UNIVERSIDADE DA BEIRA INTERIOR
Engenharia

A Blockchain System for Mobile Health Applications and Services

João Alexandre de Aguiar Amaral dos Santos

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

Orientador: Prof. Doutor Bruno Silva
Co-orientador: Prof. Doutor Pedro Inácio

Covilhã, Setembro de 2019

Resumo

Com o aparecimento das tecnologias *blockchain*, o crescimento e adaptação de características criptográficas levaram à exploração de novos usos em novas áreas, como a computação móvel para a saúde (*m-Health*). Atualmente, estas tecnologias são implementadas primáriamente como mecanismos para manter os registos de saúde eletrónicos seguros. No entanto, novos estudos têm provado que estas apresentam-se como uma ferramenta poderosa para promover o controlo da informação de saúde pelos próprios pacientes e possibilita a existência de um historial médico sem alterações errôneas, para além da responsabilização dos profissionais de saúde. Nos últimos anos, verificou-se um rápido crescimento da área da *m-Health*, sustentada numa arquitetura orientada a serviços, levando a que a adaptação de mecanismos de *blockchain* em aplicações de saúde gerasse a possibilidade da existência de um serviço mais descentralizado, pessoal e disponível. A ideia de adaptar tecnologia *blockchain* na área da prestação de serviços de saúde apresenta inicialmente alguns pontos críticos, como por exemplo como é que é assegurada a segurança e a privacidade da informação de saúde guardada na *blockchain*. Normalmente, num sistema completamente descentralizado, a informação tem de estar completamente disponível a atores externos e tem de ser guardada de forma distribuída.

Embora o armazenamento da informação de forma distribuída não apresente dificuldades, a particulariedade do tipo de informação que é guardada na *blockchain* e de que maneira esta é mantida privada e segura são questões problemáticas já conhecidas. Um breve estudo desta tecnologia é suficiente para concluir que não é adequado um registo médico de um paciente ser guardado na *blockchain*, uma vez que, devido ao tamanho do registo, iria gerar problemas de escalabilidade com o aumento do número de pacientes. Perante esta situação, o desempenho da *blockchain* iria diminuir e seria necessária uma quantidade demasiado elevada de poder computacional para a realização de tarefas básicas, gerando ainda um aumento nos requisitos de armazenamento e de transmissão em rede. Embora a *blockchain* não tenha capacidade para guardar a informação completa de um paciente, as suas características permitem que seja utilizada para guardar outros dados relacionados com a privacidade da informação da saúde. Deste modo, é precisamente no registo e controlo de acesso à informação de saúde que a tecnologia *blockchain* promete inovar. Ao registar todos os acessos à informação de saúde de um paciente, é possível criar um registo com a identificação e a autentificação de todos os utilizadores do sistema que requereram o acesso a determinada informação de saúde. Portanto, um registo de acesso consegue ser criado com uma pequena quantidade de informação, como um timestamp, com a identificação do utilizador que está a aceder aos dados e com a identificação do utilizador cujos dados estão a ser acedidos. Uma das grandes vantagens de registar a informação dos acessos numa *blockchain* é o facto de os registos serem distribuídos por várias localizações, sendo estas imutáveis e tolerantes a falhas e públicos. Deste modo, verifica-se que os problemas de escalabilidade, associados ao tamanho reduzido do registo, que surgem ao guardar informação na *blockchain* discutidos previamente conseguem ter um impacto mais reduzido.

Contudo, apesar das vantagens desta tecnologia, alguns dos aspetos da sua integração desta em *m-Health* não são compatíveis com a natureza da informação de saúde de um paciente. Para acomodar tecnologia blockchain na área da saúde, é necessário que o sistema seja construído com várias restrições em mente. Uma destas restrições é o facto de que a informação presente

na *blockchain* é normalmente pública, o que entra em conflito com o direito à privacidade dos pacientes e leva à necessidade de encriptar a informação. Outra restrição é o facto de como identificar um utilizador num registo de acesso, uma vez que normalmente a informação dos utilizadores é anónima.

O objetivo desta dissertação é estudar como a tecnologia *blockchain* consegue ser conjugada com a informação de saúde recolhida ou processada por aplicações móveis. Com a finalidade de alcançar esse objetivo, foi desenvolvido um protótipo de uma solução baseada em *blockchain* para controlar acesso à informação de saúde. Este protótipo para além de oferecer uma segurança melhorada da informação, devido à implementação de mecanismos de criptografia, oferece um historial médico imutável ao armazenar informação de eventos de saúde numa *blockchain*. A esta construção foi ainda adicionado um sistema de armazenamento de dados anónimos baseado numa arquitetura de *data lake*. Posteriormente, este protótipo foi integrado num ambiente de teste, que consistiu em várias aplicações móveis, com o objetivo de testar detalhadamente a viabilidade e desempenho de propostas similares.

Palavras-chave

Aplicações Móveis, Blockchain, Bases de Dados Distribuídas, Estado da Arte, Saúde, Segurança.

Resumo alargado

Introdução e Motivação

A tecnologia *blockchain*, conhecida principalmente pela sua aplicação na *Bitcoin*, tem tido um profundo impacto em várias áreas de estudo para além da área de criptomoedas, muito devido à forma como os dados são armazenados e às suas propriedades de segurança. Atualmente, ainda decorrem diversas investigações com o objetivo de aprofundar o conhecimento acerca da tecnologia *blockchain* e de que formas se pode usufruir das suas vantagens e como podem ser aplicadas em variadas áreas de estudo, como por exemplo em análises preditivas, finanças ou robótica. Embora se verifique claramente a existência de áreas que beneficiam da integração de tecnologia *blockchain*, em outras a discussão torna-se mais complexa e algumas das suas características intrínsecas não são facilmente entendidas. Uma das áreas onde o impacto é positivo é na área da saúde. Inicialmente, o conceito de saúde eletrónica estava associado apenas aos mecanismos de comunicação e de armazenamento entre prestadores de serviços de saúde e entre estes e os pacientes.

Registos médicos poderiam ser facilmente acedidos e comunicados para os pacientes ou outras entidades de forma quase instantânea ao utilizar dispositivos móveis. Atualmente, a área da *Mobile Health (m-Health)* está a evoluir rapidamente e as capacidades dos dispositivos aumentam de dia para dia, o que permite muito mais do que uma simples comunicação entre utilizadores. A evolução dos dispositivos móveis, como telemóveis inteligentes, permite que os dispositivos adquiram dados, que os armazenem e, inclusive, que efetuem o seu processamento diretamente. Além disso, os dispositivos móveis como telemóveis inteligentes são equipados com vários sensores que podem ser utilizados para monitorizar sinais vitais dos utilizadores em tempo real. Ao armazenar informações sobre um paciente em tempo real, torna-se possível analisar e estudar alterações nos padrões dessas informações ao longo do tempo, resultando numa maior perceção sobre a condição de saúde do paciente. Devido à natureza das informações de saúde, torna-se uma prioridade garantir que o sistema que lida com essas informações seja seguro e possa garantir a sua privacidade e a segurança de armazenamento.

Motivações e Objetivos

A motivação desta dissertação é estudar a viabilidade da implementação de *blockchain* em sistemas *m-Health*. Com o rápido crescimento que a tecnologia *blockchain* tem apresentado, juntamente com a notoriedade adquirida por ser um caso amplamente discutido de uma tecnologia que pode ser integrada em vários campos, é necessário um estudo mais aprofundado sobre a função e as vantagens da sua integração. A escolha de estudar a integração da *blockchain* no campo *m-Health* surgiu do crescente interesse dos pacientes em tratarem dos seus próprios problemas de saúde e na proteção de dados do paciente. Esse interesse é acompanhado por um aumento acentuado no número de aplicativos relacionados à saúde desenvolvidos e usados para dispositivos móveis inteligentes.

Os sistemas eletrónicos de saúde, incluindo os sistemas *m-Health*, apresentam vários problemas, incluindo a falta de propriedade das informações de saúde pelo paciente, a natureza centralizada dos sistemas de saúde atuais, a sua interoperabilidade e as práticas de segurança defeituosas na transmissão e armazenamento de informações de saúde. Após um estudo mais aprofundado dos aspetos que definem *m-Health* e *blockchain*, é concluído que várias características da *blockchain* podem ser usadas para enfrentar diretamente as dificuldades que afetam o campo da saúde eletrónica e podem ter um impacto positivo na *m-Health*. Ademais, a natureza descentralizada e aberta da *blockchain* pode ser usada para promover a descentralização dos sistemas de saúde atuais, juntamente com mais transparência das informações armazenadas.

O principal objetivo deste trabalho é estudar como a tecnologia *blockchain* pode ser usada com informações de saúde adquiridas através de aplicações móveis.

Abordagem ao Problema

Como ponto de partida, de maneira a compreender claramente a tecnologia de *blockchain* e o ecosistema de *m-Health*, é necessário um estudo aprofundado dos conceitos fundamentais e do estado da arte. Este estudo permite perceber as vantagens da *blockchain* e da integração de sistemas de *m-Health*, os desafios associados e onde as duas áreas se interceptam. Para ajudar a entender como estas tecnologias podem ser integradas em conjunto é necessário pesquisar como aplicações existentes lidam com os desafios de cada uma delas. Assim sendo, são estudadas as arquiteturas e implementações de soluções existentes, com foco no tipo de *blockchain* utilizada, como é que a informação é armazenada e transmitida e como as aplicações móveis são integradas em sistemas baseados em *blockchain*.

Após compreender as tecnologias e onde as implementações atuais são bem sucedidas e onde falham, o próximo passo é perceber como desenhar um sistema que aproveite as características da *blockchain* para melhorar sistemas de saúde similares aos usados atualmente. De maneira a ter uma ideia mais clara de como desenhar este sistema, são estudados os principais desafios associados à *blockchain* e à área da *m-Health* e são desenvolvidas propostas de soluções que são testadas posteriormente. Assim, é possivel delinear quais os principios que o sistema deve seguir de maneira a garantir que o desenvolvimento resulte numa solução de qualidade. Para ajudar nesta tarefa, e devido à necessidade da informação de saúde ser privada, é estabelecido um conjunto de requisitos de segurança.

Após definir o conjunto de princípios fundamentais e requisitos que o sistema deve respeitar, têm de ser definidas as tecnologias a serem utilizadas para construir e desenvolver a solução. Para este efeito, a investigação acerca das normas de desenvolvimento da indústria prova ser útil, sobretudo em ditar o que tem potencial para funcionar e o que já foi exposto como de fraca qualidade. Posteriormente ao desenvlvimento da solução são requiridos testes extensos para medir a sua qualidade. Deste modo, a solução proposta é integrada e testada num ambiente de teste desenhado especialmente para simular um ambiente real de *m-Health*, permitindo concluir a viabilidade da solução. Após os testes, e consoante os resultados obtidos, alterações e revisões, as conclusões são introduzidas na arquitetura e no desenvolvimento de maneira a aumentar a qualidade da solução. Os resultados de testes subsequentes podem levantar situ-

ações onde melhorias não podem ser introduzidas devido a limitações de complexidade, recursos necessários ou tempo. Assim sendo, é possível delinear trabalho futuro.

Para refletir a abordagem escolhida, esta dissertação apresenta uma revisão compreensiva do estado da arte de *m-Health* e de aplicações *blockchain* na saúde. Além disso, discute os maiores desafios e vantagens da aplicação de *blockchain* em sistemas de *m-Health*, focando nos problemas-chave. Este trabalho elabora uma proposta para um solução de blockchain para sistemas de saúde eletrónicos a nível do controlo e registo de acessos a informação de saúde, composta por vários mecanismos criptográficos que promovem a privacidade da informação de saúde no sistema. Ademais, é apresentada uma discussão da integração e funcionamento do sistema proposto num ambiente de teste. São ainda discutidos aspetos como a viabilidade e o desempenho, permitindo avaliar melhor as vantagens e o potencial da proposta.

Contribuição Principal

A principal contribuição desta dissertação é um sistema baseado em tecnologia *blockchain* que visa promover a descentralização e controlo de dados de saúde de pacientes através da integração de aplicações móveis e serviços. Este sistema foi projetado para promover a propriedade das informações de saúde por um paciente, mantendo registos imutáveis de todos os acessos às suas informações. O sistema proposto também incorpora vários recursos de segurança e infraestrutura que contribuem para a qualidade geral oferecida, bem como apresenta a integração de vários mecanismos e práticas de segurança que garantem a privacidade e a segurança das informações armazenadas. Para desenvolver o protótipo Blockchain Access Record System (BARS) foi realizado um estudo do estado da arte em sistemas e tecnologias para a saúde e *blockchain*, que culminou num trabalho de pesquisa que apresenta um levantamento desses assuntos, uma discussão sobre questões atuais e propõe possíveis soluções. Este estudo foi enviado para o *Journal of Biomedical Informatics*, publicado pela *Elsevier*, onde aguarda revisão.

Organização da Dissertação

Conceitos Fundamentais e Trabalhos Relacionados

O capítulo 2 introduz vários conceitos fundamentais sobre as tecnologias e temáticas abordadas nesta dissertação, assim como um pouco da história destas. Tendo por base este conhecimento, é possível perceber em detalhe no que consistem estas tecnologias e como a sua conjugação pode ser favorável em determinadas áreas. Assim, de maneira a introduzir a área da *m-Health*, é necessário enquadrar em que consiste, o porquê de ser necessária, o porquê do seu crescimento e que fatores o influenciaram. Para perceber o panorama atual desta área é apresentada uma revisão das suas inovações e implementações mais recentes. A privacidade de dados de saúde é um princípio fundamental para qualquer sistema de saúde eletrónico por isso, é necessário compreender como este é respeitado em soluções atuais. Assim, é feita uma apresentação dos mecanismos de segurança atualmente em uso na área da *m-Health*.

De maneira a compreender no que consiste a tecnologia *blockchain*, é elaborada uma breve explicação das suas ideias-base, tais como o porquê de ter surgido o protocolo, uma breve introdução à sua história e a sua evolução. Ademais, é apresentada a evolução das implementações do protocolo blockchain, desde *blockchain* 1.0 até 3.0. Após cobrir as bases do protocolo, as recentes inovações e implementações do protocolo são abordadas, onde vários exemplos de integração de blockchain em variadas áreas são explicados. Exemplos da integração na área das finanças, da inteligência artificial, da robótica, em Internet of Things (IoT) e do comércio.

Conceito do Sistema e Requisitos de Segurança

O capítulo 3 discute os problemas e desafios que a área de *m-Health* apresenta de maneira a conseguir delinear as suas áreas problemáticas. Ao identificar estas áreas é possível perceber como os problemas podem ser mitigados e quais os aspetos fundamentais que vão restringir o desenvolvimento da solução. Sabendo estes aspetos, e sabendo que lidamos com informação de saúde, podemos definir requisitos de segurança para a solução que podem depois guiar o desenho da proposta do sistema. Assim, neste capítulo é elaborada uma apresentação dos problemas de segurança que existem na área *m-Health* e como afetam o desenvolvimento de requisitos de segurança. Especificamente, o capítulo discute as características e a natureza das informações de saúde e que tratamento deve ser realizado para lidar com essas informações de modo que a privacidade do paciente não seja colocada em risco. Essa discussão é traduzida em vários requisitos de segurança que um sistema *m-Health* deve cumprir. Com esses requisitos em mente, é apresentada uma proposta de uma solução *blockchain* para sistemas móveis de saúde. No fim do capítulo, são discutidos os requisitos de segurança.

Integração num Ambiente de Teste e Discussão sobre a Segurança

O capítulo 4 aborda os testes do sistema que foi desenvolvido baseado na proposta apresentada no capítulo anterior, proposta que culminou no desenvolvimento do BARS. Especificamente, o capítulo introduz o ambiente de testes que foi utilizado para testar a solução desenvolvida, explicando em detalhe os componentes que constituem esse ambiente de teste e como esses componentes impactam e colaboram com o BARS. Após a realização destes testes e da análise do trabalho efetuado é possível concluir acerca da viabilidade e desempenho geral do BARS, mas também da sua facilidade de desenvolvimento continuado e integração em outros sistemas. Brevemente, o capítulo apresenta em detalhe as aplicações móveis para a saúde do ambiente de teste, usadas com o objetivo de testar o protótipo BARS. São apresentados e discutidos os resultados obtidos da avaliação de desempenho da implementação do BARS nas respetivas aplicações, bem como a viabilidade deste sistema.

Considerações Finais e Trabalho Futuro

No capítulo 5, são apresentadas as considerações finais desta dissertação, são discutidos os resultados gerais deste trabalho. Ademais, é apresentada uma reflexão acerca dos objetivos

apresentados inicialmente e a sua comparação tanto com o sistema desenvolvido como com a investigação apresentada. Depois de explorar os detalhes da execução da dissertação são apresentadas sugestões de direções de investigação para trabalho futuro.

Abstract

With the advent of blockchain, the growth and adaptation of cryptographic features and capabilities were quickly extended to new and under-explored areas, such as healthcare. Currently, blockchain is being implemented mainly as a mechanism to secure Electronic Health Record (EHR)s. However, new studies have shown that this technology can be a powerful tool in empowering patients to control their own health data, as well as for enabling a fool-proof health data history and establishing medical responsibility. With the advent of mobile health (m-Health) sustained on service-oriented architectures, the adaptation of blockchain mechanisms into m-Health applications creates the possibility for a more decentralized and available healthcare service. The idea of adapting blockchain technology into healthcare initially presents several critical points where special consideration is required, such as how privacy and security of healthcare information can be assured if information is stored into a blockchain. Usually, for a completely decentralized system, the information has to be available to everyone and is to be stored in a distributed manner. While the storage of the information being distributed is not difficult, what kind of information should be stored into the blockchain as well as how this information can be kept private and secure present issues. A brief study of blockchain technology is enough to conclude that a full patient record is not fit to be stored into a blockchain, because the size of the record would create scalability problems as the number of patient records increases. This diminishes the performance of the blockchain to where the amount of computational power needed to perform basic tasks would rise considerably, as well as the storage and network requirements needed to permanently store the information and to replicate the information throughout the whole network, respectively. However, other uses for blockchain technology arise once the nature of the health information is analyzed thoroughly.

Because of the highly personal and private aspect of health information belonging to a patient, the security of how that information is stored, transmitted and accessed becomes a main focus of health systems. It is precisely in access recording and management of healthcare information that blockchain shows promise in implementation. By recording all accesses to a the health information of a patient, it is possible to create a log of every user in a system that has had access to some information. By having a system that identifies and authenticates all users, every access to health data can be recorded as having been done by an identified user. An access record can be made with a small amount of information, such as a timestamp, an accessing user identifier and an identifier of the user whose data is being accessed. Because an access record can be accomplished with only this amount of information, the scalability issues that where discussed earlier regarding storing information into a blockchain can be mitigated. In terms of advantages, recording access information into a blockchain results in the access records being distributed across several locations, immutable, fault-tolerant and public. However, some aspects of the integration of blockchain into healthcare result in incompatibilities of the nature of health information and of blockchain. To accommodate health information and blockchain, the surrounding system must be constructed with several limitations in mind. One of which is the public nature of blockchain not being in line with the private nature of health information and therefore the information must be encrypted, or how a user can be identified in an access record if usually information in a blockchain is anonymous.

This work proposes a system that successfully integrates blockchain into an m-Health testbed, outlining how both areas have evolved and their main challenges. The proposed system offers enhanced information security both in transmission, storage and access, by integrating several cryptographic mechanisms. Furthermore it is integrated with a blockchain access system and a high volume anonymous information storage mechanism based on a data lake database architecture. This system is integrated into a testbed that allows for a more detailed discussion on viability and performance of similar concepts.

Keywords

Blockchain, Data Lake, Electronic Health Record, Health, Mobile, Security, State of the Art.

Contents

List of Figures

List of Tables

Acronyms

AES	Advanced Encryption Standard
AI	Artificial Intelligence
API	Application Programming Interface
BARS	Blockchain Access Record System
DApps	Distributed Applications
ECDHe	Elliptyc Curve Diffie-Hellman Ephemeral
EHR	Electronic Health Record
GDPR	General Data Protection Regulation
GPS	Global Positioning System
HIAS	Home Intelligent Assistant Services
HMAC	Hash-based Message Authentication Code
HSP	Health Service Provider
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
IoT	Internet of Things
IP	Internet Protocol
IT	Information Technology
m-Health	Mobile Health
ML	Machine Learning
MVC	Model-View-Controller
SHA	Secure Hash Algorithm

SQL Structured Query Languade

SSL Secure Sockets Layer

TCP Transmission Control Protocol

TLS Transport Layer Security

Chapter 1

Introduction

1.1 Scope of the Dissertation

Blockchain technology, mostly know by its application on Bitcoin [1], has nowadays a profound impact on a significant number of areas of knowledge, well beyond the cryptocurrencies application scenario. The applicability of blockchain technology affects how data is stored and its security properties. Widespread research into these technologies is still being made in order to leverage its advantages and use them in varied fields of knowledge, such as predictive algorithms, finances or robotics [2, 3]. While there are some areas that clearly benefit from the capabilities of blockchain technology, in others the discussion becomes more complex and the advantages are not well understood from the start, since research is overall in early stage. One area where the benefits are clearly comprehensible is healthcare, particularly, m-Health [4].

Initially, the concept of electronic health (e-Health) was only associated with communication mechanisms between health service providers and between them and the patients. Medical records could be easily accessed and communicated to patients or other entities almost instantly by using mobile devices like cellphones or personal computers [5]. Currently, m-Health is an evolving field with new advancements occurring every day, and its complexity and capabilities have increased exponentially, allowing much more than just communications between users. The evolution of mobile devices in recent years, enabled remote data collection, access, sharing and processing, as well as interfacing with the user in order to provide information in a comprehensible behaviour. Moreover, mobile devices are now commonly equipped with several sensors and interfaces, transforming them in perfect monitoring tools for users, that in anytime and anywhere can access information on various health metrics, enabling self-care, health education [6].

However, m-Health and any other systems that encompasses a service-oriented architecture, do not come without concerns and issues that must be addressed. These systems must guarantee service quality and safety to gain widespread credibility to the point where cooperation between traditional health service providers and these new devices can be achieved. Hence, the health system itself will change by making use of the advantages these technologies provide in order to improve availability, security and service quality [7]. Healthcare information is characterized by being of a highly private and personal nature and by the need of having records of past information. By storing past information about a patient, it becomes possible to analyze and study changes in patterns of that information through time, resulting in increased insight on the health condition of the patient. Because of the nature of health information, it becomes a priority to ensure that the system that handles this information is secure and can give guarantees regarding the privacy and storage of the health information.

1.2 Motivation and Objectives

The motivation behind this dissertation is to study the viability of the implementation of blockchain in m-Health systems. With the quick growth that blockchain technology has had, along with the notoriety gained from being a widely discussed case of a technology that is able to be integrated in several fields, deeper study into the function and advantages of integrating blockchain is needed. Choosing to study the integration of blockchain in the m-Health field comes from the growing interest in self-care and patient data protection. This interest is accompanied with a steep increase in the number of health-related applications being developed and used for mobile smart devices as well as a recent push in user data protection regulations, such as with the *GDPR* in the European Union.

Electronic health systems, including m-Health systems, present several issues including the lack of ownership of healthcare information by the patient, the centralized nature of current health systems, the interoperability of electronic health systems and the faulty security practices in transmitting and storing healthcare information. After closer study of both the aspects that define m-Health and blockchain technology, several characteristics of blockchain can be used to directly tackle difficulties plaguing the electronic health field, with many having impact on m-Health. The decentralized and open nature of blockchain can be used to promote the decentralization of current health systems along with more transparency of stored information.

The main objective of this work is to study how blockchain technology can be used with healthcare information that is either acquired or interfaced with via a mobile application. As such, a prototype of a blockchain based solution for access management of health information was constructed, with a focus on the integration of the system in a testbed consisting of several mobile applications. The development of the prototype allowed for a deeper study of blockchain technology, how it integrates with other technologies and what restrictions and conditions dealing with health information an electronic health system has.

1.3 Adopted Approach

As a starting point, to clearly understand blockchain and the m-Health ecosystems, a in-depth study of the fundamental concepts and the state of the art was need. This would allow for a better understanding of the advantages of blockchain and of the integration of m-Health systems, the challenges that are associated and where they both cross paths. To help grasp how the concepts of blockchain can be integrated into m-Health systems, it was necessary to research how existing solutions that integrate these technologies are accomplishing that. As such, studies of the architecture and construction of existing solutions were conducted, with focus on the type of blockchain that was used, how information was stored and transmitted and how mobile applications were integrated into the blockchain-based systems.

After understanding the technologies and where several current implementations succeeded of failed, the next step was to understand how to design a system that would take full advantage of

the blockchain technology in order to enhance systems similar to the ones that are currently in use. To have a clearer idea of the task, the main challenges of these technologies were studied in depth and possible solutions where proposed and developed for testing. With this, it would be possible to outline what principles the system should follow in order to guarantee that the development would result in a quality solution. To help this task, and because of the highly private nature of health information, a set of security requirements had to be established.

After having set the fundamental principles and requirements that the system would need to adhere to, the technologies that should be utilized to construct and develop the proposed solution had to be defined. To do this, research on industry standards proved useful in dictating what had potential to work and what had already been discovered as a failure. After the development of the solution had been completed, extensive testing is required in order to gauge the quality of the solution. As such, the proposed solution should be integrated into a testbed and all testing should be conducted in it, outlining the viability of the solution in similar environments.

After the testing is conducted, changes and improvements can be introduced into the proposed solution and development revisions are to be made in order for the quality of the solution to increase. Analysis of the test results can then bring up situations where the improvements cannot be introduced, because of complexity, resources or time constraints. As such, future work directions can be outlined.

To reflect the adopted approach, this dissertation presents a comprehensive review of the state of the art on m-Health security techniques and current blockchain applications in healthcare. Moreover, it presents and discusses the major challenges and advantages of blockchain application in m-Health systems, highlighting the key issues. It elaborates on a proposal for a electronic health system that integrates blockchain as an access control mechanism, as well as several security mechanisms that aim to enhance the privacy of the health information in the system. In addition, a discussion on the functioning of the proposal in a testbed is made, focusing on how the system integrates with the testbed and how it can be further enhanced. Aspects such as viability and performance of the proposed system are also discussed, allowing for gauging the advantages of the proposal.

1.4 Main Contributions

The main contribution of this work is a blockchain system for access management of healthcare data in mobile health applications and services. This system was designed in order to promote the data ownership of healthcare information by a patient by keeping immutable records of all accesses to his information. To develop the BARS prototype, study into the state-of-the-art in both electronic health, mobile health and blockchain systems and technologies was conducted. This study culminated in a research paper that presents both a survey of these subjects but also a discussion on current issues, as well as proposing possible solutions. This study was sent to the Journal of Biomedical Informatics, published by Elsevier, where it awaits review. The prototype system also incorporates several security and infrastructural features that contribute to the overall offered quality. The system features the integration of several security mechanisms

and practices that assure the privacy and safety of stored information. It was integrated into a testbed composed of several mobile applications, each one of these with enhanced security features, offered by BARS.

1.5 Thesis Organization

The remainder of this thesis is organized as follow:

- Chapter 2 - Introduces the concepts of m-Health, security in m-Health and the blockchain protocol; Specifically, the chapter discusses the recent evolution of m-Health and the technologies that have enabled the growth of the field, the security mechanisms currently in use in these systems as well as their limitations and possible solutions in the form of new technologies, and a brief introduction to what the blockchain protocol consists of and what new uses and features have been developed so far.

- Chapter 3 - Presentation of the security issues that affect the m-Health field and how they impact the development of security requirements for m-Health systems; Specifically, the chapter discusses the characteristics and nature of healthcare information and what kind of treatment must be made in order to handle this information so that the privacy of the patient is not put at risk. This discussion is then translated to several security requirements that an m-Health system should abide to. With these requirements in mind, a proposal for BARS is presented and a discussion on how it respects these requirements is made.

- Chapter 4 - Discussion of the deployment of BARS into the testbed and the security considerations made for smooth operation in the aforementioned testbed; Specifically, the chapter discusses the constitution of the testbed, how BARS was integrated into the testbed and how the functioning is impacted by the testbed itself. The security of the system is also discussed in greater detail, as well as the interaction of the whole system with the blockchain system. To finish the chapter, a discussion on the performance and viability of the proposed system is presented.

- Chapter 5 - Presentation of the final considerations of this thesis work and suggestion of research directions for future work.

Chapter 2

Fundamental Concepts and Related Work

2.1 M-Health and Enabling Technologies

2.1.1 M-Health: An Overview

In recent years, technological evolution and widespread usage of smart mobile devices have allowed new solutions to previous problems in several fields, including the health industry. Traditionally, access to health care information is considered to be a troublesome and lengthy process for patients, due to time and personal constraints. Therefore, the adaptation of mobile technologies is a compelling use case that offers a solution for data and information access [8]. Moreover, it provides several new capabilities and advantages, such as more personalized treatments as well as empowering patients to self-care, which is a possible solution to lifestyle-related chronic diseases and the ability to access health services anywhere and anytime [9]. Several pilot projects and research already show promise, with [10, 11] as clear examples.

The M-Health paradigm shifts the focus from the health service provider back to the patient, by providing the user with valuable, personalized information in a readable format. Patients are now closer to own his health information, due to smart mobile devices that give them control or data access in anytime and anywhere. This health information was and, still is, typically centralized by health service providers, such as hospitals and health professionals. M-Health contributes to a more decentralized health care service, as well as promoting the privacy of the patient health information [12]. Due to the nature of M-Health scenarios and system architectures based on cloud services, patient data is collected in a long interval of time without great direct effort from its user. Therefore, enabling remote patient monitoring and contributing to the practicality and accessibility of solutions based on M-Health [13].

With the evolution and proliferation of powerful personal technology capable of monitoring health metrics, the general population is growing awareness about their health status and living style. This is due, in part, to the availability of systems and applications that enable users to monitor and control their health in ways that have not been possible in the past. Hence, health care services are generally associated with availability problems and the lack of adaptability to the patient, but also due to the mainstream usage of smart technology such as smartphones or smartwatches [14]. While before there was only concern about personalized health data, currently there is both concern and means to implement such systems through M-Health [15].

This availability of powerful devices capable of monitoring and recording health data leads to the empowerment of several underprivileged groups. Personalized health with real time

monitoring is especially important in elderly [16], chronic, disabled [17] and young [18] patients. Moreover, this scenario is desirable when there is a lack of health professionals to treat patients individually, as it happens in many developing countries [10, 11]. Health data collection and recording for later analysis enables personalized health treatment contributing towards a more comprehensive and understandable grasp on users own health. This allows them to act in a much faster and proactive way in case of a health hazard [19].

This growing interest regarding personal health and the widespread usage of smart technology motivated companies, and developers to invest in the production of solutions to monitor personal health. Applications regarding fitness, elderly care and outdoor activity promotion are especially interesting from both a business and a technology standpoint, as we can see in [20], [21, 22] and [23], respectively.

2.1.2 M-Health Enabling Technologies

Presently, the technology that is generally used in M-Health services and applications is evolving and becoming increasingly more accessible to the public. Devices, such as, smartphones or tablets and additional accessories are already equipped with sensors that allow measurements of different metrics and vital signs that can be used to extrapolate health-related information [24]. In fact, metrics such as blood pressure, glucose, the oxygen concentration in the blood, heart rhythm, lung function, and mood can be easily monitored and used to infer problems and conditions of a patients health [25, 26, 27].

Moreover, a wide range of wearable sensors has become available to the public, providing even more biometric measurement mechanisms and possible sources of information to an already evolved network of sensors[28]. Body sensor networks (BSNs) are developed not only in terms of wireless and wearable technology [29], but also on how they interact with other devices and user. The advent of location-based technologies also had a large impact on the field of M-Health. These usually implement methods to add context and location meaning to health data previously collected, adding a new layer of significance to information [30, 31]. In addition to location-based monitoring, it is also possible to combine different aspects of a mobile device and an application, working as a tool to further user engagement. Examples of positive interactions that mobile applications can have in the lifestyle of the user can be seen in [32], with [33] as a good example of an application that uses GPS to promote the health of the users. However, the promise that many mobile applications make in terms of improving user health should not be taken as guaranteed [34].

The availability of a patient health information is a major concern and one of the utmost importance in M-Health systems. General and main issues regarding this information availability are related to its secure storage and retrieval mechanisms. Due to this, storing information in mobile devices is not an appropriate model, since it can be accessed through irregular behaviors, its recovery is not guaranteed and the availability is bound to only one device. Hence, a recently introduced solution is to migrate the data storage to cloud services. The advantages of this approach are discussed in detail in section 2.2.

The introduction and implementation of machine-learning algorithms in the analysis of health data, in order to provide predictive information and counseling to the user, is one big step in the evolution of technological implementations in healthcare services. However, implementations of such technology are yet to be fully applicable to reliable diagnostics or other important information inferring. Using different metrics gathered from biometric sensors, evolving algorithms can gather statistics from a user's behavior and adapt universal baselines to better suit user's needs. This results in solutions that have clear advantages over more general proposals, that can range not only in terms of efficiency but also practicality towards one specific user. In a smaller and non-critical scale, studies and pilot tests that use these mechanisms are typical applicable to fields such as behavior analysis, correction, prevention, and diagnostics [35, 36, 37, 38, 39, 40, 41]. These studies allow users to have a much better understanding of their conditions, as well as have personalized solutions, contributing to their self-care[42]. Although these health prediction systems are still relatively undeveloped, its unexpected interest has the potential of becoming a major source of useful and personalized information from which multiple patterns can be extracted.

The growth of M-Health applications usage can also be attributed to its demystification and evolution in design elements, especially in the ways in which they engage and interface with users. Applications that suffer from user interface problems are not able to effectively reach out to audiences such as youth, elderly, special needs and low technological literacy groups [43, 44]. Each of these groups has different needs regarding the design and functionality of the application, so different and tailored platforms can offer better responses to different kinds of user. Fortunately, technology has evolved allowing rapid development of different user interfaces that have similar root functionalities and characteristics. Hybrid web development frameworks, transformed the development of applications to different demographics in a much agile way and maintainable [45, 46] with some notable examples, such as [47, 48].

Gamification is another popular approach to improve the engagement of users towards health-related applications and commonly applied in mobile applications. This concept introduces entertainment factors into the serious field of health care [49]. Therefore, by using this method, applications can be much more appealing to young audiences, as they usually respond better to playful incentives, rewards and positive reinforcements [50]. Several examples of games that may encourage positive and healthy behaviors already exist, however, these are not M-Health applications at their core [51]. The introduction of health principles into the core of entertaining applications enables better user engagement while focusing on health concerns. This is an optimal way of raising awareness to personal health on younger demographics [52], as we can see with [53].

On older demographic groups, a reliable influx of day-to-day monitoring data is crucial for any type of healthcare service. However, real-time data collections present considerable challenges. The stems from low technological literacy that this demographic group possesses, increases the difficulty of designing simple but informative interfaces[54]. However, the evolution of mobile technologies and user experience methodologies, have improved the overall usability of applications. This enables elderly users to interact with their smart devices and collect useful information about their health condition and act upon this information in a faster and more efficient manner. [55].

2.2 Security Mechanisms in M-Health

Security of data collected by an M-Health application is a key issue in the credibility process of these systems. Health data has always been a very sensitive subject where privacy and security are important concerns for the patients. M-Health systems have a plethora of personal information that normally is not available to anyone besides the patient and the health service provider. With the introduction of e-Health, patient data began being transferred through several devices and, with the advent of M-Health, data is now accessible through a large number of smart devices, which may result in accidental or malicious leakage [56]. Therefore, the adaptation of cryptography mechanisms for the preservation of privacy in health care systems is a focal point where new implementations are constantly being researched and proposed. Hence, the security issues associated with M-Health can be broadly clustered into: i) where the data is stored and what processes are used in order to store it; ii) how the data is transmitted securely over a network; iii) and how the access is controlled [57, 58].

Currently, the transition to remote cloud storage is a prominent innovation that is sweeping across the e-Health scene, as several characteristics inherent to this method are favorable. With the use of cloud storage, several advantages are introduced into existing systems without the need for large structural changes. From increased storage flexibility to fault tolerance and data recovery support, the process of retrieving lost or modified data is simpler, more reliable and with inferior costs. Due to the online characteristic of cloud services, the availability of information and data is assured. The data is distributed between multiple devices through an Internet connection [59].

As cloud technologies evolved, it became clear that they provided an optimal solution for e-health data storage. Inversely, the common mechanisms used to temporarily store and transmit information kept by health service providers stagnated. The data handling and storage process remained largely the same, but with data being transferred and stored in the cloud.

To understand the challenges posed by the migration of health data from local, traditional data stores to the cloud, what cloud services offer and the way they work must be explored. Firstly, offers can differ in the type of service they provide, such as Platform-as-a-Service and Infrastructure-as-a-Service. Secondly, the deployment model of the cloud can range from public to private, and to hybrid. These differ in terms of challenges posed, as the security concerns can fall in either the issues that the cloud provider himself or that companies or users face when handling cloud services [59, 60]. Issues such as data breaches, faulty access management, the existence of malicious insiders, data loss and vulnerable systems, applications and APIs have been found to be most threatening to the security of cloud systems [61].

Due to the intrinsic privacy challenges linked with patient healthcare data, e-health systems are expected to possess well-made underlying structures and workings. Moreover, they are expected to deliver quality of service, secure access management of health data and performance. Current information security standard procedures related to handling of health data often have to compromise either speed, security or cost for the benefit of the others [62]. Regarding M-Health applications, the aforementioned scenario presents slight changes. On account of the significant decrease of local processing power that mobile devices have in relation to standard

servers or workstations, complex operations cannot be done locally. This, coupled with the fact that data is now only partially stored locally and mainly stored in remote storage, results in the access speed becoming much more reliant on the network quality used to communicate to the server where the data is stored.

Although in a very early stage, homomorphic encryption shows great promise in securing sensible encrypted data while it is being processed. It allows encrypted data to be used in calculations and have the same output as if the operation was made with the original decrypted data. Moreover, it would be possible to safely use cloud computational resources with patient health data in a way that would not expose any sensitive data [63, 64, 65]. This, along with collaboration between different health services, can facilitate the use of services previously barred from accessing raw, decrypted health data. Currently, these encryption schemes have poor performance compared to other widely used, but new developments have been able to increase performance [65]. New research has also show a steady gain in relative performance compared to earlier methods [66, 67]. Moreover, there has also been an increase in possible applications of these mechanisms, such as outsourced computation [63, 68] or voting systems [69]. The characteristics of this mechanism make the health industry a prime target for the integration of this technology.

The method of how data is preserved secure and private relates heavily with how it was encrypted. The weakest link in an encryption scheme is usually how to keep the encryption key safe and guarantee that only the data owner has access to it. Traditionally, this was achieved using passwords, or other similar mechanisms. As is well known, the use of passwords is dangerous and unadvised, since they are, in nature, an insecure, although practical, means of controlling access to data. Recently, the proposal for using biometric signals as a way to grant access to information has been standardized into the mainstream smart device market, providing a safer and more practical way to access data than even the old password system [70].

Moreover, efforts are being made to use biometric signals, such like the fingerprint, to serve as a basis to create encryption keys for information, allowing a much stricter and user-friendly manner to keep information confidential and safe. Technology such as ultrasonic fingerprint sensor based on Piezoelectric Micromachined Ultrasonic Transducers (PMUT) [71] is a prime example of cutting edge work being done in the biometric sensor area that can be used in enhancing the security features of an whole application. This technology, still in development, is expected to reach markets from 2019 to 2020 in flagship smartphone models and wearable technologies. With more advanced biometric signal capturing, the capability to use this type of technology in securing applications and data is a very probable reality, as both industry and the general public seem to welcome this technology, both for its security features but especially because of its practicality in everyday usage.

The usage of biometric factors is not a novel idea. Proposals for such solutions began appearing near the end of 1990 [72, 73]. Using fingerprints to complement cryptography mechanisms, and going from a password to a biometric factor unique to the user provides both a more secure and practical method to encrypt or authenticate data. However, the technology behind the biometric data collection and the cryptography mechanisms available are wildly different and more complex. The types of sensors and types of information that can now be gathered, as well as the mechanisms to guarantee the privacy, integrity and security of this information

have rapidly grown in number and potentials, paving the way for more robust, reliable and practical implementations. While a considerable amount of the research work seems to be dominated by the use of the fingerprint [74] as a key for unlocking health information, several other biometric factors and encryption techniques such as [75, 76, 77] are being researched and developed. The usage of biometric factors enables patients to have better control over their data. In addition to the above-mentioned technologies integrated into the M-Health field as new security mechanisms, the platforms for smartphones and other smart devices have also evolved, being subject of large amounts of research and testing. These contributions that are usually security updates and fixes can also be new framework proposals that aim to improve the security of current mobile operating systems [78, 79, 80, 81, 82].

According to current healthcare practices, patient data is kept confidential by using a plethora of operational policies, protocols, technologies, and obligations of compliance to applicable law [83, 84, 85, 86]. This type of sensitive data is usually handled by systems purposely built and optimized to promote data security and confidentiality. These usually include features such as patient data access management, identity proofing, multi-level authentication and authorization, and fraud detection [59, 60, 87]. In fact, the most important characteristic that a health service provider can offer regarding health data security is confidentiality, both from external and internal actors. Externally, even if resources from the cloud service provider, such as computational power, are utilized in calculations, the data should remain leak-proof. Internally, access management mechanisms should ensure that only those with permission can access and alter patient data [88, 89]. These confidentiality mechanisms, associated with proper data encryption, procedure protocols, and compliance laws, effectively ensure that a health service provider is a reliable and credible entity to store health data.

2.3 The Blockchain Protocol

2.3.1 Introduction to the Blockchain Protocol

With the advent of Bitcoin, the research of blockchain technologies on areas not directly linked with cryptocurrencies or data encryption has grown. This research has had far reaching influence in areas where before the inclusion of cryptographic technology in the core technologies that were already in use was not considered. It is especially noticeable with the development of smart contracts, stocks and bond trading, record keeping and even cloud storage solutions [90]. In fact, the biggest and most exciting thing about Bitcoin is not Bitcoin at all, it is the blockchain protocol [91].

The blockchain protocol is, in its essence, a digital distributed ledger that is composed of digital transactions and shared through a network. This protocol is based on a Peer-to-Peer architecture, with every participant forming a node in the network. These participants store an identical copy of the ledger and then work together in the process of validating and certifying digital transactions, adding new transactions to the ledger. The process of adding transactions is based on evaluating the proposed transaction and submitting it to a vote. If the majority of

the participants find the transaction to be valid, then it is added to the ledger, linking it with the previous transaction, forming a chain that cannot be altered without breaking its integrity. Each transaction that goes through the linking process is gathered in a block, which additionally contains a cryptographic hash of the previous block, and is then linearly added in chronological order to the ledger. This process can be seen in 2.1.

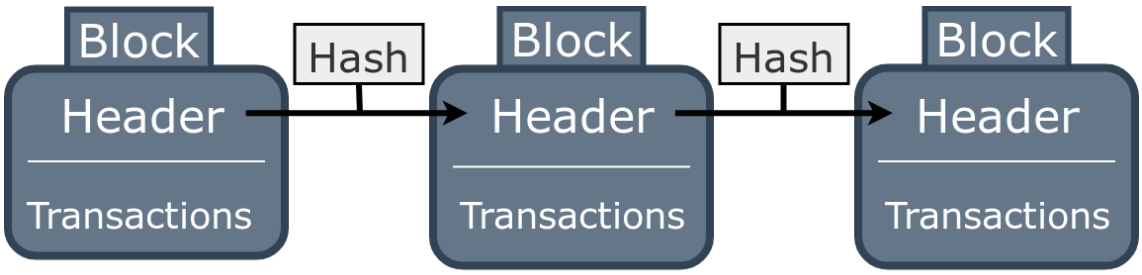

Figure 2.1: Simplified structure of a blockchain, composed by a header and a list of transactions. The blocks are linked by embedding the hash of the previous block into the header of the new block. The only exception is the first (genesis) block, common to all clients of the network.

Changes to the ledger are replicated throughout the whole network and, because of this, every participant has a complete copy of the updated ledger. This also means that no single participant has the ability to easily attack the whole distributed network [92]. While the notion of transaction remains, the data associated with one can be of any type, as the blockchain simply links data that is stored within it. The format of the transactions is defined by the underlying network supporting the blockchain, while the data present in them is defined by the participants who create them. This data can be encrypted and digitally signed in order to add additional advantages to the system such as authenticity, integrity and non-repudiation. The transactions are added to the chain when a specific consensus mechanism is verified. Some examples of consensus mechanisms are proof-of-work, proof-of-stake or proof-of importance, with several modifications in between.

Following the above-mentioned comparison with Bitcoin, a proof-of-work consensus mechanism is in place where network participants try to solve challenges utilizing their computing resources. When a challenge is successfully solved, a token specific to the blockchain platform that is in use is awarded to the user that managed to solve it. When a network participant manages to validate a pending transaction so it can be added to the chain, he is then rewarded with a certain number of Bitcoin, that he can then use as a normal currency. This way, there is an incentive for participants to help in the platform performance. [93, 94]

2.3.2 Blockchain Technology: The Road So Far

The state of the art in blockchain is mainly defined by relevant research work and implementations of either the classic blockchain protocol or some new modification of it, not exactly new constructions of the protocol itself. In fact, slight modifications of the protocol started being incorporated into various fields of digital activity. This first started as blockchain 1.0, a term

describing a distributed ledger used in the control of cryptocurrencies such as Bitcoin. The process of generalizing what the blockchain protocol could be used for peaked when the concept of a program that can be triggered to execute automatically was added to a block. This originated the concept of a smart contract, creating what is now known as blockchain 2.0 and its prime example being Ethereum [95]. Further innovation on the possible uses of smart contracts and the decentralized nature of blockchain led to the research into decentralized applications, originating blockchain 3.0. These Distributed Applications (DApps) make use of both decentralized storage and communication for their operation [96, 97].

Currently, cutting-edge research is underway in order to harness the capabilities explored in previous modifications on the usage of blockchain technology in an industry or standard infrastructural development context. This research focuses on aspects such as resource planning, automation and interoperability [98, 99, 100, 101].

Implementations following the blockchain 1.0 are already commonly understood and studied, and therefore, they are commonly mixed with other implementations that adapt characteristics more aligned with blockchain 2.0 or even 3.0. The most widely known example of this, presents itself in the form of Bitcoin and Ethereum. Although they function based on the same underlying protocol, they have glaring differences in their structure, capabilities and purpose. Ether [102, 103] is the name of the token used by the Ethereum platform [104, 105] to reward participants who successfully solve a challenge linked to the verification or validation of a transaction. Ether is different from Bitcoin in the way that it is not supposed to represent a currency in and of itself, but an incentive aimed at participants that contribute with computational resources to the network.

The main appeal of Ethereum comes in the form of smart-contracts, software written using the programming language Solidity, that are to be executed on the Ethereum network. These smart-contracts are, in essence, a way to force different parties to exchange something of value to one another in an autonomous way when the contract is executed in the network, regardless of how long ago it was made. What makes this technology so powerful is that these contracts are immune to third-party or middleman interference and are immutable once added to the blockchain, providing auditability and an immutable history of contractual transactions [106]. *Unibright*, a platform designed in early 2018, aims to integrate the advantages of blockchain without the sharp rise in complexity for business, handling the creation of workflows and smart-contracts automatically [107], already managing to advance in integrating SAP [108] into its platform [109].

The blockchain protocol has been extensively modified and several new interesting features have been discovered and adapted into existing or entirely new systems. As an example, *Tezos* [110], a crypto-ledger implemented in *OCaml* [111], aims to emulate the working of other blockchains but with mutable and evolving protocols that can adjust themselves to changes that are proposed and voted by the participants of the network [112]. Therefore, it aims to be able to change its format and meta according to evolving situations and necessities, without the need to fork the blockchain.

Another field where blockchain seems to be having fair growth is in artificial intelligence. Cutting-edge research work [113, 114, 115, 116] aims to adapt the information recording ca-

pabilities of blockchain into the data collection processes of artificial systems. Currently, a fair number of proposals indicate that from the integration of blockchain into robotic systems backed by artificial intelligence, several improvements in the productivity of these systems in production environments can be achieved [117, 114, 118, 119, 120]. By using smart-contracts to store information, triggers can be made so that certain tasks are automated when a certain contract is executed. Proposals for the use of these characteristics in conjunction with artificial intelligence systems range from integrating blockchain into cognitive commerce platforms [3] to the health field [121, 122].

In addition, research regarding the integration of blockchain technology into the internet of things shows promise. It aims to allow automatic contracts to be carried out when receiving a network command and then recording event data into the blockchain [123, 124, 125]. Research into the security aspects of blockchain implementations aims to simplify future implementations by adapting existing security solutions to work with blockchain-backed systems [126, 127].

2.4 Conclusions

In this chapter, several concepts that are fundamental to the understanding of the technologies and areas discussed in this dissertation work are presented. An introduction to m-Health is made by presenting what the concept means, why it has grown and what was behind this growth. A review of the state of the art in the area of m-Health is presented, along with the technologies that enable for the rising growth and functionality of developed applications and systems in the area. Since data privacy is a cornerstone of the area, a presentation of security mechanisms currently in use and their problems is made. To grasp the concept of blockchain, a brief explanation of the basics of the protocol as well as the history and initial developments of the protocol is shown. Furthermore, an exposition of the state of the art in blockchain implementations and technologies is presented, highlighting some of the areas where integration of the protocol is heavily researched in. As such, this chapter serves as an introduction to the technologies that are then discussed in detail in the following chapters.

Chapter 3

System Concept and Security Requirements

3.1 Discussion of Open Issues in m-Health

3.1.1 Introduction to the Challenges of M-Health

With the current rate of evolution that the m-Health field is experiencing, it has become clear that its flexible, decentralized and personalized nature can be harnessed in order to complement some faults that a traditional health system usually possesses. These faults usually range from lack of accessibility and availability to overall service quality. Mobile healthcare allows the patient to have a better understanding of their condition without having to resort to physically attending a medical appointment, empowering patients to self-care and promoting their privacy. Furthermore, the constant monitoring that an m-Health solution has of the patient allows it to provide additional layers of depth to his health condition, increasing the information that the medical professionals must work with. Moreover, this information is shared with the patient itself, increasing transparency towards the user. Although the adaptations mentioned previously into a traditional health system appear to offer several types of advantages, they also bring challenges that must be faced for these solutions to be able to be integrated successfully. The integration process itself has challenges, mainly regarding the method of how these new technologies are introduced into an already complex environment. This possibly resulting in regulation and organizational changes, infrastructure investment, staff training and informative sessions for patients. In addition, the technologies must evolve and mature in order to increase both their capabilities, their security, and their credibility. All these characteristics are linked, as an increase in features poses new security challenges and these two factors directly affect the credibility of these solutions.

3.1.2 Communication and Storage Security Issues

Regarding impact, the security of health information assumes a key role in the whole system. In a rapidly evolving environment such as m-Health, the practice of devising processes and mechanisms to secure new types of information in new storage requires research work and concept tests. The main challenges that recur from tackling the issues mentioned above are based on where the information is stored, how it is stored and how it can then be accessed [128].

Regarding where the information is stored, there are two main ways of storing e-health information : i) in a health service provider own local server or remote server, or ii) in the cloud.

As mentioned previously, cloud storage solutions introduce major advantages compared to traditional storage solutions. But there is more to it than just the difference between information stored locally or in the cloud. There are a lot of new important details to consider when cloud storage systems are introduced, especially due to new complex factors that are added to an existing system. Some of these factors are the methods for secure information storage and retrieval from the cloud [129]. When information is migrated into a cloud server several aspects regarding the format and accessibility of the information change. At first glance, the clear advantages of a cloud system seem to have no drawbacks or problems associated, as it enhances security and accessibility by allowing information to be stored remotely in a potentially more secure and always online and available site. This decreases security concerns related to the control of the physical server where the information is stored.

Due to the importance of the information, guaranteeing that it is not altered and allowing reliable access allows both health service providers and the user to have a saved and updated health history. In addition, changing this information with malicious intent can have a large impact on the results of diagnostics and possible treatments. Therefore, and because health information has a value that is independent of time, the immutability of the past information that is stored must be assured. Regarding this, due to the nature of cloud services and their information recovery and fault tolerance, this issue can also be solved when introducing cloud storage [130].

However, after a more careful approach, the cloud solution also poses problems regarding the security, access control and even ownership of the information. First off, the information is no longer under the direct control of the health service provider nor the user, which can lead to ownership problems, especially when the cloud provider policies are unclear or collaborative towards access to the information by third parties, without direct permission from the owner. Therefore, there is a need for clear and privacy-first policies regarding stored information in cloud service providers servers. In order to avoid problems originated by leakage from within, whether it be from improper tampering with information storage or from leakage in operations made in the cloud service provider infrastructure. In addition, information transportation from cloud servers must be secured by using procedures purposefully built to enhance the security of information transfers. Current studies [131] indicate that a portion of m-Health applications still demonstrates issues such as compromised confidentiality and unprotected connections between applications and their servers.

The access to the information itself presents various challenges, which can be consolidated into a situation where a user accesses his information stored in a cloud server. This situation presents two problematic issues, information access and information retrieval from the cloud server. For the user to be able to access the information, he needs to do so from a device that can verify if the accessing user either owns the information or has permission to access it. This, however, requires security measures to be implemented in order to secure access to either the device or the application that requests the information. While the implementation of biometric security seems to be an advantageous solution, it does not come without raising concerns regarding privacy issues that arise from the method of acquiring and storing biometric information , as well as other security-related issues [132, 133, 134].

Otherwise, the process of information retrieval from the cloud server must be implemented

with special attention to access management and control. Due to the private nature of health information, only information owners or special users with access permissions, such as health service providers, may be able to have access to the information. The method by which controlled access to this information can be accomplished is with the use of encryption, identity verification, and access control systems. The patient who owns the information must give permission to third parties, so they can access it. Furthermore, to ensure that the patient is in full control of his own information, this permission should be equivalent to having an information decryption key. By having information access logs, it is then possible to audit these accesses and act accordingly for illegal situations [135]. This, in turn, would amplify the information ownership of the patients. However, this situation becomes troublesome because logs can be manipulated and the access history can be tampered with or even lost, in the case of a local fault.

3.2 Security Requirements and System Proposal

3.2.1 Security Requirements

From the earlier discussion, a specific set of requirements can be identified as being fundamental to a successful implementation of an m-Health system. These requirements serve as a baseline for system implementations. These security requirements are detailed in table 3.1.

Table 3.1: Table that indicates the security requirements for a m-Health system.

Security Requirement	**Description**
User authentication	Access to any information on the system should only be possible via authentication
Logging for auditing purposes	information transactions should be recorded in a safe manner (meaning preserving privacy and integrity)
Confidentiality of medical records and personal information	m-Health systems should provide assurances of confidentiality of stored information
Access control of patient information	Patient information should have different access restrictions in place for different types of users of the system
information origin authentication	information recorded in the system should be authenticated as being from a user in the system
Anti-forgery of users	For a user to be admitted into the system, an identity check should be conducted
Non-reputability of events	information recorded in the system must be accompanied by an identifiable element of who introduced it into the system
User anonymity	All medical information and records pertaining to a user must be kept anonymous
Forward secrecy	Information that was transmitted in the past is safe from future compromises of secret keys
Backward secrecy	New additions to the system are unable to decrypt information created prior to their introduction

They highlight the features a successful health system should focus on in order to provide a credible and quality solution. These requirements are not specific for an m-Health system, being shared with traditional health systems. However, the way in which these can be met

involves the use of fundamentally different processes. This is because, in a traditional health system, the information is not directly shared with the patient. However, one of the main goals of an m-Health system should be for the patient to have access to his healthcare information and useful treatment information, promoting self-care. The requirements have three focuses regarding healthcare information, these being privacy, authenticity and access.

healthcare information privacy is critical to prevent malicious leveraging of health conditions in order to force the patient into doing something contrary to his will. In addition, having access to health information from different people results in traceability of a person by having behavioural knowledge regarding treatments. It is crucial that health information regarding a patient is only shared with those whose patient treatments depend on. Regarding the authenticity of health information, there are two aspects impacting the quality of the health service. First, recorded health information should be confirmed as being from the correct patient and inserted via the correct means. Secondly, all recorded health information should be immutable, and any alterations to the information should be recorded as well. Having these two principles in mind, it can be assured that information in the system is truthful, integrate and incorruptible.

When handling access to healthcare information, special attention should be given to who is accessing the information, what kind of authorization is needed or, in case of an attempt to change the information , if it is valid. Conceptualizing a health system with these concepts in mind leads to the establishment of several security requirements that aid in adding quality to the solution. With the specified security requirements in mind, there is a clear focus on information privacy, its authenticity and how it is accessed. The ability to audit access records of information in a health system in order to act upon irregular situations is also critical. In addition to the security considerations, several other should be considered, such as the cost of integration into existing solutions, overall interoperability and infrastructure requirements. With these constraints in mind, discussion of conceptual solutions is possible.

3.2.2 System Proposal

In this section, a system that aims to improve upon current healthcare information access records is proposed. This improvement is achieved by integrating several security mechanisms as well as the blockchain protocol into an m-Health system. Systems that handle healthcare information are expected to perform to the highest standards regarding information protection and privacy. The methods in which information is communicated and stored in such a system are critical. The following system proposal brings advantages in four main areas, which are patient information ownership, access control of patient healthcare information, the increase of interoperability between different health service providers and the ability to use patient information for research purposes without it ever being linked to a patient.

The ability to use real healthcare information for research with the guarantee that it is completely anonymous presents several advantages for health research. While this is not specifically due to the implementation of blockchain into a system, it is more easily achievable with the use of blockchain. By using a blockchain as an access record mechanism, every access to information from a patient is immutably recorded with cryptography identifiers for each user in the

system. These identifiers would have nothing to do with the identity of the user. In addition, all health information would be linked to these identifiers and not to any kind of information from the user.

As such, in concept, the system would behave following these guidelines:

1. A blockchain would be created to serve as an access record. When a user accesses the health information of a patient, information regarding the involved parties and when the access occurred should be recorded as a transaction and later added to the blockchain. This information should be accessible by the said patient;

2. In the previously mentioned blockchain should be a field regarding the state of the information present, such as a cryptographic hash of the information regarding the patient;

3. Patients should have the ability of, through a mobile application, inspect the access records to their health information ;

4. Information stored in the blockchain should be encrypted using cryptography factors only know to the specific users;

5. All the above points should be integrated into existing systems using open standards and technologies.

The architectural implementation of the proposed system can be seen in figure 3.1.

Regarding this system concept, the biggest contributions come from the ability to greatly enhance control and ownership of health information. The information present in a public blockchain is completely open, so privacy must be considered by adding encryption and other mechanisms so that the privacy of this information is assured. Several proposals have risen that handle this issue, such as [136, 137, 126, 138]. In cases where there is no direct control of the information by the patient, he can still clearly see who accesses it. This is due to the blockchain being openly available, which increases audit ability and, therefore, trust in the system.

With this kind of blockchain access integration, medical history could also be closely monitored for changes and, depending on the kind of implementation, either a sign of change or detailed change records could be achieved. By having an m-Health application on which patients can rely upon to access their health information and to see who accessed their information empowers them to have a clear idea of possible privacy leaks and act upon this information, taking advantage of the immutability of the access records. Based on these guidelines, BARS was constructed. BARS consists of three basic building blocks, these being user applications, the blockchain module that leverages blockchain technology to record access to medical data, and database modules where health information is stored.

A patient can go through several types of medical events during his life, these ranging from exams to appointments with medical professionals. All healthcare information of a patient is gathered from these events, starting with the birth of a subject and following exams, to routine check-ups, to urgent medical procedures. Briefly, all healthcare information related to

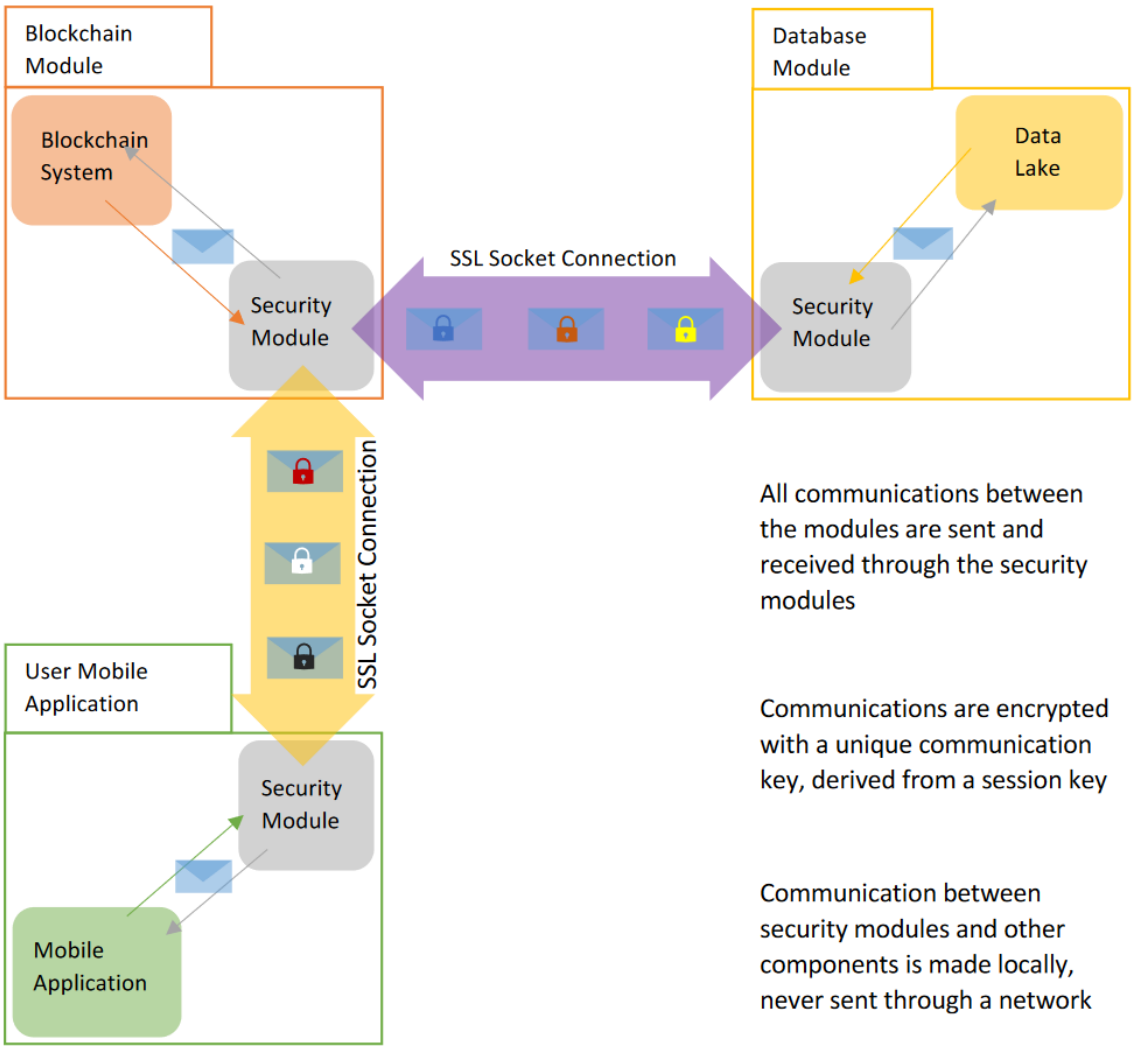

Figure 3.1: Overview of the design and communication scheme of BARS.

a patient is generated in several events. It is possible to record these events and additions to the healthcare information of a patient, linking them. Events have information associated with them, such as when, where and to whom they occurred, the medical professional responsible for the patient, and all the new patient information that was discovered. The proposed system makes use of the blockchain protocol in order to link events with their associated healthcare information. This is carried out by recording patient events in a blockchain. This process can be seen in figure 3.2.

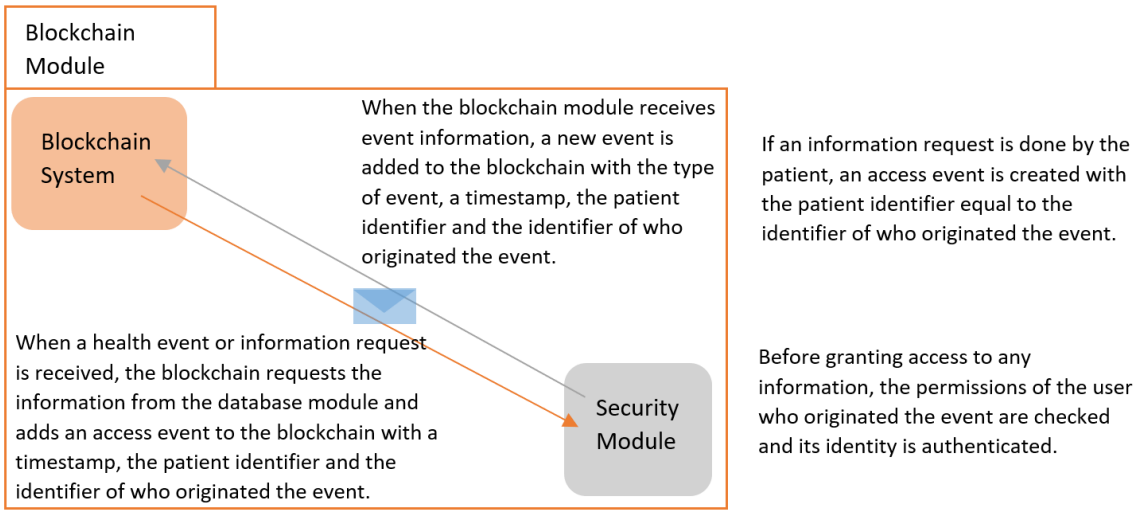

Figure 3.2: Overview of the inner workings of the blockchain module, with possible use cases.

However, since recording the associated healthcare information in the blockchain is not feasible because of scalability problems, this information is stored in healthcare information databases and a link to this information entry is recorded in the transaction, later added to the blockchain. As such, only the event classification, timestamp, patient identifier, medical professional identifier and a link to the healthcare information, as well as a cryptographic hash of the information, is stored in the blockchain. The healthcare information regarding a specific event is then stored on a distributed database system, whose functionality is like a data lake. An event is connected to a healthcare information entry by a link present in both the blockchain event record and the respective database entry, and not with any other identifier. With this, the scalability problems that blockchain demonstrates are directly tackled, by storing as little information as possible in each transaction. This allows for health care information for specific events to be collected by using the information in the blockchain.

It also allows for checking the integrity and authenticity of information stored in the databases, by comparing the hash values of what was recorded in the blockchain and what is present in the database. To allow recording accesses to patient information, the process of accessing is considered an event and is also recorded in the blockchain. Auditing access to the healthcare information of a patient is possible by collecting the information access events from the blockchain. Using the identifiers and timestamps present in the event, it is possible to determine who accessed the information and at what time. By removing identifiable personal elements and traits from the healthcare information stored in the healthcare information database, this database can then be accessed by medical research institutions. This allows the promotion of medical research, using real data to perform various studies.

In this case, the privacy of the patient should be assured by dividing the information storage sites for different types of information. Identifiable information, such as given names, ages, heights, weights, and others, should be stored in secure access databases. Information regarding events should be stored in the blockchain, with each event and information access being recorded into singular transactions, later validated and replicated through the network. Healthcare information linked with events, such as the results of an exam, should be stored anonymously in secure access distributed data lakes. This process can be seen in figure 3.3.

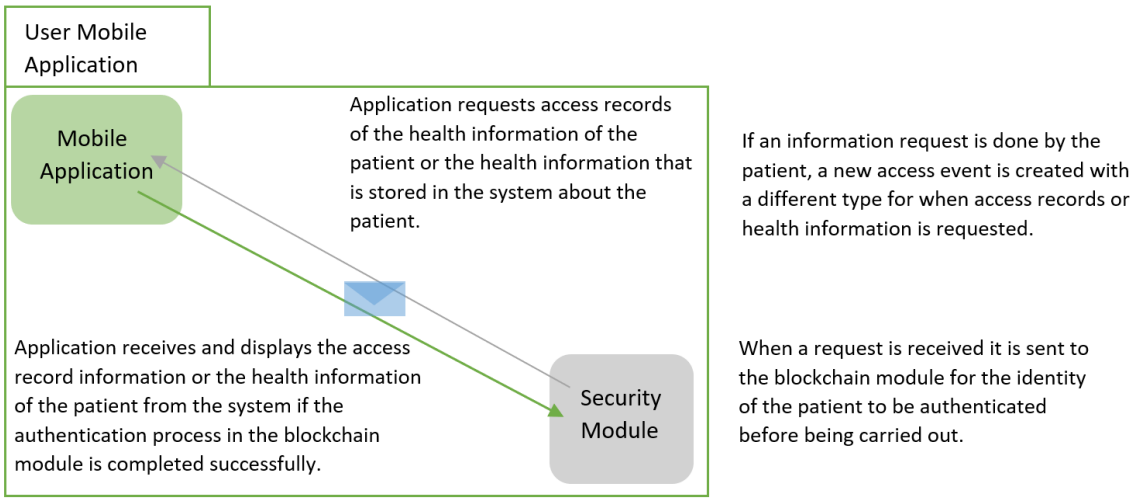

Figure 3.3: Overview of the inner workings of the database module, with possible use cases.

The applications are the methods by which the users can communicate with the modules mentioned above. Different types of users have access to different applications that, while sharing all security features, allow specialized access to functionalities that are otherwise restricted. An application used by a health service provider allows for audited access to healthcare information of different patients, while the application used by a patient only allows access to his own healthcare information and access records. This process can be seen in figure 3.4.

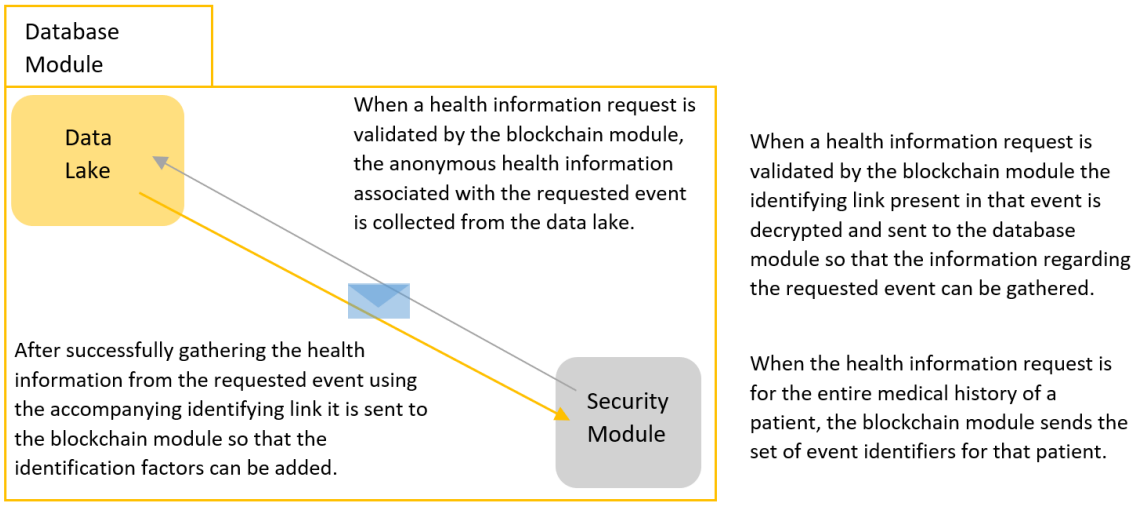

Figure 3.4: Overview of the inner workings of the user applications, with possible use cases.

The means by which secure access is guaranteed, network infrastructure, communication processes and the database itself are jointly referred to as identification modules. The module that guarantees secure communication processes, network infrastructure and access to the

blockchain, as well as auxiliary functions to the blockchain protocol are referred to as blockchain modules. Processes and mechanisms that handle secure communication and administer the data lakes are referred to as database modules. To increase the security guarantees of BARS, these modules should function in different physical machines. Distributing the system throughout several machines helps to safeguard against malicious intrusion of one module making all other modules vulnerable.

3.2.2.1 Analysis of Used Technologies

The two pillars that support a system that handles health information are security and privacy. In order to build a system that upholds the above statement, all communications with it and the users must be protected against security attacks. To increase the security of communications of healthcare information , a set of mechanisms was devised, based on state-of-the-art cryptography techniques. The communication between the users and the system is performed using several cryptography mechanisms, such as public-key cryptography, Secure Sockets Layer (SSL) sockets, elliptic curve cryptography and various key exchange protocols.

In the development of the communication and information storage processes, healthcare information needed to be obscured in order to maintain the privacy of the patient. When this information is communicated and stored in several locations and even systems, having a means to forcibly guarantee that information is kept private becomes a necessity. This was accomplished by using public-key cryptography. As such, each user in the system is given unique public and private keys, generated with the use of elliptic curves. The curve selected for the prototype was *secp256k1* due to being the same as the one used in Bitcoin, allowing for performance comparisons. In addition, every user application is loaded with a *X509* certificate upon installation, that authenticates the device and application as trusted, with the public key of the server. When a user registers in the system, this certificate is used to produce a SSL socket connection with the server. This enables for more secure transmission of information between the client application and the server. To register a new user, a password also must be given.

In communications, no passwords are ever sent, instead sending cryptography hashes of the passwords, calculated locally on the applications themselves. However, simply hashing the password in the client side is not an appropriate solution either, as the password hash from the client side would have to be compared, on the server, with the hash that was stored in the database in order to authenticate the user. This would effectively mean that the hash would become the new user password. In this case, leakage of the database with hashed passwords would have the same negative impact as leakage of a database with clear-text passwords. As such, the initial hash that is sent to the server is performed by appending the password, an immutable string and the client public key and sent. After it is received in the server, the hash is then appended with a random salt and stored. At the end of the register process, the server generates a X509 certificate for the user, with information such as the public-key, name and device identifier. After, a user can authenticate himself towards the server, granting access to his healthcare information records. This authentication is performed by having the user submit his password in the device that was registered in the previous step.

Both certificates mentioned previously are used in this process, one for identifying the user device and another to authenticate the user regarding the device. At this point, the authentication process has been concluded, the user and his device have been authenticated towards the server. Depending on the type of user, the options that are made available are different. A patient has the options to access both his healthcare information and the access records pertaining to that information. A health service provider has the options to access healthcare information of several patients, but not any access records. An auditor has the options to retrieve the access records of healthcare information pertaining to different patients but cannot access the healthcare information itself. Regarding the security and privacy of the information transmitted through the network between the different modules, it is communicated through SSL sockets. These sockets are used in order to establish an encrypted link between two modules. They allow for sensitive information to be transmitted securely between trusted parties by encrypting the communications by using SSL certificates for authentication purposes. In addition, all information that is communicated through the network is also encrypted using public-key cryptography, using the public key of the receiver. Also, the integrity of the information is checked by using message authentication codes with cryptographic hashes.

With these security measures and mechanisms, the communications are ensured to be private, authentic, integral, non-repudiable and anonymous. When a connection is established, every message sent over it is encrypted with public-key cryptography, using a derived unique communication key from a unique session key. To generate the session key, the Elliptyc Curve Diffie-Hellman Ephemeral (ECDHe) key exchange protocol is used. First, a communication channel is opened by initiating a SSL socket connection between the two parties. After, the transmitting party generates an ephemeral public key-pair and sends the ephemeral public key to the receiving party. The receiving party uses the received ephemeral public key in conjunction with his private key as the session key-pair. The transmitting party uses the generated ephemeral private key in conjunction with his public key as the session key-pair. With this session key-pair, each communication key is derived from the session key by appending a set of characters to the session key and hashing it. This process is done in both parties whenever a new message is received, or a message is to be sent.

As an example, when a session key has been established, a communication key can be generated by appending the character ”a” to the end of the key and hashing the result with Secure Hash Algorithm (SHA)-256. With each received message, a counter is incremented, maintaining the order of the appended characters on both parties. With this, the keys that are used in the communications are unique. Also, the keys used in encrypting or decrypting a communication cannot be used in decrypting older messages.

With these security practices, the users can freely communicate health information to the system while also being able to recover the access records to their information. In addition to this, auditing entities are also able to inspect who accessed the information, as well as when and for what reason it happened. To increase the integrity of information access records, an integration of these record mechanisms into a blockchain network was devised. With it, it becomes possible to record access to patient information that is immutable over time and against interference or faults.

Several properties of the blockchain protocol are expected to deliver improvements when ap-

plied to the health industry. These properties are fundamentally gained when the storage method of healthcare information is adapted to take advantage of the blockchain mechanisms mentioned above. The fundamental blockchain characteristics for e-health improvement are its ubiquitous and secure network infrastructure, the ability to verify and authenticate the identity of its participants. In addition, it offers increased security regarding information integrity, reliability, accessibility and an immutable history of all transactions [139]. But how do these properties compare against traditional e-health systems? First, due to its ubiquitous, anonymous but verifiable nature, the access and control of healthcare information by the patients is promoted.

This is due to the chain being openly available to the public and not be bound to a remote secure database in a healthcare service provider own server. In addition, the methods to audit interactions are built into the blockchain itself, allowing for greater control and monitoring of access. Important information such accessed the information identification, access date, location and with what authority the information was accessed can be quickly recorded. Also, because of the cryptographic hash built into each block of the blockchain, it is possible to know if any of the previous blocks were tampered with in any way. If they were, the correct version of the chain can be easily collected from another network participant, due to its distributed nature [140].

In general, the healthcare industry can benefit in terms of information privacy, control, access and safety, as well as accountability and identity verification [141]. For the Information Technology (IT) platforms that support current health systems, several advantages arise from the integration of blockchain, mostly due to the open and distributed nature of the software. These advantages include more effective operations between different IT platforms in the health ecosystem and between these platforms and patients. This ease of use stems from using open Application Programming Interface (API)s to exchange information , as well as increasing the reliability of the information storage method. In addition, as information is distributed to several locations, it lowers the risk that a severe database malfunction would compromise information of several patients. A simple scenario that shows the advantage of applying blockchain to m-Health over the more traditional systems can be seen in figures 3.5 and 3.6.

The advantages of the adaptation of blockchain mechanisms to the m-Health field add to the ones mentioned previously. This is because the use of blockchain technologies in conjunction with information stored in the cloud can have a profound impact on the way that m-Health applications store and use information. Moreover, blockchain technology promotes the effectiveness, reliability and credibility of information access management, which helps the m-Health field to be an accepted and more mainstream complement to traditional health systems. To achieve successful uses in m-Health, key elements such as scalability and information privacy in both access to the user device and the main remote storage must be considered.

Inherent to the nature of the blockchain protocol itself, key characteristics such as real-time transaction record, immutable history, anonymity, and its open APIs may translate into several desirable advantages to healthcare systems. As such, the main appeal associated with the integration of blockchain into existing healthcare systems would come in the form of increased interoperability between health service providers, increased access control by the user who owns the information and immutable history of accesses and changes to information.

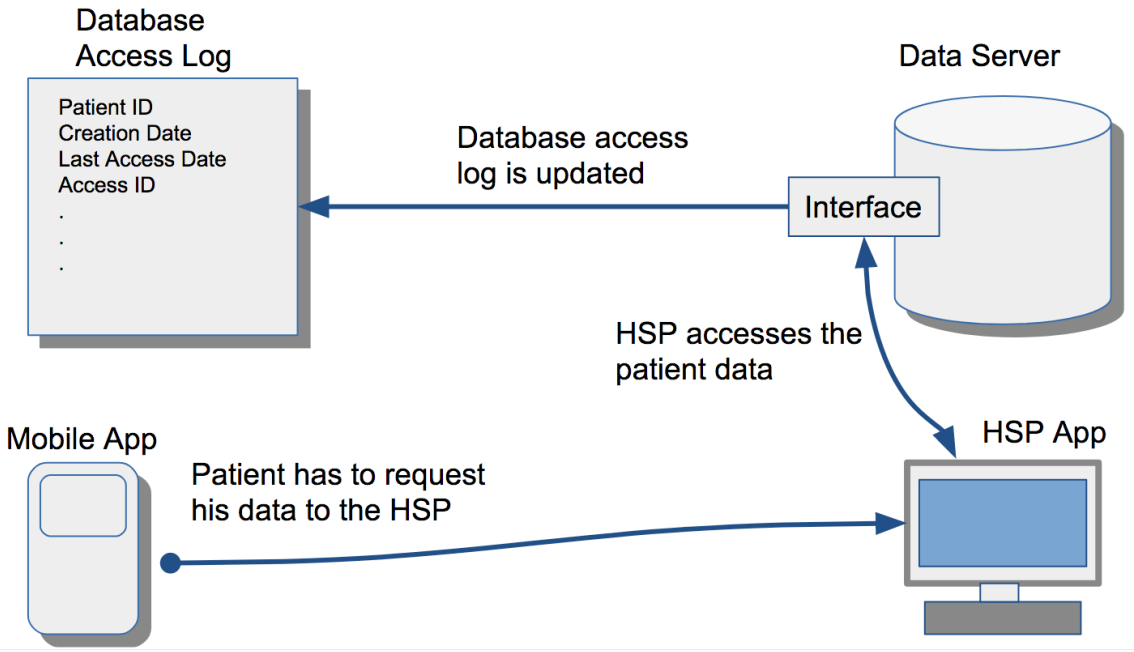

Figure 3.5: Traditional health systems scenario, where a patient must request his information to a HSP. The patient does not have direct access to his own information and has no direct way to monitor the access records of said information. The records are not public and do not offer guarantees in terms of immutability.

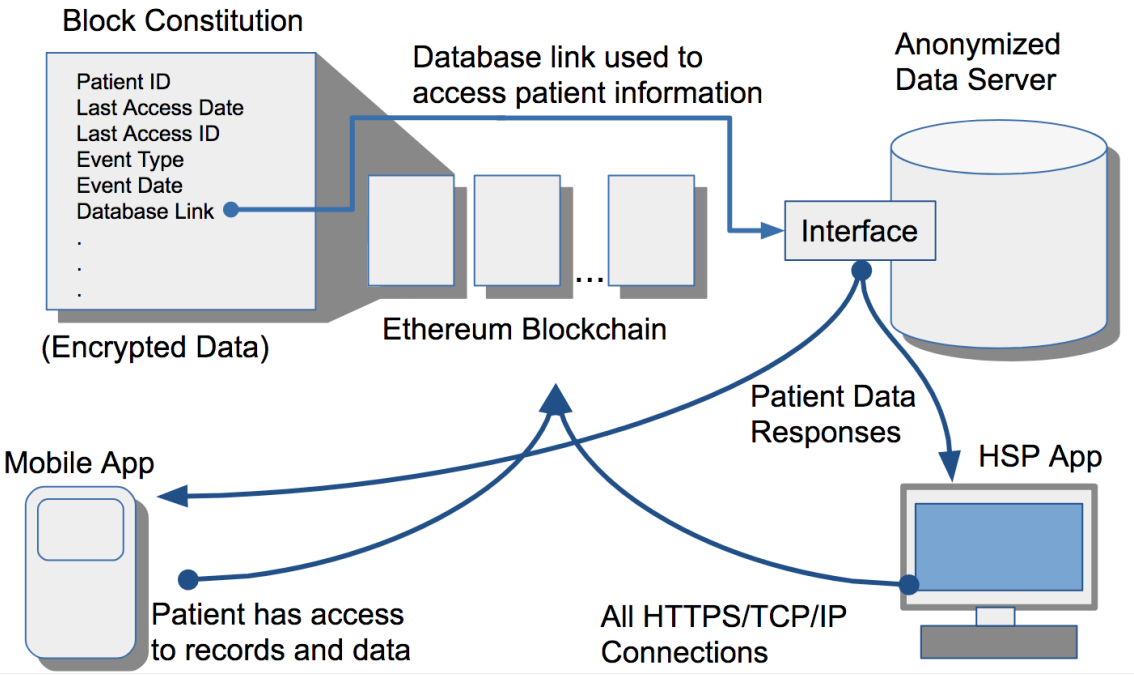

Figure 3.6: Health system with blockchain and m-Health integration, allowing the patient to both retrieve his information and its access records, stored in a public blockchain, guaranteeing immutability and allowing for better audit ability. Can also guarantee information anonymity in the information server by encrypting the identifiable metrics from the patient health information.

Obviously, the introduction of blockchain technology raises several concerns and challenges, such as the cost of transition and continued operation, the means of storage, the consensus mechanics that are to be used and scalability concerns. These challenges must be faced and addressed for this technology to form a credible and reliable means of improving the capabilities

of existing health systems.

The advantages that come from the successful integration of blockchain into existing health systems must be weighed against the cost of the integration process. Transitioning these systems to be able to take advantage of blockchain technologies may have a crippling cost of adaptation and continued operation in comparison to continuing to utilize the system as is. When considering the adaptation of blockchain to new systems, the structure and architecture of the system must be designed from the ground considering the blockchain architecture. For example, factors such as, how new transactions are verified and added to the network, how the transaction verification system works, how changes are propagated to other participants of the network and how can access control and monitoring be achieved are dependent on the system that interacts with the blockchain.

In addition, specifics to the cryptographic structure of the blockchain also must be designed with its performance and reliability in mind. Aspects, such as, the format of the chain, how and what information is encrypted in the chain and, most importantly, how the blockchain is to be used to improve the system, also must be given special attention. Most of these factors are complex on their own and slight changes in any of them can originate entirely different systems with different advantages and disadvantages. In fact, the precise cost of operating these new systems incorporated with blockchain technology is still not known, as well as the scalability concerns that may arise from the growing number of transactions recorded in the blockchain. This is due to these implementations still being in a proof-of-concept stage, as there is not enough test information to precisely conclude on the feasibility and even performance gains that these systems propose when compared against the cost of development in a real environment.

Because of this, it becomes difficult to accurately gauge the extent to which these changes affect the performance of new systems that make use of the blockchain protocol. This is especially true when considering how the verification, addition, and broadcast of new transactions to the other network participants would work. While there is a significant amount of theoretical information that seems to indicate advantages, this may prove to be less indicative of the advantages of early systems using blockchain than expected. There is a need for expectations and researches to be adjusted to reflect the results from tests made in production environments [142].

When considering blockchain storage, while the size of a block can be negligible, the combined size of the blockchain, replicated through several devices and storage, can have a very large impact in the way that a healthcare service provider handles its storage limits. A Bitcoin block is comprised of five main fields, these being a ”magic” identifier of the message origin network, a command, a length, a checksum, and a payload. Considering a very simplistic scenario of implementation of the blockchain protocol in an m-Health application, it can be expected that, as the user base of the application grows, the size of the chain becomes a problem. By taking this into consideration, both the transmission and storage of the whole chain becomes extremely complicated.

One of the biggest challenges that future health systems with blockchain integration must overcome is how to handle the verification process of transactions that are to be added to the chain. In traditional blockchain systems, such as Bitcoin, after a network user manages to solve the

challenge associated with a new transaction, he then receives compensation in the form of some value of Bitcoin. However, when adapting blockchain to a health system, this process becomes slightly more complex. Questions such as who will handle the verification of transactions, what kind of reward is given and how is the reward given, pose challenges that are difficult to solve without some sort of compromise. The following proposals are primarily meant towards m-Health systems but can be transposed to traditional health systems with some adjustments.

The easiest way to approach to these issues is to use the device of the patient as a network participant, using the resources of the device to verify transactions. In terms of reward for the patient, it would be the ability to use the application, allowing more control over his health information. While this may seem like a suitable solution to the problem, as the number of users increases, the number of transactions would be expected to increase even more, and challenges would increase over time. This, coupled with the relatively low processing power of mobile devices and with the fact that only a small part of this processing power can be asked of from the user, increases the solving time of the challenges to a point where the systems would become unusable. Inversely, instead of using the patient's devices, the computational resources could be gathered from a larger infrastructure, like a national health system or a service provider backed and monitored by a government entity. This approach, however, renders the decentralized nature of the blockchain system quite mute.

Another approach to this problem is to provide the adaptation of blockchain to an m-Health application as a paid service. For example, consider an application that allows patients to control access to their health information , where the information is encrypted and stored in a cloud server accessible by several health service providers. By having a user fee, much like in a form of health insurance, their healthcare information would be aggregated, encrypted and stored in a cloud server. This access is then stored in a blockchain comprised of past accesses and the fees would serve as an incentive for successful validation of the block by a participant in the blockchain network. In addition to choosing what approach to take, the consensus mechanism also needs to be chosen, having a deep impact on the morphology of the whole system [143, 144].

Due to these issues, it becomes clear that blockchain presents several scalability concerns that must be addressed for these systems to be able to withstand large user bases. In addition to this, implementations of the blockchain protocol still present security issues, with sybil attacks being a looming threat, and events such as [145] still being a reality. Another problem that must be addressed is the cost of operation in the blockchain. While reading information from the blockchain is a fairly simple process, writing information into new blocks is costly in time, computer resources and power. As such, while in a proof-of-concept phase this cost can be ignored as to test the technical viability of the system, it must be addressed when considering an implementation in a real environment.

Since every time a user health information is changed it must be recorded into the blockchain, the cost of writing this information becomes a considerable bottleneck. This can be amended by implementing second-layers to the blockchain, platforms and protocols that sit on top of the blockchain base and improve on the disadvantages of blockchain implementations [146, 147], with several rising ones such as [148, 149, 150]. A resume of these challenges, advantages and constraints of applying blockchain to m-Health systems are presented in tables 3.2 and 3.3.

Table 3.2: Table that indicates the advantages that a blockchain based implementation can have on problems that manifest in current traditional health systems.

Current Problems	Blockchain Solution
Ownership of medical information	Accesses recorded in the blockchain
information leaks and deficient audit ability	information is encrypted OR anonymized
Interoperability between providers	Use open source blockchain APIs
Following a patient medical process	Events recorded in the blockchain
Real medical information in research	No identifiable traits in the information

Table 3.3: Table that indicates both the biggest challenges and the main advantages of implementing the specific solutions to the problems mentioned in table 3.2.

Challenges	Main Advantage
Scalability (number of records)	Empowerment of the patients
Storage providers open to external audits	Increased transparency
Updating existing systems	General compatibility
Scalability (events per patient)	Transparent medical process
information protection laws	Privacy in medical research

With the previously detailed concept proposal, the security requirements that were discussed in 3.1 are addressed. Some additional procedures are required for a smooth operation of BARS, such as:

- Patient information must never be accessed without the access being recorded into the blockchain;
- Under no circumstances is personal information to be stored in the blockchain;
- All information in the health information database must retain anonymity, without any identifying elements in order to be able to be used for research purposes;
- For each access to patient information , the entity who requested the information must be recorded;
- Every user of the system must have a unique public-key encryption key-pair;
- Each block in the blockchain should have a cryptographic hash to be able to verify if any improper changes were made;
- The blockchain should not be openly available in its entirety to everyone. Only the information regarding a specific user should be shared with him and medical professionals. Access to the whole blockchain is limited to the system itself and to auditing entities;
- After the initial register process, all communications should be made using communication keys derived from unique session keys. These keys are constructed based on ephemeral keys that are established using ECDHe - and then used to generate session keys using symmetric key encryption as Advanced Encryption Standard (AES);
- Server must only give information about the health information or access records about the

patient for which it is being requested. This information must be handled and formatted in order to obscure details about the blockchain transaction used to recover them;

- Each of the modules that constitute the server (communication, user database, blockchain) should be implemented in different physical machines or with advanced logical separation (containerized);

- All communication with the system should come from the user applications, since they were designed specifically to increase security of the system;

- Each user should have several different wallets associated with him, in order to decrease link ability in the blockchain;

- The user application for the system must be packaged in a way that makes reverse-engineering difficult;

- The user application must be run as a local standalone application, it should not be a service hosted outside of the user machine as to prevent initial key-pair leakage;

- The certificates that are given to users must be created with information that identifies the user in the system, with expiring dates fit for them to be renewed;

- All public-key cryptography algorithms must be constructed based on Elliptic Curves as to improve the strength of the encryption schemes;

- All input into the server must be sanitized in order to prevent intrusion;

- All communications should be initiated and conducted using SSL Sockets, with Transport Layer Security (TLS);

- The system should be based on open standards and APIs, in order to increase interoperability;

- Health information handling should respect all standards and regulations regarding private information.

Table 3.4 details how each of the security requirements are addressed.

As such, the proposed system meets all the requirements that were indicated before. In addition, with small changes to the architecture of the system, requirements such as anti-forgery can be met with better quality, by using government authentication.

Table 3.4: Table that indicates how the security requirements of a m-Health system are addressed by the proposed system.

Security Requirement	Description
User authentication	Every user of the system is identified by a set of public-key cryptography key pair, a password and an accessing device identifier
Logging for auditing purposes	All healthcare and access information are logged into events in a blockchain
Confidentiality of medical records and personal information	Healthcare information present on the system is separated from identifying elements, as well as stored securely and encrypted
Access control of patient information	Patients can only access information pertaining to them, health professionals can access medical information from several patients, auditors can only retrieve access records
Information origin authentication	Information can only be added to the system by authenticated users, which must go through a heavy authentication process
Anti-forgery of users	For a user to use the system, he must be registered with a factor unique to that person, such as his citizenship identification
Non-reputability of events	All events recorded into the system are accompanied with a key that identifies who introduced the event into the system as well as to whom it concerns
User anonymity and Privacy	Information pertaining to a user is stored anonymously in data lakes, without any directly identifying information
Forward secrecy	Each message is encrypted with a hash of the session key with a ascending character
Backward secrecy	Each communication is encrypted with a secret key unique to the sending user

3.3 Conclusions

In this chapter, the open issues on m-Health security were discussed, with a focus on the growing capabilities of mobile devices, cloud storage techniques and challenges, mobile operating systems vulnerabilities and the challenges associated with securely accessing the information stored in a m-Health system. The security requirements of a m-Health system were derived from the characteristics that healthcare information has, as well as what is needed in order to guarantee privacy and confidentiality. A general set of guidelines for blockchain implementations in m-Health systems is presented, as well as explanations for the motivations behind these guidelines. In addition, a solution proposal is made, with explanations regarding the technologies that were used in the design and development, and the inner workings, of the system. Insights on how blockchain can be applied to m-Health systems and conceptual use cases are presented, as well as the main challenges associated with blockchain implementations. Finally, the solution proposal is analysed in order to check if the security requirements presented before are met, including explanations as to how some problems associated with blockchain are faced. With this, BARS is presented, allowing for a more complete study of the system in a testbed, done in the following chapter.

Chapter 4

Deployment on a Testbed and Discussion on Security

4.1 Introduction to the Testbed

In this section, the testbed that was used to make preliminary testing of the viability and performance of the system is described in detail. This allows for a clearer understanding of how the concept proposed in the previous chapter can be implemented. The testbed that was used as target for the integration of the BARS system was based on Home Intelligent Assistant Services (HIAS), with several modifications and additions.

The HIAS system is an IoT-based healthcare ecosystem with a cloud architecture and focus on security. It was built by members (including the author) of the *NetGNA* laboratory and was designed with three main requisites: 1) Easy integration of new users, applications or other devices, such as, sensors and actuators; 2) the ecosystem should consider indoor and outdoor scenarios, including mobility environments; and 3) All health data and user authentication should be private and secure.

The testbed consists of a health-focused system of mobile applications that interact with each other to both introduce new information and access existing information on the system. The architecture of the testbed was designed in such a way that the functioning of the identification, blockchain and database modules could be tested, in terms of overall functionality and regarding the security requirements. In general, the testbed consists of three applications providing data to the three previously mentioned modules and another application to provide access to data in the system. These applications interface with the identification modules, which in turn communicate with the blockchain modules. The blockchain modules communicate with both the identification modules and the database modules.

First, the applications that were constructed are detailed, followed by the way in which they interact with the modules. The system consists of the following applications:

1. A back office application for introducing users to the system, classifying them as a patient, a health service provider or an auditor;

2. An application that can be accessed by patients in the system that shows healthcare information and the access records of that information;

3. An application that reads heart rate and periodically records the rates and requests for them to be recorded as an event in the blockchain. If any abnormal heart rate is detected,

the event identifier is sent to the emergency contact application;

4. An application that contacts emergency services when it receives the identifier of an abnormal heart rate event from the monitor application.

With these four applications, every major interaction that both a patient, a health service provider or an auditor can have with the system is covered. This is because these applications cover how users are added to the system, how user types are controlled, how health information is recorded and how it can be recorded into the system. A simplified overview of the workflow and communication scheme of the applications with BARS can be seen in 4.1.

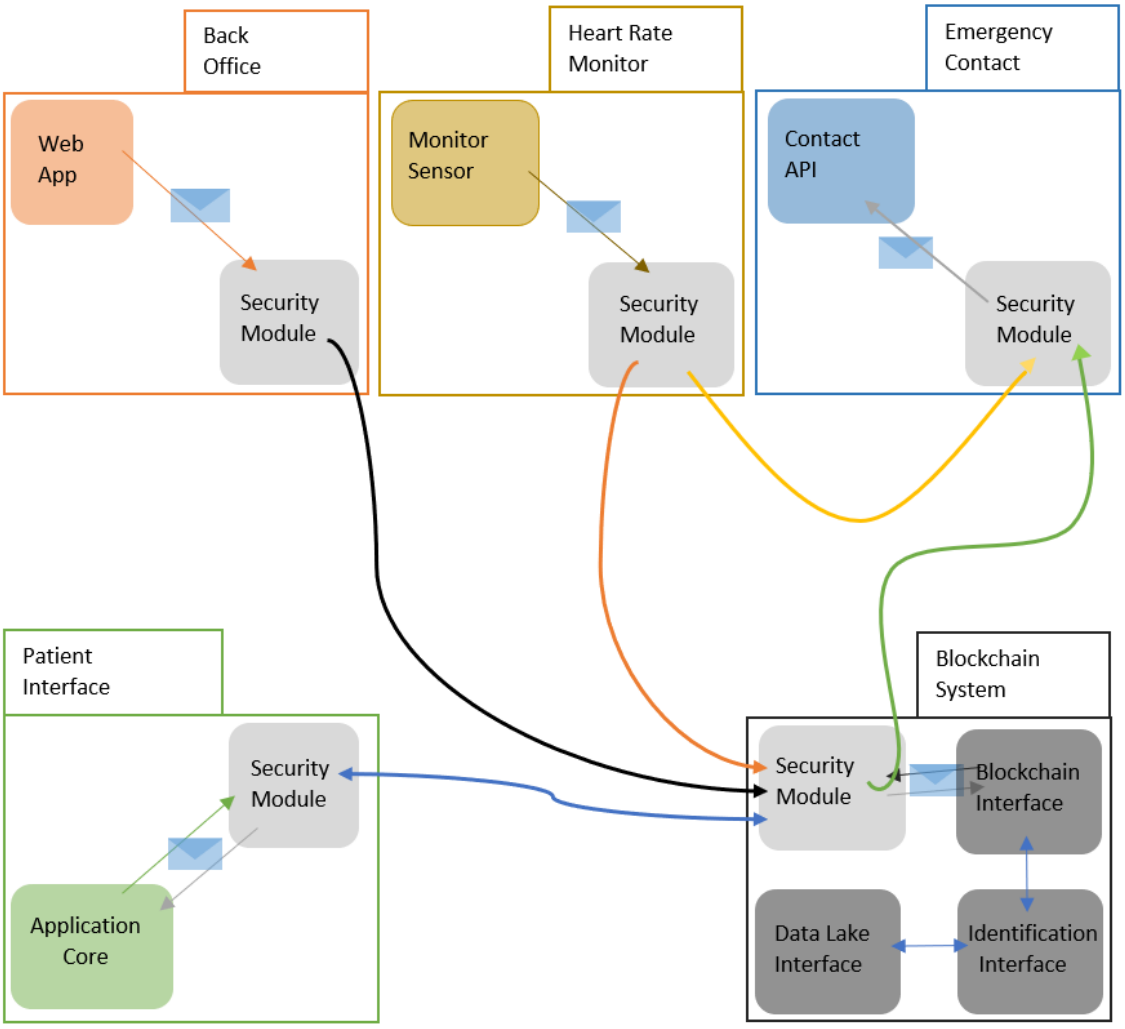

Figure 4.1: Overview of the workflow and communication scheme of the applications with BARS. While communications are encrypted and conducted over SSL Sockets, the figure was simplified.

The back office application serves as an entry point for users, that are registered in the system by a trustworthy third party, that can guarantee several security requirements, such as authenticity of identity. This application not only adds new users to the system but also classifies the inserted user with a specific role. These roles are then used to filter the users that only have access to their own health information and records (patients), users that have access to the health information of other users but not their access records (health professionals) and users that have access to other the access records of other users (auditors). The interactions between the

back office application and the blockchain system can be seen in 4.2.

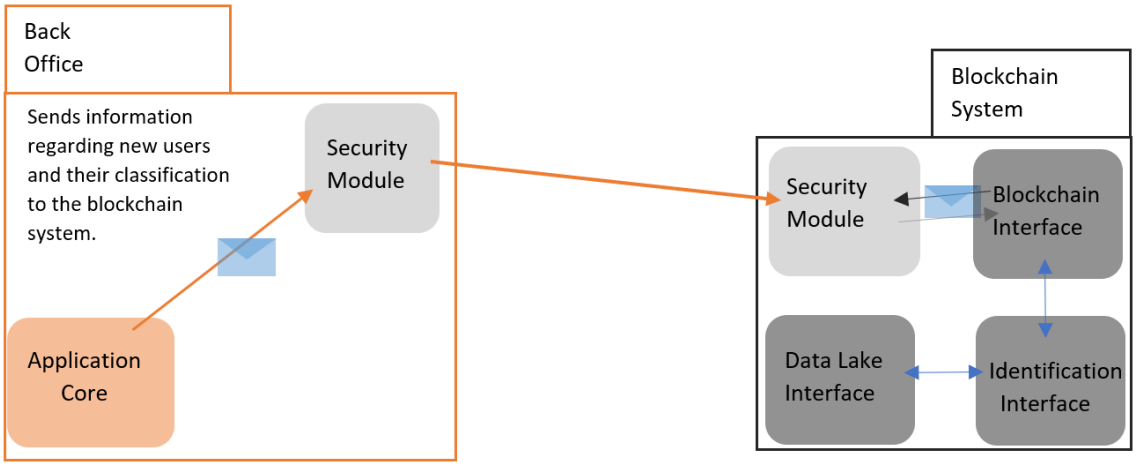

Figure 4.2: Overview of the interactions between the back office application and the blockchain system.

The application responsible for granting access of both healthcare information and the access records of that data is the web application. This web application works in two different ways, depending if the user is a patient or an auditor. In the first case, the application allows a patient to gather his healthcare information present in the system, promoting self-care, as well as allowing the patient to see the access records of his health information. In the second case, the auditor is unable to gather healthcare information, but can gather access records of health information belonging to a patient, identified by his walled identifier in the blockchain. All access to data on the system is restricted to personnel that was authenticated previously to being registered in the system. The interactions between the patient interface (web application) and the blockchain system can be seen in 4.3.

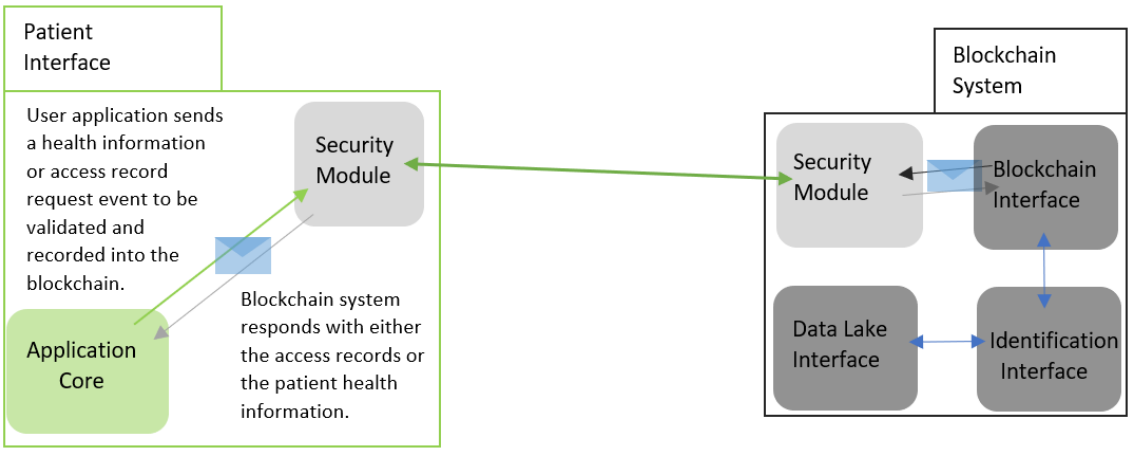

Figure 4.3: Overview of the interactions between the patient interface (web application) and the blockchain system.

The information that is recorded from the heart rate application is processed in the application and is recorded as events in BARS. Information regarding the heart rate events is saved anonymously into the data lake, with a link that ties the event to the respective information. The application that reports highly abnormal heart rates to emergency services allows for the integration of several important functionalities in a single workflow. The heart rate monitoring application sends a message containing the transaction identifier to the emergency applica-

tion every time a highly abnormal heart rate event occurs. This is followed by the emergency application requesting access to the transaction from the blockchain module and, if previous authorization by the patient was granted, the abnormal event information as well as some information about the patient is disclosed.

This information is then used to aid in the description of the emergency to responding personnel, allowing for quick intervention. As such, the application can request access to information, to gather that information from the data lake, to handle that information and to record the abnormal event into the system. Briefly, it inserts new information into the system as well as gathering and processing information already present, as well as communicating with another application to enhance functionality, forming a complete workflow. The interactions between the heart rate monitor application and the emergency contact application and the blockchain system can be seen in 4.4.

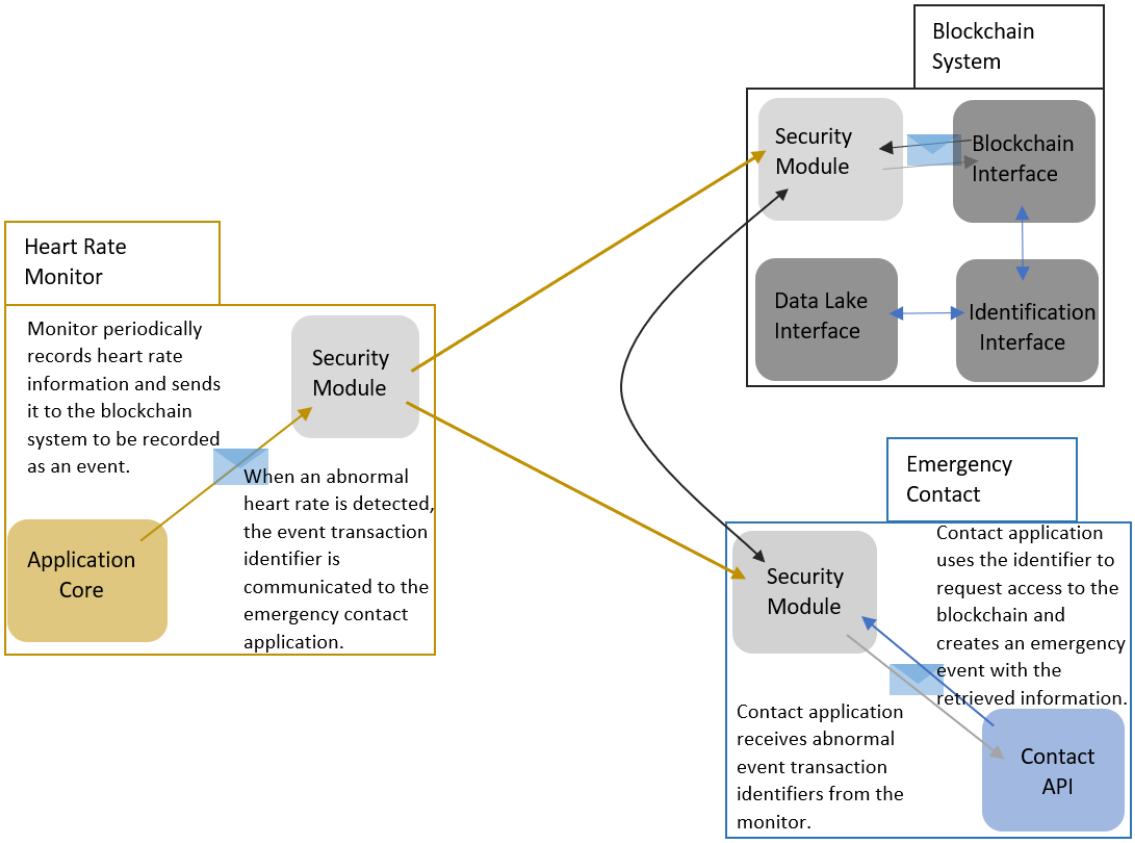

Figure 4.4: Overview of the interactions between the heart rate monitor application and the emergency contact application and the blockchain system.

The architecture of the applications follows a Model-View-Controller (MVC) structure. All applications communicate between each other and BARS through SSL Sockets, and all information is exchanged between the server and clients in *JSON* format, a simple and fast format. Data models are responsible for aggregating and matching all acquired data. The view is responsible for sending and receiving the data. The view does not care about the data types or how they are acquired, it is only limited to visually presenting the result. In this case, it is responsible to send information for applications that complete this system. All services that are part of the controller add, update, extract or read data from the database. These services were developed in an *ASP .NET Core* Web Application in *C#*, which offers a totally object oriented programming

and freedom to interact with other software developed in other programming languages.

Each service has an associated HTTP request link. Then each customer makes a selection of the services they want to use, and links them to the source code of the software they are developing. Since the testbed has a service-based architecture, services are the main pillars of the whole system. As mentioned earlier, and with the goal of integrating various applications and software into one architecture, the services were developed aiming at to allow CRUD operations on data. To read the information present in the database, GET methods are used. This method was chosen because it does not allow modification of the data. To add and update data POST methods are used. Requests using this method are never cached and do not remain in the browser history, which ensures a high security for this system. These POST requests have no data length restrictions, which allows large data to be used by this method. One such example is the electrocardiographic readings, which is a fairly long list of data but is saved from the database without any problem.

All of these services make a direct connection to the database and, depending on what they do, execute Structured Query Languade (SQL) commands to manipulate or query information. Finally, add and update services return a flag depending on the execution of the command - success or failure flag. There is also in this system a single registration layer for all applications: the user will only need to register once, and will be able to login in all applications that are part of this universe. This is because there is a unique database shareable between all applications provided by the BARS system where all identifying information elements about a patient are stored, separate from the remainder of his health information.

A simplified figure of the architecture of HIAS can be seen in 4.5.

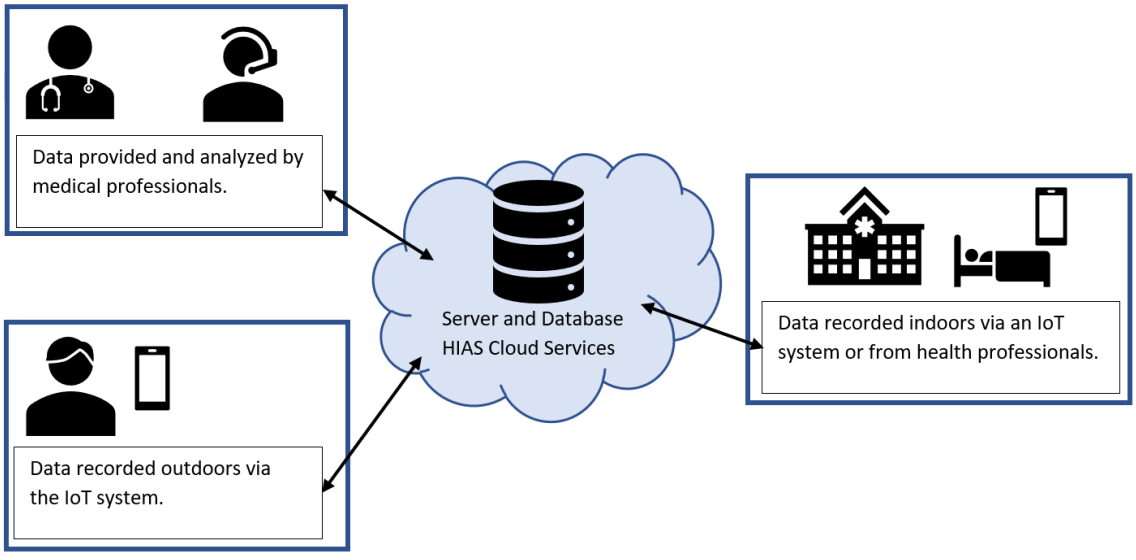

Figure 4.5: System Architecture of the proposed IoT-based Healthcare Ecosystem for HIAS.

The way that the testbed integrates with BARS is by being the mediator of communications between the applications. This enables for health information to be recorded into the system every time new information is transmitted. As such, BARS stands between the applications and the storage system used to store the health information. Since one of the features of the system is a high volume anonymous data lake, integration of BARS also replaces the standard storage

system in use.

4.2 Proof-of-Concept on a Testbed

The BARS prototype was implemented with the use of several technologies, which will now be described in more detail:

- Ethereum - a test network was set up on a machine that was responsible for both running the network and validating transactions; this test network was set up so that BARS could be tested with no actual monetary investment in one of the public networks;

- Python - the applications that compose the testbed were developed using Python, as well as the various modules of BARS; the security modules where prepared from the ground up with the help of *pyOpenSSL*, a Python implementation of the *OpenSSL* library; the blockchain modules were built with *Web3* and *solc*, to communicate with the Ethereum network and to handle the smart contracts, respectively;

- SSL Sockets - the *socket* library was used to construct the connections between the various modules; the sockets were initiated with the help of *x509* certificates;

- Apache Cassandra - the database system used to store the information of the patients in the data lake, chosen because of the distributed nature and fault tolerance nature it has;

- Ganache CLI - this tool was used to simulate full client behavior to quicken development of the prototype in terms of setting up and interfacing with the Ethereum private network.

Briefly, the testbed was laid out to enable testing communication security, information and access recording and the user interface. BARS was devised as a proof-of-concept, aiming to demonstrate the viability and positive aspects that blockchain technology has when applied to m-Health. It is a system that can make use of the decentralized nature of blockchain technology in order to promote the decentralization of healthcare services, promoting self-care and patient ownership of his own health information. The system addresses the main issues that were pointed out in the previous chapter.

A discussion on the viability of blockchain-based solutions whose architecture resembles the one on BARS is discussed in section 4.3. In addition, a discussion on how the security requirements of the system may not be met under a different testbed is made, as well as a description of how a different testbed may impact the functioning of BARS. The testing was conducted by evaluating the implementation of the security mechanisms that BARS uses to guarantee privacy and anonymity. As such, the testing can be divided in three different stages, where each function of the security mechanisms is tested individually:

i) Communication encryption schemes: the encryption schemes that were used are widely known and have been studied, having guaranteed security features if implemented cor-

rectly. As such, the implementation of these schemes is analyzed;

ii) Blockchain properties: the blockchain that was used for the proof-of-concept is Ethereum, because it is widely know and has precisely defined methods of implementation and limitations;

iii) Data storage and access: the way in which the secure, private and anonymous storage and accessing of information stored in the system is done, how using standard database queries over secure connections can guarantee data safety.

4.2.1 Communication Encryption Schemes

The encryption schemes utilized in the implementation of the system are based on elliptic-curve cryptography. Elliptic-curve cryptography is based on how elliptic curves are structured over finite fields and on the intractability of discrete logarithm problems. While having the same security-related features as other public-key systems, elliptic-curve based systems have smaller key sizes, demanding less storage space to store them and improving their transmission over a network. In BARS, elliptic-curve based keys are using the *secp256k1* curve, that is also used by Bitcoin. This curve was selected because it allows for increased efficiency in calculations, due to how the curve was defined and to draw similarities in implementation and performance to Bitcoin.

To establish key-exchange protocols between modules, the Elliptic-curve Diffie-Hellman protocol was used. In addition to this protocol, some minor adjustments were made in order to utilize an ephemeral key-pair, which has his public key sent over the network. Using the ephemeral key-pair, the generation of communication keys from the session key to encrypt the messages being sent guarantees that, even in the case of leakage of information, an attacker could not decrypt the information being sent. In addition, an attacker cannot encrypt and send messages to one of the participants of the system pretending to be another user because the private key would not match the public key, making future decryption impossible. These adjustments help promote the security features of the protocol when it comes to exchanging key information over an insecure communication channel. When information must be communicated from one module of the system to another, the following occurs:

1. The sender module uses his own certificate to create an SSL socket communication with the receiving module. The certificates used are embedded into an authenticated application and are all signed by a trustworthy root authority. After both the certificates from the sender and the receiver are verified, a communication channel is open between the two modules;

2. After the initial communication channel is opened, the identity of both modules is verified by a challenge that consist of sending randomly generated 64 bytes messages to the receiving end and awaiting their return in a signed form. When they return, they are signed using the private key of the receiving module and, if this signature can be verified by using the public key present in the certificate used to form the communication channel, the

identity is confirmed;

3. After the identity of both modules is validated, they are confirmed as having clearance to have access to the system. The level to which access is granted is dependent on the role that the user that is currently engaging with the modules has. Different users may have different roles, which results in different options in the applications and different information that they can access. When the user is confirmed as having a specific role, the modules function in different ways;

4. With the identification and classification of the user that is interfacing with the modules, the modules can now prepare for sending and receiving communications. This preparation is done by one of the modules generating an ephemeral public key-pair and sending the ephemeral public key to the other module. The receiving module can now utilize that public key in addition to his private key as his session key pair. The sending module uses his original public key in addition to the ephemeral private key that was generated as his public key-pair;

5. For each message that is sent over the communication channel, the modules encrypt the information using a communication key that is derived from the session key. The Diffie-Helman key exchange protocol is utilized in order to handle the key generation and transmission. The generated keys are unique, and previous keys can not be derived from more recent keys, as one of the factors for creating the keys is time dependent. This guarantees both forward and backward secrecy.

For each individual communication that is exchanged between two modules, there is a layer of public key cryptography encryption used. In addition, there is a check to see if the integrity of the original message is maintained, using Hash-based Message Authentication Code (HMAC)-SHA-256. While the resulting hash is relatively small compared to other hashing algorithms, such as SHA-512, it was deemed enough, also having positive impacts in the transmission speed of the messages.

4.2.2 Blockchain Properties

As Ethereum was used for the implementation of the prototype, both smart contracts and accounts received special focus. Ethereum has these two prominent features that separate it from earlier implementations of the blockchain protocol. These two features becomes especially useful when applied to the prototype and, therefore, the quality of the implementation would be severely decreased if not for them. Using smart contracts, every interaction with the blockchain can be done with increased transparency and without the need for a middleman. These contracts define the rules and penalties around an agreement while also enforcing the obligations. These contracts are also stored in the decentralized ledger, increasing their security and immutability. Several properties of these contracts have advantageous impacts on BARS, such as their autonomy, trust, safety and the fact that they are always safely backed up.

In terms of the Ethereum accounts, since the system handles patients and their health records,

there needs to be a way of easily procuring records from a certain patient. By using the patient account to search for the health records present in the chain, there is a clear way of gaining access to this information. While collecting information about one patient being faster is advantageous, it also creates linkability in the blockchain. While the information in the blockchain is encrypted and access to it is restricted, it is possible to have insights on how many healthcare events a patient has had over a period of time, if access to the blockchain would be exposed. To tackle this issue, BARS attributes each patient with several wallets, and healthcare events are distributed through these wallets randomly. This makes it difficult to link a patient to certain healthcare events, improving the privacy of this information and the safety of the patients. The nounce that is present on each Ethereum account also helps to prevent a healthcare event from being duplicated, which could have severe impacts.

4.2.3 Data Storage and Access

Data storage and access: the way in which the secure, private and anonymous storage and accessing of information stored in the system is done, how using standard database queries over secure connections can guarantee data safety. When using the Cassandra database to store the information, it is important to make sure that the information is anonymized. In BARS, this means that the information regarding an health event is stored separately from the identification of the patient. The identification of the patient is stored in a separate module that communicates directly with all the APIs of the system. Access to this database is restricted and the information present is used to verify and authenticate the identity of the users in the system. When a healthcare event occurs, it is recorded into the blockchain with an identifier that allows for the information regarding that event to be retrieved from the database storage. Since all information that is stored in the databases is encrypted using cryptography keys unique to the patient, even if the information present in the database is leaked, the privacy and security of the information is assured.

4.3 Discussion on Viability and Performance

In this section, the overall performance of the system is evaluated based on how viable the constructed prototype is to implementation in a real-world scenario. Briefly, the evaluation consists of judging if the functionality and advantages of the implementation of BARS to control access to health information through blockchain and security modules integration are enhanced. Since the system is merely a prototype and the blockchain implementation is conducted on a private Ethereum network, comparing the performance of data gathering on this system in relation to a traditional database-based system does not make sense. The implementation of the solution in a private Ethereum network main goal was that the cost of operation of the system would not be a bottleneck to producing the prototype. As such, the discussion will be focused around the implementation cost of BARS in relation to a traditional healthcare information system where healthcare information and access management is done mainly via a database management system.

Before discussing the behaviour of BARS integrated into the testbed, how the correct functioning of the system is dependent on the design of the test should be addressed. There are security requisites that need external factors to the system itself to be met, such as the authentication of the identity of a patient. This kind of feature is not feasible to implement in a prototype of this magnitude because of the lack of information present in the system to actually validate an identity. To validate the identity of a patient some kind of validation based on a government identification must be done. Another way to identify a user is to use biometric factors exclusive to that patient, such as the a fingerprint or a government identification card digital factor. As discussed in 2.2, the usage of biometric factors can be accomplished as a way to authenticate a person once it has been introduced into the system, but there is a risk that the fingerprint that is to be recorded in the system is not from the correct person.

As such, there needs to be a database of people records that can identify to whom a fingerprint belongs to, so that the solution can be trustworthy of being implemented. Traditional health systems already have this information and are able to verify it because a patient needs to confirm his identity *in loco*. This type of verification is not suited to being implemented in the scope of the development of BARS. To be able to build the system in such a way that there is verification of identity and to prevent identity forgery, the identity of a user must be verified by an external source before it is allowed to use the system.

It must be acknowledged that, since elemental aspects such as this are dependent of external factors, that the testbed was developed with these constraints in mind. If the composition of the testbed should change, the whole functioning of the system would change and a new discussion on the security of the system should be conducted. With these considerations addressed, the discussion on the implementation of the system in the testbed and similar environments can occur.

Since the prototype system consists of several modules that handle health information, the need for enhanced security is clear. In addition, if the development and integration of the security measures is modular, like in BARS, it can be used for multiple purposes with different kinds of data to be transmitted and stored. As such, the security modules that were developed introduce advantages to the system while being able to be used in entirely different conditions. An example of this behaviour can be seen in the fact that applications in the testbed communicate with BARS and the internal modules of BARS communicate with each other using the same security modules. The modularity of the security modules signifies a decrease in development time of components to integrate the testbed, since the same security modules are used in the different components.

In terms of the blockchain module advantages, the access records of health data as well as the health event records can be saved into an immutable ledger, that is then distributed over the whole participating network, becoming tolerant to faults. In addition, several techniques can then be used in the blockchain so that both the size and computational resource restraints to find something in the blockchain are decreased. These techniques include pruning, to reduce the size of the blockchain while retaining all of the advantageous properties for long-term storage, or using Ethereum accounts to find information based on the wallet identifier of the patients.

The main constraint of the development of this prototype was in the small size of the private

network and overall test environment it was deployed into. If the prototype was integrated into a the framework of a traditional electronic healthcare system, it could make use of several factors to enhance itself. These factors include:

1. Larger number of devices that comprise the electronic health system, that can now be used to further distribute the information and to enhance the computational power of the network;

2. Federated authentication, that comes from the usage of government databases to validate the identity of a user of the system;

3. Clarity in the access of health information for research, because the federated authentication could be used to guarantee that whoever requests access to anonymous healthcare information in a qualified professional.

Regarding the direct advantages that integration of BARS would have in the overall functioning of a health service, the following can be outlined:

1. Greater medical responsibility, that comes from identification of health professionals being mandatory and because what can be recorded in the system is now larger, as the system has access to events that happen in health institutions;

2. Increased availability of health services, as patients can now have access to their health information without having to visit the hospital, resulting in the promotion of self-care and freeing up the health institutions resources;

3. Transparency of health services, since interactions with patients are recorded in detail and immutably, enabling for any patient to have access to his healthcare information.

4.4 Conclusions

In this chapter, the deployment of BARS into the developed testbed is discussed, starting with an introduction to the testbed itself where the main goal, overall architecture and the applications that were developed are explained. The applications are explained in detail, with focus to what kind of complexity they introduce to the system and how they impact the working of the system in regards to the workflows that the system should respond to. An explanation on the workflow that was designed to be tested with the integration of the system into the testbed is also made, to further explain the foundation of the testbed. The integration and functioning of the system into the testbed is explained as a proof-of-concept, where both the several technologies that were utilized are introduced and explaining how each technology or methodology furthers the goal of addressing the issues pointed out in the previous chapter. In addition, the constitution, functioning and roles that the three modules that compose the system are further explained, going into detail into how the communication encryption schemes were made, how the blockchain properties increase the value of the system and how secure data

storage and access is achieved. To conclude, a discussion on the viability of the system and performance of the proof-of-concept in the testbed is made in order to outline how this system introduces the advantages mentioned previously as well as how the integration of the proof-of-concept into a real electronic health system like a national health system could bring even more advantages to the system while decreasing the difficulty caused by some of the challenges of blockchain.

Chapter 5

Final Considerations and Future Work

5.1 Main Conclusions

The evolution that m-Health services and applications experienced in recent years has led to several breakthroughs and new integration of mobile technologies in traditional health systems, shifting the focus form the health service provider to the patient. To further advance m-Health, the integration of security measures is mandatory, as data privacy and security are key issues. To enhance how access control and event recording is done in current health systems, a blockchain based conceptual system is proposed and a prototype was developed and integrated into a testbed. This testbed was specifically designed in order to simulate a workflow where several applications interface with the system in order to save and retrieve information. A discussion of the specific advantages and challenges proposed throughout this thesis work is made, highlighting the key issues as well as proposing solutions to them. If implemented with caution and following the proposals stated in this study, it is believed that m-Health applications can have a reliable and trustworthy blockchain system. This system in cooperation with traditional health systems, can improve the quality of service, monitoring and diagnose capabilities and overall empowering patients towards true ownership of their health data.

The main objective of this thesis was to study how to integrate blockchain technology into the m-Health ecosystem while both introducing the advantages commonly associated with blockchain and to tackle the challenges associated with traditional healthcare systems. To accomplish this objective and to enhance the overall quality of the system to a level where integration on a real-world health system would be possible, the proposed state-of-the-art study and several technologies were used in order to create a conceptual system proposal. Based on this proposal, a prototype of the system was developed and integrated into a testbed that closely resembles a workflow where multiple mobile applications could communicate directly with a electronic health system.

This prototype was then tested on both the viability that similar solutions could have and the performance constraints that such solutions present and possible solutions. The results where then compiled and an analysis on the main advantages from successful integration where confirmed. A discussion on the positive effect that integration of the prototype system into a major electronic health system like a national health system is had, with focus on the advantages that this integration would bring as well as proposing methods to deal with some of the challenges of using blockchain technology in a larger scale. This integration is the main point of the future work for this thesis work.

As such, all of the proposed objectives for this dissertation work were successfully accomplished.

5.2 Future Work

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

- Integration of BARS into a large scale health system, like a national health system, and study the impacts in terms of availability of service, patient usability and integration into existing systems and methodologies;

- Optimization of the smart-contract algorithms to improve the performance of certain tasks, like collecting all health event from a patient;

- Addition of biometric identity authentication for accessing patient information (discussed in detail in 2.2;

- Optimization of the overall functionality of the prototype in order to be able to compare the performance of a blockchain-based system in comparison to a database management system implementation;

- Running BARS in one of the Ethereum main networks and explore how to outsource health event recording to the computational resources of the network.

Bibliography

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008, Last accessed in: 2019-04-29. [Online]. Available: https://bitcoin.org/bitcoin.pdf 1

[2] L. B. Harman, C. A. Flite, , and K. Bond, “STATE OF THE ART AND SCIENCE Electronic Health Records: Privacy, Confidentiality, and Security,” *American Medical Association Journal of Ethics No. 9*, vol. 14, pp. 712–719, Sep 2012. 1

[3] Eligma, “White paper: Eligma - ”AI-driven and blockchain-based cognitive commerce platform”,” March 2018, Last accessed in: 2019-04-29. [Online]. Available: https://eligma.com/pdf/eligma-white-paper_v1.1.pdf 1, 13

[4] B. M. Silva, J. J. Rodrigues, I. de la Torre Díez, M. López-Coronado, and K. Saleem, “Mobile-health: A review of current state in 2015,” *Journal of Biomedical Informatics*, vol. 56, pp. 265 – 272, 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1532046415001136 1

[5] A. K. Jha, C. M. DesRoches, E. G. Campbell, K. Donelan, S. R. Rao, T. G. Ferris, A. Shields, S. Rosenbaum, and D. Blumenthal, “Use of electronic health records in US hospitals,” *New England Journal of Medicine*, vol. 360, no. 16, pp. 1628–1638, 2009. 1

[6] M. K. Boulos, S. Wheeler, C. Tavares, and R. Jones, “How smartphones are changing the face of mobile and participatory healthcare: an overview, with example from eCAALYX,” *Biomedical engineering online*, vol. 10, no. 1, p. 24, 2011. 1

[7] H. R. Jara and E. Schafir, “E-health: An introduction to the challenges of privacy and security,” in *2014 IEEE Central America and Panama Convention (CONCAPAN XXXIV)*, Nov 2014, pp. 1–5. 1

[8] S. Steinhubl, E. Muse, and E. Topol, “Can mobile health technologies transform health care?” *Jama*, vol. 310, no. 22, pp. 2395–2396, 2013. 5

[9] C. L. Ventola, “Mobile devices and apps for health care professionals: uses and benefits,” *P&T No. 5*, vol. 39, May 2014. 5

[10] K. Källander, J. Tibenderana, O. Akpogheneta, D. Strachan, Z. Hill, A. Asbroek, L. Conteh, B. Kirkwood, and S. Meek, “Mobile health (mHealth) approaches and lessons for increased performance and retention of community health workers in low-and middle-income countries: a review,” *Journal of medical Internet research*, vol. 15, no. 1, 2013. 5, 6

[11] C. Aranda-Jan, N. Mohutsiwa-Dibe, and S. Loukanova, “Systematic review on what works, what does not work and why of implementation of mobile health (mHealth) projects in Africa,” *BMC public health*, vol. 14, no. 1, p. 188, 2014. 5, 6

[12] L. K. . E. Topol, “Unpatients—why patients should own their medical data,” *Nature Biotechnology*, vol. 33, p. 921–924, Sep 2015. 5

[13] R. Shahriyar, F. Bari, G. Kundu, S. I. Ahamed, and M. Akbar, “Intelligent mobile health monitoring system (IMHMS),” in *International Conference on Electronic Healthcare*. Springer, 2009, pp. 5–12. 5

[14] M. Sarwar and T. R. Soomro, “Impact of Smartphone’s on Society,” *European journal of scientific research*, vol. 98, no. 2, pp. 216–226, 2013. 5

[15] S. Fox and M. Duggan, *Mobile health 2010*. Pew Internet & American Life Project Washington, DC, 2010. 5

[16] A. Lorenz and R. Oppermann, “Mobile health monitoring for the elderly: Designing for diversity,” *Pervasive and Mobile Computing*, vol. 5, no. 5, pp. 478–495, 2009. 6

[17] V. Chan, P. Ray, and N. Parameswaran, “Mobile e-Health monitoring: an agent-based approach,” *IET communications*, vol. 2, no. 2, pp. 223–230, 2008. 6

[18] A. Holzinger, S. Dorner, M. Födinger, A. C. Valdez, and M. Ziefle, “Chances of increasing youth health awareness through mobile wellness applications,” in *Symposium of the Austrian HCI and Usability Engineering Group*. Springer, 2010, pp. 71–81. 6

[19] B. M. Silva, I. M. Lopes, J. J. P. C. Rodrigues, and P. Ray, “SapoFitness: A mobile health application for dietary evaluation,” in *2011 IEEE 13th International Conference on e-Health Networking, Applications and Services*, June 2011, pp. 375–380. 6

[20] Nike Inc., “Nike+,” 2019,
Last accessed in: 2019-04-29. [Online]. Available: https://www.nike.com/us/en_us/c/nike-plus/training-app 6

[21] Z. Lv, F. Xia, G. Wu, L. Yao, and Z. Chen, “iCare: a mobile health monitoring system for the elderly,” in *Green Computing and Communications (GreenCom), 2010 IEEE/ACM Int’l Conference on & Int’l Conference on Cyber, Physical and Social Computing (CPSCom)*. IEEE, 2010, pp. 699–705. 6

[22] A. Bourouis, M. Feham, and A. Bouchachia, “Ubiquitous mobile health monitoring system for elderly (UMHMSE),” *arXiv preprint arXiv:1107.3695*, 2011. 6

[23] Fitbit Inc., “Fitbit,” 2019,
Last accessed in: 2019-04-29. [Online]. Available: https://www.fitbit.com/eu/technology 6

[24] M. del Rosario, S. Redmond, and N. Lovell, “Tracking the evolution of smartphone sensing for monitoring human movement,” *Sensors*, vol. 15, no. 8, pp. 18 901–18 933, 2015. 6

[25] C. Otto, A. Milenkovic, C. Sanders, and E. Jovanov, “System architecture of a wireless

body area sensor network for ubiquitous health monitoring," *Journal of mobile multimedia*, vol. 1, no. 4, pp. 307–326, 2006. 6

[26] V. Jones, V. Gay, and P. Leijdekkers, "Body sensor networks for mobile health monitoring: Experience in europe and australia," in *Digital Society, 2010. ICDS'10. Fourth International Conference on*. IEEE, 2010, pp. 204–209. 6

[27] M. Milošević, M. T. Shrove, and E. Jovanov, "Applications of smartphones for ubiquitous health monitoring and wellbeing management," *JITA-JOURNAL OF INFORMATION TECHNOLOGY AND APLICATIONS*, vol. 1, no. 1, 2011. 6

[28] A. Pantelopoulos and N. G. Bourbakis, "A survey on wearable sensor-based systems for health monitoring and prognosis," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 40, no. 1, pp. 1–12, 2010. 6

[29] M. Chen, S. Gonzalez, A. Vasilakos, H. Cao, and V. C. Leung, "Body area networks: A survey," *Mobile networks and applications*, vol. 16, no. 2, pp. 171–193, 2011. 6

[30] Y. Wu and P. Chen, "Multi-channel data-acquisition and controller for mobile health monitoring system with HSDPA and GPS," in *2009 Second International Conference on the Applications of Digital Information and Web Technologies*, Aug 2009, pp. 227–231. 6

[31] L. Huang, Y. Xu, X. Chen, H. Li, and Y. Wu, "Design and Implementation of Location Based Mobile Health System," in *2012 Fourth International Conference on Computational and Information Sciences*, Aug 2012, pp. 919–922. 6

[32] H. Holmen, A. Torbjørnsen, A. K. Wahl, A. K. Jenum, M. C. Småstuen, E. Årsand, and L. Ribu, "A mobile health intervention for self-management and lifestyle change for persons with type 2 diabetes, part 2: one-year results from the Norwegian randomized controlled trial RENEWING HEALTH," *JMIR mHealth and uHealth*, vol. 2, no. 4, 2014. 6

[33] ASICS Digital Inc., "RunKeeper," 2018, last accessed in: 2019-04-29. [Online]. Available: https://runkeeper.com/ 6

[34] D. S. Eng and J. M. Lee, "The promise and peril of mobile health applications for diabetes and endocrinology," *Pediatric diabetes*, vol. 14, no. 4, pp. 231–238, 2013. 6

[35] N. Stein and K. Brooks, "A Fully Automated Conversational Artificial Intelligence for Weight Loss: Longitudinal Observational Study Among Overweight and Obese Adults," *JMIR Diabetes*, vol. 2, p. e28, Nov 2017. 7

[36] R. Miotto, F. Wang, S. Wang, X. Jiang, and J. T. Dudley, "Deep learning for healthcare: review, opportunities and challenges," *Briefings in Bioinformatics*, vol. 19, no. 6, pp. 1236–1246, 2018. [Online]. Available: http://dx.doi.org/10.1093/bib/bbx044 7

[37] B. Liu, S. Shi, Y. Wu, D. Thomas, L. Symul, E. Pierson, and J. Leskovec, "Predicting pregnancy using large-scale data from a women's health tracking mobile application,"

arXiv preprint arXiv:1812.02222, 2018. 7

[38] D. Ravi, C. Wong, B. Lo, and G.-Z. Yang, "A deep learning approach to on-node sensor data analytics for mobile or wearable devices," *IEEE journal of biomedical and health informatics*, vol. 21, no. 1, pp. 56–64, 2017. 7

[39] L. Nie, M. Wang, L. Zhang, S. Yan, B. Zhang, and T.-S. Chua, "Disease inference from health-related questions via sparse deep learning," *IEEE Transactions on Knowledge and Data Engineering*, vol. 27, no. 8, pp. 2107–2119, 2015. 7

[40] R. L. Rosa, G. M. Schwartz, W. V. Ruggiero, and D. Z. Rodriguez, "A Knowledge-Based Recommendation System that includes Sentiment Analysis and Deep Learning," *IEEE Transactions on Industrial Informatics*, 2018. 7

[41] Y. Cao, C. Liu, B. Liu, M. J. Brunette, N. Zhang, T. Sun, P. Zhang, J. Peinado, E. S. Garavito, L. L. Garcia *et al.*, "Improving tuberculosis diagnostics using deep learning and mobile health technologies among resource-poor and marginalized communities," in *2016 IEEE First International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE)*. IEEE, 2016, pp. 274–281. 7

[42] N. D. Lane and P. Georgiev, "Can deep learning revolutionize mobile sensing?" in *Proceedings of the 16th International Workshop on Mobile Computing Systems and Applications*. ACM, 2015, pp. 117–122. 7

[43] E. Kangas and T. Kinnunen, "Applying user-centered design to mobile application development," *Communications of the ACM*, vol. 48, no. 7, pp. 55–59, 2005. 7

[44] A. Holzinger and M. Errath, "Mobile computer Web-application design in medicine: some research based guidelines," *Universal Access in the Information Society*, vol. 6, no. 1, pp. 31–41, 2007. 7

[45] E. Miluzzo, N. D. Lane, K. Fodor, R. Peterson, H. Lu, M. Musolesi, S. B. Eisenman, X. Zheng, and A. T. Campbell, "Sensing meets mobile social networks: the design, implementation and evaluation of the cenceme application," in *Proceedings of the 6th ACM conference on Embedded network sensor systems*. ACM, 2008, pp. 337–350. 7

[46] A. Charland and B. Leroux, "Mobile application development: web vs. native," *Queue*, vol. 9, no. 4, p. 20, 2011. 7

[47] Adobe Systems Inc., "Phonegap," 2019,
Last accessed in: 2019-04-29. [Online]. Available: https://phonegap.com/ 7

[48] Framework7, "Framework7," 2019,
Last accessed in: 2019-04-29. [Online]. Available: https://framework7.io/ 7

[49] D. King, F. Greaves, C. Exeter, and A. Darzi, "'Gamification': Influencing health behaviours with games," 2013. 7

[50] C. Lister, J. H. West, B. Cannon, T. Sax, and D. Brodegard, "Just a fad? Gamification in health and fitness apps," *JMIR serious games*, vol. 2, no. 2, 2014. 7

[51] T. Alahäivälä and H. Oinas-Kukkonen, "Understanding persuasion contexts in health gamification: A systematic analysis of gamified health behavior change support systems literature," *International journal of medical informatics*, vol. 96, pp. 62–70, 2016. 7

[52] D. Johnson, S. Deterding, K.-A. Kuhn, A. Staneva, S. Stoyanov, and L. Hides, "Gamification for health and wellbeing: A systematic review of the literature," *Internet interventions*, vol. 6, pp. 89–106, 2016. 7

[53] T. Althoff, R. W. White, and E. Horvitz, "Influence of Pokémon Go on Physical Activity: Study and Implications," *CoRR*, vol. abs/1610.02085, 2016. [Online]. Available: http://arxiv.org/abs/1610.02085 7

[54] K. Chen, A. Chan, and S. Tsang, "Usage of Mobile Phones amongst Elderly People in Hong Kong," *Lecture Notes in Engineering and Computer Science*, vol. 2, pp. 1016–1019, 03 2013. 7

[55] J.-M. Díaz-Bossini and L. Moreno, "Accessibility to mobile interfaces for older people," *Procedia Computer Science*, vol. 27, pp. 57 – 66, 2014, 5th International Conference on Software Development and Technologies for Enhancing Accessibility and Fighting Info-exclusion, DSAI 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1877050914000106 7

[56] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," *IEEE Wireless communications*, vol. 17, no. 1, 2010. 8

[57] W. Wilkowska and M. Ziefle, "Privacy and data security in E-health: Requirements from the user's perspective," *Health informatics journal*, vol. 18, no. 3, pp. 191–201, 2012. 8

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

[59] R. L. Krutz and R. D. Vines, *Cloud security: A comprehensive guide to secure cloud computing*. Wiley Publishing, 2010. 8, 10

[60] D. Chen and H. Zhao, "Data security and privacy protection issues in cloud computing," in *Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on*, vol. 1. IEEE, 2012, pp. 647–651. 8, 10

[61] Top Threats Working Group CSA, "The Treacherous 12 Cloud Computing Top Threats in 2016," *Cloud Security Alliance*, Feb 2016. 8

[62] G. Apostolopoulos, V. Peris, and D. Saha, "Transport Layer Security: How much does it really cost?" in *INFOCOM'99. Eighteenth Annual Joint Conference of the IEEE Computer*

and Communications Societies. Proceedings. IEEE, vol. 2. IEEE, 1999, pp. 717–725. 8

[63] Q. Wang, D. Zhou, and Y. Li, "Secure outsourced calculations with homomorphic encryption," *arXiv e-prints*, Dec. 2018. 9

[64] C. Gentry and D. Boneh, *A fully homomorphic encryption scheme*. Stanford University Stanford, 2009, vol. 20, no. 09. 9

[65] C. Gentry and S. Halevi, "Implementing gentry's fully-homomorphic encryption scheme," in *Annual international conference on the theory and applications of cryptographic techniques*. Springer, 2011, pp. 129–148. 9

[66] W. Wang, Y. Hu, L. Chen, X. Huang, and B. Sunar, "Accelerating fully homomorphic encryption on GPUs," in *Proceedings of the IEEE High Performance Extreme Computing Conference*. Citeseer, 2012. 9

[67] J. Liu, Y.-H. Lu, and C.-K. Koh, "Performance analysis of arithmetic operations in homomorphic encryption," 2010. 9

[68] S. Kim, M. Omori, T. Hayashi, T. Omori, L. Wang, and S. Ozawa, "Privacy-Preserving Naive Bayes Classification Using Fully Homomorphic Encryption," in *International Conference on Neural Information Processing*. Springer, 2018, pp. 349–358. 9

[69] S. M. T. Toapanta, L. J. C. Chalén, and J. G. Ortiz, "A Homomorphic Encryption Approach in a Voting System in a Distributed Architecture," 2018. 9

[70] A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: a tool for information security," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, pp. 125–143, June 2006. 9

[71] Y. Qiu, J. V. Gigliotti, M. Wallace, F. Griggio, C. E. M. Demore, S. Cochran, and S. Trolier-McKinstry, "Piezoelectric micromachined ultrasound transducer (PMUT) arrays for integrated sensing, actuation and imaging," *Sensors*, vol. 15, no. 4, pp. 8020–8041, 2015. 9

[72] C. C. Schroeder, "Biometric security process for authenticating identity and credit cards, visas, passports and facial recognition," Jul. 28 1998, uS Patent 5,787,186. 9

[73] F. Deane, K. Barrelle, R. Henderson, and D. Mahar, "Perceived acceptability of biometric security systems," *Computers & Security*, vol. 14, no. 3, pp. 225–231, 1995. 9

[74] O. G. Martinsen, S. Clausen, J. B. Nysæther, and S. Grimnes, "Utilizing characteristic electrical properties of the epidermal skin layers to detect fake fingers in biometric fingerprint systems—A pilot study," *IEEE transactions on biomedical engineering*, vol. 54, no. 5, pp. 891–894, 2007. 10

[75] R. M. Seepers, C. Strydis, I. Sourdis, and C. I. D. Zeeuw, "Enhancing Heart-Beat-Based

Security for mHealth Applications," *IEEE Journal of Biomedical and Health Informatics*, vol. 21, no. 1, pp. 254–262, Jan 2017. 10

[76] J. Galbally, S. Marcel, and J. Fierrez, "Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition," *IEEE Transactions on Image Processing*, vol. 23, no. 2, pp. 710–724, Feb 2014. 10

[77] G. Iovane, C. Bisogni, L. D. Maio, and M. Nappi, "An encryption approach using Information Fusion techniques involving prime numbers and Face Biometrics," *IEEE Transactions on Sustainable Computing*, pp. 1–1, 2018. 10

[78] M. Hussain, A. Al-Haiqi, A. Zaidan, B. Zaidan, M. Kiah, S. Iqbal, S. Iqbal, and M. Abdulnabi, "A security framework for mhealth apps on android platform," *Computers & Security*, vol. 75, pp. 191 – 217, 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404818300798 10

[79] M. Hussain, A. A. Zaidan, B. B. Zidan, S. Iqbal, M. M. Ahmed, O. S. Albahri, and A. S. Albahri, "Conceptual framework for the security of mobile health applications on android platform," *Telematics and Informatics*, vol. 35, no. 5, pp. 1335 – 1354, 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0736585317308225 10

[80] W. Enck, D. Octeau, P. D. McDaniel, and S. Chaudhuri, "A study of android application security." in *USENIX security symposium*, vol. 2, 2011, p. 2. 10

[81] S. Iqbal, A. Yasin, and T. Naqash, "Android (nougats) security issues and solutions," in *2018 IEEE International Conference on Applied System Invention (ICASI)*. IEEE, 2018, pp. 1152–1155. 10

[82] T. Dehling, F. Gao, S. Schneider, and A. Sunyaev, "Exploring the far side of mobile health: information security and privacy of mobile health apps on ios and android," *JMIR mHealth and uHealth*, vol. 3, no. 1, 2015. 10

[83] 104th Congress of the United States of America, "HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996," 1996,
Last accessed in: 2019-04-29. [Online]. Available: https://www.govinfo.gov/content/pkg/PLAW-104publ191/html/PLAW-104publ191.htm 10

[84] C. M. of Justice, "Personal Information Protection and Electronic Documents Act," 2000, Last accessed in: 2019-04-29. [Online]. Available: https://laws-lois.justice.gc.ca/PDF/P-8.6.pdf 10

[85] A. L. R. Commision, "Australian Privacy Law & Practice - Key Recommendations for Health Information Privacy Reform," *S.C. 2000, c. 5*, 2000,
Last accessed in: 2019-04-29. 10

[86] E. Vayena, J. Dzenowagis, J. S. Brownstein, and A. Sheikh, "Policy implications of big data in the health sector," *Bulletin of the World Health Organization*, vol. 96, no. 1, pp.

66–68, 2018. 10

[87] D.-G. Feng, M. Zhang, Y. Zhang, and Z. Xu, "Study on cloud computing security," *Journal of software*, vol. 22, no. 1, pp. 71–83, 2011. 10

[88] B. R. Kandukuri, A. Rakshit *et al.*, "Cloud security issues," in *Services Computing, 2009. SCC'09. IEEE International Conference on*. IEEE, 2009, pp. 517–520. 10

[89] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage," *IEEE Transactions on computers*, vol. 62, no. 2, pp. 362–375, 2013. 10

[90] D. Tapscott and A. Tapscott, *Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world*. Penguin, 2016. 10

[91] M. Iansiti and K. R. Lakhani, "The truth about blockchain," *Harvard Business Review*, vol. 95, no. 1, pp. 118–127, 2017. 10

[92] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Generation Computer Systems*, 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X17318332 11

[93] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, "Untangling Blockchain: A Data Processing View of Blockchain Systems," *IEEE Transactions on Knowledge and Data Engineering*, vol. 30, no. 7, pp. 1366–1385, July 2018. 11

[94] J. R. B. MICHAEL J.W. RENNOCK, ALAN COHN, "BLOCKCHAIN TECHNOLOGY AND REGULATORY INVESTIGATIONS," *The Journal*, Mar 2018. [Online]. Available: https://www.steptoe.com/images/content/1/7/v2/171967/LIT-FebMar18-Feature-Blockchain.pdf 11

[95] Ethereum Foundation, "Ethereum," 2019,
Last accessed in: 2019-04-29. [Online]. Available: http://ethereum.org 12

[96] G. Wood, "DApps: What Web 3.0 Looks Like," April 2014,
Last accessed in: 2019-04-29. [Online]. Available: http://gavwood.com/dappsweb3.html 12

[97] W. Cai, Z. Wang, J. B. Ernst, Z. Hong, C. Feng, and V. C. M. Leung, "Decentralized Applications: The Blockchain-Empowered Software System," *IEEE Access*, vol. 6, pp. 53 019–53 033, 2018. 12

[98] C. Shen and F. Pena-Mora, "Blockchain for Cities - A Systematic Literature Review," *IEEE Access*, pp. 1–1, 2018. 12

[99] S. Li, "Application of Blockchain Technology in Smart City Infrastructure," in *2018 IEEE International Conference on Smart Internet of Things (SmartIoT)*, Aug 2018, pp. 276–2766. 12

[100] K. Biswas and V. Muthukkumarasamy, “Securing Smart Cities Using Blockchain Technology,” in *2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, Dec 2016, pp. 1392–1393. 12

[101] D. Nagothu, R. Xu, S. Yahya Nikouei, and Y. Chen, “A Microservice-enabled Architecture for Smart Surveillance using Blockchain Technology,” *arXiv e-prints*, p. arXiv:1807.07487, Jul. 2018. 12

[102] Ethereum Foundation, “Ether,” 2019,
Last accessed in: 2019-04-29. [Online]. Available: http://ethereum.org/ether 12

[103] B. V. Vogelsteller, F., “ERC-20 Token Standard. RFC 20, Ethereum,” November 2015,
Last accessed in: 2019-04-29. [Online]. Available: https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md 12

[104] V. Buterin, “White Paper: A Next-Generation Smart Contract and Decentralized Application Platform,” November 2013,
Last accessed in: 2019-04-29. [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper 12

[105] G. Wood, “White Paper: Ethereum: A secure decentralized generalized transaction ledger,” January 2014. [Online]. Available: http://gavwood.com/paper.pdf 12

[106] C. Dannen, “Introducing Ethereum and Solidity,” *Apress*, 2017. 12

[107] M. J. Stefan Schmidt, “Unibright - the unified framework for blockchain based business integration,” Apr 2018,
Last accessed in: 2019-04-29. [Online]. Available: https://unibright.io/download/Unibright_Whitepaper.pdf 12

[108] SAP, “CSAP Information,” 2019,
Last accessed in: 2019-04-29. [Online]. Available: https://www.sap.com/corporate/en/company.html 12

[109] Unibright, “Current state of development - SAP integration,” Nov 2018,
Last accessed in: 2019-04-29. [Online]. Available: https://medium.com/unibrightio/ 12

[110] Tezos Foundation, “Tezos,” 2019,
Last accessed in: 2019-04-29. [Online]. Available: http://tezos.com 12

[111] INRIA, “OCaml,” 2019, last accessed in: 2019-04-29. [Online]. Available: https://ocaml.org/ 12

[112] L. M. Goodman, “White Paper: Tezos: a self-amending crypto-ledger,” Sep 2014. [Online]. Available: https://tezos.com/static/papers/white_paper.pdf 12

[113] DeepBrainChain, “White paper: Deepbrain chain artificial intelligence computing platform driven by blockchain,” 2017. [Online]. Available: https://www.deepbrainchain.org/assets/pdf/DeepBrainChainWhitepaper_en.pdf 12

[114] V. Lopes and L. A. Alexandre, “An Overview of Blockchain Integration with Robotics and Artificial Intelligence,” *arXiv e-prints*, p. arXiv:1810.00329, Sep. 2018. 12, 13

[115] T. Marwala and B. Xing, “Blockchain and Artificial Intelligence,” *CoRR*, vol. abs/1802.04451, 2018. [Online]. Available: http://arxiv.org/abs/1802.04451 12

[116] S. Omohundro, “Cryptocurrencies, Smart Contracts, and Artificial Intelligence,” *AI Matters*, vol. 1, no. 2, pp. 19–21, Dec. 2014. [Online]. Available: http://doi.acm.org/10.1145/2685328.2685334 12

[117] V. Lopes and L. A. Alexandre, “Detecting Robotic Anomalies using RobotChain,” in *2019 IEEE International Conference on Autonomous Robot Systems and Competitions (ICARSC)*, April 2019. 13

[118] E. C. Ferrer, “The blockchain: a new framework for robotic swarm systems,” *CoRR*, vol. abs/1608.00695, 2016. [Online]. Available: http://arxiv.org/abs/1608.00695 13

[119] V. Lopes, L. A. Alexandre, and N. Pereira, “Controlling Robots using Artificial Intelligence and a Consortium Blockchain,” *arXiv e-prints*, p. arXiv:1903.00660, Mar 2019. 13

[120] V. Lopes, N. Pereira, and L. A. Alexandre, “Robot Workspace Monitoring using a Blockchain-based 3D Vision Approach,” in *2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, June 2019. 13

[121] N. Inc., “White paper: Nam Coin - revolution in medical care with AI and blockchain,” Jul 2018. [Online]. Available: https://namchain.net/whitepaper/EN_whitepaper_20180728134338.pdf 13

[122] SweatCo. LTD, “Sweatcoin,” 2019,
Last accessed in: 2019-04-29. [Online]. Available: https://sweatco.in/about 13

[123] M. Conoscenti, A. Vetrò, and J. C. D. Martin, “Blockchain for the Internet of Things: A systematic literature review,” in *2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA)*, Nov 2016, pp. 1–6. 13

[124] T. M. Fernández-Caramés and P. Fraga-Lamas, “A Review on the Use of Blockchain for the Internet of Things,” *IEEE Access*, vol. 6, pp. 32 979–33 001, 2018. 13

[125] K. Christidis and M. Devetsikiotis, “Blockchains and Smart Contracts for the Internet of Things,” *IEEE Access*, vol. 4, pp. 2292–2303, 2016. 13

[126] S. Kiyomoto, M. S. Rahman, and A. Basu, “On blockchain-based anonymized dataset distribution platform,” in *2017 IEEE 15th International Conference on Software Engineering*

Research, Management and Applications (SERA), June 2017, pp. 85–92. 13, 19

[127] P. K. Sharma, M. Chen, and J. H. Park, "A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT," *IEEE Access*, vol. 6, pp. 115–124, 2018. 13

[128] I. Chiuchisan, D. Balan, O. Geman, I. Chiuchisan, and I. Gordin, "A security approach for health care information systems," in *2017 E-Health and Bioengineering Conference (EHB)*, June 2017, pp. 721–724. 15

[129] A. Meri, M. Hasan, M. Danaee, M. Jaber, N. Safei, M. Dauwed, S. K. Abd, M. Al-bsheish *et al.*, "Modelling the Utilization of Cloud Health Information Systems in the Iraqi Public Healthcare Sector," *Telematics and Informatics*, 2018. 16

[130] D. P. Lorence and R. Churchill, "Incremental adoption of information security in healthcare organizations: implications for document management," *IEEE Transactions on Information Technology in Biomedicine*, vol. 9, no. 2, pp. 169–173, June 2005. 16

[131] F. C. M. Müthing J., Jäschke T., "Client-focused security assessment of mhealth apps and recommended practices to prevent or mitigate transport security issues," *JMIR Mhealth Uhealth*, Oct 2017. 16

[132] L. Lai, S. Ho, and H. V. Poor, "Privacy–Security Trade-Offs in Biometric Security Systems—Part I: Single Use Case," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 1, pp. 122–139, March 2011. 16

[133] ——, "Privacy–Security Trade-Offs in Biometric Security Systems—Part II: Multiple Use Case," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 1, pp. 140–151, March 2011. 16

[134] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric Recognition: Security and Privacy Concerns," *Security & Privacy, IEEE*, vol. 1, pp. 33 – 42, 04 2003. 16

[135] Deloitte and Oracle, "Securing Electronic Health Records (EHRs) to Achieve "Meaningful Use" Compliance, Prevent Data Theft and Fraud," *HealthITNews privacy and security survey*, Mar 2011. 17

[136] H. Wu and C. Tsai, "Toward Blockchains for Health-Care Systems: Applying the Bilinear Pairing Technology to Ensure Privacy Protection and Accuracy in Data Sharing," *IEEE Consumer Electronics Magazine*, vol. 7, no. 4, pp. 65–71, July 2018. 19

[137] H. Zhao, P. Bai, Y. Peng, and R. Xu, "Efficient key management scheme for health blockchain," *CAAI Transactions on Intelligence Technology*, vol. 3, no. 2, pp. 114–118, 2018. 19

[138] R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain in Electronic Health Records Systems," *IEEE Access*, vol. 6, pp. 11 676–11 686, 2018. 19

[139] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," in *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, Oct 2017, pp. 1–5. 25

[140] C. Esposito, A. D. Santis, G. Tortora, H. Chang, and K. R. Choo, "Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?" *IEEE Cloud Computing*, vol. 5, no. 1, pp. 31–37, Jan 2018. 25

[141] L. Mertz, "(Block) Chain Reaction: A Blockchain Revolution Sweeps into Health Care, Offering the Possibility for a Much-Needed Data Solution," *IEEE Pulse*, vol. 9, no. 3, pp. 4–7, May 2018. 25

[142] K. M. B. Linn, L.A., "Blockchain for health data and its potential use in health it and health care related research," *HealthIT*, 2017. [Online]. Available: https://www.healthit.gov/sites/default/files/11-74-ablockchainforhealthcare.pdf 27

[143] S. Das, A. Kolluri, P. Saxena, and H. Yu, "On the Security of Blockchain Consensus Protocols," in *International Conference on Information Systems Security*. Springer, 2018, pp. 465–480. 28

[144] A. Baliga, "Understanding blockchain consensus models," *Persistent*, 2017. 28

[145] J. Wilmoth, "Bitcoin Gold Hit by Double Spend Attack, Exchanges Lose Millions," May 2018,
Last accessed in: 2019-04-29. [Online]. Available: https://www.ccn.com/bitcoin-gold-hit-by-double-spend-attack-exchanges-lose-millions/ 28

[146] E. Gaetani, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, "Blockchain-based database to ensure data integrity in cloud computing environments," 2017. 28

[147] F. Glaser, "Pervasive decentralisation of digital infrastructures: a framework for blockchain enabled system and use case analysis," 2017. 28

[148] Counterfactual, "Counterfactual," 2019,
Last accessed in: 2019-04-29. [Online]. Available: https://www.counterfactual.com/technology/ 28

[149] C. R. Jason Teutsch, "A scalable verification solution for blockchains," Nov 2018,
Last accessed in: 2019-04-29. [Online]. Available: https://people.cs.uchicago.edu/~teutsch/papers/truebit.pdf 28

[150] Agoric, "Agoric," 2019,
Last accessed in: 2019-04-29. [Online]. Available: https://agoric.com/about/ 28