
ctx contractapi.TransactionContextInterface
,interventionData string) (string, error) {
    if len(interventionData) == 0 {
        return "", fmt.Errorf("Wrong intervention data")
    }
    var inter Intervention
    err := json.Unmarshal([]byte(interventionData), &inter)
    if err != nil {
    return "", fmt.Errorf("Error during unmarshalling. \%s", err.Error())
    }
    interventionAsBytes, err := json.Marshal(inter)
    if err != nil {
        return "", fmt.Errorf("Error during unmarshalling. \%s", err.Error())
    }
    ctx.GetStub().SetEvent("CreateAsset", interventionAsBytes)
    return ctx.GetStub()
    .GetTxID(), ctx.GetStub().PutState(inter.ID, interventionAsBytes)
}
```

Finally, it is possible to install the smart contract dependencies listed and create a chaincode package, finalizing the first step of the Fabric chaincode lifecycle. The listing 3.4 exhibits the command utilized for the installation of the Go packages in a vendor folder and the command utilized to create a package .tar.gz ready to be installed in the peers.

Listing 3.4: Commands used to install smart contract dependencies and package chaincode

```
GO111MODULE=on go mod vendor
peer lifecycle chaincode package ${CC_NAME}.tar.gz \
--path ${CC_SRC_PATH} --lang ${CC_RUNTIME_LANGUAGE} \
--label ${CC_NAME}_${VERSION}
```

As aforementioned, the next step, in the Fabric chaincode lifecycle, is the installation of the smart contract in the peers that will endorse the transaction. In this system model, the endorsement policy was not altered, which is set to the majority of the channel member by default, therefore the chaincode must be installed on two of the three peers of the system, each one in different organizations. To continue the installation, it is necessary to set up environment variables(enable Transport Layer Security (TLS) and indicate the root certificate, select the MSP of the peer and the MSP configuration path, and the address where the peer is running) to use the binaries peer with the command *peer lifecycle chaincode install ${CC_NAME}.tar.gz* to complete the installation for one of the peers.

Continuing the steps of the Fabric chaincode lifecycle, the next step, used in the installation of the chaincode on the channel, was the approval of the chaincode definition by the majority of the members of a channel. Since that this Hyperledger Network is composed of three organizations and the endorsement policy is based on a majority system, only two of the three organizations need to approve the chaincode definition. The approval of the smart contract must be made by an identity in the organization with an admin role, being necessary to change some configuration variable to indicate the MSP directory containing an identity admin.

After the approval of the chaincode by the majority of the organizations in the channel, using Org 1, the last step of the chaincode lifecycle was started by committing the chaincode definition transaction on the channel. This implementation was successful since the majority of the members on the channel approved this definition, allowing committing the transaction and the agreement of the chaincode definition on the channel. Succeeding this last step, the chaincode was started and in all the peers of the channel were the chaincode was installed, ready to be invoked by the API and Application Module.

3.3.2 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 3.4 illustrates a RM 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 3.4. 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.

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.

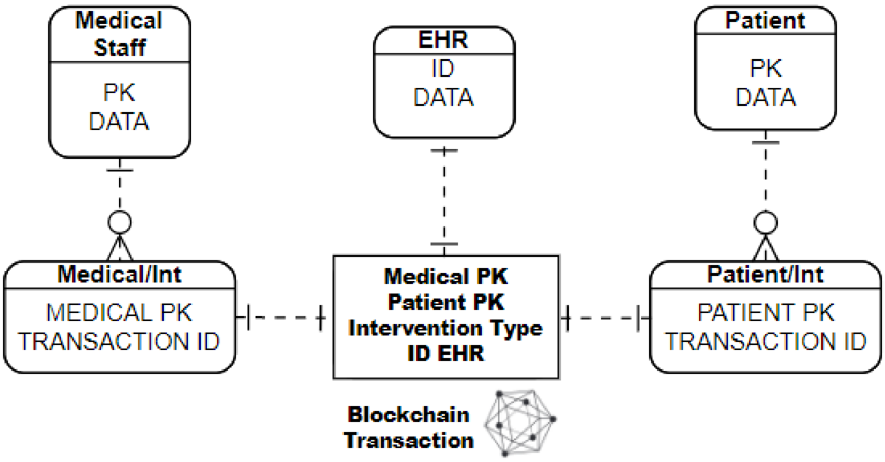


Figure 3.4: RM defining the intercommunication between the parts of the system (though, the blockchain component uses different technology).

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 by medical research, allowing to perform of medical research and studies.

3.3.3 API and Application 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 HyperText Transfer Protocol (HTTP) request link facilitating the integration of the applications to the system, with the goal of enabling Create Read Update Delete (CRUD) operations on the system.

3.4 Conclusion

In this chapter, the system requirements were identified, and a proposal for a novel system able to fulfill was introduced. In the section 3.3, the proposed model was split into three different critical components: Blockchain Module, Database Module, and Application and API module, each one encapsulating important components of the system.

The model of the proposed system passed by various iterations until reaching the actual state of separation of healthcare data and personal data, allowing anonymity yet guarantying data traceability by the blockchain module. It can be stated that this chapter, is a paramount support for all the ensuing chapters.

Chapter 4

Deployment and Viability of the System in a Real Scenario

4.1 Introduction

This chapter 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 (PHR) collections.

The remainder of this chapter is structured as follows: Section 4.2 presents a Proof-of-Concept (POC) for the system, designed to verify the functionality of the system with the integration of the modules of the system (Blockchain, Database, and API and Application) while inserting intervention events and query previously inserted events. Section 4.3 discusses the viability of the system based on the defined requirements while discussing the changes needed to be implemented in an existing environment. Lastly, section 4.5 contains the conclusions for the chapter.

4.2 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 4.1 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 State Of The Art (SOTA) cryptography techniques based on elliptic curve cryptography, public-key cryptography, Secure Socket Layer (SSL) and several key exchange protocols. These components were not implemented in this proposed system by being already discussed by a colleague in [SSI19]. 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.

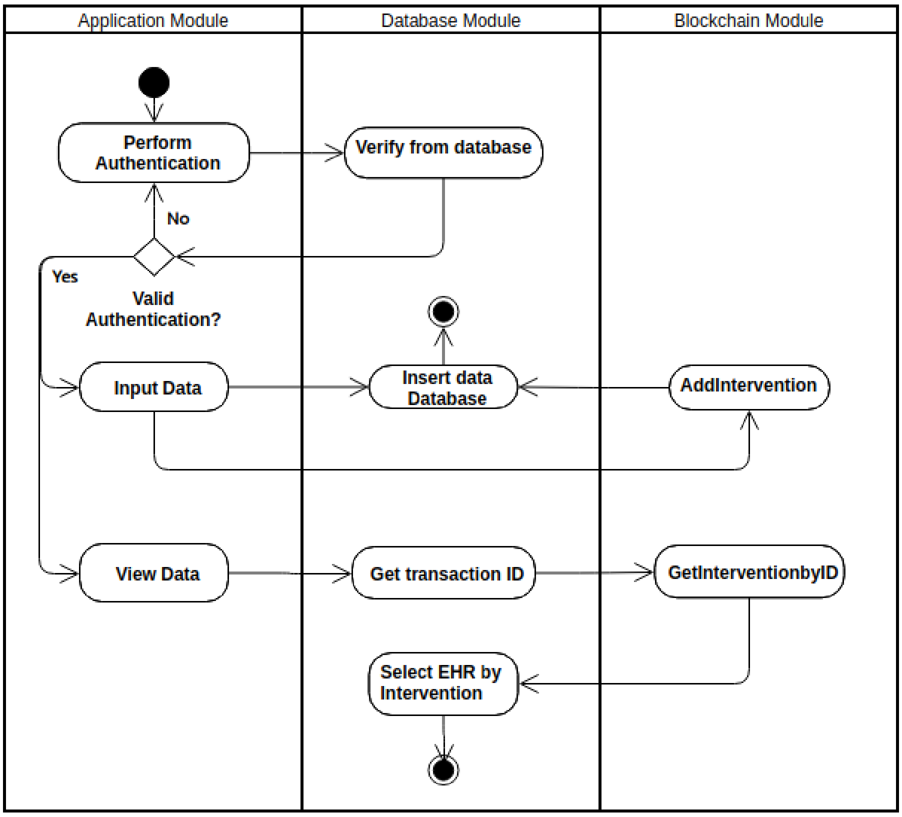


Figure 4.1: Activity Diagram depicting the flow and the integration between the three modules of the system: Application, Database, and Blockchain.

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 for 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.

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.

4.3 Viability of the System

For the proposed system to be considered viable, it must be able to fulfill the requirements provided in Table 3.1, in section 3.2, needed for a blockchain m-health system. 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 Representational State Transfer (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 5.3.

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.

As aforementioned, user authentication to assure the identity of every user present in the system is fundamental in a m-health system. The focus of this dissertation work was not on this subject, however, the study of communications and user identification in and with a m-health system is extensively analyzed by a colleague in [SSI19] and the solutions proposed could be implemented to the proposed system.

4.4 Discussion on Possible Advantages and Drawbacks of Implementing the Proposed System in a Real Scenario

In this dissertation, the possibility of implementing a m-health system that utilizes blockchain technology to enable health data traceability and promote the ownership of data was evaluated. In this section, the proposed system will be evaluated by the viability of this proof-of-concept in a real-world implementation. Consequently, this evaluation and discussion will be embodied by analyzing if the advantages provided by the proposed system enhance the m-health system enough to outweigh any possible disadvantage related to the implementation of blockchain technology.

However, the proposed system is a proof-of-concept implementation without some complexities necessary for a fully-fledged integration on a real-world EHR system. This subject will receive a deeper scrutiny in Chapter 6. The focus of the remaining sections of the chapter is on identifying the advantages achieved with the proposed system and the drawbacks encountered during implementation that may influence the implementation in a real-world system.

4.4.1 Advantages in Integrating Blockchain in a m-health System

A complete implementation of the proposed system in a real-life scenario would surely bring advantages to any traditional health system. Firstly, the possibility of having irreversible medical records promotes medical responsibility. The health records could be identified by a blockchain transaction guarantying that the records could not be altered or deleted, creating a permanent and chronologically ordered set of records. These records could also be made available to the patient-user, by integrating an application capable of receiving and presenting this information, promoting the ownership of personal health data by the patient.

Secondly, by creating a permanent and chronologically ordered set of records, the logging capabilities for evaluation or auditing purposes are also empowered. Alongside the increasing implementations of EHR, the number of EHR event logs also increases, generating the necessity of better handling this data. These records need to be stored, auditable, and protected from inappropriate accesses, all possible with the integration of blockchain.

Finally, as a result of the separation of database modules by a blockchain module in between, it is possible to have access to anonymous healthcare information. In a real-world implementation, provided that some type of federated authentication was previously integrated into the system, it should be possible for an identity verified as a qualified healthcare professional to access anonymous healthcare information. This healthcare information remains anonymous, without a direct identifier for any personal information.

4.4.2 Possible Drawbacks in a Blockchain Integration

Although the inclusion of blockchain technology provides various characteristics that enable and generate confidence on m-health systems and IoT systems in general, the implementation of this technology still presents constraints and possible drawbacks in need to be mitigated.

One of the more evident drawbacks, identified during the early steps of planning for the proposed system, is the extra storage necessary to host an organization and peers, each one with one ledger. To mitigate this problem, the proposed system was created in a way that most of the data is stored off-chain in databases and the transactions are kept simple. However, this necessary off-chain storage introduces issues related to access/authentication, security, and performance [Aul18], creating the need to develop shared networks to support the members of the blockchain channel.

Another drawback is the cost of the use of blockchain technology. For the implementation of the proposed system (private permissioned blockchain) in a real-world environment, it would be necessary a significant investment in hardware and/or cloud-based storage solutions to maintain an active node or organization. Furthermore, if the system utilized a public non-permissioned blockchain, it would be necessary the analysis of the fee cost per transaction on the chain.

4.5 Conclusion

This chapter described how the integration of blockchain in m-health system can be made. The proposed system is proficient at creating intervention events by using smart contracts. These smart contracts enable the read and write operation in the ledger, making it possible to maintain data traceability between all the system modules in spite of being separate structures. This chapter also exhibits the viability of the proposed system by being capable of complying to previously defined set of requirements for a m-health system. As a result of the various modular technologies chosen to implement this system, the proposed system itself, could be upscaled to reach the necessary capabilities of a m-health system implementation in a real environment.

Chapter 5

System Evaluation

5.1 Introduction

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. Section 5.2 describes the parameters used in the environment where the system was deployed in order to enable the reproducibility of the data acquired. Section 5.3 addresses the performance and scalability evaluation tests realized, presenting the research data acquired. Section 5.3 also focuses on evaluating the other components of the system, such as the integration with the API and database and the extra data needed to be stored compared with a traditional healthcare system. Finally, Section 5.4 presents the conclusions of the chapter.

5.2 Test Environment

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 [PG18]. This test network was implemented on a remote virtual server with 4 Gigabyte (GB) of Random access memory (RAM), 2 cores, and a processor clock speed of 3000 Megahertz (MHz) running an installation of Ubuntu 20.04.2 Long Term Support (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, so as 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 JavaScript Object Notation (JSON) data based on previously inserted data by receiving an Identifier (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 KiloByte (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.

5.3 Proposed System Evaluation

The evaluation of the proposed Hyperledger Configuration comprised various tests focusing primarily on performance and measuring the extra storage needed to implement Blockchain technology compared to a traditional system. All the tests were realized on the test environment defined in section 5.2. The System Under Test (SUT) during the performance evaluation is considered as all the defined configuration, software, and hardware required to sustain the blockchain network. Hyperledger Caliper was used to create a load-generating client capable of submitting transactions to the blockchain network, creating reports to evaluate performance on the predefined cases (*CreateIntervention* and *GetInterventionByID*). For the testing of the extra storage needed, the SUT consisted of all the components of the system (Blockchain, Database and API) using the REST API and a test script as a load-generating client to insert large quantities of data in the whole system.

5.3.1 Hyperledger Fabric Configuration Performance 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 [PG18]) and Throughput (Rate at which valid transactions are committed in a defined time. Measured in Transactions per second (TPS) [PG18]). 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 5.1 and 5.2 illustrate the results acquired for each function while changing the size of the blocks. In the case of the test of throughput (Figure 5.1), 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 5.2) 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.

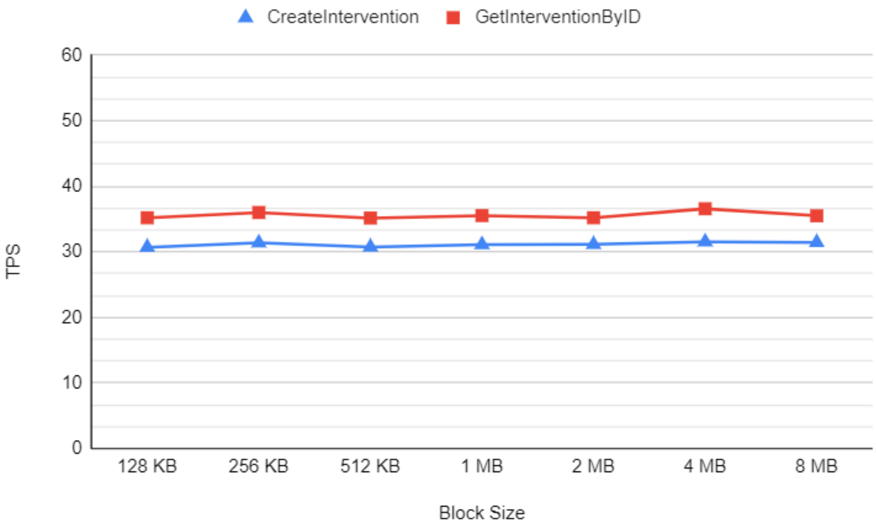


Figure 5.1: Results of throughput (measured in TPS) of the Hyperledger Fabric network and chaincode functions used, while varying the block size (using 10 transactions per block).

Figures 5.3 and 5.4 illustrate the results obtained for the functions while modifying the number of transactions per block. From the results presented in figure 5.3, 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 [MCS$^+$21]. 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.

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.

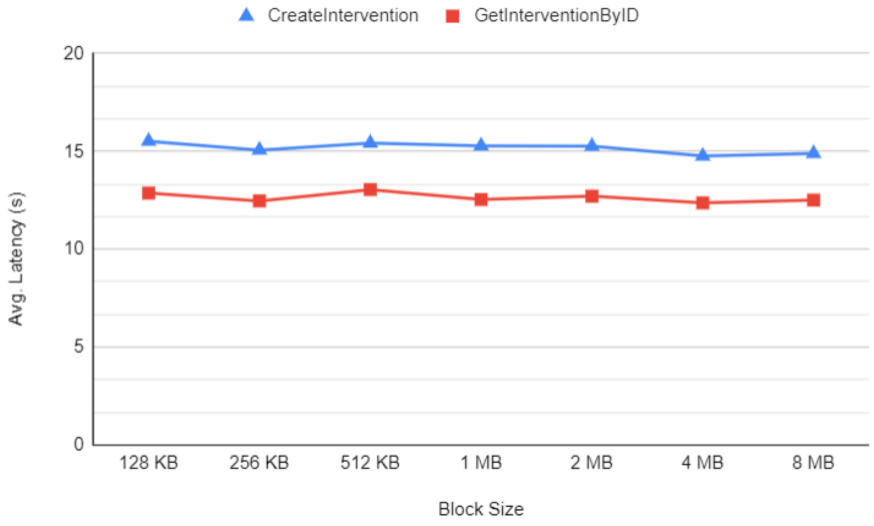


Figure 5.2: Results of latency (measured in seconds) of the Hyperledger Fabric network and chaincode functions used, while varying the block size (using 10 transactions per block).

It is important to remind that the evaluation of a Hyperledger Network is intrinsically connected to the test environment used for the 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.

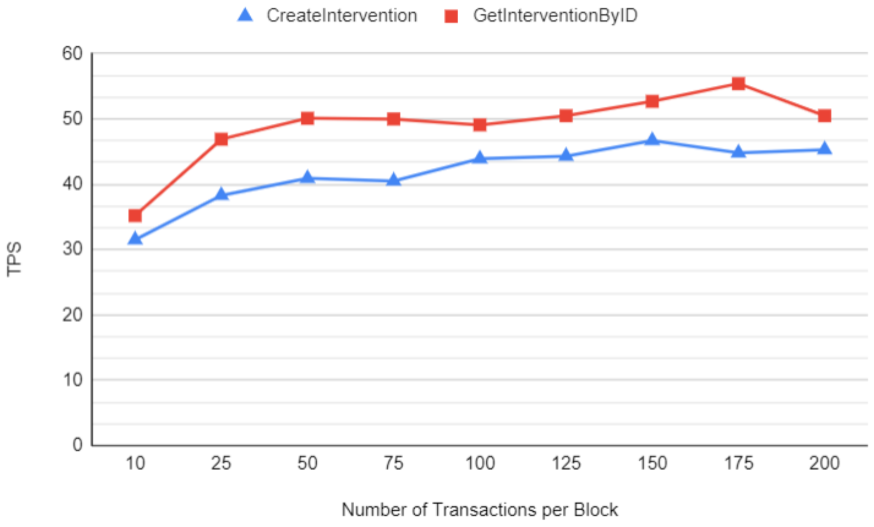


Figure 5.3: Results of throughput (measured in TPS) of the Hyperledger Fabric network and chaincode functions used, while varying the number of transactions per block (using a block size of 2 MB).

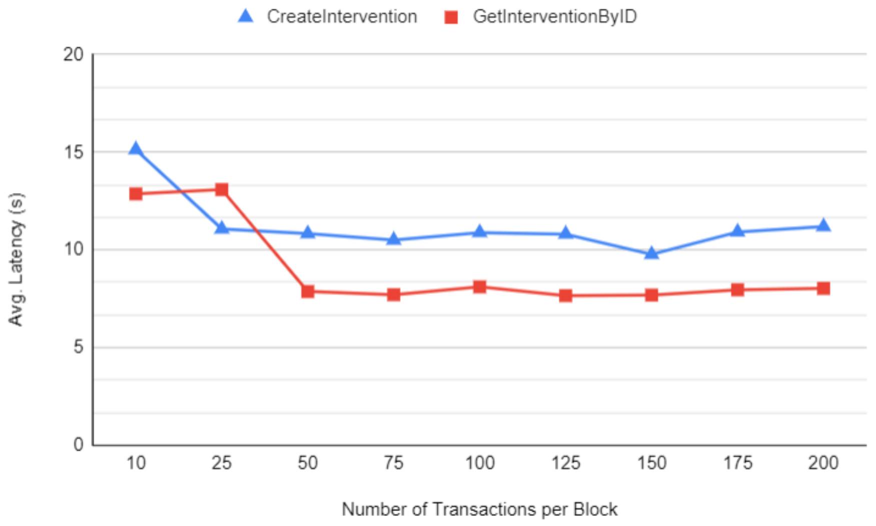


Figure 5.4: Results of latency (measured in seconds) of the Hyperledger Fabric network and chaincode functions used, while varying the number of transactions per block (using a block size of 2 MB).

5.3.2 API and Database Evaluation

To evaluate the API and database capabilities, a Python language script was created to communicate with the API. The REST API after receiving the load generated, creates the necessary links between the transaction and the database module and submits the transactions to the Blockchain module (Hyperledger Fabric network), and inserting the personal information data and the health record data in different databases. The proposed implementation allowed the separation between personal records and health records while maintaining the traceability of the data by integrating as a blockchain module connecting both databases. After the insertion of the data, the reading of data was tested by using a ID stored in one of the databases and using the chaincode function *GetInterventionByID* to access the data from the database containing the health records. The success of this evaluation shows the capabilities of the entire system, integrating blockchain technology in a health record system.

5.3.3 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 5.5 illustrates the amount of disk space used in each group of transactions.

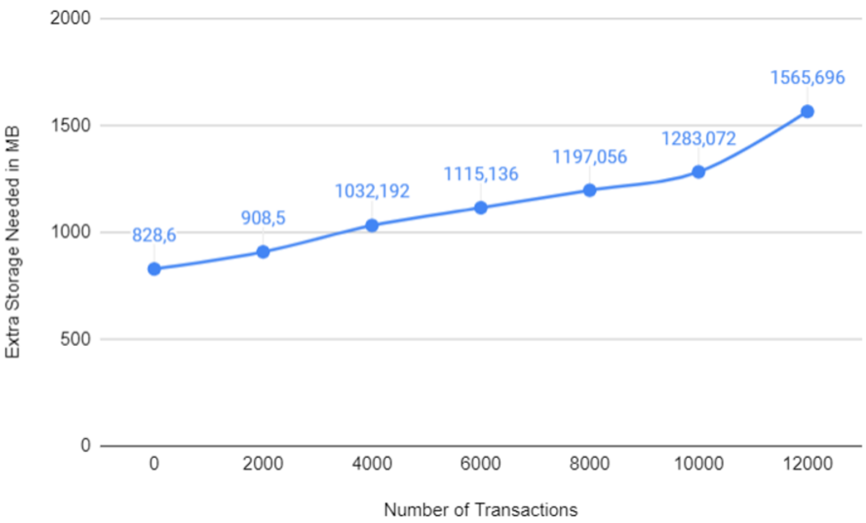


Figure 5.5: Extra storage necessary to implement blockchain technology to traditional healthcare records.

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 5.2 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.

5.4 Conclusion

This chapter described how the system and the Hyperledger Fabric network performance were evaluated. These evaluation tests allowed for the implementation of a network with preferable throughput and reduced latency in the possible test environment. The analysis of the amount of possible storage needed was also fulfilled in order to realize the viability of the integration of blockchain technology in a traditional health record system based only on databases. Conclusively, this chapter served to test the viability of the system and evaluating the performance of the Hyperledger Network running on the test environment defined.

Chapter 6

Conclusions and Future Work

6.1 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 reach this primary objective, it was necessary to study blockchain technology and how it can be integrated with health systems and develop a novel Proof-of-Concept for a m-health system capable of enabling data traceability and 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 [MHO+19], [NPDS19], [GOK+18], [ZL18], [LZS+18], [IKU17], [BBR18], [SSI19]. 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 any 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.

Ultimately, it can be concluded that all the defined objectives for this work were successfully achieved.

6.2 Future Work

To conclude this work, suggestions of research directions for future work will now be presented:

- **Implementation of Authentication:** The implementation of a robust fully-fledged authentication and communication system is a crucial component of every m-health system. However, it was not implemented by being out of the defined scope of this work. Additionally, the integration of the system in a real-world environment would also require the integration with federated authentication methods in order to validate the identity of the users of the system;
- **Integration with Applications:** The proposed system implements a system structure that enables data traceability and ownership of data due to the blockchain module implement. However, to completely promote the ownership of the health data, the patient-user must be able to use an application to connect to the proposed system and access all the health data owned by the user. This process is supported by the proposed system, yet an application was not developed to utilize this resource. Furthermore, an application that uses IoT devices to generate health record information could also be integrated into the system with ease;
- **Further Optimization of the Database and Blockchain Modules:** Further analysis of the performance of the blockchain network and introduce a cryptographic robust solution for the data stored off-chain. The off-chain solution should be implemented in a secure and scalable manner, further enabling the potential of blockchain implementation in a system such as this;
- **Integration in a Real-Life Environment:** After the implementation of the previously mentioned suggestions, the next step should be the integration of the system in a large-scale health system. The results of such implementation should be analyzed in terms of performance and availability, integration with fully implemented health systems, and patient usability and ownership of data.

Bibliography

[ABB^{+}18] Elli Androulaki, Artem Barger, Vita Bortnikov, Christian Cachin, Konstantinos Christidis, Angelo De Caro, David Enyeart, Christopher Ferris, Gennady Laventman, Yacov Manevich, Srinivasan Muralidharan, Chet Murthy, Binh Nguyen, Manish Sethi, Gari Singh, Keith Smith, Alessandro Sorniotti, Chrysoula Stathakopoulou, Marko Vukolić, Sharon Weed Cocco, and Jason Yellick. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. In *Proceedings of the Thirteenth EuroSys Conference*, EuroSys '18, New York, NY, USA, 2018. Association for Computing Machinery. Available from: `https://doi.org/10.1145/3190508.3190538`. 18

[Aul18] Michael Ault. Why new off-chain storage is required for blockchains Document version 1.0. October 2018. Available from: `https://doi.org/10.13140/RG.2.2.34421.22242`. 31

[BBG10] Kylie Bennett, Anthony Bennett, and Kathleen Griffiths. Security Considerations for E-Mental Health Interventions. *Journal of medical Internet research*, 12:e61, 12 2010. Available from: `https://doi.org/10.2196/jmir.1468`. 7

[BBR18] James Brogan, Immanuel Baskaran, and Navin Ramachandran. Authenticating Health Activity Data Using Distributed Ledger Technologies. *Computational and Structural Biotechnology Journal*, 16:257 – 266, 2018. Available from: `http://www.sciencedirect.com/science/article/pii/S2001037018300345`. 12, 13, 39

[But15] Vitalik Buterin. A Next-Generation Smart Contract and Decentralized Application Platform. 2015. Available from: `https://ethereum.org/en/whitepaper/`. 8, 9

[fS18] International Organization for Standardization. ISO 9241-11:2018(en) - Ergonomics of human-system interaction — Part 11: Usability: Definitions and concepts. Standard, International Organization for Standardization, 2018. 7

[GOK^{+}18] Kristen Griggs, Olya Ossipova, Christopher Kohlios, Alessandro Baccarini, Emily Howson, and Thaier Hayajneh. Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. *Journal of Medical Systems*, 42, 06 2018. 11, 13, 39

[GW17] Varadraj P. Gurupur and Thomas T. H. Wan. Challenges in implementing mHealth interventions: a technical perspective. *mHealth*, 3(8), 2017. Available from: `https://mhealth.amegroups.com/article/view/16006`. 7

[Hyp] A blockchain platform for the enterprise. Available from: https://hyperledger-fabric.readthedocs.io/en/release-2.2/ [cited 2021-08-07]. 8, 9, 11, 18, 20

[IKU17] Daisuke Ichikawa, Makiko Kashiyama, and Taro Ueno. Tamper-resistant mobile health using blockchain technology. *JMIR Mhealth Uhealth*, 5(7):e111, Jul 2017. Available from: http://mhealth.jmir.org/2017/7/e111/. 12, 13, 14, 39

[Kam16] Manaschandra Kamana. Investigating usability issues of mhealth apps for elderly people : A case study approach. Faculty of Computing Blekinge Institute of Technology, 2016. 7

[Kar00] Kristiina Karvonen. The beauty of simplicity. In *Proceedings on the 2000 Conference on Universal Usability*, CUU '00, page 85–90, New York, NY, USA, 2000. Association for Computing Machinery. Available from: https://doi.org/10.1145/355460.355478. 7

[KKOM17] Tsung-Ting Kuo, Hyeoneui Kim, and Lucila Ohno-Machado. Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association*, 24:1211–1220, 11 2017. 9

[KNPS13] Sudhakar Kumar, Wendy Nilsen, Misha Pavel, and M. Srivastava. Mobile Health: Revolutionizing Healthcare Through Transdisciplinary Research. *IEEE Computer Society*, 46:28–35, 01 2013. Available from: https://doi.org/10.1109/MC.2012.392. 5

[LA18] Vasco Lopes and Luís A. Alexandre. An Overview of Blockchain Integration with Robotics and Artificial Intelligence. *CoRR*, abs/1810.00329, 2018. Available from: http://arxiv.org/abs/1810.00329. 8

[LKM12] D. D. Luxton, R. A. Kayl, and M. C. Mishkind. mHealth data security: The need for HIPAA compliant standardization. *elemedicine and e-Health*, 18(4):284––288, 2012. 7

[LO09] A. Lorenz and R. Oppermann. Mobile health monitoring for the elderly: Designing for diversity. *Pervasive and Mobile Computing*, 5(5):478––495, 2009. 6

[LZS+18] Hongyu Li, Liehuang Zhu, Meng Shen, Feng Gao, Xiaoling Tao, and Sheng Liu. Blockchain-based data preservation system for medical data. *Journal of Medical Systems*, 42, June 2018. 12, 13, 39

[MCS+21] G. Mendes, D. Chen, B. C. Silva, C. Serrão, and J. Casal. A novel reputation system for mobile app stores using blockchain. *IEEE Computer Society*, 54(02):39–49, February 2021. Available from: https://doi.org/10.1109/MC.2020.3016205. 18, 35

[MHO+19] Tomomitsu Motohashi, Tomonobu Hirano, Kosuke Okumura, Makiko Kashiyama, Daisuke Ichikawa, and Taro Ueno. Secure and Scalable mHealth Data Management Using Blockchain Combined With Client Hashchain: System Design and Validation. *Journal of Medical Internet Research*, 21(5):e13385, May 2019. Available from: `http://www.jmir.org/2019/5/e13385/`. 10, 13, 39

[Nag14] Khaled Nagaty. Mobile health care on a secured hybrid cloud. *cyber journals Multidisciplinary Journals in Science and Technology Journal of Selected Areas in Health Informatics (JSHI)*, 3, 04 2014. 7

[Nak09] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2009. Available from: `http://www.bitcoin.org/bitcoin.pdf` [cited 2021-09-14]. xiii, 8

[Nov14] G. Novak. Developing a usability method for assessment of M-Commerce systems : a case study at Ericsson. Faculty of Computing Blekinge Institute of Technology, 2014. 7

[NPDS19] 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*, 7:66792–66806, 2019. 11, 13, 14, 39

[OO14] D. Ongaro and J. Ousterhout. In search of an understandable consensus algorithm. *USENIX*, pages 305–320, 01 2014. 20

[PDG18] María Pérez, Carlos Dafonte, and Ángel Gómez. Traceability in Patient Healthcare through the Integration of RFID Technology in an ICU in a Hospital. *Sensors*, 18:1627, 05 2018. 10

[PG18] Hyperledger Performance and Scale Working Group. Hyperledger blockchain performance metrics, Oct 2018. Available from: `https://www.hyperledger.org/learn/publications/blockchain-performance-metrics`. 33, 34

[SLRR11] B. M. Silva, I. M. Lopes, J. J. P. C. Rodrigues, and P. Ray. Sapo fitness: A mobile health application for dietary evaluation. *2011 IEEE 13th International Conference on eHealth Networking, Applications and Services*, 310(22):375–380, 2011. 6

[SMT13] S. Steinhubl, E. Muse, and E. Topol. Can mobile health technologies transform health care? *Jama*, 310(22):2395–2396, 2013. 1, 6

[SSI19] J. Santos, B. Silva, and P. Inácio. A blockchain system for mobile health applications and services. Master's thesis, 2019. 1, 6, 8, 27, 30, 39

[Sza97] Nick Szabo. Formalizing and Securing Relationships on Public Networks. *First Monday*, 2(9), September. 1997. Available from: `https://journals.uic.edu/ojs/index.php/fm/article/view/548`. 9

[Top16] Top Threats Working Group CSA. ”the treacherous 12 cloud computing top threats in 2016”, February 2016. Available from: `https://cloudsecurityalliance.org/press-releases/2016/02/29/cloud-security-alliance-releases-the-treacherous-twelve-cloud-computing-top-threats-in-2016/` [cited 2021-03-02]. 7

[WZ12] W. Wilkowska and M. Ziefle. Privacy and data security in e-health: Requirements from the user’s perspective. *Health informatics journal*, 18(3):191––201, 2012. 7

[ZL18] Aiqing Zhang and Xiaodong Lin. Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. *Journal of Medical Systems*, 42, 06 2018. 11, 13, 39