Programa de Pós-Graduação em

Computação Aplicada

Mestrado Acadêmico

André Henrique Mayer

FogChain: A Fog computing architecture integrating Blockchain and Internet of Things for Personal Health Records

São Leopoldo, 2020

André Henrique Mayer

FOGCHAIN: A FOG COMPUTING ARCHITECTURE INTEGRATING BLOCKCHAIN AND INTERNET OF THINGS FOR PERSONAL HEALTH RECORDS

Dissertação apresentada como requisito parcial para a obtenção do título de Mestre pelo Programa de Pós-Graduação em Computação Aplicada da Universidade do Vale do Rio dos Sinos — UNISINOS

Advisor:
Prof. Dr. Cristiano André da Costa

São Leopoldo
2020

M468f Mayer, André Henrique.
Fogchain : A Fog computing architecture integrating Blockchain and Internet of Things for Personal Health Records / André Henrique Mayer. – 2020.
92 f. : il. ; 30 cm.

Dissertação (mestrado) – Universidade do Vale do Rio dos Sinos, Programa de Pós-Graduação em Computação Aplicada, 2020.
"Orientador: Prof. Dr. Cristiano André da Costa."

1. Internet das coisas. 2. Blockchain. 3. Computação em neblina. 4. Modelo(s) de formação. 5. Sistemas distríbuidos. I. Título.

CDU 004.732

Dados Internacionais de Catalogação na Publicação (CIP)
(Bibliotecária: Amanda Schuster – CRB 10/2517)

AGRADECIMENTOS À CAPES

This study was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Finance Code 001.

AGRADECIMENTOS

Gostaria de agradecer primeiramente à Deus por me proporcionar esta oportunidade e me dar forças e saúde para trilhar este belo caminho de formação acadêmica, também agradeço à minha esposa Gislaine Mayer, meus pais Vilmar e Ana Mayer, meu irmão Rafael e demais familiares por todo o apoio, paciência e dedicação, sem eles nada disso seria possível. Agradeço imensamente ao Prof. Dr. Cristiano André da Costa, meu orientador, que me proporcionou muito conhecimento, apoio e orientação, principalmente em momentos de dificuldade. Agradeço também aos professores e colegas de pós-graduação, Rodrigo da Rosa Righi, Rodolfo Antunes, Rafael Kunst, Cristiano Both, Igor Nardin, Thiago Lopes, Junior Marostega, Luis Gubert, Humberto Costa e João Montenegro, pela discussão e auxílio em atividades de todos os tipos. Por fim, agradeço à CAPES pela bolsa que me permitiu entrar em uma pós-graduação.

RESUMO

A adoção da Internet das Coisas cresce significativamente e é bem-sucedida em diversos domínios diferentes. No entanto, a crescente demanda por mais dispositivos conectados aumenta o requisito de arquiteturas de IoT escaláveis, capazes de manter a segurança e a privacidade dos dados coletados. Este último é um aspecto particularmente crítico ao considerar dados sensíveis, por exemplo, registros médicos. Uma solução para enfrentar esse desafio é modificar o modelo de arquitetura centralizado, para um distribuído baseado em Blockchain, alterando a maneira como os dados da IoT são armazenados e compartilhados, fornecendo uma rede ponto a ponto descentralizada. A tecnologia Blockchain permite nomear e rastrear dispositivos conectados e, no caso deste trabalho, apresenta uma alta disponibilidade de registros pessoais de saúde, protegendo ainda a privacidade do paciente através do uso de criptografia. Além disso, a adição de mecanismos de computação em neblina permite o processamento local de dados, otimizando o tempo de resposta das aplicações de saúde. Como resultado, os dispositivos podem contar com um ecossistema local mais resiliente para operação. Nossa motivação reside no sentido em que os pacientes geralmente deixam seus dados médicos espalhados por várias organizações (por exemplo, hospitais), à medida que os eventos da vida os afastam do silo de dados, de um provedor e para outro e, ao fazê-lo, perdem o acesso fácil aos dados pregressos, uma vez que é o provedor de saúde, e não o paciente, quem geralmente mantém a administração primária sobre tais registros. Neste contexto, este trabalho tem como objetivo propor uma solução disruptiva para o domínio da saúde, através da utilização de uma rede Blockchain distribuída para gerenciamento dos registros pessoais de saúde, descrevendo um modelo de arquitetura que combina as tecnologias Blockchain, Computação em neblina e Internet das Coisas. Nossa principal contribuição é a concepção do modelo FogChain e suas características voltadas para superar as limitações dos dispositivos IoT, adicionando uma camada intermediária de neblina próxima à borda para melhorar suas capacidades e recursos. Para tal, foi desenvolvido um protótipo para avaliação, através de projetos de código aberto como por exemplo, Node.js e Hyperledger Fabric, enquanto simulações e testes de desempenho foram executados em um ambiente de neblina, coletando métricas e informações como cadência da aplicação e latência da rede em relação a esse integrador de tecnologias. Durante nossos experimentos, o ambiente de computação em neblina demonstrou um tempo de resposta ao menos duas vezes mais rápido em comparação com a computação em nuvem e apontou a viabilidade do modelo proposto, como sendo capaz de atingir seus objetivos de armazenar com segurança registros de saúde, mantendo o desempenho da aplicação. Tais experimentos demonstraram apenas uma fatia de como a tecnologia Blockchain pode vir a ser empregada no domínio da saúde, beneficiando-se de sua natureza criptográfica e à prova de adulteração, o que adiciona uma camada de segurança adicional tão necessária para aplicativos da medicina e, entretanto, é seguro dizer que a computação em neblina pode desempenhar um grande papel em aplicativos deste setor, fornecendo maior poder de processamento local, serviços e aumentando a disponibilidade de recursos. No entanto, mais pesquisas, ensaios e experimentos devem ser realizados para garantir que um sistema seguro e estável seja implantado antes de usar nosso modelo em um cenário real de assistência médica, tendo em vista que a natureza dos dados de saúde do paciente é uma informação demasiada sensível e crítica.

Palavras-chave: Internet das Coisas. Blockchain. Computação em Neblina. Sistemas Distribuídos.

ABSTRACT

The Internet of Things adoption grows significantly and is successful in many different domains. Nevertheless, the ever-growing demand for more connected devices pushes the requirement for scalable IoT architectures capable of maintaining the security and privacy of collected data. The latter is a particularly critical aspect when considering sensitive data, e.g., medical records. One solution to address this challenge is to modify the centralized back-end model to one based on a Blockchain, changing the way IoT data is stored and shared by providing a decentralized peer-to-peer network. This technology enables naming and tracking for connected devices, and in the case of this article, it features a high availability of Personal Health Records, yet protecting patient's privacy through the use of cryptography. Furthermore, the addition of fog computing mechanisms may assist healthcare applications to achieve faster local data processing, thus improving overall response time. As a result, devices have a local and more resilient ecosystem for operation. Our motivation lies when patients often leave their medical data scattered across various organizations (e.g. hospitals) as life events take them away from one provider's data silo and into another, and, in doing so, they lose easy access to past data, as the provider, not the patient, generally retains primary stewardship. In this context, this work aims to propose an architecture model named FogChain, placing a distributed Blockchain network for management of patient's personal health records, while integrating the Blockchain, Fog computing, and the Internet of Things technologies for the healthcare domain. Our expected main contribution is the FogChain model itself, and its concept of overcoming IoT constraints by adding an intermediary fog layer near to the edge to improve their capabilities and resources. To do so, a prototype was developed for evaluation, trough open-source projects, and structures for application development such as Node.js and Hyperledger Fabric Blockchain, while simulations and benchmarks were executed in a fog-like environment to collect metrics and information such as throughput and network latency regarding this technologies integrator. During our end-to-end experiments, the fog computing environment demonstrated a response time to be at least twice faster in comparison with cloud computing and pointed out that our proposed model is capable of achieving its goals of safely storing personal health records while retaining application performance. The FogChain implementation for PHR management demonstrated satisfactory proofs regarding the feasibility of FogChain architecture, while it demonstrated only a slice of how Blockchain could be employed in the healthcare domain, benefiting from its cryptographic and tamper-proof nature, which adds an additional security layer so necessary for healthcare applications, and in the meantime, it is safe to say that fog computing can play a big role in healthcare applications, providing local processing power, services, and increasing resources availability. However, more research, trials, and experiments must be carried out to ensure a secure and stable system is implanted before using our model in a real healthcare scenario, given the nature of patient's health data being critical sensitive information.

Keywords: Blockchain. Internet of Things. Fog Computing. Distributed Systems.

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

DLT	Distributed Ledger Technology
P2P	Peer-to-Peer
PHR	Personal Health Records
EHR	Electronic Health Records
EMR	Electronic Medical Record
HIE	Health Information Exchange
BaaS	Blockchain as a Service
IoT	Internet of Things
IoHT	Internet of Health Things
FOG	Fog Computing
SLR	Systematic Literature Review
PPL	Physical Perception Layer
NL	Network Layer
AL	Application Layer
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
AWS	Amazon Web Services
TX/s	Transactions per second
API	Application Programming Interface
HTTP	Hypertext Transfer Protocol
HDD	Hard Drive Disk
SSD	Solid State Drive
SDK	Software Development Kit
PBFT	Practical Byzantine Fault Tolerant
ACL	Access Control Language
CA	Central Authority
IPFS	InterPlanetary File System
ISP	Internet Service Provider
VM	Virtual Machine
MP	Measurement Point
IPDV	IP Packet Delay Variation
GQM	Goal Question Metric

CONTENTS

1 INTRODUCTION

Internet of Things (IoT) refers to the network of numerous physical objects (also called Things) which are provided with an Internet connection, acquiring information about the surrounding environment, communicating with each other device and with external systems through the Internet (CONOSCENTI; VETRO; De Martin, 2016). These devices collect, process, and exchange vast amounts of data as well as privacy-sensitive information without any human intervention (BISWAS; MUTHUKKUMARASAMY, 2016), and hence are appealing targets to cyberattacks (DORRI et al., 2017).

The privacy of data collected by the Things may be at risk when stored and managed by outsourced companies on centralized servers (cloud hosting), which may make unlawful use, selling information about the behavior and preferences of its owners, or even having the clouds on their centralized servers invaded by cyberattacks, thus causing a data leak (CONOSCENTI; VETRO; De Martin, 2016). Given that IoT devices spend most of their available energy and computational resources to execute core application functionalities and data collection, supporting extra security and privacy turns to be quite challenging (DORRI et al., 2017).

Having a Blockchain in place may assist IoT systems by allowing IoT applications that previously could run only through a trusted intermediary may now operate in a decentralized way, without the need for a central authority, achieving the same functionality with the same amount of certainty (CHRISTIDIS; DEVETSIKIOTIS, 2016). It enables trustless networks because the parties can transact even though they do not trust each other. The heavy use of cryptography, a key characteristic of Blockchain networks, brings authoritativeness behind all the interactions in the network (CHRISTIDIS; DEVETSIKIOTIS, 2016). Moreover, Blockchain has the fundamental role to register and authenticate all operations performed on IoT devices data (CONOSCENTI; VETRO; De Martin, 2016).

Recent researches predict that centralized clouds, which are frequently used in current IoT systems, will be unlikely to deliver satisfactory services to customers in the near future (SHARMA; CHEN; PARK, 2018). From the core to the edge of the network, adoption of fog computing alternatives are encouraged and can be viewed as a layered service structure that is an extension of the cloud computing paradigm (SHARMA; CHEN; PARK, 2018). It will be able to provide faster cloud services such as storage, computing, and networking capabilities to end users, with each fog node located near the IoT devices at the edge of the IoT network, thus reducing communication latency and then aiming to provide a closer to real-time communication with the Things layer (BUYYA; SON, 2018; SHARMA; CHEN; PARK, 2018; PAN; MCELHANNON, 2018).

The network latency and its implications in the healthcare domain are one of our concerns in this work. Latency, also known as delay, may be defined as the difference between the one-way-delay of selected packets within a stream of packets going from measurement

point one (MP1) to measurement point two (MP2) end-to-end. This difference's technical terminology is called "IP Packet Delay Variation" (**IPDV**), measured in milliseconds and also, it may vary depending on the physical distance that data must travel through cables, wireless networks and the like to reach its destination. (KHLIFI; GRÉGOIRE, 2004; DEMICHELIS; CHIMENTO, 2002). In healthcare applications, having low-latency is really important, where seconds of delay could implicate in late diagnosis and affecting medical response time.

The Blockchain technology may have the potential to transform the healthcare field, placing the patient at the center of the health system and increasing the medical data security, privacy, and help building bridges for interoperability of health data (ROEHRS; COSTA; ROSA RIGHI, 2017). For example, this technology could provide a new model for health information exchanges (HIE) by making electronic health records (EHR) more available, efficient and secure (RABAH; RESEARCH; KENYA, 2017).

Therefore, this work aims to propose an architecture based on fog computing for the assistance of IoT and Blockchain technologies, in order to have a faster and secure communication between them, allowing a closer to real-time data processing given that the patient's Personal Health Records (PHR) will be locally available near the edge, thus, improving physicians response time and decision making (ROEHRS et al., 2017), which is our greatest motivation.

1.1 Motivation

Motivated by the opportunity to research and propose innovative solutions for healthcare domain, such as safer health records storage and privacy control, we sought to identify the main challenges and open questions in the area, in order to be able to propose a suitable model that complies with healthcare needs in a more patient-centric approach.

Public healthcare concerns every citizen and is very motivating to have the opportunity to work on research and development of new technologies to address this matter in innovative ways. Moreover, every research in this area is an opportunity to rethink current standards and to propose better solutions for the patients.

Regarding our research motivation, we were driven by the desire of improving patients experience when interacting with their health records, given they often interact in a fragmented manner.

1.2 Research Question

This work seeks to answer the following research question:

How could be described a model for the integration of Blockchain and Internet of Things technologies for Personal Health Records (PHR), using Fog Computing technology?

To answer our research question, a literature review was conducted, to verify the state of the art of our research topics, providing fundamental grounds needed to achieve our main goal beyond answering the research question, but also an architectural model that integrates Blockchain and Internet of Health Things (IoHT) technologies to achieve demanded levels of security and confidentially mandatory in healthcare applications.

The Internet of Health Things (IoHT) is an extension of the IoT concept, but in the healthcare context, and consists of interconnected objects with the capacity of exchanging and processing data to improve patient health (COSTA et al., 2018).

A patient-centric architectural model, where the patient ideally would have full control of its own medical records and gets the power to decide with who he shares its own data. Moreover, we plan to gather pertinent information in the literature review, hopefully, allowing us to plot a taxonomy classification into the state of the art of our study subject.

Regarding the Blockchain technology also present in our model, it has been researched and implemented in different domains, but just recently in the health domain (ROEHRS et al., 2019). As part of our research question, we want to verify the Blockchain integration with the healthcare domain through health records management while adopting fog computing techniques.

1.3 Objectives

Aiming to bring together and integrate the Internet of Things and Blockchain technologies for the storage and management of medical records, this work is going to explore the recent literature and studies related to these technologies, sought to identify challenges and open questions and then propose an architectural model for integrating these technologies in benefit of the healthcare field through EHR/PHR management.

This work general objective is to propose an architectural model for storing personal health records, such as vital signs, in a Blockchain distributed ledger, while integrating with surrounding Internet of Things devices around the patient such as wearables, and supported by a local fog computing middleware architecture. For achieving this objective we devised some specific objectives:

(i) Perform initial researches for understanding basic concepts necessary for comprehending Blockchain, Internet of Things and Fog computing technologies;

(ii) Conduct a Systematic Review of Literature to obtain the state of the art of our object of study, which potentially will give us a more in-depth understanding of these technologies, also the patient comprehension in this matter and applications with Personal Health Records (PHR);

(iii) Compare related studies, identifying challenges and finding opportunities;

(iv) Propose an architectural model that possibly fill identified gaps;

(v) Implement an initial prototype of the architecture model;

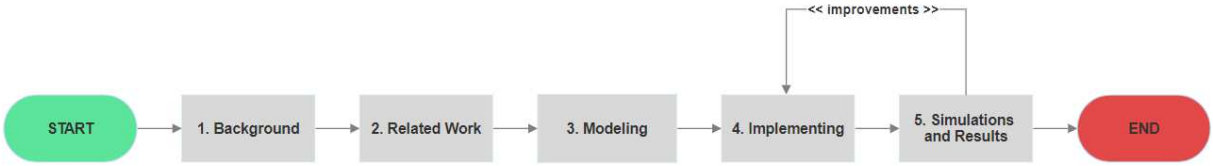
(vi) Run tests over the prototype and evaluate results.

1.4 Steps of the Research process

Our research process is divided into 5 steps, and started as soon as we had identified our Research Questions:

- ***Background***: Consisting of Literature Review and investigation, this step provided more in-depth knowledge about the problem area;
- ***Related Work***: Identify works trough a Systematic Literature Review, and compare with our proposed model;
- ***Modeling***: In this step we managed to abstract modeling FogChain and its ecosystem;
- ***Implementing***: When Modeling was done we started implementing a prototype of our FogChain;
- ***Simulation and Results***: After setting up our FogChain and Blockchain we went to simulations, evaluating obtained results and verify if that the research question could be answered.

Figure 1 – Flowchart representing stages of the research process.



Source: Elaborated by the author.

1.5 Text Organization

This work is organized into main five sections. Initially, a Background chapter presents fundamental concepts for the understanding of the rest of the work. Followed by a Related Work chapter, which presents studies related to our research theme, and enlightens

existing state of the art, as well identifying problems and challenges in the area and more importantly, helping us answer our Research Questions. Then, a Model chapter introduces our proposed architecture in this paper while trying to fill the gaps identified in the previous chapter, as well as to achieve the objectives of this work. Finally, the Conclusion chapter presents the preliminary conclusions obtained and which were the expected conclusions at the end of this research.

2 BACKGROUND

In this chapter, we will bring to light an overview of technologies such as Blockchain, Internet of Things and Fog Computing and its ecosystems that are our subject of research and study. Furthermore, an architectural model combining these technologies will be proposed in the following chapters, and this background literature will gives us the basis and a better comprehension of these technologies and applications in the healthcare field.

2.1 Internet of Things

In this section, the Internet of Things concept and technology is better described and detailed, as well, its applications and surrounding technologies.

2.1.1 Defining Internet of Things

Internet of Things (IoT) is considered one of the promising technologies that has attracted a lot of attention in both industrial and academic fields these years. It aims to integrate seamlessly both physical and digital worlds in one single ecosystem that makes up a new intelligent era of the Internet (KOUICEM; BOUABDALLAH; LAKHLEF, 2018). Consisting of sophisticated sensors, actuators, and chips embedded in the physical devices which are connected together and exchange data between them and with other digital components without any human intervention (KOUICEM; BOUABDALLAH; LAKHLEF, 2018).

Securing and protecting the data exchange in IoT is challenging due to low resource capabilities of the vast majority of devices, immense scale, heterogeneity among the devices, and lack of standardization. Moreover, many of these IoT devices collect and share large amounts of data from our personal spaces, thus opening up significant privacy concerns (DORRI; KANHERE; JURDAK, 2017).

2.1.2 IoT Architectures

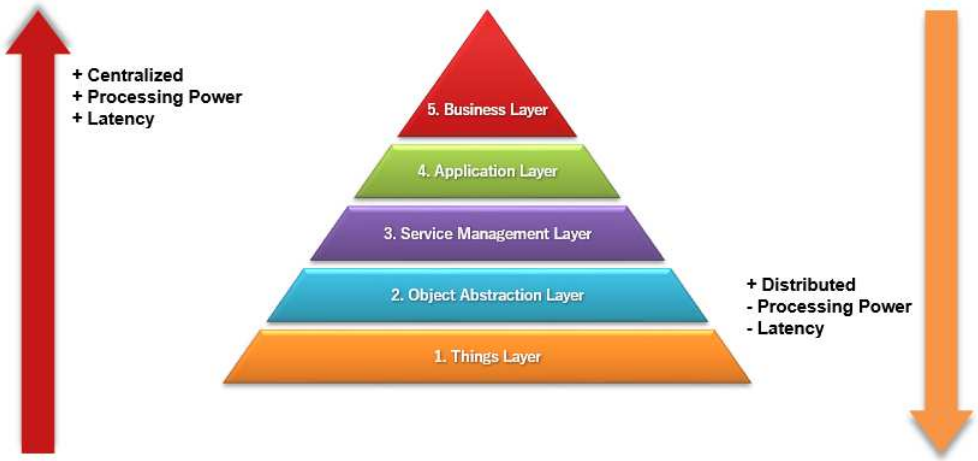
To the present date, there are established reference models regarding models and architecture definition for IoT Systems, as per example the basic model proposed by (YAN; ZHANG; VASILAKOS, 2014) consisting of a three-layer architecture, having a Physical Perception Layer (PPL), a Network Layer (NL) and an Application Layer (AL), but also, a five-layer architecture is described in (AL-FUQAHA et al., 2015) and is represented in Figure 2, which seems to be the most applicable model for IoT applications in recent literature:

- ***Objects Layer***: The first layer of the five-layers model is called Objects Layer and

also known as Things Layer, which constitutes our perception layer. It has the task to collect and process information of the surrounding environment, through sensors and actuators;

- ***Object Abstraction Layer***: Second layer, responsible for transferring collected data from first layer and sending it to the third layer through secure channels;
- ***Service Management Layer***: Third layer, pairs a service with its requester based on addresses and names;
- ***Application Layer***: The fourth layer provides the services requested by clients. The importance of this layer for the IoT is that it has the ability to provide high-quality services. It may cover numerous markets and industries, such as smart home, transportation, industrial automation, and smart healthcare;
- ***Business Layer***: The fifth layer, our last layer, manages the overall IoT system activities and services. The responsibilities of this layer are to build a business model, graphs, flowcharts, etc. based on the received data from the Application layer.

Figure 2 – IoT Five Layers model.



Source: Elaborated by the author.

2.1.3 Internet of Health Things

The concept of the Internet of Things (IoT) has evolved since its original proposition in 1999, an interconnected global network, and since then, many different concepts and applications have been proposed for IoT, varying, from environmental data sensing to services for communications and exchanging information. Thus, IoT may have

different interpretations depending on the context where it is applied, for example, the things-centric (e.g., from the sensor's point of view), moreover, it could potentially be patient-centric by consisting of interconnected objects with the capacity of exchanging and processing data to improve patient's health (COSTA et al., 2018).

Relying on the use of sensors, wearables, or other medical devices that communicate via RFID, NFC, or Bluetooth to a smartphone, which transmits collected data even further, to a middleware, typically within a fog or cloud computing infrastructure, creating this way the Internet of Health Things (IoHT), a patient's health-focused approach to IoT (COSTA et al., 2018). In this sense, IoHT may consist of interconnected objects with the capacity of exchanging and processing data to improve patient health, and, as proposed by authors (COSTA et al., 2018) this patient-centric view involves four distinct layers:

- **Acquisition**: consisting of Smart Health Objects (SHO), such as medical devices and wearables. The main purpose of an SHO is to gather data related to vital signs or other patient physiological conditions. They typically have communication capabilities in one of the many possible technologies (e.g., Bluetooth, WiFi) or standard protocols (e.g., from the umbrella of ISO, HL7, DICOM, and others);

- **Storage**: in charge of representing the collected data in a highly scalable and interoperable format. More recently, on account of the high latency of health monitoring applications, a variation of cloud computing has been advocated for IoHT. This variation is called fog computing, which provides cloud computing services in a distributed fashion, seamlessly integrating local devices (sometimes called edge computing) with remote resources in the cloud;

- **Processing**: dealing with the analysis of patient data. Instead of using traditional heuristic approaches, we argue for the use of intelligent algorithms based on machine learning techniques. We expect advanced data fusion and predictive analytics to facilitate a better inference of patient health deterioration, optimizing resources;

- **Presentation**: appearance of results as a combination of the previous layers. These can take the form of alerts, suggested actions, graphs, and charts. Epidemiological views can be obtained by combining deidentified data from different PHRs within a particular context (e.g., region, city, or hospital).

2.2 Blockchain

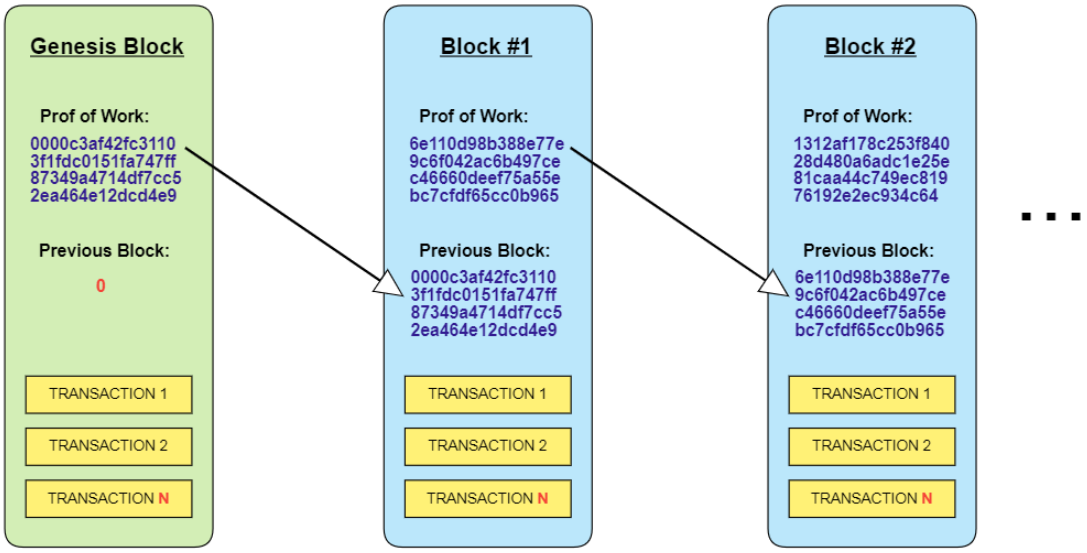
The Blockchain concepts and the technical aspects of the technology will be explained in this section.

2.2.1 Defining the Blockchain technology

The Blockchain by definition, is a Peer-to-peer (**P2P**) distributed ledger database (**DLT**) for transactions that does not need a central authority and eliminates the need for third-party verification (CONOSCENTI; VETRO; De Martin, 2016). A Blockchain contains sets of chained blocks and every block contains a hash of the previous block. Genesis block is described as the first block in a Blockchain and it is almost always hard-coded into the software, also it is the only special case in that it does not reference a previous block (NOVO, 2018) which is illustrated in Figure 3.

Blocks have a set of transactions. A transaction is a transfer of values (data/assets) between different entities/members that are broadcast to the network and collected into the blocks. All transactions are visible in the Blockchain (NOVO, 2018). To issue transactions, public key cryptography is employed. A user is provided with a public and a secret key: the secret key is used for signing transactions, while the public one is used as an address in the system. So, no real-world identity is needed for transactions, turning to be a form of pseudonymity (CONOSCENTI; VETRO; De Martin, 2016).

Figure 3 – Chained blocks structure.



Source: Elaborated by the author.

In summary, a Blockchain is a distributed ledger protocol originally associated with Bitcoin (HONGWEI; XINHUI; SANYANG, 2004). It uses public key cryptography to create an append-only, immutable and time-stamped chain of content (RABAH; RESEARCH; KENYA, 2017). It was originally designed for keeping a financial ledger, but the Blockchain paradigm can be extended to provide a generalized framework for implementing decentralized compute resources even into the Healthcare ecosystem (HONGWEI; XINHUI; SANYANG, 2004).

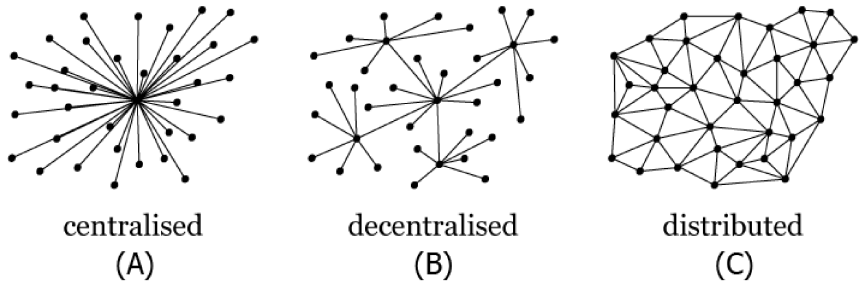
Centralization (a) and decentralization (b) often refer to the level of control over the data (e.g. control is shared among one or several independent entities), while distribution (c) refers to differences on the data location (localization), as highlighted below and illustrated in Figure 4.

(a) ***Centralized***: A single central authority (**CA**) and point of data collection, having full control over participants of the network, ability to add or remove them and manage those who can join the consensus process;

(b) ***Decentralized***: control is shared among several independent entities, and the work that maintains the Blockchain integrity is shared among each peer participant in the network, thus, not going through any central authority or server;

(c) ***Distributed***: Each member in the network stores an identical copy of the Blockchain and contributes to the collective process of validating and certifying digital transactions for the network (LINN; KOO, 2016).

Figure 4 – Data localization principles.



Source: Elaborated by the author.

2.2.2 Consensus protocols

Consensus is a fundamental problem in distributed systems that require two or more agents to mutually agree on a given value needed for computational purposes. Some of these agents may be unreliable, and therefore the consensus process needs to be reliant. Blockchains can use various consensus algorithms as per example: Proof-of-Work (PoW), Proof-of-stake (PoS), Byzantine Fault Tolerance (BFT), among others (NOVO, 2018).

In the IoT scenario, it could be useful to take into consideration less computationally-expensive alternatives to Proof of work (PoW), which implementation behaves as a cryptographic puzzle for which the difficulty is proportional to the total computing power of the network (MANNARO et al., 2018). In fact, it requires very high computational

power, and so IoT devices with limited capabilities would not be able to add blocks in the Blockchain (CONOSCENTI; VETRO; De Martin, 2016). Thus it is one of the main reasons why IoT devices are not connected directly to the Blockchain as network members and collaborators.

Blockchain's ability to create/store/transfer digital assets in a distributed, decentralized and tamper-proof way is of a large practical value for IoT systems (SAMANIEGO; DETERS, 2017). More benefits and aggregated values that Blockchain technology can bring to IoT (DORRI et al., 2017):

2.2.3 Access Control

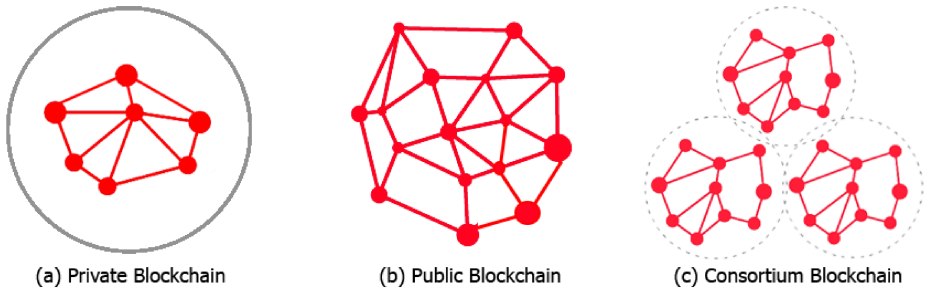
Current Blockchain access control policies can be divided into three types which are described below and respectively illustrated in Figure 5:

(a) ***Private Blockchain***: Nodes will be restricted, not everyone can participate in this Blockchain, has strict authority management on data access;

(b) ***Public Blockchain***: Everyone can participate in the distributed network, check data transactions and verify it, and can also participate the process of getting consensus;

(c) ***Consortium Blockchains***: It means the node that has authority may be chosen in advance, usually has partnerships, such as business to business. The data in Blockchain can be open or private and considered as a partly decentralized network.

Figure 5 – Blockchain's access control configurations.



Source: Elaborated by the author.

Regarding the infrastructure costs of these three different access control configurations, it may vary, for example, private Blockchains usually imposes no interaction costs to its users (e.g., transaction fees) while public Blockchain tends to not be free of charge. However, the convenience provided by a public Blockchain may justify the cost of usage versus the costs of licensing, running, and maintaining a private clinical data exchange infrastructure (ZHANG et al., 2018).

2.2.4 Smart Contracts

Another key feature of the Blockchain architecture is smart contracts. A smart contract is a software program that executes programs in a Blockchain, it can read other contracts, make decisions, and execute other contracts (NIRANJANAMURTHY; NITHYA; JAGANNATHA, 2018). Smart contract can be used to store digital assets into Blockchain and claim the ownership of the asset. The asset is managed by the smart contract which is executed automatically by the program code.

The smart contract code defines the rules and conditions to manage and trigger the action of the asset ownership (SHAE; TSAI, 2017). Providing the ability to directly track and execute complex agreements between parties without human interaction (NOVO, 2018).

When applied in healthcare, we believe smart contracts could help to create intelligent representations of existing medical records that are stored within individual nodes on the network through metadata about the record ownership, permissions and data integrity.

2.2.5 Blockchain and Health Records (EHR / PHR)

Blockchain technologies are a promising means to address the barriers with distributed PHRs by forming a unified view of patient's personal health records. Its technology has been researched and implemented in various domains, initially in the financial domain with virtual currencies (cryptocurrency) and more recently in the health domain (ROEHRS et al., 2019).

Health records are critical and highly sensitive private information for diagnosis and treatment in healthcare, frequently distributed and shared among multiple organizations, such as healthcare providers, insurance companies, among others. Currently, most of these organizations store patient data as Electronic Health Records (EHR) and Personal Health Records (PHR) which are both digital format structure representation of a patient's health data, that are created and maintained throughout their life (HONGWEI; XINHUI; SANYANG, 2004), and their main difference is that unlike EHR that often is managed and maintained by practitioners (Nurses/Physicians), the PHR is managed by the patient.

The process of collecting vital signs in hospital wards varies, and different approaches are used worldwide. In some cases, data is only manually collected, and stored in spreadsheets that are discarded after the patient is discharged (COSTA et al., 2018). Thus, to overcome these old fashion approaches, the Blockchain technology may provide a new model for health information exchanges (**HIE**) by making health records management more efficient and secure (RABAH; RESEARCH; KENYA, 2017).

2.3 Fog Computing

The fog computing may have an important role in the healthcare field, recent studies point out benefits of adopting it on organization's internal infrastructure, and these benefits could be extended to patients on clinics and hospitals for example. In this section, concepts of fog computing are going to be detailed and explained aspects where it could make the difference.

2.3.1 Defining the Fog Computing

The term Fog computing was initially coined by industry as a metaphor for the main architectural idea behind it, where fog is somewhere between the cloud (data centers) and the ground, where devices are located (KRAEMER et al., 2017).

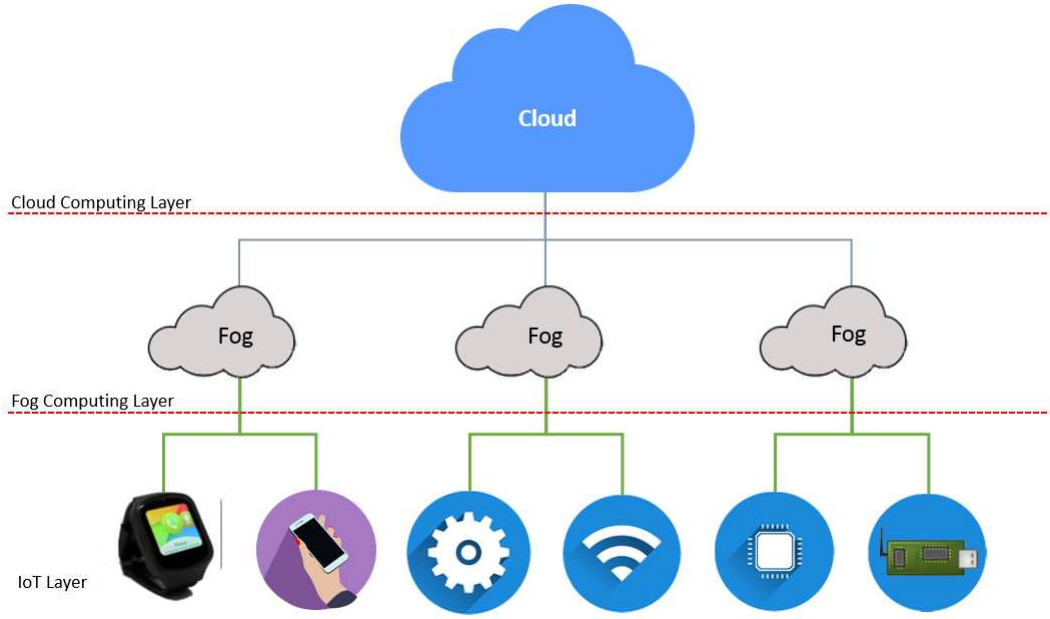
An accepted Fog computing (**Fog**) definition is that it consists of a geographically distributed computing architecture with a resource pool of one or more ubiquitous connected heterogeneous devices on the edge of a network. These resources may elastically provide computing power, communication, storage or other services. For example, the processing or storage of collected data via network-capable devices closer to the end customer (at the edge of the network) without it being transferred directly into a cloud environment. (KELLER; KESSLER, 2018).

From the core to the edge of the network, fog computing may be viewed as a layered service structure that is an extension of the cloud computing paradigm. It will be able to provide faster cloud services such as storage, computing, and networking capabilities to end users, with each fog node located near the IoT devices at the edge of the IoT network (SHARMA; CHEN; PARK, 2018).

Fog computing architecture and infrastructure may aid IoT applications with the inclusion of a new supporting layer between IoT devices and back-end services, potentially facilitating their integration (REYNA et al., 2018). It has emerged as an alternative to cloud, bringing computing and storage capabilities **physically** closer to applications and data sources and consequently mitigating **latency**. Preventing unavailabilities and delays on healthcare applications is of the most importance, otherwise, they can hamper the diagnosis and the physicians' decisions, therefore resulting in greater complications to the patients' health. (SILVA et al., 2019). Delays and unavailabilities that, if prevented, may assist health organizations to improve their services and, ultimately, benefit their patients.

In Figure 6, it is illustrated a common fog computing application example, where it serves as a middleware layer between IoT devices and Back-end services such as Cloud services and others. Moreover, it is possible to observe its better proximity to the edge devices such as IoT sensors and wearable, thus, enabling local processing and storage of collected data.

Figure 6 – Local Fog layer representing its extension of the cloud.



Source: Elaborated by the author.

2.3.2 Fog Computing Applied to Health

Health systems face enormous challenges in many countries, that will increase due to the aging population and the increase in chronic diseases. Many countries also face a growing shortage of nursing staff. At the same time, there is a demand to reduce costs by maintaining high-quality patient care, but many hospital resources are still wasted by manually measuring biometric parameters and transferring data between systems, often involving pen and paper.

To bridge these existing gaps in health informatics exists the Fog computing approach. An architectural style for distributed systems in which application-specific logic resides not only in data centers (Cloud), but also in the infrastructure components between them (KRAEMER et al., 2017).

Healthcare applications relying on Cloud computing may suffer delays that are intolerable for medical applications, and so, the Fog computing may be used in the development of more efficient technological solutions for the health field (SILVA et al., 2019), and reducing the amount of times a system access the cloud.

Authors (SILVA et al., 2019) comment on current lack of studies on health data management approach with Fog, stating that there is no proposed solution to use it as an infrastructure to provide more efficient storage repositories and that in fact, most studies address solutions that exploit the capacity of Fog processing power. In addition, they conducted tests to evaluate potential impact of Fog computing on health applications, and these tests revealed that the use of Fog computing positively favors performance.

3 RELATED WORK

This chapter aims to present studies and work from different authors, related to our proposed thematic and model, taking into account private, academic and governmental researches.

3.1 Research Questions

According to authors Petticrew and Roberts (PETTICREW; ROBERTS, 2008) and Kitchenham and Charters (KITCHENHAM et al., 2010), the definition of research questions is the most important part of any systematic review. Therefore, we seek to identify and classify the technologies related to Blockchain, IoT and health records (**PHR / EHR / EMR**). In this sense, specific and general research questions were formulated to address subjects related to features, problems, challenges, and solutions that are currently being considered, and the research opportunities that exist or are emerging.

General research questions have been refined into more specific questions for better classification and subject analysis, as well as to pinpoint promising research directions for further investigation. Our research questions are classified into two categories: general question (GQ) and specific question (SQ) as follows:

- GQ1: What is the taxonomy for PHRs in a Blockchain?
- GQ2: What are the challenges and open questions related to health records in a Blockchain?
- SQ1: What are the important principles behind Blockchain when it is applied to healthcare?
- SQ2: What are the healthcare protocols and standards that should apply in a Blockchain network?
- SQ3: What are the types, models and or approaches of a Blockchain architecture?
- SQ4: How can Blockchain indefinitely store the "ever-growing" patient health records?

3.2 Research Methodology

Gathering related work articles process is conducted through a Systematic Literature Review (SLR) methodology. A systematic literature review (often referred to as a systematic review) is a means of identifying, evaluating and interpreting all available research relevant to a research question, topic area, or phenomenon of interest (KITCHENHAM et al., 2010). Most research starts with a literature review of some sort. However, unless

a literature review is thorough and fair, it is of little scientific value. This is the main rationale for undertaking systematic reviews. A systematic review synthesizes existing work in a manner that is fair and seen to be fair (KITCHENHAM et al., 2010).

3.2.1 Study Design

This section focuses on enlightening the adopted research methodology, presenting procedures and outlining the main subsequent decisions through a systematic literature review designed to provide an overview of studies and possible related works regarding the integration between Blockchain and Internet of Things technologies in the Healthcare research area, also establishing whether research evidence exists on this topic, and provide qualitative evidence on this matter.

More reasons for the Systematic literature review approach adoption is the goal to group and synthesize available academic contents of the subject theme and identify its challenges, limitations and promising directions. And for that, SLR is recognized by its empirical guidelines, which were followed and carried out by defining and executing the following activities which are SLR protocol and steps described in (KITCHENHAM, 2012) (QIU et al., 2014):

1. **Research questions**: introduce the research questions to be investigated;
2. **Search strategy**: outline the strategy and libraries explored to collect data;
3. **Article selection**: explain the criteria for selecting the studies;
4. **Distribution of studies**: present how studies are distributed chronologically;
5. **Quality assessment**: describe the quality assessment of the selected studies;
6. **Data extraction**: compare the selected studies and research questions.

3.2.2 Search Strategy

As our first step on SLR, aiming to answer our Research Questions in a way that it could be later reproducible, a proper search strategy is defined and conducted, and for that, it is necessary to define a scope and search keywords underlying key concepts of our research questions in order to retrieve accurate results.

When building an optimal Search String, authors Kitchenham and Charters (KITCHENHAM et al., 2010) suggest breaking down the research question into individual facets as research units, where their synonyms, acronyms, abbreviations, and alternative spellings are all included and combined by Boolean operators (KITCHENHAM et al., 2010). In addition, Petticrew and Roberts (PETTICREW; ROBERTS, 2008) propose the PICOC

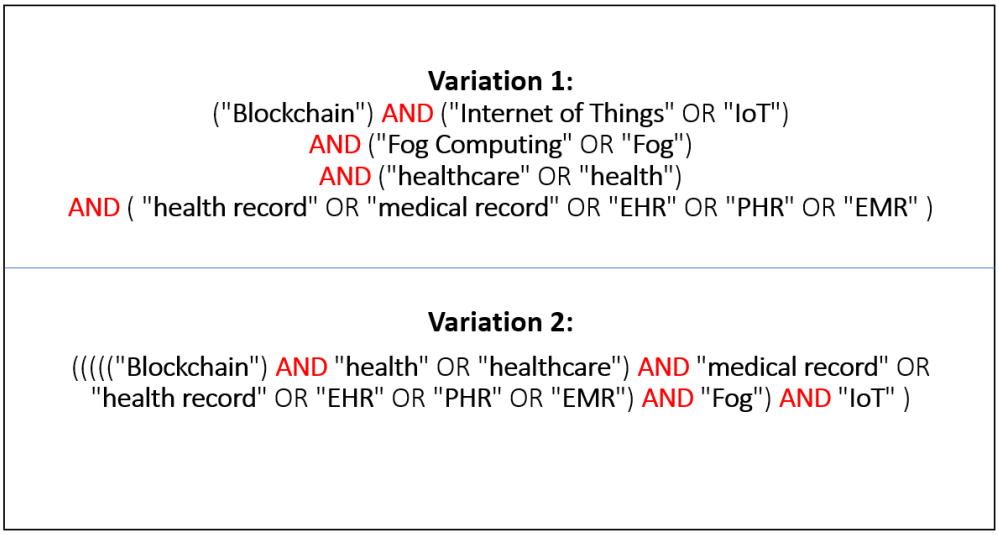
(population, intervention, comparison, outcome, and context) criteria, which is a method used to describe these five elements of a searchable question and serve as guidelines to properly define such research units.

The final search string is derived from these three steps:

1. Identification of synonyms, acronyms, and related words;
2. Identification of terms and related words in abstracts of the articles found from the first research;
3. Construction of the search string using Boolean characters such as OR and AND operators;

Finally, we came up with two variations of the same search string, in order to handle query language differences between electronic databases, since they can differ in parsing and syntax rules:

Figure 7 – Proposed search string keywords.



Source: Elaborated by the author.

3.2.3 Article Selection

Articles selection was carried out through exclusion processes, where articles which do not completely address the research questions were removed with the purpose of working with a corpus that matches the proposition of this work. To apply the exclusion criteria, we used the terms of population and intervention criteria as follows:

- **Exclusion criterion 1**: removal of articles that does not address "Blockchain" or related acronyms.

- **Exclusion criterion 2**: removal of articles that does not address "Internet of Things" or related acronyms.
- **Exclusion criterion 3**: removal of articles that does not address “healthcare”, “health” or related acronyms.

The steps of the filtering process were executed as follows: (1) Duplicate removal, (2) Exclusion criteria, (3) impurity removal, (4) filtering by title, (5) filtering by abstract, and finally, (6) filtering by full text.

All these filtering steps were created to ensure the quality assessment of the research corpus resulted from the search string and intending to aggregate to this work mainly articles which had been elaborated and ideally reviewed by peer in accordance with good practices and academic rules. Blog posts, magazines and any other kind of results that were not scientific were just ignored and or removed.

Many impurities on the search results were removed, for example, articles correlated to the Bitcoin’s Blockchain, which is a financial ledger, were present in the search results, mainly because of the Blockchain characteristics, and had to be removed since it is out of our Healthcare context.

The title and abstract section of all remaining articles were analyzed and those that did not address our subject were removed. Furthermore, all the remaining studies were grouped, duplicates were removed and finally, a full text review ended up with our final corpus of articles.

3.2.4 Quality Assessment

It is important to assess the quality of the selected studies, with quality criterions intended to verify that the article is relevant (KITCHENHAM et al., 2010). We evaluated the selected articles regarding the purpose of research, contextualization, literature review, related work, methodology, results obtained, and conclusion in accordance with objectives and indication of future studies. To verify all these requirements, the article’s quality was evaluated by submitting the articles to questions to validate that these studies met the quality criteria:

- Does the article clearly show the purpose of the research?
- Does the article describe the literature review, background, or context?
- Does the article present related work?
- Does the article have an architecture proposal or research methodology?
- Does the article have research results?
- Does the article have a conclusion?

3.3 Research Results

In this section, we are eager to report the findings of our research and present the obtained results with conducted steps.

3.3.1 Recruitment Process

To answer each proposed research question, a total of forty-four (44) full articles and scientific studies, related to the research topic, were assessed. This literature reviewing steps are described in the following subsections through information synthesis. As a result, aside from answering the research questions, an updated taxonomy is proposed, a summary about main challenges, issues and open questions, followed by a discussion section.

3.3.2 Conducting the Search Strategy

To cover as many related studies as possible, we selected articles from reliable academic repositories such as IEEE, PMC, Google Scholar, Springer, ACM Digital Library and Science Direct as our main electronic databases for our literature review, which covers relevant journals and conferences within the computer science and healthcare field. To limit our search, we set a filter for year of publication ranging from 2009 to 2019.

The electronic database search with defined keywords in Figure 7 was conducted and included all papers published up until 30 April 2019 on academic repositories aforementioned. These databases index research articles and abstracts from most major academic publishers and repositories worldwide, including both free and subscription sources. Finally, we have opted to exclude patents, citations and selecting articles strictly written in the English language.

3.3.3 Proceeding with Article Selection

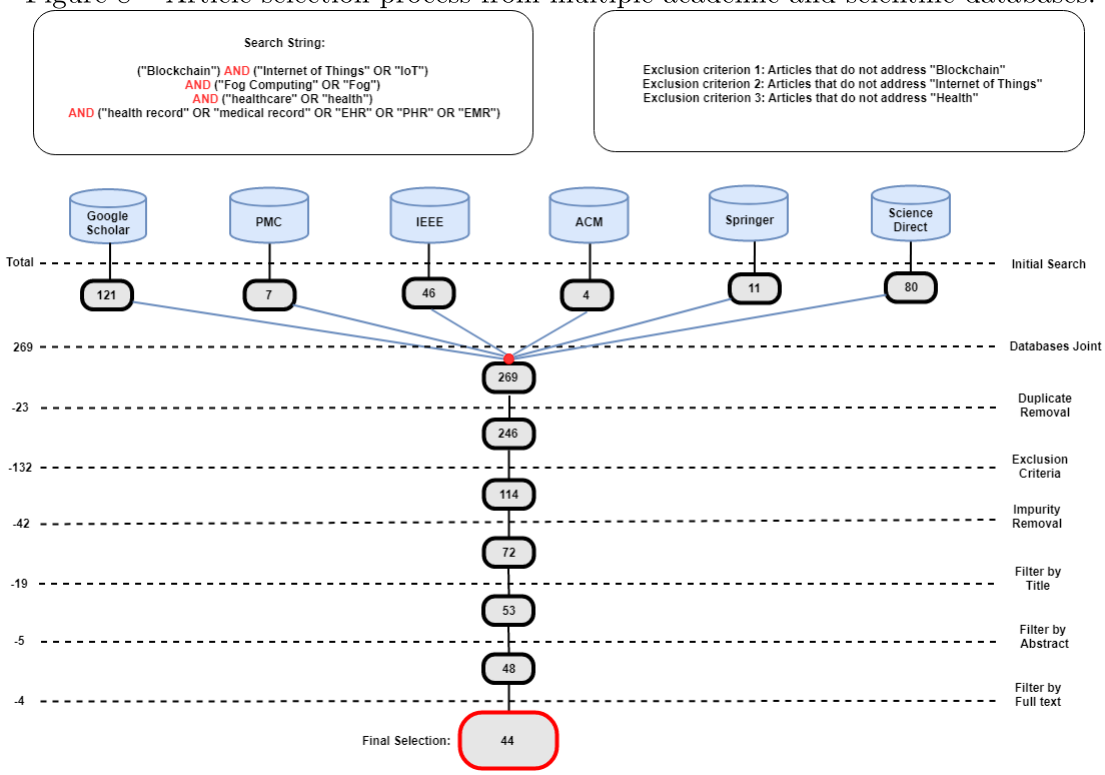
The article selection process is summarized in Figure 8, which illustrates step by step the filtering process. Initially, a total of 269 articles were returned from search string resulting from Databases Joint and before applying our three exclusion criteria proposed in the "Article Selection" at subsection 3.2.3; of these a total of 23/269 (-8.55%) articles were removed due to duplicate removal, where few articles were retrieved repeatedly in more than one database; then a total of 92/246 (-37.39%) articles were removed when applying the first exclusion criterion, which identified articles that did not properly address the Blockchain technology, for example articles where the Blockchain keyword was only mentioned in the author's biography, or that only appears in the reference section.

Continuing with the Exclusion criteria number 2, we identified articles that did not fully address Internet of Things aspects and applications, resulting in the removal of 19/154 (-12.33%) articles and the last Exclusion criteria removed 21/135 (-15.55%) of articles that did not address health or healthcare studies.

Continuing the process, a total of 42/114 (-36.84%) articles were removed because contained impurities, for example articles that were only addressing Bitcoin subject. Then the Filter by Title step removed 19/72 (-26.38%), and last but not least, a total of 5/53 (-9.43%) were removed by the Abstract analysis review, leading us to a total of 48 articles ready for a full text review.

Finally, a total of forty-four (44) full articles were selected as the baseline for this study. Analyzing our final corpus, it was possible to observe that the number of articles has increased in recent years. An overview of all primary studies is presented in Table 1, with the identifier, reference, publication year, publisher, and type, which are sorted by year of publication.

Figure 8 – Article selection process from multiple academic and scientific databases.



Source: Elaborated by the author.

Table 1 – List of selected articles ordered by Year of publication (ascending).

Reference	Authors	Year	Publisher	Type
A01	(LINN; KOO, 2016)	2016	HealthIt	Journal
A02	(HONGWEI; XINHUI; SANYANG, 2004)	2016	IEEE	Conference
A03	(YUE et al., 2016)	2016	Springer	Journal
A05	(NICHOL; BRANDT, 2016)	2016	Researchgate	Journal
A16	(HASHEMI et al., 2016)	2016	IEEE	Conference
A04	(ROEHRS; COSTA; ROSA RIGHI, 2017)	2017	Elsevier	Journal
A07	(YANG; YANG, 2017)	2017	NISK	Conference
A10	(SMITH; DHILLON, 2017)	2017	AMCIS	Conference
A11	(RABAH; RESEARCH; KENYA, 2017)	2017	MRJOURNALS	Journal
A12	(CHENG et al., 2018)	2017	Taylor Francis	Journal
A13	(LIU et al., 2017)	2017	IEEE	Conference
A15	(ICHIKAWA; KASHIYAMA; UENO, 2017)	2017	JMIR	Journal
A19	(KSHETRI, 2017)	2017	Elsevier	Journal
A21	(SHAE; TSAI, 2017)	2017	IEEE	Conference
A23	(KARAFILOSKI; MISHEV, 2017)	2017	IEEE	Conference
A24	(XIA et al., 2017)	2017	IEEE	Journal
A25	(THOMASON, 2017)	2017	GHJ	Journal
A26	(DUBOVITSKAYA et al., 2017)	2017	JAMIA	Journal
A27	(LEMIEUX, 2017)	2017	IEEE	Conference
A29	(PRIISALU; OTTIS, 2017)	2017	Springer	Journal
A35	(KUO; KIM; OHNO-MACHADO, 2017)	2017	JAMIA	Journal
A06	(CYRAN, 2018)	2018	Partners in Digital Health	Journal
A08	(PATEL, 2018)	2018	SAGE	Journal
A09	(DAGHER et al., 2018)	2018	Elsevier	Journal
A14	(RIBITZKY et al., 2018)	2018	Partners in Digital Health	Journal
A17	(ZHANG et al., 2018)	2018	JNCA - Elsevier	Journal
A18	(NIRANJANAMURTHY; NITHYA; JAGANNATHA, 2018)	2018	Springer	Journal
A20	(GUO et al., 2018)	2018	IEEE	Journal
A22	(FAN et al., 2017)	2018	IET Comm	Journal
A28	(MANNARO et al., 2018)	2018	IEEE	Conference
A30	(WANG; SONG, 2018)	2018	Springer	Journal
A31	(KLEINAKI et al., 2018)	2018	Elsevier	Journal
A32	(BANERJEE; LEE; CHOO, 2018)	2018	Elsevier and KeAi	Journal
A33	(GORDON; CATALINI, 2018)	2018	Elsevier	Journal
A34	(GROVER; KAR; DAVIES, 2018)	2018	Elsevier	Journal
A36	(JIANG et al., 2018)	2018	IEEE	Conference
A37	(MAMOSHINA et al., 2018)	2018	Impact Journals	Journal
A38	(ROMAN-BELMONTE; De la Corte-Rodriguez; RODRIGUEZ-MERCHAN, 2018)	2018	MEDKNOW Publications	Journal
A39	(BADR; GOMAA; ABD-ELRAHMAN, 2018)	2018	Elsevier	Journal
A40	(KELLER; KESSLER, 2018)	2018	IEEE	Conference
A41	(RAHMAN et al., 2019)	2019	IEEE	Journal
A42	(SILVA et al., 2019)	2019	Hindawi	Journal
A43	(TULI et al., 2019)	2019	Elsevier	Journal
A44	(SHEN; GUO; YANG, 2019)	2019	MDPI	Journal

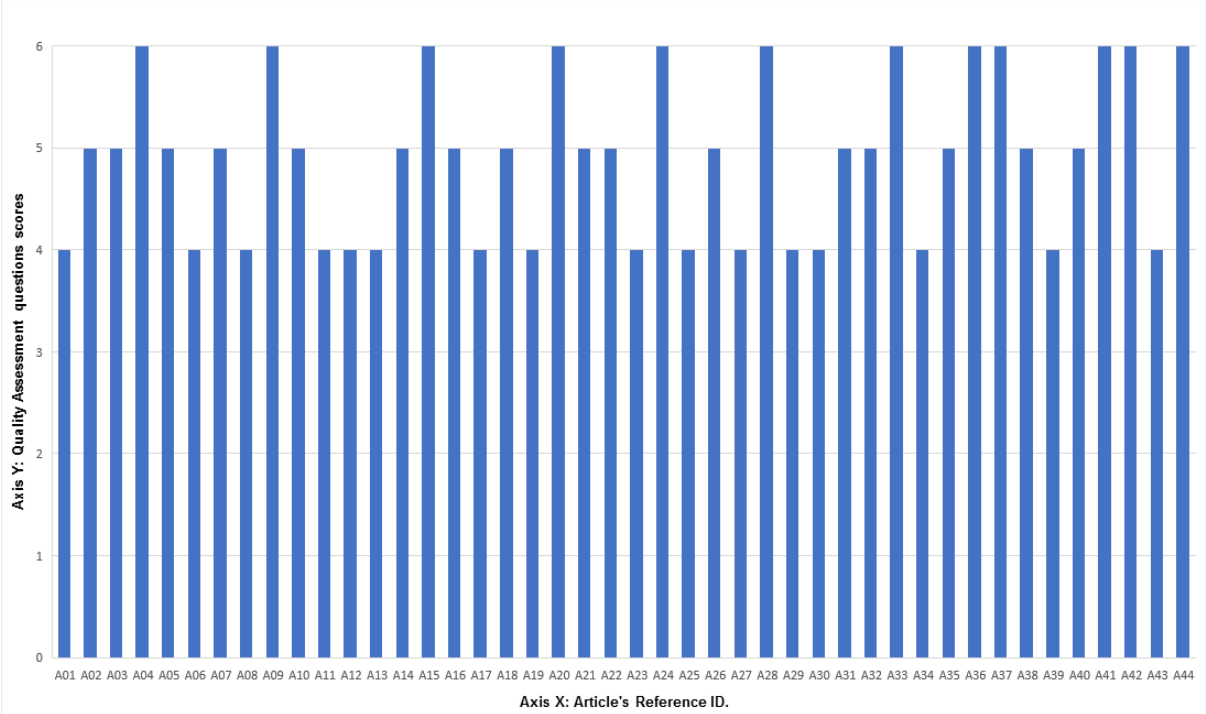
Source: Elaborated by the author.

3.3.4 Performing the Quality Assessment

The proposed quality criteria scores were assessed for each article obtained. Even that most articles did not fully met all the six criteria for evaluation, they responded positively to at least 4 out of 6 quality assessment criteria described in the Section 3.2.4 "Quality Assessment". All the assessed articles clearly presented their research purpose, sustained by a literature review and were somehow supported by a research methodology, bibliographical references, models or architectural proposals. This time the quality assessment evaluation did not exclude articles from the corpus and was conducted to ensure selected articles had a minimum satisfying structure and organization.

Whenever an article responded positively to one of our six quality assessment questions, it scored 1 point, up to a maximum of 6 points, which is illustrated in the histogram chart in Figure 9.

Figure 9 – Quality assessment chart based on criteria defined in section 3.2.4.



Source: Elaborated by the author.

3.3.5 Data Extraction and Answers to the Research Questions

Finally, we discuss and answer in this section the general questions listed in this work.

- **GQ1: What is the taxonomy for PHRs in a Blockchain?**

To ease the understanding and provide a better view of Personal Health Records within Blockchain, we created a taxonomy which is available in Figure 2. The primary purpose of the taxonomy was to create a schema, to categorize and summarize ideas from a corpus, applying organization to clear concepts and build connections.

Under the literature review of selected articles, several current issues were investigated that address health records, Blockchain and IoT. Therefore, this taxonomy is created to answer the first general research question and to gather and organize the various possibilities related to the proposed study. The taxonomy aims to represent and illustrate important EHR and Blockchain's characteristics, also this taxonomy could help to classify, compare, and evaluate different EHR Blockchain types. Moreover, this classification can provide an overview of possible alternatives in terms of aims, content, and techniques.

The proposed taxonomy represents the fundamental characteristics of personal health records in a Blockchain, combining the properties that arise from the intersection of both concepts. We primarily divided the taxonomy in six main characteristics: Governance, Interoperability, Patient Data, Privacy, Scalability, and Security. Each characteristic is further subdivided in specific possibilities for addressing each one of these proprieties in the representation of PHR using Blockchain. The taxonomy uses a "has-a" type of relation among nodes.

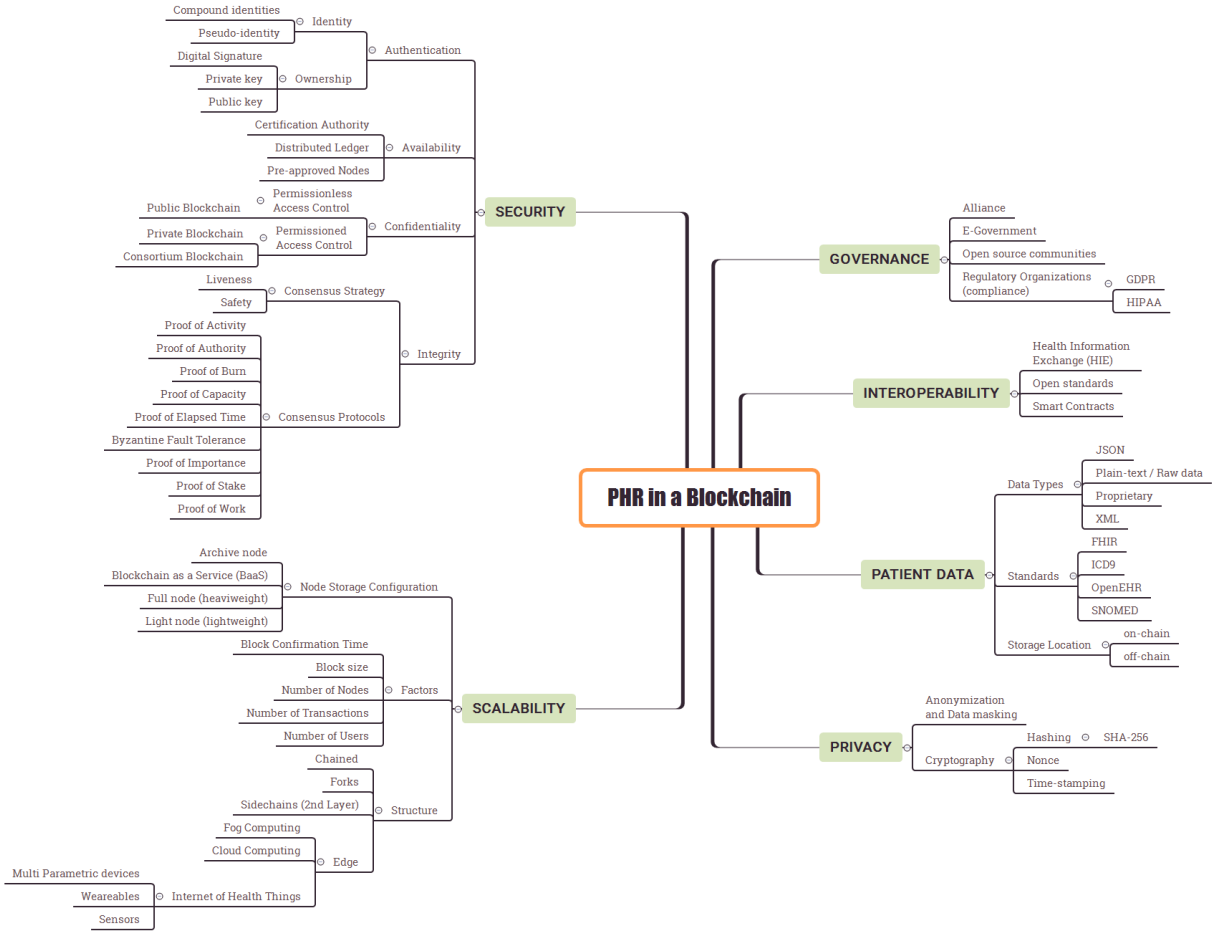
Our taxonomy's aspects and characteristics are mostly self-explaining, however, the Security field is too broad, so we decided to break it down in four criteria as suggested by authors in (BODIN; GORDON; LOEB, 2005):

- **Confidentiality**: Prevent sensitive information from reaching the wrong people, while making sure that the right people can in fact get it;
- **Integrity**: The information is accurate, complete, and consistent, and only authorized individuals may change it;
- **Availability**: The information is available to authorized users when needed;
- **Authentication**: The system makes sure users are who they claim to be.

- **GQ2: What are the challenges and open questions related to health records in a Blockchain?**

To answer this question, we listed and identified challenges, open questions, aspects, issues, and common concerns in the adoption of storing health records in a Blockchain among the analyzed studies. Aspects related to interoperability, privacy, and authorization (access control) are among the major concerns and challenges found in the EHR/PHR Blockchain literature. These aspects and concerns are presented in Table 2.

Figure 10 – PHR in a Blockchain taxonomy, divided in the six main characteristics that arise from the combination of both concepts.



Source: Elaborated by the author.

Interoperability challenges between different provider and hospital systems pose additional barriers to effective data sharing. This lack of coordinated data management and exchange means health records are fragmented, rather than cohesive (HONGWEI; XINHUI; SANYANG, 2004). Many studies have highlighted concerns regarding this data interoperability and heterogeneity, and regarding possible solutions to this concerns some studies have pointed out the adoption of open standards and compliance with Regulatory bodies.

As healthcare data is already distributed across multiple stakeholders, the Blockchain's distributed ledger technology (DLT) infrastructure could be much better than existing centralized systems for accessing, extending and securing the data. Decentralized systems could also streamline costs, reduce time for transactions, and be more efficient than centralized systems due to lower overhead and fewer intermediaries.

Regarding infra-structure costs, private Blockchains usually imposes no interaction costs (e.g., transaction fees) while public Blockchain tends to not be free of charge. How-

Table 2 – Challenges and open questions related to health records into Blockchain.

Challenges	Reference Article
Interoperability: lack of Open Standards; trust between all parties; data integration.	A01, A02, A04, A05, A06, A07, A09, A10, A11, A14, A16, A17, A19, A20, A21, A22, A23, A24, A25, A27, A28, A29, A33, A35, A36, A37, A38, A40, A42, A44
Scalability: limit on the "block size"; storage capacity.	A02, A04, A09, A12, A16, A19, A22, A23, A24, A26, A27, A32, A33, A35, A37, A38, A40, A41, A43, A44
Privacy: patients privacy violations; health records access control (ownership).	A01, A03, A04, A06, A07, A09, A10, A11, A12, A13, A14, A16, A17, A18, A19, A20, A21, A22, A23, A24, A26, A28, A29, A30, A31, A32, A33, A34, A35, A36, A37, A38, A39, A40, A42, A44
Identification: Personally Identifiable Information (PII); global unique identity; authenticity.	A04, A05, A09, A10, A11, A12, A13, A14, A16, A17, A18, A19, A20, A21, A22, A23, A24, A25, A26, A27 A28, A29, A30, A33, A35, A36, A37, A38, A39, A41, A42, A44
Infrastructure Costs: deploying; infrastructure supporting and around Blockchain; power consumption.	A06, A11, A13, A14, A15, A16, A17, A18, A19, A20, A25, A28, A30, A31, A32, A33, A35, A37, A38, A40, A41, A42, A43, A44
User Experience: how patients interact with their health data.	A08, A14, A43

Source: Elaborated by the author.

ever, the convenience provided by a public Blockchain may justify the cost of usage versus the costs of licensing, running, and maintaining a private clinical data exchange infrastructure (ZHANG et al., 2018).

- **SQ1: What are the important principles behind Blockchain when it is applied to healthcare?**

Literature review highlighted important principles regarding Blockchain technology. These principles are listed in the Table 3.

In the Blockchain, all transactions are logged. This register includes information on the date, time, participants, and amount of every single transaction. Each node in the network owns a full copy of the Blockchain and on the basis of cryptographic principles, the transactions are verified by the so-called "miners", who maintain the ledger integrity (HASHEMI et al., 2016). These principles also ensure that these nodes automatically and continuously agree about the current state of the ledger and every transaction in it. If anyone attempts to corrupt a transaction, the nodes will not attain a consensus and hence will refuse to incorporate the transaction in the Blockchain (HASHEMI et al., 2016).

Regarding transparency, historically, the dominant principle for protecting health-related data in the Healthcare field has been to keep the records themselves generally

Table 3 – Blockchain principles in healthcare.

Principles	Reference Article
Immutability: data integrity and authenticity.	A05, A06, A08, A09, A11, A14, A17, A18, A19, A20, A24, A27, A28, A33, A35, A36, A37, A38, A39, A40, A41, A42, A44
Cryptography: privacy; anonymity.	A01, A02, A03, A04, A05, A06, A07, A08, A09, A10, A11, A12, A13, A14, A15, A16, A17, A18, A19, A20, A21, A22, A23, A28, A29, A30, A31, A32, A35, A36, A37, A38, A39, A42, A44
Distribution: across all the peers participating in the network.	A01, A02, A04, A05, A06, A07, A08, A09, A10, A11, A13, A14, A15, A16, A17, A18, A19, A20, A21, A22, A23, A24, A25, A26, A27, A28, A29, A30, A31, A32, A33, A35, A36, A37, A38, A39, A40, A41, A42, A43, A44
Decentralization: network operates on a user-to-user (or peer-to-peer) basis and every full node has a Blockchain full copy.	A01, A02, A03, A04, A05, A06, A07, A08, A09, A10, A11, A13, A14, A15, A16, A17, A18, A20, A21, A22, A23, A24, A25, A26, A27, A28, A29, A30, A35, A36, A37, A38, A40, A41, A42, A43, A44
Transparency: EHR may be open to viewing and yet ensure patient's anonymity (due cryptography).	A01, A02, A05, A06, A07, A09, A11, A13, A14, A15, A16, A18, A19, A20, A21, A22, A23, A25, A26, A27, A28, A29, A30, A33, A35, A37, A38, A40, A41
Auditability: systematic examination of blocks and network aiming to determine whether operation is correct or not (according to the consistency rules).	A02, A04, A07, A17, A18, A23, A24, A31, A32, A33, A35, A37, A38, A40, A44
Non-repudiation: proof of the integrity and origin.	A05, A10, A16, A31, A36, A37, A44

Source: Elaborated by the author.

inaccessible except to those directly involved in a patient's care. The Blockchain privacy model keeps data records widely accessible, but the patients to whom they refer are either secret or anonymized (CYRAN, 2018).

Centrally-stored data has often proved disastrous in our modern age of cyberattacks and data leaks (YUE et al., 2016). Having this health data distributed over the network makes it persistent, mainly because of consensus and the digital record, Blockchain transactions can't catch fire, be misplaced, or become damaged by water (FORREST; MILLER, 2003).

When it comes to Blockchain applications in healthcare, one important characteristic is the immutability which may conflict directly with the privacy rights. For example, in a case where a patient has the right to be forgotten, requiring the deletion of their stored health records from the Blockchain clashes with the immutability goal of the Blockchain-

enabled solution. In these cases, health data can be stored off-chain, and if a patient exercises their right to be forgotten, their personal information stored off-chain could be deleted (RIBITZKY et al., 2018).

- **SQ2: What are the healthcare protocols and standards that should apply in a Blockchain network?**

Healthcare providers may use both open standards and proprietary formats to organize their health records that usually are used by internal applications and encountered in different formats (CHENG et al., 2018). To answer this research question, standards found in the literature review were listed, and are summarized in Table 4 and present a vast number of organizational data patterns for health records.

Table 4 – Healthcare protocols and standards applied in Blockchain.

Protocols and Standards	Reference Article
OpenEHR	A04
HL7 FHIR (Fast Healthcare Interoperability Resources, from Health Level 7): standard describing data formats and elements for exchanging EHR.	A02, A04, A05, A06, A13, A14, A17, A33, A35
HIPAA (Health Insurance Portability and Accountability Act): legislation that provides data privacy and security provisions for safeguarding medical information.	A02, A04, A08, A09, A11, A12, A13, A14, A16, A19, A26, A33, A37
GDPR (General Data Protection Regulation)	A14, A33
IHE (Integrating the Healthcare Enterprise)	A04, A08
ISO (International Organization for Standardization): ISO/IEEE 11073 and ISO 14721	A13, A27
SNOMED (Systematized Nomenclature of Medicine)	A04
DICOM (Digital Imaging and Communications in Medicine)	A04, A08, A13, A29, A33
HIE (Health Information Exchange)	A05, A08, A11, A26, A33, A35, A38, A40
PII (Personally Identifiable Information)	A02, A08, A14, A19, A35, A37

Source: Elaborated by the author.

Electronic Health Records, so far, were not designed to manage multi-institutional, lifetime medical records. Patients leave data scattered across various organizations as life events take them away from one provider's data silo and into another. In doing so, they lose easy access to past data, as the provider, not the patient, generally retains primary stewardship (YUE et al., 2016; GUO et al., 2018). Blockchain architecture may help addressing this problem by supporting the development of interoperability standards and requirements that address privacy and enable secure exchange of data across systems. Open standards play a big role in the health data exchange by providing system flexibility and helping achieve interoperability (YUE et al., 2016).

Countries or regions with different regulations, often have their own healthcare protocols and standards due to national medical regulations (RIBITZKY et al., 2018). The

standards are intended to systematize the patients' clinical datasets and define protocols to make the health information uniform. These are usually dedicated to standardize the storage and to regulate the clinical and demographic data about patients. Health records typically incorporate data regarding vital signs, laboratory exams results, evolution, and diagnosis (CHENG et al., 2018).

Without the adoption of interoperable data standards (such as HL7 FHIR and OpenEHR), clinical data can vary in formats and structures that are hard to interpret and integrate into other systems. Therefore, standards-based architecture is needed to ensure the integration with existing telemedicine systems to enable secure and scalable clinical data sharing for improving collaborative decision support (ZHANG et al., 2018).

Regarding patient's identification on the Blockchain, some authors propose the adoption of a PII (Personally Identifiable Information), also known as UPID (Unique Patient Identifier), which is a standard that assigns an alphanumeric identification code designed to uniquely represent a patient in a hospital. It is used by the Medical Information System (MIS) and other sub-systems, as well as all the paper forms and manual processes related to the patient and may serve as identification of patient inside Blockchain (CHENG et al., 2018).

- **SQ3: What are the types, models and or approaches of a Blockchain architecture?**

Reviewed architectural components often are composed of connected devices, sensors, and a collector that collect data and send to the Blockchain network for storage (NIRANJANAMURTHY; NITHYA; JAGANNATHA, 2018). These data originated from mobile devices and wearable sensors is growing at an exponential rate and architectures based on commodity hardware provide cost efficient high scalability (PETTICREW; ROBERTS, 2008).

Blockchains are currently the most popular form of Distributed Ledger Technology (DLT) being adopted today (RIBITZKY et al., 2018). Blockchain technologies can be divided into three types (ICHIKAWA; KASHIYAMA; UENO, 2017):

- **Public Blockchain**: Everyone can participate in the distributed network, check data transactions and verify it, and can also participate the process of getting consensus;

- **Consortium Blockchains**: It means the node that has authority may be chosen in advance, usually has partnerships, such as business to business. The data in Blockchain can be open or private and considered as a partly decentralized network;

- **Private Blockchain**: Nodes will be restricted, not everyone can participate in this Blockchain, has strict authority management on data access.

Regarding models, there are a set of proposed architectures and models presented in the literature review. Blockchain usually is the central piece of these architectures being responsible for the persistence (storage), authorization and with the assistance of open standards as healthcare interoperability infrastructure enabled, among others. Proposed Blockchain architectures should support storage of medical data, including formal medical records as well as health data from mobile applications and wearable sensors, and would follow an individual user throughout his life. Another advantage of Blockchain's distributed architecture is built-in fault tolerance and disaster recovery (PETTICREW; ROBERTS, 2008).

Blockchain's address generation mechanism for authentication and authorization in the network employs public key cryptography to manage identities in the framework. In public key cryptography, a pair of mathematically related public and private keys are used to create digital signatures and encrypt data. It is computationally infeasible to obtain the private key based on the public key. Public keys can thus be shared freely, allowing users to encrypt content and verify digital signatures. Likewise, private keys are kept secret to ensure only the owners of the private keys can decrypt the content and create digital signatures (ZHANG et al., 2018).

Another key feature of the Blockchain architecture is smart contracts. A smart contract is a software program that executes programs in a Blockchain; it can read other contracts, make decisions, and execute other contracts (NIRANJANAMURTHY; NITHYA; JAGANNATHA, 2018). Smart contract can be used to store digital assets into Blockchain and claim the ownership of the asset. The asset is managed by the smart contract which is executed automatically by the program code. The smart contract code defines the rules and conditions to manage and trigger the action of the asset ownership (SHAE; TSAI, 2017).

When applied in healthcare, smart contracts may create intelligent representations of existing medical records that are stored within individual nodes on the network. Smart contracts may contain metadata about the record ownership, permissions and data integrity.

- **SQ4: Can Blockchain indefinitely store the "ever-growing" patient health records?**

Blockchain directory model supports the ability to grow and change dramatically throughout its lifetime by adding new participants and changing organizational relationships (YUE et al., 2016). Its technology is particularly useful for recording continuous and steady growth of transactions. For the EHR system, there is an upper bound of the number of records, which is the number of citizens it serves. Population growth is relatively slower than the case of monetary transactions, as an example the Bitcoin's Blockchain (CHENG et al., 2018).

Blockchain's chain structure also helps to support the ever-growing medical records, by having a continuously growing linked list of medical records, each block contains a timestamp (which is the current time of an event is recorded) and a link to a previous block (PATEL, 2018). An alternative solution for the ever-growing problem would be Blockchain containing pointers to off-chain data, metadata associated with such pointers can include information required to support interoperability (RIBITZKY et al., 2018; ZHANG et al., 2018; DUBOVITSKAYA et al., 2017). Doing so, heavyweight data, including imaging exams (X-Ray and others), could be stored off-chain (in external servers).

In the context of imaging exams sharing, a few authors proposed storing encrypted health information directly on the Blockchain itself, however, storing the encrypted imaging studies of all patients would result in an enormous Blockchain size, far too large for a node running for example, on a mobile device or even a modern workstation to download, store, and validate. Blockchain size is a problem under active study and has been shown to be a limiting factor even for chains that store simple transactional data, much less the massive blocks that would be required to store medical imaging studies (CYRAN, 2018).

As a Blockchain continues to grow, the scalability of the system may be compromised, because only users with large storage spaces and computational power will be able to partake in the Blockchain as miners or full nodes. To overcome this issue, Blockchain usually supports three different types of nodes: full nodes, light nodes, and archive nodes:

- **Full nodes**: Process every transaction and store every block in the Blockchain (YANG; YANG, 2017);

- **Light nodes**: It is possible to verify transactions without running a full network node. Users only needs to keep a copy of the block headers of the longest proof-of-work chain, which they can get by querying network nodes until obtaining the longest chain (WRIGHT, 2019). By storing the block header, the light node can verify certain transaction have not been altered, without committing large portions of memory to the Blockchain. Light nodes also can access specific data they desire (YANG; YANG, 2017);

- **Archive nodes**: Stores every transaction and block on the Blockchain. Additionally, store transaction receipts and the entire state trie (YANG; YANG, 2017).

The versatility of these three different types of nodes increases the scalability of the Blockchain such that large corporations and individual users are allowed to interact with the Blockchain for their respective purposes and with their available resources (LINN; KOO, 2016).

3.4 Discussion and Comparison

During our research, it was possible to verify that to the present date there are very few studies combining specific technologies in the way we are proposing on our FogChain model for the healthcare domain, and that currently, most healthcare providers are still storing health records on private centralized servers, and in different data formats, which difficult interoperability.

We successfully managed to identify both quantitative and qualitative set of studies that allowed us to obtain a better view of the ecosystem regarding Blockchain, IoT and Fog computing technologies and its architectures when applied to the PHR management and Healthcare context on the last 10 years of publications. Aiming to identify several common aspects of studies to better answering our research questions, we were able to propose a taxonomy classification of the involved technologies and identify open questions to be further researched that represent challenges and issues that have been detected in recent years. In summary, many relevant studies of the field were highlighted according to systematic selection criteria and were incorporated in this work through helping us answering our research questions.

Some Blockchain studies aim to address recordkeeping challenges, such as greater patient control over sensitive health information (LEMIEUX, 2017), and, some of the main findings present in this review are the importance of having EHR/PHR interoperability through the adoption of Blockchain by healthcare providers and the definition of open standards. These might be the key to the improvement of health care services due to health data sharing, availability, and integration. Furthermore, the use of Blockchain technology in clinical trials may enhance the development of drugs and medical devices (ICHIKAWA; KASHIYAMA; UENO, 2017).

EHR is seen as a standardized information model, enabling integration among multiple healthcare providers, and this integration is considered their main advantage. EHR has several benefits, ranging from supporting medical prescriptions, improving disease management and contributing to the reduction of severe medication errors. However, EHR has limitations regarding interoperability, e.g.: when health organizations adopt international but heterogeneous standards (CHENG et al., 2018).

Blockchain applications in healthcare still are in early stages of development and evaluation and these obstacles might eventually be overcome, then opening the path for other possibilities (KARAFILOSKI; MISHEV, 2017), which is in line with our findings in the literature review, and to the best of our knowledge, there are very few studies combining these specific technologies in the way as we are proposing on our FogChain model for the Healthcare field. Given that Blockchain technology conception still very recent, so are its academic studies too, and most healthcare providers are still storing health records on centralized servers, and in different formats, which difficult interoperability. Also, it is

clear the need for more investments and efforts in consolidating open standards, seeking to establish better interoperability levels among providers and patients, which would benefit and ease the Blockchain adoption from healthcare industry.

Overall, we sought to identify articles that would more closely approximate to the architectural model that we aim to propose, which combines technologies such Blockchain, Internet of Things and Fog Computing, in the healthcare field, and ultimately, we created a comparison table to present five of these studies that successfully managed to present an architecture feasible of comparison, where main similarities and differences are available and highlighted in Table 5 and a brief description with the highlight points of each related work:

- **Multi-tier**: Multiple layers Blockchain framework for EHRs systems using Elliptic Curve Cryptography (ECC), which may introduces more security strength compared to other cryptography approaches, however, on this Multi-tier design the health records are not available locally, close to the edge.

- **Label-chain**: a consortium parties which together form the platform network for physical traceability, separation from the physical and financial flow of goods. It recommends the fog computing adoption, however, it seems to not be available in their final version, meaning that even if Label-chain could be adapted for the healthcare domain it still would not provide the health records locally.

- **MEC-tier**: Leverages a Blockchain and off-chain framework to store IoT raw data related to sharing economy services, for example e-Health, with the support of A.I. and fog computing infrastructures. Their choice for the Blockchain framework was Ethereum which charges each running transaction with an internal pricing fee (Gas), which may be a limitation depending on the target audience.

- **FogNode**: Designed to enable the management of medical records, it describes a case study that evaluates the performance, privacy, and interoperability requirements of the proposed architecture in a home-centered healthcare scenario with fog computing support. In comparison with the FogChain, one of the main differences is that our model focuses on the patient level of control over IoHT collected data and not limiting to home care but also clinics and hospitals where our model is designed to support Physicians users in the network.

- **FogBus**: Framework to integrate different IoT-enabled systems to both Fog and Cloud infrastructures into a computing environment where it integrates finger pulse oximeters as IoT devices with Smartphone-based gateway and Raspberry Pi-based Fog nodes for Sleep Apnea analysis.

- **MedChain**: MedChain focus on developing a decentralized framework to attain more scalability without trusting a third party, however it still needs healthcare

providers to manually upload the information of data streams to the Blockchain service and the directory, which is one of the limitations to be handled in the FogChain proposal.

Table 5 – Related work comparison.

Author	**Name**	**Platform**	**Applications**	**Patient-centered**	**Records available locally**
(BADR; GOMAA; ABDELRAHMAN, 2018)	Multi-tier	Ethereum	Healthcare	No	No
(KELLER; KESSLER, 2018)	Label-chain	Hyperledger	Cross-industry	No	No
(RAHMAN et al., 2019)	MEC-tier	Ethereum	Cross-industry	No	No
(SILVA et al., 2019)	FogNode	Ethereum	Healthcare	No	No
(TULI et al., 2019)	FogBus	DHT	Cross-industry	No	No
(SHEN; GUO; YANG, 2019)	MedChain	DHT	Healthcare	No	No
-	FogChain	Hyperledger	Healthcare	Yes	Yes

Source: Elaborated by the author.

3.4.1 Research gaps

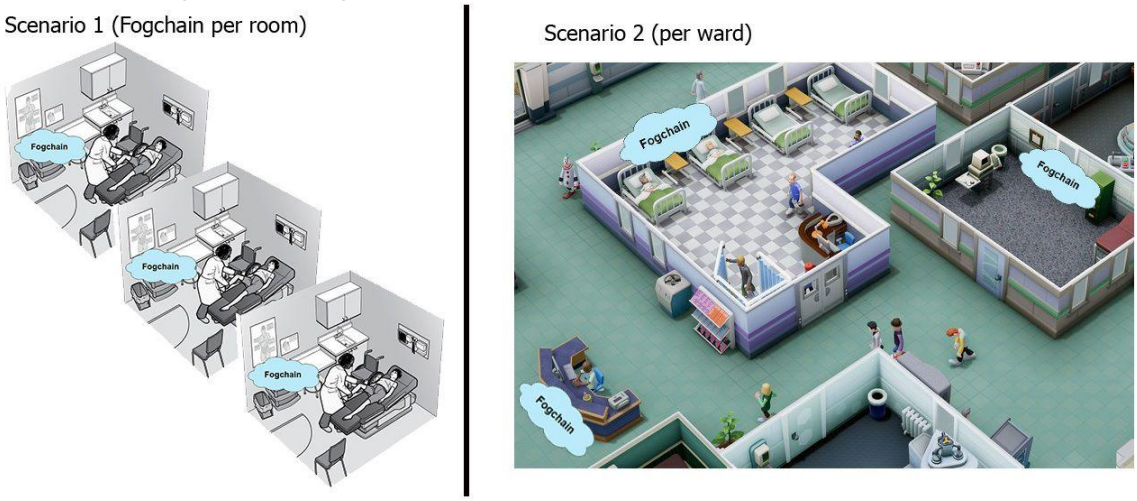
During our research, several authors highlighted the healthcare domain needs and the importance of having safer mechanisms when dealing with medical records. The possibility of having such sensitive data as health records, stored locally through fog computing and Blockchain seemed only natural to fill this literature gap and thus, to be employed in our model, not only to position it as an alternative to the traditional cloud-like architectures but also to take advantage of various benefits of this combination of technologies that are so required by the healthcare domain, for example, reduce dependence on external services, provide local processing power near edge, no single point of failure, and yet empowering patient's experience while retaining application's performance by mitigating latency and supporting multiple nodes.

4 FOGCHAIN MODEL

Traditional cloud-hosted IoT and IoHT applications often struggle with significant latency issues caused by Internet network congestion and traffic (CYRAN, 2018). Our proposition is to evaluate whether the use of Fog computing as a middleware layer between sensor devices and the Blockchain could better suit the IoHT needs.

Our architecture aims to enable real-time data processing, storage, and decision making given by the *smart contracts* feature. Whenever dealing with critical and or sensitive information, the response time is crucial and must be taken into account. Our approach of approximating the Blockchain peer to the IoHT devices through hosting itself a peer inside of the Fog attempts to reduce the physical distance gap between system elements.

Figure 11 – FogChain's healthcare application scenarios example.



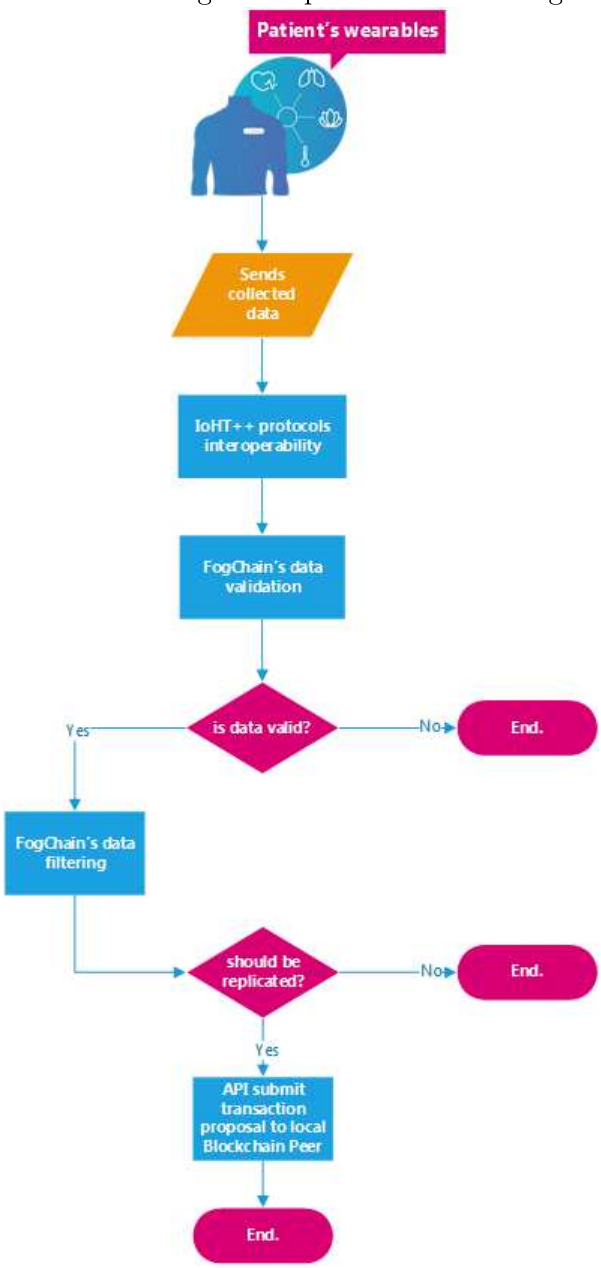
Source: Elaborated by the author.

Application scenarios where real-time features may actually make a difference are, for example, inside a hospital, where seconds matters and multi-parametric sensors and wearables are collecting vast quantities of data from patients, such as vital signs readings to support physicians in decision making; however, these data points are often sent to the hospital's cloud server, which basically depends on Internet service provider (ISP) and which one day may stop responding. Precisely at this point is where FogChain with its Fog computing paradigms may be a handful. FogChain could essentially run in healthcare organizations such as hospital floors and wards, handling their internal demand. Also, it could be possible to have a FogChain inside each patient room, handling patient's sensors and environment information collected from devices in rooms. These possible scenarios are illustrated in Figure 11.

In summary, we are proposing a model that aims at managing patients' health records through the employment of Fog computing architecture and paradigm. In our proposed

model, Fog, Blockchain, and IoHT are combined to better provide the requirements based on challenges and opportunities identified in the previous chapter of research and literature review. Thus, Fog computing-based techniques were used to ensure high availability and performance, and Blockchain-based strategies were used to provide the privacy and tamper-proof required in the healthcare domain. Additionally, the architecture is designed in a way where the entire process is transparent for the patient, from the collection of vital signs until its storage in the Blockchain, without need for human intervention. The flowchart at Figure 12, does illustrate the end-to-end process and requests life-cycle.

Figure 12 – Flowchart describing the request flow in the FogChain architecture.



Source: Elaborated by the author.

4.1 Project Decisions

To provide an overview of the FogChain model, we present four definitions that are essential for this work:

1. Propose and build a feasible solution for the healthcare domain, possibly contributing to future research and implementations;
2. Application of fog computing architecture to improve Blockchain and IoHT integration, checking for possible reduction of network latency and increasing availability of resources near the edge;
3. Focus on personal health records (PHR) to increase patient control over its medical data;
4. Preference for adoption of open-source projects and structures on the application's development.

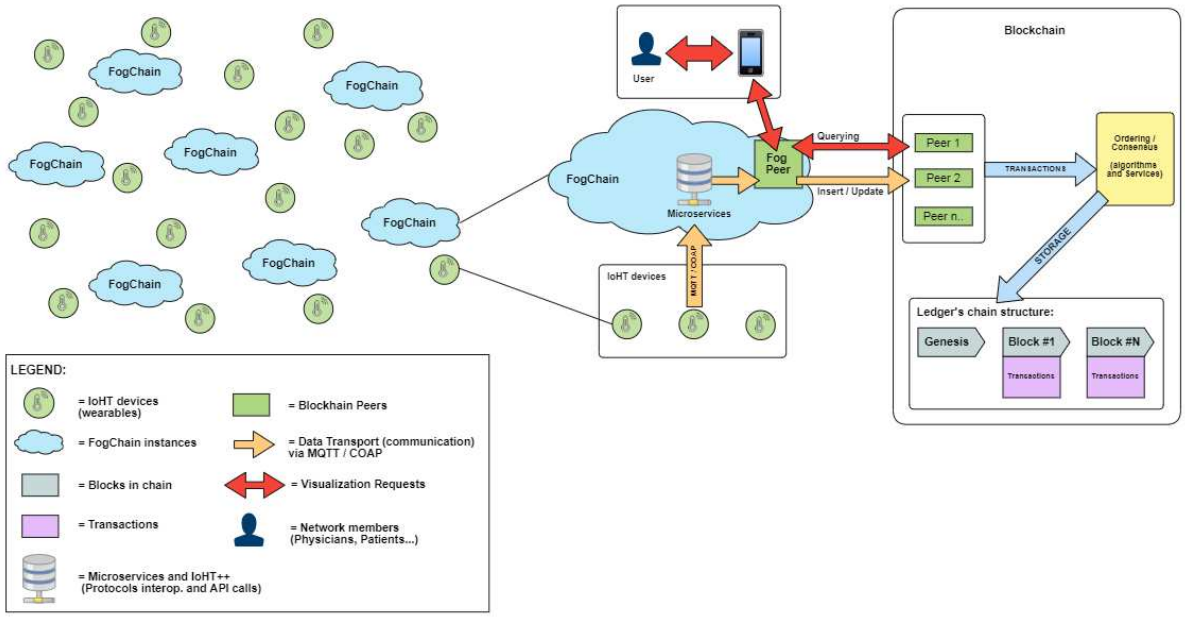
We focused the conception of this model on designing a Blockchain-enabled solution for safer personal health records storage, supported by the fog computing architecture providing performance boost for the application, improving the health things capabilities and ultimately the patient's experience. Hence, it is safe to say that we focused the scope of this project entirely on medical informatics field. However, we understand that the model, as it is today, could be used in different domains, as long as some adaptation is made in the Blockchain data structure.

4.2 Architecture

The FogChain, as the name suggests, is the union of Fog computing and Blockchain technologies. It means we aim to run both in the same container at a Fog computing level. It aims at managing patients' health records through the employment of Fog computing architecture and paradigms, where a local Fog layer combined with Blockchain and IoHT technologies may suit the requirements identified in the previous steps of research and literature review. Thus, Fog computing-based techniques were used to ensure high availability and performance, and Blockchain-based strategies were used to provide the privacy and tamper-proof required in the healthcare domain.

In the FogChain architecture, the first interaction with the Health Things layer (IoHT devices) is given through an internal component named IoHT++, which is responsible for exchanging messages and communicating with these IoHT devices, providing some level of protocol interoperability by supporting various protocols and standards, as illustrated in Figure 13 where it can be visualized multiple FogChain's instances attending edge devices closer to it.

Figure 13 – FogChain's architecture macro visualization.



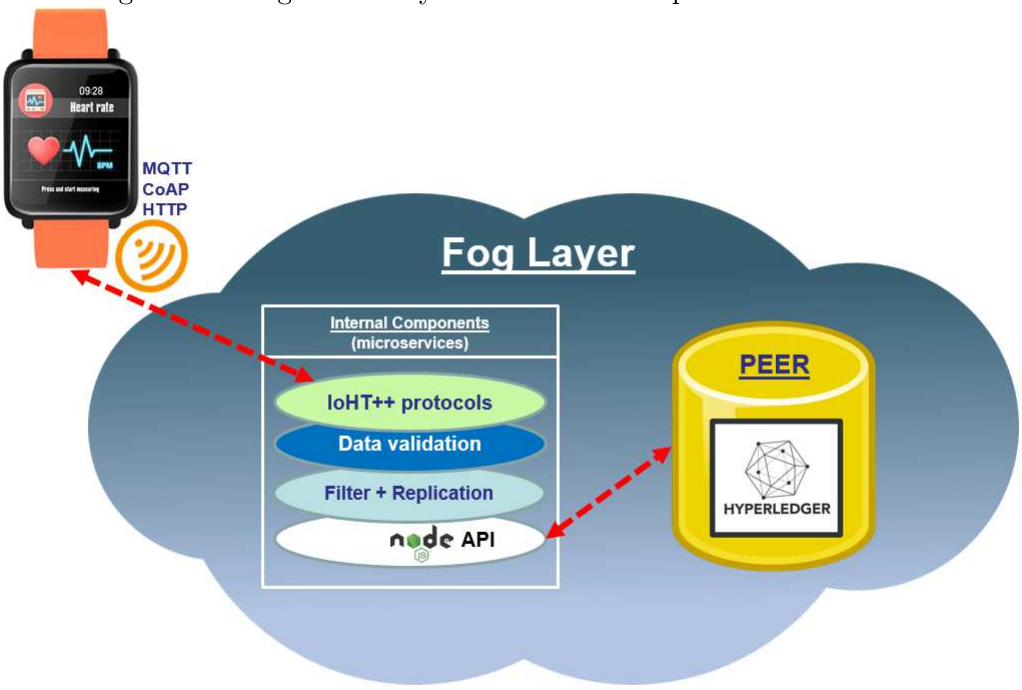
Source: Elaborated by the author.

Whenever a new message arrives, its data is **validated** in order to prevent, for example, blank, null, and/or corrupted information from being sent to the Blockchain peer in the following steps. Moreover, a **filtering** function is applied, where it is possible to determine which information we want to store or discard in the distributed ledger, for example, if a wearable device is collecting multi-parametric values. This filtering function allows us to decide which parameters are important and should be broadcasted to all peers of the Blockchain.

4.3 Components

The FogChain architecture is divided into layers, being each responsible for a part of the process, beginning with the collecting of vital signs until the storage in Blockchain. A layered visualization of the proposed architecture is illustrated in Figure 14, and it can be divided into four different main components:

Figure 14 – FogChain's layered view and components distribution.



Source: Elaborated by the author.

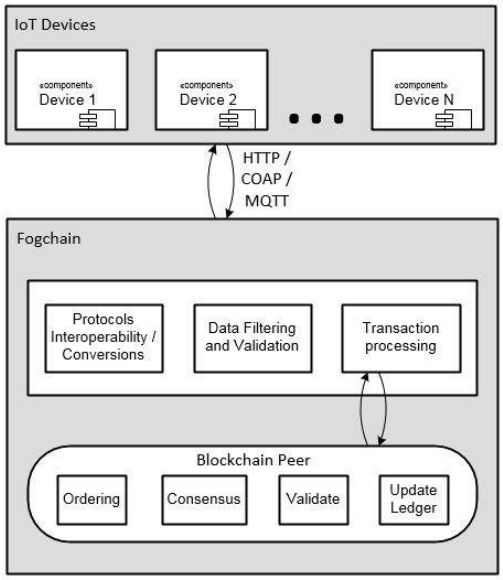
4.3.1 IoHT devices (Health Things):

The points of contact with the physical world (CHRISTIDIS; DEVETSIKIOTIS, 2016). Devices belonging to a wireless sensor network are often limited in terms of computing capacity, storage, memory, and energy availability (NOVO, 2018), and for this reason, the data is usually not stored in the devices themselves, but instead sent to the Fog layer. Once there, the middleware handles communication protocols known as the Health Things, including **CoAP** (Constrained Application Protocol), **MQTT** (Message Queuing Telemetry Transport), and **HTTP** (Hypertext Transfer Protocol).

4.3.2 Fog Layer:

Located between the edge devices (Things) and the Blockchain services. It comprises a solution based on Fog computing, where its technology is used for scaling solutions for cloud computing, being able to provide storage and computation close to the end-user and edge devices (MOKHTARI; ANVARI-MOGHADDAM; ZHANG, 2019). Also, FogChain has mechanisms to provide further communication and interoperability capabilities for devices. FogChain is responsible for dealing with communication protocols, filtering and validating data collected, and finally, transacting with the Blockchain network through an API, which is better illustrated in Figure 15.

Figure 15 – FogChain's internal view structure and components.



Source: Elaborated by the author.

The Fog layer can be described as a middleware component providing **microservices** responsible for handling, filtering, and validating incoming data from edge devices, prior to process requests to be persisted in the Blockchain ledger. It also has internal features that can be described as a message broker with general pub/sub capabilities. Dividing messages into topics (categories of messages) and allows for multiple interested clients to both produce and consume messages from topics. Beyond usual HTTP [1], it also accepts MQTT [2] and CoAP [3] communication protocols in order to exchange information with IoHT devices. Each Fog layer hosts a peer of the Blockchain, so it has stored on it a full chain copy (Ledger) as close as possible to the edge's border.

A feature to be available in each Fog layer instance is the communication protocols interoperability support, from the IoHT++ subcomponent (RIGHI et al., 2018). It has two main internal components: **middleware core** and **I/O boundaries**. The first can be described as a message broker with general pub/sub capabilities. It divides messages into topics (categories of messages) and allows for multiple interested clients to both produce and consume messages from these topics. Its implementation uses the *Apache Kafka*[4] software platform, which is a distributed publish-subscribe messaging framework made available by the *Apache Software Foundation* [5].

This Fog layer's sub-component (IoHT++), can either translate incoming client communication semantics into messages that are produced in the middleware core or consume

[1] https://tools.ietf.org/html/rfc2616
[2] http://mqtt.org/
[3] https://tools.ietf.org/html/rfc7252
[4] https://kafka.apache.org
[5] https://www.apache.org

messages from the core, communicating them to the clients. These boundaries are configured and executed in separate processes and were implemented by the original authors as services using the *Clojure* [6] programming language, all of them running on top of the Java Virtual Machine (**JVM**): MQTT subscriber, MQTT publisher, CoAP server, CoAP client, and HTTP client.

The IoHT environment is usually heterogeneous, which means that devices may communicate in different protocols and channels. So while having some level of protocol interoperability is really great, it may as a small downside minimally affect performance. A benchmark presented by the authors in Table 6 displays its results (RIGHI et al., 2018).

Table 6 – Throughput benchmark results.

MQTT - MQTT	CoAP - HTTP	HTTP - CoAP	MQTT - CoAP	MQTT - HTTP
53.51 msg/s	6.4 msg/s	35.08 msg/s	0.14 msg/s	49.89 msg/s

Source: (RIGHI et al., 2018)

It is precisely at the Fog layer level where we are going to have most of our microservices running at a fog computing level close to the edge, as illustrated in Figure 14, it acts not only as an entry-point, handling the interoperability of the IoHT protocol but also executing many essential steps such as **data validation** and the **filtering** step, where we are able to choose whether a collected information should be replicated to the local and following Blockchain peers, or if it is to be discarded, as described:

- **Validation step**: The data validation step is one of the Fog's layer sub-process, where we employ data cleaning to ensure the quality of the information before sending it to Blockchain. It is executed through routines where we enforce validation rules to it, and in cases it fails, e.g. malformed data and or blank/null the data is aborted;

- **Filtering step**: While data flows on our microservices, before it is sent to be persisted on the Blockchain ledger, it does necessarily passes through the filtering step, where parameterized business rules may be applied, e.g., deciding whether data should be accumulated in batches before sending to the Blockchain, or for example, in a health provider that is hosting a FogChain instance, where their specialty is cardiovascular diseases, it may not be of their interest that a patient's wearable sends information regarding glucose, this way enabling some level of governance for local peer owners.

Whenever incoming data succeeds in these steps, it is then finally prepared to be sent to the Blockchain network as a transaction proposal, through our API's which interfaces with our network.

[6] https://clojure.org

4.3.3 Blockchain:

The Blockchain technology is a key component in our model, and is responsible for safely storing clinical data collected by the IoHT devices, such as vital signs and exams. In terms of data structure, the Blockchain can be configured to support the storage in a way where existing data formats and open standards are applied, such as FHIR, OpenEHR, among others already established in the health sector (ROEHRS; COSTA; ROSA RIGHI, 2017).

Considering the volume of patient medical data can grow indefinitely, which may scale along with a large amount of collected data for each patient, an alternative solution might be storing fragments and parts of medical data in an off-chain way, through the use of pointers (links) to external directories such as an IPFS solution.

The IoHT devices' hardware is usually too restricted to actively contribute to the Blockchain network since consensus algorithms are complex and require large processing capacity and CPU storage capacity. To overcome these limitations, the FogChain model proposes adding a Blockchain peer inside the Fog instances, where ideally hardware tends to be more robust. Each FogChain peer would have a copy of the ledger and could actively contribute to the network through helping to achieve consensus among existing peers. To ensure that, the peers have a sequential workflow process:

1. **Transaction Proposal**: Applications generate a transaction proposal which they send to each of the required set of peers for endorsement;

2. **Ordering and packaging transactions into blocks**: Receives transactions containing endorsed transaction proposal responses from many applications, and orders the transactions into blocks;

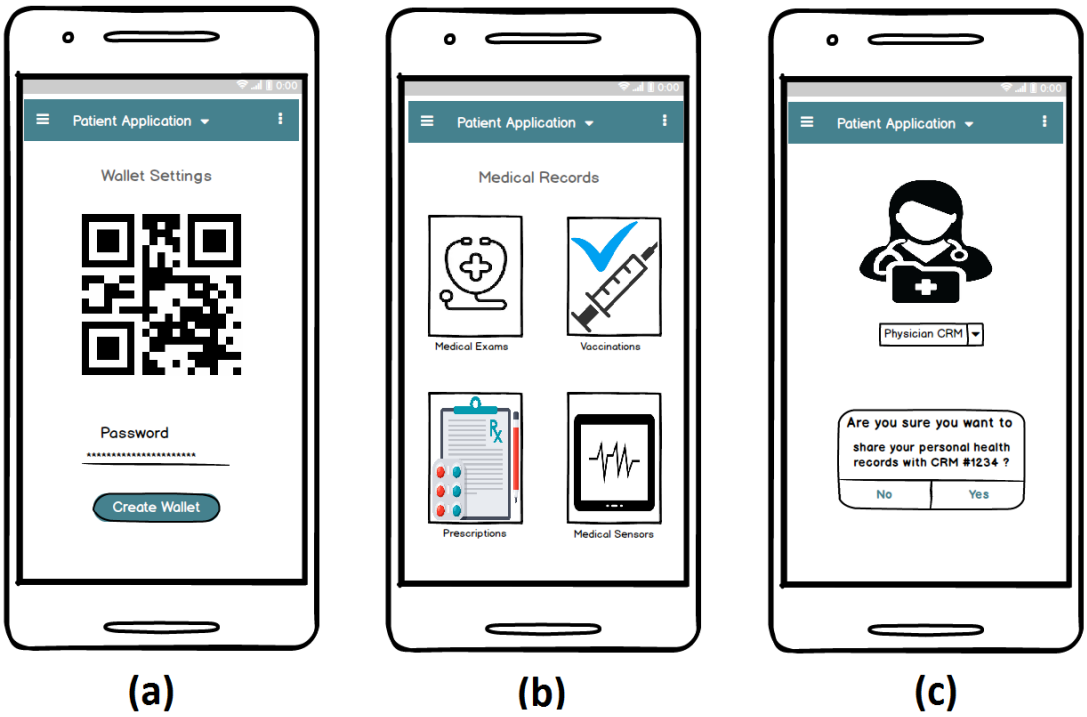
3. **Validation and commit**: Involves the distribution and subsequent validation of blocks and transactions before it can be persisted to the ledger. Every transaction within a block must be validated in order to ensure that it is valid and has been consistently endorsed by consensus peers.

This entire transaction workflow process helps to achieve consensus because all peers have reached agreement on the order and content of transactions in a process that is mediated by orderers. The consensus is a multi-step process, and applications are only notified of ledger updates when the process is complete.

The process where participants (patients and physicians) join the network may be facilitated by the employment of smartphones, for example, having smartphones interfacing with the FogChain and acting as a thin-client to the network. This thin-client is supported by the Hyperledger Fabric and represents the entity that acts on behalf of an

end user. It must connect to a peer to communicate with the Blockchain. The thin-client can connect to any peer of their choice and submit transaction proposals.

Figure 16 – Sample smartphone's screen mockup interfacing with FogChain API's.



Source: Elaborated by the author.

The proposed wireframes do provide a front-end design concept to interface with our FogChain back-end API and services, and are better described as follow:

(a) A welcome screen for users (patients and physicians) permitting identification and authentication through their public keys and or QR code. It should allow new users to register (create wallet) and existing users to effectuate login on the platform;

(b) Patients are allowed to visualize and manage their personal health records fragments;

(c) Each patient is responsible for whom they decide to share their health records, for example, by informing the physician id (CRM).

4.3.4 Smart Contracts:

Set of programs and protocols stored in Blockchain that facilitate, verify, and guarantee the execution of a contract between members of the network. For example, a patient allows / authorizes a physician to visualize their medical history. These programs provide the

ability to directly track and execute complex agreements between parties without human interaction (NOVO, 2018).

The term smart contract, also referred to as **chaincode**[7] is an important component of our model. Basically, it provides self-executing logic that encodes rules for network transactions. The chaincode, often written in the extensible programming languages, is installed and instantiated into the channel's peers by an admin; however, its internal logic may apply to all members, depending on the code itself.

In the e-health IoHT scenario, smart contracts may be very useful, especially in cases where it is possible to define thresholds for collected data; thus, having smart contracts executed automatically in the background could help physicians in decision making.

In our model, the smart contracts feature improvements in the interaction between monitored patients and health providers by automating and self-executing pre-defined agreements over parties, for example, when evaluating healthcare information collected by IoHT devices, such as multi-parametric devices for vital signs, then comparing these readings with customized threshold values. It could trigger notification events or alerts for the patient itself or healthcare providers such as physicians and nurses when these thresholds are exceeded, providing many possibilities to extend the network and assisting interactions between patients and healthcare providers.

In the code snippet 4.1 a sample chaincode implementation is presented. It has two main functions **Init** and **Invoke**. The Init function is called when the chaincode is first installed, while the Invoke function is called anytime we need the chaincode to query or modify the state of the ledger.

Listing 4.1 – Hyperledger Smart Contract in Go Language example.

```
1  package main
2
3  import (
4    "fmt"
5    "github.com/hyperledger/fabric/core/chaincode/shim"
6    pb "github.com/hyperledger/fabric/protos/peer"
7  )
8
9  type SmartContract struct { }
10
11 func (t *SmartContract) Init(stub shim.ChaincodeStubInterface) pb.Response
       {
12   fmt.Println("Init")
13   return shim.Success(nil)
14 }
15
16 func (t *SmartContract) Invoke(stub shim.ChaincodeStubInterface) pb.
     Response {
17   fmt.Println("Invoke")
```

[7] https://hyperledger-fabric.readthedocs.io/en/release-1.4/smartcontract.html

```
18    function, args := stub.GetFunctionAndParameters()
19    if function == "grantAccess" {
20       return t.grantAccess(stub, args)
21    }
22    return shim.Error("Invalid invoke function name.")
23 }
24
25 func (t *SmartContract) grantAccess(stub shim.ChaincodeStubInterface, args
       []string) pb.Response {
26
27    //TODO: here goes the smart contract logic
28
29    var err = stub.PutState("res", []byte("granting access..."))
30    if err != nil {
31       return shim.Error(err.Error())
32    }
33    return shim.Success(nil)
34 }
35
36 func main() {
37    err := shim.Start(new(SmartContract))
38    if err != nil {
39       fmt.Printf("Error starting chaincode: %s", err)
40    }
41 }
```

Once the main components of FogChain are designed and described, we move towards a prototype implementation to be able to test and validate our model.

5 IMPLEMENTATION

A multi-organization Blockchain network is desired, where each organization may, for example, represent a clinic or hospital, and each organization is allowed to have multiple peers spread over its infrastructure, with each peer encapsulated into a FogChain and with support for smart contracts, providing many possibilities to extend the network and assisting with interactions between patients and healthcare providers.

During the research steps, we studied a set of available Blockchain technologies to find which best suits our model's first implementation. Consequently, in Table 7 we present a comparison between available Blockchain platforms, which helped us in identifying possible strengths and weakness over these platforms for our model's application.

Among the assessed Blockchain platforms, we decided to pick the *Hyperledger Fabric*[1] Blockchain project due to the permissioned aspects of the platform, open source license, no charging fees, modularity, tool support, maturity and specially because of the smart contracts support.

To build this network, we have used a set of tools for the development of Blockchain networks, for example, the Hyperledger Composer, which is a collaboration tool, distributed by the Linux Foundation and built with JavaScript, including Node.js, NPM, and CLI, facilitating the development and maintenance process for developers.

5.1 Prototype

In order to implement our FogChain model, we have chosen the *Hyperledger Fabric* Blockchain distribution, which is a solution for distributed ledger technology (DLT), has an open source license, and is made readily available by *The Linux Foundation*[2].

The Hyperledger project was designed for corporate and organizational architectures, with a set of customizable rules, allowing, for example, to operate with different consensus protocols, such as: **PBFT** (Practical Byzantine Fault Tolerant)[3], **Kafka**[4], **SOLO**[5], among others. It differs from other Blockchain platforms because it focuses on development of private and authorized networks, mainly suitable for organizations, rather than a public and open network, not allowing unknown identities to participate, thus, allowing the location of medical records to remain secure and restricted to hospitals and clinics infrastructure.

To properly create a FogChain prototype, one of the requisites was to start defining and modeling who would be able to join the network and also what kind of information and

[1] https://www.hyperledger.org/projects/fabric
[2] https://www.linuxfoundation.org
[3] http://zoo.cs.yale.edu/classes/cs426/2012/bib/castro02practical.pdf
[4] https://hyperledger-fabric.readthedocs.io/en/release-1.4/kafka.html
[5] https://hyperledger-fabric.readthedocs.io/en/release-1.4/orderer/ordering_service.html

Table 7 – Available Blockchain platforms comparison table.

	Ethereum	**Hyperledger Fabric**	**Corda**	**MultiChain**
Platform Description	Generic blockchain platform	Modular blockchain platform	Specialized distributed ledger platform for financial industry	Based on bitcoin's blockchain, for multi-asset financial transactions.
Decentralization	Yes	Partially	Partially	Partially
Transaction Model	Contract–message	Contract–message	Input–output	Input–output
Privacy Features	Public (Permissionless) - Everyone can see transactions history	Private (Permissioned) - Only members can see transactions history	Private (Permissioned) - Only members can see transactions history	Private (Permissioned) - Only members can see transactions history
Governance	Ethereum developers	The Linux Foundation	R3 Consortium	MultiChain developers and Coin Sciences Ltd
Smart Contracts	Smart contract code (e.g., Solidity)-Deterministic execution	Smart contract code (e.g., Go, Java)	*Smart contract code (e.g. Kotlin, Java)*Smart legal contract (legal prose)	none
Supported Consensus Alg.	Proof-of-Work (PoW)	Pluggable framework (generally PBFT)	Pluggable framework (multiple approaches)	Mining diversity scheme
Consensus Level	Ledger level	Transaction level	Transaction level	varies
Currency / Token	Ether (ETH).	None	None	Native multi-currency support.
Code visibility	Blockchain	Counterparties + endorsers	Counterparties + dependents	Blockchain
Transactions per second (TPS)	∼15 tx/sec	∼1.000 tx/sec	Varies	500-1000 tx/sec
Mining / Transaction Fees	Yes	No	No	No
Niche	cross-industry	cross-industry	initially financial sector	financial sector
Block Interval	∼15s	N/A (Batch configuration)	N/A	customizable

Source: Elaborated by the author.

in which format data would be stored. For that, an important feature of the Hyperledger Composer was very helpful, the object-oriented modeling language that is used to define the domain model for a business network definition and can be used to express information or knowledge. A Hyperledger Composer CTO[6] model file is composed of:

- A single namespace where all resource declarations within the file are implicitly in this namespace;

[6]https://hyperledger.github.io/composer/latest/reference/cto_language

- A set of resource definition syntax for assets, transactions, participants, and events;
- Optional import declarations that import resources from other namespaces.

Our network is designed to have two main types of participants. Their interaction and attributes were modeled within *Composer* and are presented in Listing 5.1:

Listing 5.1 – Modeling Hyperledger network participants and assets (health records).

```
namespace br.unisinos.uhospital.ehr

participant Patient identified by cartaoSUS {
      o String cartaoSUS
      o String name
      o String dob
      o Address address
}

concept Address {
      o String street
      o String city
      o String state
      o String cep
      o String phone
      o String email
}

participant Physician identified by physicianId {
      o String physicianId
      o String name
      o String CRM
      o String specialties
      o Address address
      --> Patient[] myPatients optional
}

asset MedicalRecord identified by recordId {
      o String recordId
      o String format
      o String description
      o String offchainDataLink optional
      o String medicalHistory optional
      o String allergies optional
      o String currentMedication optional
      o Boolean smoking optional
      --> Patient owner
      --> Physician[] authorizedPhysicians optional
}

transaction grantAccess {
```

```
42      --> Physician authorisedToModify
43      --> MedicalRecord medicalRecord
44  }
45
46  transaction revokeAccess{
47      --> Physician revokeThisPhysician
48      --> MedicalRecord medicalRecord
49  }
50
51  transaction createMedicalRecord{
52      o String format
53      o String description
54      o String offchainDataLink optional
55      o String medicalHistory optional
56      o String allergies optional
57      o String currentMedication optional
58      o Boolean smoking optional
59      --> Patient owner
60  }
```

(a) **Patient**: The Patient entity represents any person receiving or registered to receive medical treatment. During their life, they may have many medical records entries. The Patient gets to choose who these medical records are shared with. Only physicians allowed by the Patient may see the Patient's medical history;

(b) **Physician**: The Physician entity represents any physician working in the healthcare system and may interact with Patients' medical records if the patient authorizes them.

These two well-defined types of participants can only interact with each other through pre-defined transaction operations ***grantAccess*** and ***revokeAccess***, where they exchange permission over the ***MedicalRecord*** asset. These two operations allow us to grant to the patient full control over their health records, which is one of our main contributions to empower the patients by proposing a model where they can manage their own personal health records (**PHR**). Another important contribution in this model is the presence of an optional field named **"offchainDataLink"**, which belongs to the ***MedicalRecord*** asset, and could potentially assist our model to better scale by allowing storage of more heavyweight information such as clinical images (X-Ray, etc), into external file system servers as per example the **IPFS**[7], a peer-to-peer distributed file system that seeks to connect all computing devices with the same system of files.

In order to establish boundaries among what participants can or can not do, share or access, the Hyperledger Composer provides an access control language (**ACL**[8]) that

[7]http://ipfs.io
[8]https://hyperledger.github.io/composer/latest/reference/acl_language.html

provides declarative access control over the elements of the domain model. By defining ACL rules we can determine which users/roles are permitted to create, read, update or delete elements in a network's domain model. At code snippet presented in Listing 5.2 we do exemplify few of our network rules built to protect participants level of control over other participants and assets (PHR).

Listing 5.2 – Hyperledger Access Control Language (ACL) rules example.

```
rule LimitAccessToAutorisedPhysicians {
   description: "Physician may update a record which they have permission"
   participant(h): "br.unisinos.uhospital.ehr.Physician"
   operation: READ, UPDATE
   resource(m): "br.unisinos.uhospital.ehr.MedicalRecord"
   condition: (
     m.authorizedPhysicians.some(function (authorizedPhysicians) {
         return authorizedPhysicians.getIdentifier() === h.getIdentifier();
         } )
   )
   action: ALLOW
}

rule PhysicianSeeOnlyTheirPatients {
   description: "Physician see only patients they are authorised to modify"
   participant(h): "br.unisinos.uhospital.ehr.Physician"
   operation: READ
   resource(m): "br.unisinos.uhospital.ehr.Patient"
   condition: (
     h.myPatients.some(function (patient) {
         return patient.getIdentifier() === m.getIdentifier();
         } )
   )
   action: ALLOW
}

rule GrantAccessTransaction {
    description: "Allow all patient to submit grantAccess transactions"
    participant: "br.unisinos.uhospital.ehr.Patient"
    operation: ALL
    resource: "br.unisinos.uhospital.ehr.grantAccess"
    action: ALLOW
}

rule RevokeAccessTransaction {
    description: "Allow all patient to submit RevokeAccess transactions"
    participant: "br.unisinos.uhospital.ehr.Patient"
    operation: ALL
    resource: "br.unisinos.uhospital.ehr.revokeAccess"
    action: ALLOW
}
```

In order for patients to be able to join the network, a new identity (also known as wallet[9]) must be issued using the API and or command line. This invokes the Hyperledger Fabric certificate authority (**CA**) to register the new enrollment certificates and ultimately generate an enrollment secret that can be given to the participant, who can then use it to request their certificate and private keys from the Hyperledger Fabric certificate authority. After a new identity is issued, the identity can be used by the participant to interact in the network in the context of that participant. In our case, patients interact with their personal health records and get to choose with whom they share the information.

At the end of the prototyping stage, a Blockchain network was set in place with the Hyperledger Fabric Blockchain for the storage and management of PHR, supported by an initial version of the FogChain Fog-like infrastructure. This allowed us to start collecting metrics of the IoHT, Fog computing, and Blockchain integration and led us to the next section, where we carry evaluations, executing tests and verifying its results.

[9]https://hyperledger.github.io/fabric-sdk-node/release-1.4/module-fabric-network.Wallet.html

6 EVALUATION

This chapter presents the metrics and evaluations carried out during our work, which include two evaluations focused on the prototype developed based on the FogChain model. The results of each evaluation are presented individually, along with its discussion.

6.1 Evaluation Methodology

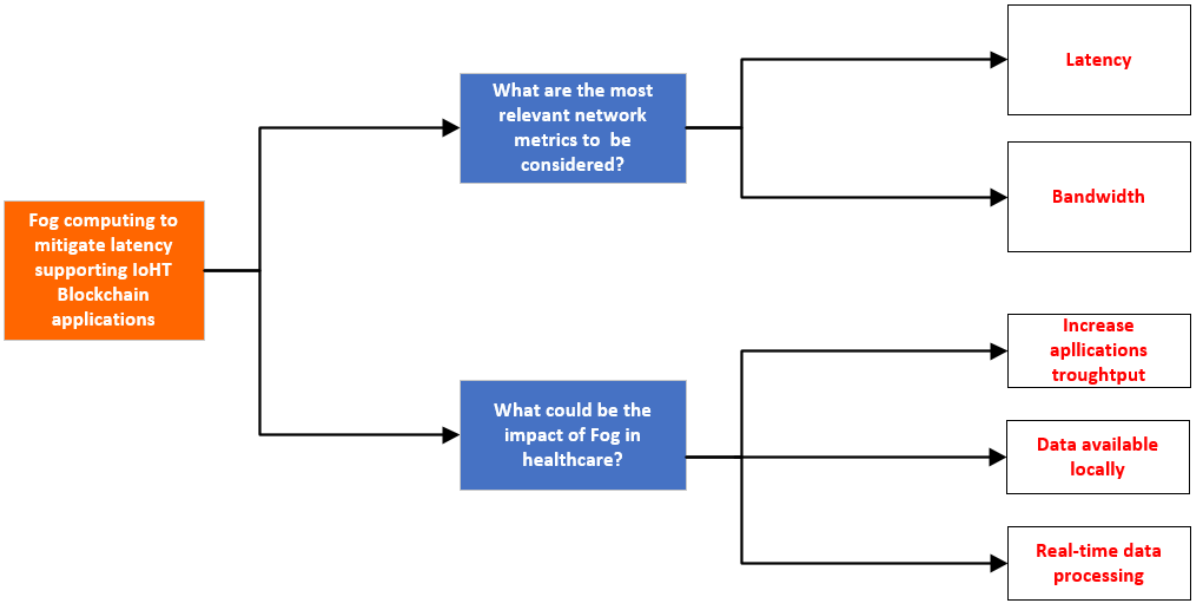
Prototyping is a method that confronts users with a partially implemented model of a system intended to obtain quick feedback, for example, on its appearance and or performance. It is especially useful when it is applied together with the benchmark method. The benchmark tests are used to evaluate the performance of information systems and to test their compliance with user requirements. In general, benchmarking is considered a systematic tool that allows, through metrics, to pursue and determine whether a process and or application is performing at its best. It allowed us to make improvements on the model and adapt specific components, usually with the aim of increasing some aspect of performance and is employed as a continuous process in which we continually seek for performance improvements (HAGGE; KREUTZKAMP, 2003).

6.2 Evaluation Metrics

In order to obtain meaningful metrics for our evaluation, to be monitored and assessed during our experiments and analysis, we employed the Goals/Questions/Metrics (**GQM**) approach, which is a software metric approach in software engineering that propose steps for conducting the identification of the correct metrics for the creation and maintenance of a software system and to clarify which variables are important to take into account during our simulations and test executions. It is carried by identifying a set of quality and/or productivity goals, e.g. improve system performance. From those goals and based upon models of the object of measurement and metrics, we derived questions that define those goals as completely as possible (BASILI; CALDIERA; ROMBACH, 1994).

The latency metrics and its calculation was carried by the execution of multiple end-to-end requests, first in the Fog environment and subsequently in a cloud-like environment and thus calculating the average results in comparison with each other. While the bandwidth metric measures how much data can flow through a specific connection at one time, it turns out it strongly relies on the physical hardware used in the experiment, for example, a gigabit Ethernet connection has a bandwidth of 1,000 Mbps, while the Fast Ethernet compliant network may transfers data at rates up to 100 Mbps. So, considering the local nature of the Fog, its bandwidth relies on the local infrastructure itself, while in the cloud-like environments the bandwidth is restrained by the Internet Service Provider

Figure 17 – GQM - The Goal Question Metrics approach.



Source: Elaborated by the author.

(**ISP**) plans and rates. More specifically in our scenario, the patient's wearable sensors are usually collecting and transferring raw data, which are typically lightweight, thus, not consuming extensively the network bandwidth. However, the more the sensors tend to evolve, the more the need for larger bandwidth on the network.

6.3 Virtual Machine Evaluation

To evaluate the model and verify the integration of FogChain components, our first tests were carried out by implementing a Virtual Machine (**VM**) to process and store medical data information from a set of data (also known as **dataset**) provided by the University of Queensland (LIU; GÖRGES; JENKINS, 2012), having the following hardware specifications to be used in the simulations:

- **Operating Systems Ubuntu 16.04 (64-bit)**
- **Intel core i7-4700MQ @2.40Ghz;**
- **4Gb RAM**
- **HDD 40Gb**;

We have installed and configured Hyperledger Blockchain peers on two of our virtual machine instances, in order to also be able to test the data replication between them. All libraries and dependencies were managed through the Node library and the Node Package

Manager (**NPM**). Through consuming the Hyperledger Rest API, it was possible to write a Python application that sends the medical data originated from the electrocardiogram (ECG) column of the dataset, where each request becomes a transaction proposal, to be validated and persisted in the ledger. The code is available on the *Github*[1] code repository platform.

Figure 18 – Electrocardiogram fragment stored in Blockchain.

Curl

```
curl -X GET --header 'Accept: application/json' 'http://localhost:3000/api/Member/31'
```

Request URL

```
http://localhost:3000/api/Member/31
```

Response Body


```
{
  "$class": "br.unisinos.uhospital.ehr.Member",
  "cartaoSUS": "31",
  "nome": "Thread 3",
  "dataNascimento": "2018-11-29T22:10:06.013Z",
  "prontuario": {
    "$class": "br.unisinos.uhospital.ehr.EHR",
    "id": "1",
    "descricao": "ECG: -0.30500",
    "formato": "ECG - Eletrocardiograma"
  },
  "historicoMedico": [],
  "authorized": []
}
```


Response Code

```
200
```

Source: Elaborated by the author.

6.3.1 Results

We obtained an average response time of two and a half seconds for requests made through our Hyperledger Rest API over the HTTP protocol. Possibly, better response times could be obtained if we had a solid state drive (**SSD**) instead of a common hard drive disk (**HDD**) in place, in a way that writing operations would tend to be faster. Using the Rest API also adds an overhead of the protocols. An alternative was to directly use Node.js, which has native integration with Blockchain through a Software Development Kit (**SDK**) provided by Hyperledger.

Concluding this evaluation, we have implemented an Blockchain network with Hyperledger framework, conceived into a Virtual Machine simulating a fog environment, in order to first verify the viability and technologies integration for the PHR management.

[1] https://github.com/andremayer/sandbox/blob/master/blockchain/AddMembersRest.py

In terms of performance, the throughput has been impacted by the hardware and VM limitations under our initial tests. The next steps are to execute more trials but in a fog-like environment instead of in a VM, as well as engage with different approaches to interact with the Blockchain, in order to create transaction proposals directly through Node.js programming rather than communicating through REST API, which end-up adding several protocols overhead.

6.4 Fog Evaluation

The results obtained in the virtual machine environment pointed out possible viability of the model in our initial prototype, however, it demanded performance improvements, leading us to a more robust implementation, evaluation and guidance on solid approaches and methodology.

To better evaluate the model and verify the integration of FogChain components the first improvement was on moving the prototype from the virtual machine and installing it on a local machine to simulate our Fog environment for local processing and storing IoHT medical data information from the clinical vital signs dataset provided by the University of Queensland (LIU; GÖRGES; JENKINS, 2012), and this time with an improved hardware for our benchmark:

- **Operating Systems Ubuntu 16.04 (64-bit);**
- **Processor Intel Xeon E5-2620v4 2.1GHz;**
- **32Gb RAM;**
- **HDD SAS 600Gb RAID 5 (10.000 RPM);**

Considering that benchmarking our prototype is in our scope, in order to verify the application capabilities in terms of throughput (transactions per second) and response time (latency), and to ensure it can be a suitable solution for the healthcare domain, some improvements were carried on our fog layer services for this evaluation, given that healthcare applications should be highly available and capable of processing huge amounts of data.

The Hyperledger Fabric Blockchain is consequently installed and configured on our Fog-like environment and it is working as intended, a component of the FogChain architecture. Its libraries and dependencies were also managed through Node.js and *Node Package Manager* (NPM), and our modeling files and configurations were in now place, making our network ready and available for tests.

Once the FogChain components were all in place in the Fog environment, it allowed us to improve our battery of tests and subsequently better metrifying the test scenarios, in

a more end-to-end approach where each component is being responsible for a small part of the vital signs collection automation, for example, having the collected IoHT health records fragments becoming transaction proposals, to be validated and only then persisted on the ledger.

At Listing 6.1 we present a snippet of code utilizing the Hyperledger Composer API, full code available at *uHospital's Bitbucket*[2] repository, where more tests and tests scenarios are available.

Listing 6.1 – Sample PHR transaction block.

```
const NS = 'br.unisinos.uhospital.ehr';
const assetType = 'MedicalRecord';
const assetNS = NS + '.' + assetType;

const registry = await conn.getAssetRegistry(assetNS);

const phr = factory.newResource(NS, assetType, phrId);

phr.owner = factory.newRelationship(NS, type, ownerId);
phr.recordId = phrId;
phr.format = 'Systolic blood pressure';
phr.description = '130 mm Hg';
phr.medicalHistory = 'hypertension';
phr.allergies = 'iodine';
phr.currentMedication = 'Nebilet';
phr.smoking = false;

await registry.add(phr);
```

6.4.1 Results

In this section we are going to demonstrate all results obtained during the research and development of our prototype, carried simulations and benchmarks.

Determined to check how long it would take for a single transaction to reach completion under our Fog computing environment, we executed an initial test using the *add*[3] operation from the Hyperledger Composer API, which expects only a single asset as the input parameter. It resulted in an average of 180 milliseconds for a transaction to be created, ordered, validated, and ultimately persisted in the ledger, which if executed multiple times sequentially would lead to approximately five transactions per second as throughput.

Seeking performance improvements, transactions were organized in bulk (batches) to verify a possible increase of throughput. For that, instead of sending transactions one by one sequentially, we employed the *addAll*[4] operation, which expects as input parameter

[2]https://bitbucket.org/uhospital/fogchain/src/multi-org
[3]https://hyperledger.github.io/composer/latest/api/runtime-assetregistry#add
[4]https://hyperledger.github.io/composer/latest/api/runtime-assetregistry#addall

an array of assets, in our case, an array of vital sign readings. In other words, the interaction with our Blockchain network was changed to work in batches and the tricky part was finding an optimal batch size. This process also implies our FogChain prototype accumulates data and organizes the data in an array structure before sending it onto the Blockchain.

Performance degradation was noticed when working with larger batch sizes, for example, a batch with a thousand transactions would take approximately twenty-three seconds to completion, giving us an low average of forty-three transactions per second, while a smaller batch with half the number of transactions (500 tx) would take approximately six seconds, providing a better throughput and indicating that our optimum batch size was likely to be a smaller number.

The evaluation was carried by a total of ten executions (n=10) for each of the three main scenarios (Light, Medium and Heavy), where we were variating the batch size, and the number of concurrent sessions, ranging it from ten in the Light scenario to a hundred in the Heavy one. It was possible to conclude that to obtain the best performance possible, our optimum persistence configuration would be having requests with batch sizes ranging from ten to fifty transactions per batch. The obtained results are displayed in a more consolidated manner in Table 8 and illustrated in Figure 19.

Table 8 – Average results from ten executions at Fog with 95% confidence interval.

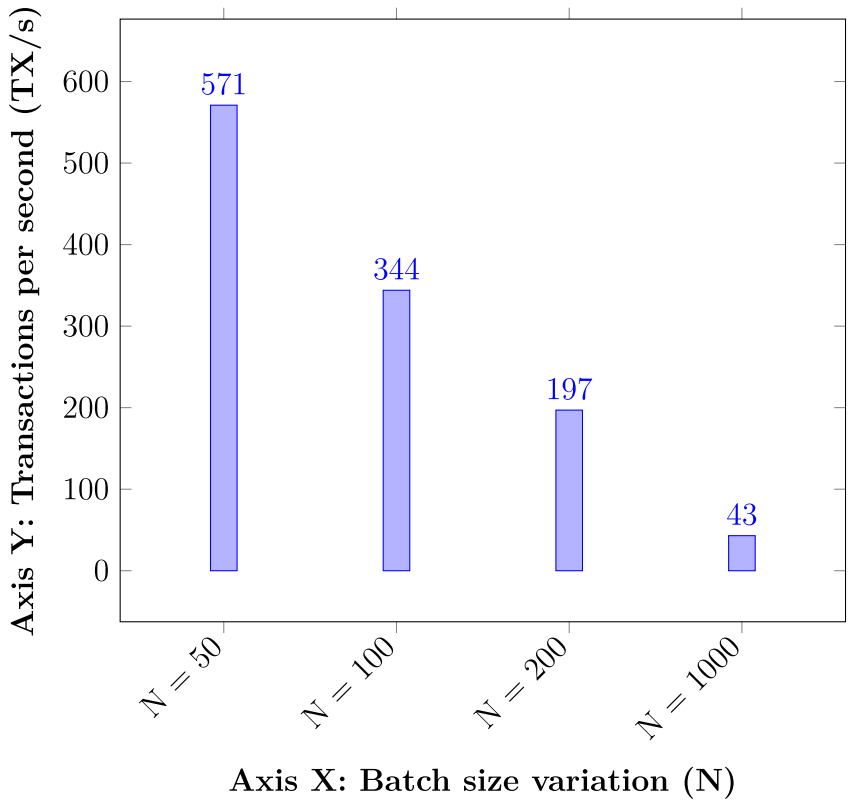
Rated item	**Light Load**	**Medium Load**	**Heavy Load**
CPU usage (GHz)	0.2 ± 0.05 ($\sigma = 0.09$)	0.34 ± 0.06 ($\sigma = 0.11$)	0.41 ± 0.09 ($\sigma = 0.15$)
Memory usage (GB)	0.5 ± 0.05 ($\sigma = 0.08$)	0.8 ± 0.06 ($\sigma = 0.10$)	1.1 ± 0.08 ($\sigma = 0.14$)
Throughput (TPS)	579 ± 2.33 ($\sigma = 3.76$)	502 ± 3.30 ($\sigma = 5.32$)	453 ± 4.41 ($\sigma = 7.12$)
Latency (ms)	169 ± 1.20 ($\sigma = 1.93$)	185 ± 1.73 ($\sigma = 2.79$)	193 ± 2.81 ($\sigma = 4.53$)

Source: Elaborated by the author.

Once we had the results obtained in the Fog environment, we decided to compare its network latency metric against a similar setup but in the cloud, where our goal on this test was to verify and ensure the latency mitigation of the Fog over the cloud on this matter. Not surprisingly, during this experiment, the Fog computing environment demonstrated a response time to be at least twice faster in comparison to cloud computing as illustrated in Figure 20, where we compared our aforementioned response time from Fog to a cloud-hosted setup at Amazon Web Services (**AWS**), having in place a thing device called **"arn:aws:iot:us-west-2:205818066477:thing/sensor"** sending information directly to our Blockchain network by invoking our API endpoints through the cloud.

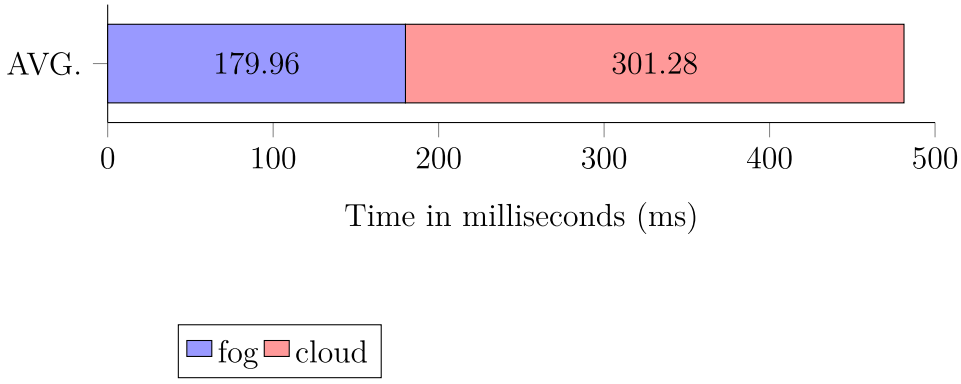
To complement our benchmark, hardware metrics were also collected, such as **CPU** and memory **RAM** resources. These resources were monitored during a time-boxed window of one hundred seconds for each resource individually, creating snapshots for individual analysis that verified an average of 6% increase of CPU consumption during the benchmark workload, as seen in Figure 21.

Figure 19 – Batch benchmark results.



Source: Elaborated by the author.

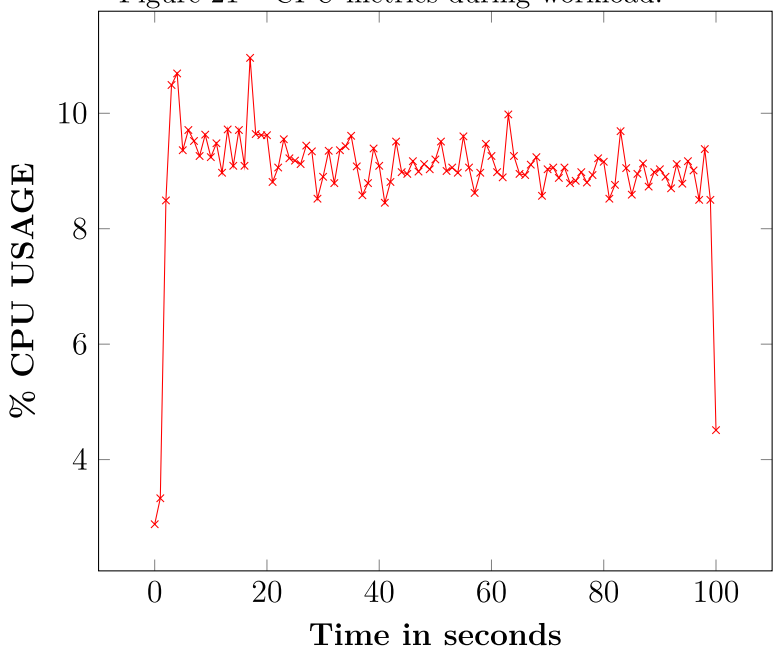
Figure 20 – Latency comparison of Fog vs Cloud.



Source: Elaborated by the author.

It is important to note that in the first and last points marked on the CPU graph are representing the scenario where the application is not yet operating under full-load because it has just received and or finished processing the request, meaning the processor was initially idle, then received our workload increasing its consumption and lastly finished its processing backing to its original state.

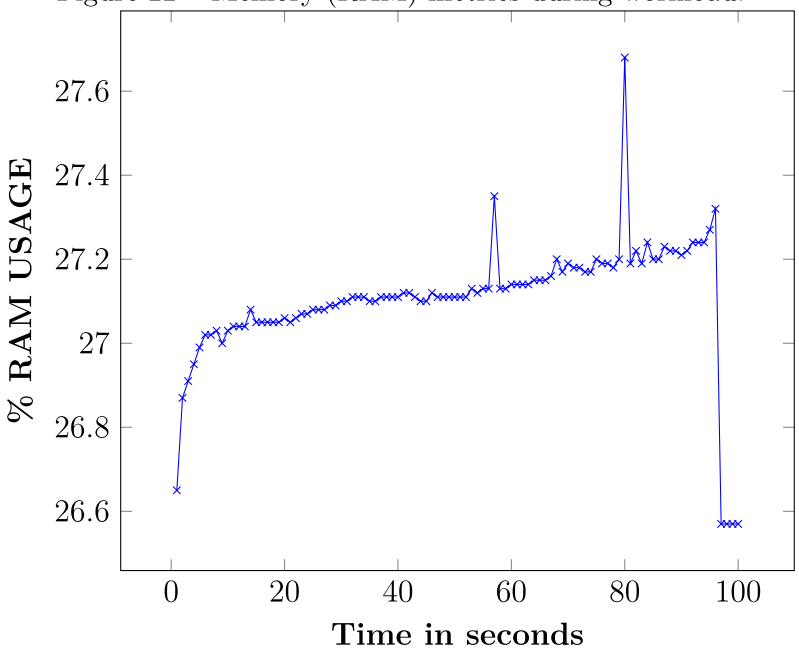
Figure 21 – CPU metrics during workload.



Source: Elaborated by the author.

While the regular workload consumed an average of ~500Mb RAM, during bigger batch sizes an additional of more ~500Mb RAM was detected, followed by a memory flush at the end of the test window, as demonstrated in Figure 22, having the first and last dots in the graph representing the application in idle state, when it is not processing requests, consequently not consuming additional memory.

Figure 22 – Memory (RAM) metrics during workload.



Source: Elaborated by the author.

6.5 Discussion

The prototype evaluation demonstrated the capacity of our architecture as a technology integrator, providing an alternative to traditional Cloud-IoT solutions. Obtained results for latency and throughput metrics did highlight the performance boost driven by the Fog computing adoption.

Moreover, working with batches of transactions demonstrated to be favorable, and with this approach in place, we managed to obtain a satisfactory application throughput, which in other words led us to performance improvements of transactions per second capacity on our architecture, combined with the local Fog computing as an intermediary layer mitigating latency and promoting a closer to real-time process of collecting, securing, and storing these vital signs.

The FogChain implementation for PHR management demonstrated a slice of how Blockchain could be employed in the healthcare domain, benefiting from its cryptographic and tamper-proof nature, which adds an additional security layer so necessary for healthcare applications.

Moreover, having the patient's complete medical history available in loco turns out to be an intangible benefit for the healthcare domain, leaving the solution with no external dependencies such as ISP and/or services, which is in contrast to previous models assessed in the related work section. Aiming to ease the understanding of these benefits identified in the adoption of fog computing during our evaluations, and to enrich the discussion, we have prepared a comparative table that highlights the main differences between the cloud and the Fog in Table 9:

Table 9 – Key differences between Fog computing and cloud.

	Cloud	**Fog**
Architecture	Centralized	Distributed
Things communication	From a distance	Directly from the edge
Data processing	Remote	Local
Latency	High	Low
Connectivity	Internet (ISP)	Variety of protocols
Computing capabilities	Higher	Lower
Number of nodes	Few	Very large

Source: Elaborated by the author.

Among these Fog characteristics, the main aspect where our model benefits from it is through the possibility of having local processing and storage near the edge, and it is at this point where we mostly differentiate from the other related works.

7 FINAL REMARKS

Fog computing can play a big role in healthcare applications by mitigating latency and providing local processing, services, and resource availability near the edge. It allows applications to decrease the amount of access to the cloud, where the connection is subject to delays in worldwide network traffic, thus, becoming a viable and potential integrator of IoHT and Blockchain technologies.

The FogChain implementation for PHR management demonstrated how Blockchain could be employed in the healthcare domain and benefit from its cryptographic and tamper-proof nature, which adds a necessary security layer for healthcare applications. However, the FogChain model is not limited to the healthcare domain only and could also be adapted to other domains, for example, supply chains, smart-city, and cross-industry applications, as long as some adaptations are made, e.g. changes on the expected Blockchain's data structure.

Moreover, the benchmark provided satisfactory proof regarding the initial feasibility of our architectural model proposition. However, more research, trials, and experiments must be carried out to ensure a secure and established system is implanted before using our model in a real healthcare scenario, given a patient's health data is personal, sensitive, and critical information.

7.1 Contributions

Our main contribution is the FogChain model itself, and its intrinsic concept of overcoming IoT constraints by adding an intermediary fog layer near to the edge to improve their capabilities and resources. Moreover, discussions, the proposed taxonomy, and answered research questions might somehow contribute to future academic research in the area.

During the process of researching and evaluating this work, an article was submitted to the Health Informatics Journal (**HIJ**)[1] regarding state-of-the-art EHR in a Blockchain, which was accepted and published in September 2019 (MAYER; COSTA; RIGHI, 2019). Additionally, a second article is in progress for submission, where we shed light on the FogChain model and its architecture for the academic community.

7.2 Future Works

As future works for this project, we do suggest extending the FogChain model, not only adding more participants and roles to the Blockchain network (e.g. allowing insurance companies to join it), but also proposing and implementing interoperability features for

[1] https://journals.sagepub.com/home/jhi

the PHR storage regarding data format and transaction block structures in a way that allows many organizations to join the network without the need to rewrite their legacy systems.

The lack of a global healthcare data standard, technological constraints, and infrastructure costs were some of the limitations identified. Moreover, current Blockchain solutions may not adequately address the desired requirements for the healthcare domain and might not have full compliance with regulatory organizations such as **HIPAA** and **GDPR**. For example, in a scenario where a patient has the right to be forgotten, requiring the deletion of their stored health data in the Blockchain, this demand directly clashes with the immutability attribute of the Blockchain solution.

Furthermore, our model itself does not solve the intrinsic interoperability issues regarding different data format usages between health providers, which are a broader concern in the healthcare area. Another vital variable to take into account when considering the Blockchain solution is the scalability constraints in terms of the trade-off between the volume of transaction and computer power for processing time of transactions.

The existing right to be forgotten concern, where a user may ask for entire deletion of his records which clashes with the immutability principle of the Blockchain and the compliance with regulatory organizations, we may rely on many ongoing alternative solutions to be tested, e.g. a study released by the European Parliamentary Research Service (**EPRS**)[2] which listed some possible techniques:

- ***Zero knowledge proofs***: can be used to provide a binary true/false answer without providing access to the underlying data. The ledger merely reveals whether a transaction has occurred, not which public key was used or what value (if any) was transferred;

- ***Stealth addresses***: can be used to generate a one-time transaction that relies on hashed one-time keys. The use of one-time accounts for transactions requires that every transaction must completely empty at least one accounts and create one or multiple new accounts;

- ***Homomorphic encryption***: is an advanced method of encryption that enables the computation of cyphertexts. It allows for encrypted data to be subjected to computation, generate an encrypted result that, which decrypted produces the same results than if the computation had been done on unencrypted data;

- ***The addition of noise***: an approach where several transactions are grouped together so that from the outside it is impossible to discern the identity of the respective senders and recipients of a transaction.

[2]https://www.europarl.europa.eu

Another possibility is to improve the FogChain's "**off-chain**" data link solution previously mentioned, to support not only heavyweight information such image's exams externally but also extending it to sensitive information, thus, storing all personally identifiable information (**PII**) in separate off-chain databases, in order to have only references along with a hash of corresponding data in the Blockchain that can be later completely erased and this way losing its linkage to the patient permanently.

Nevertheless, more research, trials, and experiments must be carried out to ensure a secure and established system is in place before using our model in a real healthcare scenario, given that a patient's data is personal and very sensitive information.

REFERENCES

AL-FUQAHA, A. et al. Internet of things: a survey on enabling technologies, protocols, and applications. **IEEE Communications Surveys and Tutorials**, v. 17, n. 4, p. 2347–2376, 2015.

BADR, S.; GOMAA, I.; ABD-ELRAHMAN, E. Multi-tier blockchain framework for iot-ehrs systems. **Procedia Computer Science**, v. 141, p. 159–166, 2018.

BANERJEE, M.; LEE, J.; CHOO, K.-K. R. A blockchain future for internet of things security: a position paper. **Digital Communications and Networks**, v. 4, n. 3, p. 149–160, 2018.

BASILI, V. R.; CALDIERA, G.; ROMBACH, H. D. The goal question metric approach. **Encyclopedia of Software Engineering**, v. 2, p. 528–532, 1994.

BISWAS, K.; MUTHUKKUMARASAMY, V. Securing smart cities using blockchain technology. In: 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), 2016., 2016. **Anais...** [S.l.: s.n.], 2016. p. 1392–1393.

BODIN, L. D.; GORDON, L. A.; LOEB, M. P. Evaluating information security investments using the Analytic hierarchy process. **Communications of the ACM**, v. 48, n. 2, p. 78–83, 2005.

BUYYA, R.; SON, J. Software-defined multi-cloud computing: a vision, architectural elements, and future directions. In: INTERNATIONAL CONFERENCE ON COMPUTATIONAL SCIENCE AND ITS APPLICATIONS, 2018. **Anais...** [S.l.: s.n.], 2018. p. 3–18.

CHENG, E. C. et al. Healthcare services across china–on implementing an extensible universally unique patient identifier system. **International Journal of Healthcare Management**, v. 11, n. 3, p. 210–216, 2018.

CHRISTIDIS, K.; DEVETSIKIOTIS, M. Blockchains and Smart Contracts for the Internet of Things. **IEEE Access**, v. 4, p. 2292–2303, 2016.

CONOSCENTI, M.; VETRO, A.; De Martin, J. C. Blockchain for the internet of things: a systematic literature review. In: IEEE/ACS INTERNATIONAL CONFERENCE ON COMPUTER SYSTEMS AND APPLICATIONS, AICCSA, 2016. **Proceedings...** [S.l.: s.n.], 2016. v. 0, p. 1–6.

COSTA, C. A. da et al. Internet of health things: toward intelligent vital signs monitoring in hospital wards. **Artificial Intelligence in Medicine**, v. 89, p. 61–69, 2018.

CYRAN, M. A. Blockchain as a Foundation for Sharing Healthcare Data. **Blockchain in Healthcare Today**, 2018.

DAGHER, G. G. et al. Ancile: privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. **Sustainable cities and society**, v. 39, p. 283–297, 2018.

DEMICHELIS, C. .; CHIMENTO, P. **IP Packet Delay Variation Metric for IP Performance Metrics (IPPM)**. : s.n.], 2002.

DORRI, A. et al. Blockchain for iot security and privacy: the case study of a smart home. In: IEEE INTERNATIONAL CONFERENCE ON PERVASIVE COMPUTING AND COMMUNICATIONS WORKSHOPS, PERCOM WORKSHOPS 2017, 2017., 2017. **Anais...** [S.l.: s.n.], 2017. p. 618–623.

DORRI, A.; KANHERE, S. S.; JURDAK, R. Towards an optimized blockchain for IoT. In: IEEE/ACM 2ND INTERNATIONAL CONFERENCE ON INTERNET-OF-THINGS DESIGN AND IMPLEMENTATION, IOTDI 2017 (PART OF CPS WEEK), 2017., 2017. **Proceedings...** [S.l.: s.n.], 2017. p. 173–178.

DUBOVITSKAYA, A. et al. Secure and Trustable Electronic Medical Records Sharing using Blockchain. In: AMIA ... ANNUAL SYMPOSIUM PROCEEDINGS. AMIA SYMPOSIUM, 2017. **Anais...** [S.l.: s.n.], 2017. v. 2017, p. 650–659.

FAN, K. et al. Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5g. **IET Communications**, v. 12, n. 5, p. 527–532, 2017.

FORREST, J. L.; MILLER, S. A. Evidence-based decision making in action: part 2 - evaluating and applyingthe clinical evidence. **Journal of Contemporary Dental Practice**, v. 4, n. 1, p. 38–51, 2003.

GORDON, W. J.; CATALINI, C. Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability. **Computational and Structural Biotechnology Journal**, v. 16, p. 224–230, 2018.

GROVER, P.; KAR, A. K.; DAVIES, G. "Technology enabled Health" – Insights from twitter analytics with a socio-technical perspective. **International Journal of Information Management**, v. 43, p. 85–97, 2018.

GUO, R. et al. Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems. **IEEE Access**, v. 6, p. 11676–11686, 2018.

HAGGE, L.; KREUTZKAMP, J. A benchmarking method for information systems. In: IEEE INTERNATIONAL CONFERENCE ON REQUIREMENTS ENGINEERING, 2003. **Proceedings...** [S.l.: s.n.], 2003. v. 2003-January, p. 245–253.

HASHEMI, S. H. et al. World of empowered IoT users. In: IEEE 1ST INTERNATIONAL CONFERENCE ON INTERNET-OF-THINGS DESIGN AND IMPLEMENTATION, IOTDI 2016, 2016., 2016. **Proceedings...** [S.l.: s.n.], 2016. p. 13–24.

HONGWEI, L.; XINHUI, W.; SANYANG, L. Feasible direction algorithm for solving the SDP relaxations of quadratic {-1, 1} programming problems. In: OPTIMIZATION METHODS AND SOFTWARE, 2004. **Anais...** [S.l.: s.n.], 2004. v. 19, n. 2, p. 125–136.

ICHIKAWA, D.; KASHIYAMA, M.; UENO, T. Tamper-resistant mobile health using blockchain technology. **JMIR mHealth and uHealth**, v. 5, n. 7, p. e111, 2017.

JIANG, S. et al. Blochie: a blockchain-based platform for healthcare information exchange. In: IEEE INTERNATIONAL CONFERENCE ON SMART COMPUTING, SMARTCOMP 2018, 2018., 2018. **Proceedings...** [S.l.: s.n.], 2018. p. 49–56.

KARAFILOSKI, E.; MISHEV, A. Blockchain solutions for big data challenges: a literature review. In: IEEE INTERNATIONAL CONFERENCE ON SMART TECHNOLOGIES, EUROCON 2017 - CONFERENCE PROCEEDINGS, 17., 2017. **Anais...** [S.l.: s.n.], 2017. p. 763–768.

KELLER, T.; KESSLER, N. Yet another blockchain use case–the label chain. In: IEEE 15TH INTERNATIONAL CONFERENCE ON E-BUSINESS ENGINEERING (ICEBE), 2018., 2018. **Anais...** [S.l.: s.n.], 2018. p. 187–194.

KHLIFI, H.; GRÉGOIRE, J. C. Estimation and removal of clock skew from delay measures. In: CONFERENCE ON LOCAL COMPUTER NETWORKS, LCN, 2004. **Proceedings...** [S.l.: s.n.], 2004. v. 1, p. 144–151.

KITCHENHAM, B. A. Systematic review in software engineering. **System Engineering and Computer Science Department COPPE/UFRJ, Technical Report ES**, v. 679, n. 05, p. 1, 2012.

KITCHENHAM, B. et al. Systematic literature reviews in software engineering-A tertiary study. **Information and Software Technology**, v. 52, n. 8, p. 792–805, 2010.

KLEINAKI, A. S. et al. A Blockchain-Based Notarization Service for Biomedical Knowledge Retrieval. **Computational and Structural Biotechnology Journal**, v. 16, p. 288–297, 2018.

KOUICEM, D. E.; BOUABDALLAH, A.; LAKHLEF, H. Internet of things security: a top-down survey. **Computer Networks**, 2018.

KRAEMER, F. A. et al. Fog Computing in Healthcare-A Review and Discussion. **IEEE Access**, v. 5, p. 9206–9222, 2017.

KSHETRI, N. Blockchain's roles in strengthening cybersecurity and protecting privacy. **Telecommunications Policy**, v. 41, n. 10, p. 1027–1038, 2017.

KUO, T. T.; KIM, H. E.; OHNO-MACHADO, L. Blockchain distributed ledger technologies for biomedical and health care applications. **Journal of the American Medical Informatics Association**, v. 24, n. 6, p. 1211–1220, 2017.

LEMIEUX, V. L. A typology of blockchain recordkeeping solutions and some reflections on their implications for the future of archival preservation. In: IEEE INTERNATIONAL CONFERENCE ON BIG DATA, BIG DATA 2017, 2017., 2017. **Proceedings...** [S.l.: s.n.], 2017. v. 2018-January, p. 2271–2278.

LINN, L. A.; KOO, M. B. Blockchain For Health Data and Its Potential Use in Health IT and Health Care Related Research. In: ONC/NIST USE OF BLOCKCHAIN FOR HEALTHCARE AND RESEARCH WORKSHOP, 2016. **Anais...** [S.l.: s.n.], 2016. p. 1 – 10.

LIU, D.; GÖRGES, M.; JENKINS, S. A. University of queensland vital signs dataset: development of an accessible repository of anesthesia patient monitoring data for research. **Anesthesia and Analgesia**, v. 114, n. 3, p. 584–589, mar 2012.

LIU, W. et al. Advanced block-chain architecture for e-health systems. In: IEEE 19TH INTERNATIONAL CONFERENCE ON E-HEALTH NETWORKING, APPLICATIONS AND SERVICES (HEALTHCOM), 2017., 2017. **Anais...** [S.l.: s.n.], 2017. p. 1–6.

MAMOSHINA, P. et al. Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare. **Oncotarget**, v. 9, n. 5, p. 5665–5690, 2018.

MANNARO, K. et al. A blockchain approach applied to a teledermatology platform in the sardinian region (italy). **Information**, v. 9, n. 2, p. 44, 2018.

MAYER, A. H.; COSTA, C. A. da; RIGHI, R. d. R. Electronic health records in a blockchain: a systematic review. **Health Informatics Journal**, p. 1460458219866350, 2019.

MOKHTARI, G.; ANVARI-MOGHADDAM, A.; ZHANG, Q. A New Layered Architecture for Future Big Data-Driven Smart Homes. **IEEE Access**, v. 7, p. 19002–19012, 2019.

NICHOL, P. B.; BRANDT, J. Co-creation of trust for healthcare: the cryptocitizen framework for interoperability with blockchain. **ResearchGate**, v. 24, n. 1, p. 1–9, 2016.

NIRANJANAMURTHY, M.; NITHYA, B.; JAGANNATHA, S. Analysis of blockchain technology: pros, cons and swot. **Cluster Computing**, p. 1–15, 2018.

NOVO, O. Blockchain meets iot: an architecture for scalable access management in iot. **IEEE Internet of Things Journal**, v. 5, n. 2, p. 1184–1195, 2018.

PAN, J.; MCELHANNON, J. Future Edge Cloud and Edge Computing for Internet of Things Applications. **IEEE Internet of Things Journal**, v. 5, n. 1, p. 439–449, 2018.

PATEL, V. A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. **Health informatics journal**, p. 1460458218769699, 2018.

PETTICREW, M.; ROBERTS, H. **Systematic reviews in the social sciences**: a practical guide. John Wiley & Sons, 2008. 1–336 p.

PRIISALU, J.; OTTIS, R. Personal control of privacy and data: estonian experience. **Health and technology**, v. 7, n. 4, p. 441–451, 2017.

QIU, D. et al. Regression testing of web service: a systematic mapping study. **ACM Computing Surveys**, v. 47, n. 2, p. 21, 2014.

RABAH, K.; RESEARCH, M.; KENYA, N. Challenges & opportunities for blockchain powered healthcare systems: a review. **Mara Research Journal of Medicine and Health Sciences**, v. 1, n. 1, p. 45–52, 2017.

RAHMAN, M. A. et al. Blockchain and iot-based cognitive edge framework for sharing economy services in a smart city. **IEEE Access**, v. 7, p. 18611–18621, 2019.

REYNA, A. et al. On blockchain and its integration with IoT. Challenges and opportunities. **Future Generation Computer Systems**, v. 88, p. 173–190, 2018.

RIBITZKY, R. et al. Pragmatic, interdisciplinary perspectives on blockchain and distributed ledger technology: paving the future for healthcare. **Blockchain in Healthcare Today**, 2018.

RIGHI, R. R. et al. Exploring extensibility and interoperability in the internet of things landscape. In: INTERNATIONAL CONFERENCES ON WWW/INTERNET 2018 AND APPLIED COMPUTING 2018, 2018, 2018, Budapeste. PROCEEDINGS OF THE INTERNATIONAL CONFERENCES ON WWW/INTERNET 2018 AND APPLIED COMPUTING 2018. Lisboa. **Proceedings...** IADIS, 2018. p. 339–343.

ROEHRS, A.; COSTA, C. A. da; ROSA RIGHI, R. da. Omniphr: a distributed architecture model to integrate personal health records. **Journal of biomedical informatics**, v. 71, p. 70–81, 2017.

ROEHRS, A. et al. Personal health records: a systematic literature review. **Journal of Medical Internet Research**, v. 19, n. 1, p. e13, 2017.

ROEHRS, A. et al. Analyzing the performance of a blockchain-based personal health record implementation. **Journal of Biomedical Informatics**, v. 92, p. 103140, 2019.

ROMAN-BELMONTE, J. M.; De la Corte-Rodriguez, H.; RODRIGUEZ-MERCHAN, E. C. How blockchain technology can change medicine. **Postgraduate Medicine**, v. 130, n. 4, p. 420–427, 2018.

SAMANIEGO, M.; DETERS, R. Blockchain as a Service for IoT. In: IEEE INTERNATIONAL CONFERENCE ON INTERNET OF THINGS; IEEE GREEN COMPUTING AND COMMUNICATIONS; IEEE CYBER, PHYSICAL, AND SOCIAL COMPUTING; IEEE SMART DATA, ITHINGS-GREENCOM-CPSCOM-SMART DATA 2016, 2016., 2017. **Proceedings...** IEEE, 2017. p. 433–436.

SHAE, Z.; TSAI, J. J. On the design of a blockchain platform for clinical trial and precision medicine. In: IEEE 37TH INTERNATIONAL CONFERENCE ON DISTRIBUTED COMPUTING SYSTEMS (ICDCS), 2017., 2017. **Anais...** [S.l.: s.n.], 2017. p. 1972–1980.

SHARMA, P. K.; CHEN, M. Y.; PARK, J. H. A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT. **IEEE Access**, v. 6, p. 115–124, 2018.

SHEN, B.; GUO, J.; YANG, Y. Medchain: efficient healthcare data sharing via blockchain. **Applied Sciences (Switzerland)**, v. 9, n. 6, p. 1207, 2019.

SILVA, C. C. A. et al. A fog computing-based architecture for medical records management. **Wireless Communications and Mobile Computing**, v. 2019, 2019.

SMITH, K. J.; DHILLON, G. Blockchain for digital crime prevention: the case of health informatics. In: AMCIS 2017 - AMERICA'S CONFERENCE ON INFORMATION SYSTEMS: A TRADITION OF INNOVATION, 2017. **Anais...** [S.l.: s.n.], 2017. v. 2017-August.

THOMASON, J. Blockchain: an accelerator for women and children's health? **Global Health Journal**, v. 1, n. 1, p. 3–10, 2017.

TULI, S. et al. Fogbus: a blockchain-based lightweight framework for edge and fog computing. **Journal of Systems and Software**, v. 154, p. 22–36, 2019.

WANG, H.; SONG, Y. Secure cloud-based ehr system using attribute-based cryptosystem and blockchain. **Journal of medical systems**, v. 42, n. 8, p. 152, 2018.

WRIGHT, C. S. **Bitcoin**: a peer-to-peer electronic cash system. Manubot, 2019.

XIA, Q. et al. Medshare: trust-less medical data sharing among cloud service providers via blockchain. **IEEE Access**, v. 5, p. 14757–14767, 2017.

YAN, Z.; ZHANG, P.; VASILAKOS, A. V. A survey on trust management for Internet of Things. **Journal of Network and Computer Applications**, v. 42, p. 120–134, 2014.

YANG, H.; YANG, B. A Blockchain-based Approach to the Secure Sharing of Healthcare Data. In: NORWGIAN INFORMATION SECURITY CONFERENCE, 2017. **Anais...** [S.l.: s.n.], 2017.

YUE, X. et al. Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. **Journal of medical systems**, v. 40, n. 10, p. 218, 2016.

ZHANG, P. et al. Fhirchain: applying blockchain to securely and scalably share clinical data. **Computational and Structural Biotechnology Journal**, v. 16, p. 267–278, 2018.