**Universidade do Minho**
Escola de Engenharia

Tiago André Saraiva Guimarães

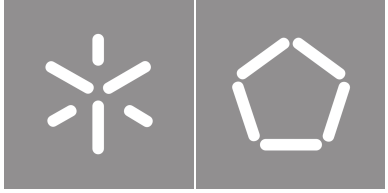
# Improving Veracity and Value of Data in Healthcare Data Flows

September, 2024

Improving Veracity and Value of Data in Healthcare Data Flows

Tiago Guimarães

UMinho | 2024



**Universidade do Minho**
Escola de Engenharia

Tiago André Saraiva Guimarães

# Improving Veracity and Value of Data in Healthcare Data Flows

Doctorate Thesis
Doctorate in Doctoral Programme in Biomedical Engineering

Work developed under the supervision of:
**António Carlos da Silva Abelha**
**Manuel Filipe Vieira Torres dos Santos**

September, 2024

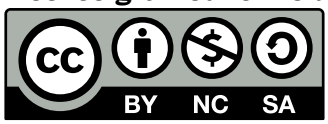
**COPYRIGHT AND TERMS OF USE OF THIS WORK BY A THIRD PARTY**

This is academic work that can be used by third parties as long as internationally accepted rules and good practices regarding copyright and related rights are respected.

Accordingly, this work may be used under the license provided below.

If the user needs permission to make use of the work under conditions not provided for in the indicated licensing, they should contact the author through the RepositoriUM of Universidade do Minho.

***License granted to the users of this work***




**Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International**
**CC BY-NC-SA 4.0**

https://creativecommons.org/licenses/by-nc-sa/4.0/deed.en

# Acknowledgements

It's been a long time coming. This journey has been long and challenging, and, at times, I truly believed I wouldn't have made it to fruition.

Now, the dawn has finally come, and I have plenty to be thankful for and who to thank:

My mentors and supervisors, António Abelha, José Machado, and Manuel Filipe Santos, thank you for all the incredible continuous support, guidance, and wisdom. you paved the path to a whole generation of creative minds and are constantly treading the path of hard work, persistence, continuous curiosity, purpose and brilliance, each in your own way.

My friends and colleagues from KEG, AIDA and AR, thank you for continuously setting a higher bar for me to reach. Work is easier with fun, curious and brilliant minds like yours.

All my friends from all sorts of life, and I am fortunate enough to have them of extremely high quality: from Priorado, University (*Estagiários*), Consuwhales, Bruncheiros and all the amazing friends I earned through my loving wife. You make me live life and enjoy every moment of it. You make me more adventurous, curious, fun (and specially fat). Without this balance, I wouldn't have made it in any way.

My family: my mother, my father, my two brothers and two sisters (two of which in addition) and their beautiful sons; my In-laws and brothers–in–law; my close cousins by blood and affinity. With this brilliant support group, failure would be impossible. I owe you way more than I can ever repay. My appreciation for what you already accomplished and continuously do every day is immeasurable.

To my unconditional, Mariana. I honestly wouldn't have made it without you. You are a force of nature: smart, loving, kind, fun, and with a willpower like I have never seen. You are an endless source of energy with the biggest FOMO I have ever seen! You give everything you have to others, and more. You make me want more and do more, be better, and aim higher than I ever thought I could.

And finally, to my extraordinarily brilliant son, the source of my strength, Henrique. You gave me the motivation and the why. I look forward to every step you'll take and every moment we'll have. Everything I do is for you and, ultimately, yours.

## STATEMENT OF INTEGRITY

I hereby declare having conducted this academic work with integrity. I confirm that I have not used plagiarism or any form of undue use of information or falsification of results along the process leading to its elaboration.

I further declare that I have fully acknowledged the Code of Ethical Conduct of the Universidade do Minho.

_____, _____

(Place) (Date)

_____

(Tiago André Saraiva Guimarães)

”

*“I have no special talent.*
*I am only passionately curious.”*

**— Albert Einstein**, Letter to Carl Seelig, March 11, 1952
(Theoretical physicist)

# Resumo


## Melhorar a Veracidade e o Valor dos Dados em Fluxos de Dados Na Àrea da Saúde

Num cenário da saúde em rápida evolução, garantir a precisão, a segurança e a acessibilidade dos dados é fundamental. À medida que as instituições de saúde se esforçam por melhorar a qualidade clínica, reduzir custos e aumentar a segurança dos doentes, a gestão dos fluxos de dados de saúde surge como um desafio crítico. O volume e a complexidade dos dados de saúde disponíveis exigem soluções robustas para preservar a integridade dos dados e apoiar a tomada de decisões informadas.

Esta tese de doutoramento explora a integração de tecnologias emergentes como Blockchain e IoT para enfrentar os recorrentes desafios na gestão de dados de saúde. Foca-se principalmente no aumento da veracidade e do valor dos dados presentes nos sistemas de saúde. Esta tese investiga de que forma tecnologias emergentes podem ser aplicados em distintos ambientes na área da saúde através de uma série de contribuições.

A investigação está estruturada em quatro fases principais: uma extensa revisão da literatura para identificar as tendências e os desafios atuais na gestão de dados de saúde; uma revisão dos fluxos de dados hospitalares para identificar áreas vulneráveis a problemas de integridade de dados; uma avaliação das soluções adaptadas a estes desafios específicos; e o desenvolvimento e teste de protótipos para avaliar a eficácia destas soluções.

Esta investigação demonstra que tecnologias como Blockchain podem melhorar significativamente a segurança, a privacidade e a interoperabilidade dos dados de saúde, contribuindo assim para melhorar os cuidados prestados aos doentes e a eficiência do sistema. Por outro lado, o estudo também identifica potenciais limitações e desafios, incluindo questões de escalabilidade e sustentabilidade e a necessidade de uma integração perfeita com os padrões de saúde existentes. Esta tese contribui para o crescente conhecimento das aplicações de blockchain na área da saúde. Fornece estratégias relevantes para profissionais de saúde, legisladores, desenvolvedores e investigadores que procuram melhorar as práticas de gestão de dados na àrea da saude.



**Palavras-chave:** Blockchain; Cuidados de saúde; Fluxos de dados; Gestão de dados de cuidados de saúde; Interoperabilidade

# Abstract


## Improving Veracity and Value of Data in Healthcare Data Flows

With the continuous changes throughout the healthcare industry, ensuring the accuracy, security, and accessibility of data is paramount. With the continuing pressure to enhance clinical quality and patient safety while containing costs, managing healthcare data flows emerges as a critical challenge. The volume and complexity of healthcare data now available require robust solutions to preserve data integrity and support informed decision-making.

This doctoral thesis explores integrating emerging technologies like Blockchain and IoT to overcome the prevailing difficulties in managing healthcare information systems. It mainly focuses on improving the veracity and value of data within healthcare systems. This thesis examines how emerging technologies can be applied in different healthcare settings and environments through a series of contributions.

The research is structured into four main phases: an extensive literature review to identify current trends and challenges in healthcare data management; a review of hospital data flows to pinpoint areas vulnerable to data integrity issues; an evaluation of solutions tailored to these specific challenges; and the development and testing of prototypes to assess the effectiveness of these solutions.

This research reveals that technologies such as blockchain can greatly improve the security, privacy and interoperability of healthcare data and, therefore, help to enhance patient care and the technology's overall efficiency. On the other hand, research has also identified potential limitations and challenges, including scalability and sustainability issues and the need for seamless integration with existing healthcare standards. This thesis contributes to the growing knowledge of blockchain applications in healthcare. It provides relevant strategies for healthcare providers, policymakers, developers, and researchers seeking to improve health sector data management.



**Keywords:** Blockchain; Data Flows; Healthcare; Healthcare Data Management; Interoperability

# Contents

**List of Figures** **xii**

**List of Tables** **xiv**

**Acronyms** **xv**

## I Introduction 1

### 1 Introduction and Research Design 2

1.1 Background and Motivation . . . . . 3
1.2 Challenges in Healthcare Data Management . . . . . 3
1.3 Research Phases . . . . . 4
1.4 Research Questions and Objectives . . . . . 5
1.5 Thesis Structure . . . . . 7

## II Methodologies and Methods 8

### 2 Understanding Methodologies and Methods 9

2.1 Design Science Research (DSR) . . . . . 10
2.2 SWOT . . . . . 11

## III Literature Review 14

### 3 Healthcare Information Systems 15

3.1 Healthcare data flows . . . . . 16
3.2 Healthcare Data Management . . . . . 16

3.3 Interoperability . . . 17
3.4 Data Standards . . . 19
3.5 Data Repositories . . . 23
3.6 Internet of Things . . . 24

**4 Blockchain 28**
4.1 Privacy and Confidentiality . . . 29
4.2 Consensus Algorithms . . . 30
4.3 Smart Contracts and Chaincodes . . . 32
4.4 Blockchain-related concepts, tools and technologies . . . 32
4.5 Blockchain Analytics . . . 39
4.6 Blockchain for Healthcare Data Management . . . 40

**IV Contributions 45**

**5 Understanding the contributions 46**

**6 C1 - Context-aware electronic health record-an IoT and blockchain approach 49**
6.1 Introduction . . . 49
6.2 Research Methodology . . . 50
6.3 Objectives . . . 50
6.4 Design and Development . . . 51
6.5 Experimentation . . . 58
6.6 Discussion . . . 61
6.7 Related Work . . . 62
6.8 Summarize . . . 63

**7 C2 - Blockchain Analytics - Real-time Log Management in Healthcare 64**
7.1 Introduction . . . 64
7.2 Objectives . . . 65
7.3 Design and Development . . . 65
7.4 Summarize . . . 68

**8 C3 - Leveraging Standardized Real-Time Data Repositories and Blockchain to Enhance an AI-driven Healthcare Decisions 70**
8.1 Introduction . . . 71
8.2 Research Methodology . . . 73
8.3 Objectives . . . 74
8.4 Proposed Model . . . 74

8.5 Summarize . . . 79

**9 C4 - The Role of Blockchain Technology in Ensuring Security and Immutability of Open Data in Healthcare 81**

9.1 Why openEHR with blockchain in healthcare? . . . 82
9.2 Objectives . . . 83
9.3 Architecture . . . 83
9.4 Results and Discussion . . . 85
9.5 Summarize . . . 87

**10 C5 - IPFS and Hyperledger Fabric: Integrity of Data in Healthcare 89**

10.1 Introduction . . . 89
10.2 Related Works . . . 90
10.3 Objectives . . . 91
10.4 Architecture . . . 92
10.5 Discussion . . . 96
10.6 Summarize . . . 97

**11 C6 - Decentralized Healthcare Marketplace 98**

11.1 Introduction . . . 98
11.2 Objectives . . . 99
11.3 Decentralized Clinical Data-sharing Platform . . . 99
11.4 Summarize . . . 102

**12 C7 - Scalable and Sustainable Blockchain: Architecting Infrastructure and Developing a Platform for Efficient Management and Exploration 104**

12.1 Introduction . . . 104
12.2 Infrastructure Architectures . . . 105
12.3 Evaluation . . . 107
12.4 Discussion . . . 109
12.5 Platform for Efficient Blockchain Management and Exploration . . . 111
12.6 Summarize . . . 120

**V Conclusion and Final Remarks 122**

**13 Improve the Veracity and Value of Healthcare Data Flows 123**

13.1 Overview of the Research . . . 124
13.2 Future Directions . . . 126

**Bibliography** **128**

# List of Figures


1 Main Research Methodology: Design Science Research. Adapted from: (Hevner et al., 2004). . . . . 10

2 Pyramid of Interoperability, adapted from (IMPRIVATA, 2019) . . . . . 18

3 Example Health Level Seven International (HL7) message - ADT A04 . Adapted from (HL7International, 2022). . . . . 20

4 Blockchain process of Validation . . . . . 29

5 Context-Aware EHR - Communication between entities – Phase A . . . . . 53

6 Simulated Hospital Floor Plan with Bluetooth Beacons . . . . . 53

7 Context-Aware EHR - Architecture – Phase B . . . . . 54

8 Context-Aware Electronic Health Record (EHR) - Mobile Application Screens . . . . . 55

9 Context-Aware EHR - Architecture – Phase C . . . . . 56

10 API call to Create Medical Device in the Blockchain . . . . . 58

11 Blockchain Performance Metrics (10k Transactions per function) . . . . . 59

12 Blockchain Performance Metrics (1k Transactions per function) . . . . . 59

13 Blockchain Benchmarking - Average Send Rate vs. Throughput . . . . . 60

14 Blockchain Benchmarking - Average Failed Transactions . . . . . 60

15 Blockchain Benchmarking - Latencies . . . . . 61

16 Real-time Log Management - Architecture . . . . . 67

17 Real-time Log Management - Log Data Consult . . . . . 68

18 Real-time Log Management - Log Data Analysis . . . . . 68

19 Main Research Methodology: Design Science Research. Adapted from: (Hevner et al., 2004). . . . . 73

20 Proposed Architecture for the Real-time Data Repository . . . . . 75

21 Blockchain Technology and Open Data - First Scenario . . . . . 84

22 Blockchain Technology and Open Data - Second Scenario . . . . . 84

23 InterPlanetary File System (IPFS) and Hyperledger Fabric - Layered Architecture . . . . . 92
24 Master Node . . . . . 93
25 IPFS and Hyperledger Fabric: Network design . . . . . 94

26 Scalable and Sustainable Blockchain - Proposed Architecture 1 - Docker . . . . . 105
27 Scalable and Sustainable Blockchain - Proposed Architecture 2 - Kubernetes . . . . . 106
28 Scalable and Sustainable Blockchain - Proposed Architecture 3 - Kubernetes with Load Balancer . . . . . 106
29 Scalable and Sustainable Blockchain - Performance metrics - Architecture 1 . . . . . 108
30 Scalable and Sustainable Blockchain - Performance metrics - Architecture 2 and 3 . . . 109
31 Chosen Architecture - Kubernetes with Load Balancer . . . . . 111
32 Block Explorer - Dashboard . . . . . 112
33 Block Explorer - Network . . . . . 113
34 Block Explorer - Blocks . . . . . 113
35 Block Explorer - Transactions . . . . . 114
36 Block Explorer - Chaincodes . . . . . 114
37 Block Explorer - Channels . . . . . 115
38 General Network Overview - Dashboard . . . . . 115
39 General Network Overview - Resources . . . . . 116
40 General Network Overview - Network Visualization . . . . . 116
41 Peer Config - Upload Configs . . . . . 117
42 Peer Config - Fetch Channels . . . . . 117
43 Peer Config - Install Chaincode . . . . . 118
44 Peer Config - Custom Commands . . . . . 118
45 Orderer Config - Creating Channel . . . . . 119
46 Orderer Config - Query Channel . . . . . 119
47 Orderer Config - Custom commands . . . . . 120

# List of Tables


1 DSR Focus and Research Phases . . . . . 11

2 Contributions Overview . . . . . 46

3 Cross-Reference Table Between Contributions and Research Questions . . . . . 47

4 Smart contract functions and Application Programming Interfaces (API) . . . . . 57

5 Blockchain Technology and Open Data - Analise between two Scenarios . . . . . 86

6 Blockchain Technology and Open Data - Additional tests for Scenario 2 . . . . . 87

7 SWOT Analysis . . . . . 96

8 Max/peak values of Performance metrics . . . . . 109

9 Characteristics Comparison between Docker and Kubernetes . . . . . 110

# Acronyms

**AI** Artificial Antelligence *(pp. 16, 42, 43, 71, 126, 127)*
**AM** Archetype Model *(pp. 22, 23)*
**ANSI** American National Standards Institute *(p. 19)*
**AP** Access Point *(p. 26)*
**API** Application Programming Interfaces *(pp. xiv, 21, 56–58, 72, 75, 78, 79, 83, 84, 92, 110, 111, 120)*

**BA** Blockchain Analytics *(p. 126)*
**BI** Business Intelligence *(pp. 24, 88)*
**BLE** Bluetooth low-energy *(pp. 26, 27, 52)*

**CA** Certificate Authority *(pp. 36, 92, 94, 117)*
**CDA** Clinical Document Architecture *(pp. 20, 21)*
**CKM** Clinical Knowledge Management *(p. 23)*
**CRUD** Creating, Reading, Updating, or Deleting *(p. 96)*

**DAOs** Decentralized Autonomous Organizations *(pp. 32, 34)*
**DApps** Decentralized Applications *(p. 32)*
**DeFi** Decentralized finance *(pp. 32–34, 98, 100)*
**DLT** Distributed Ledger Technology *(pp. 33, 35)*
**DSR** Design Science Research *(pp. 9–11, 50, 73)*

**ECG** Electrocardiogram *(p. 25)*
**EHR** Electronic Health Record *(pp. xii, 15, 16, 22, 23, 41, 46, 49–52, 54, 55, 61, 63, 71, 76, 81–83, 91)*
**ETL** Extract, Transform, and Load *(pp. 88, 126)*

**FAIR** Findability, Accessibility, Interoperability, and Reuse *(pp. 19, 22, 70–72, 79)*

**FHIR** Fast Healthcare Interoperability Resources *(pp. 6, 19–21, 73, 76, 80, 125)*

**GDPR** General Data Protection Regulation *(p. 103)*

**HDM** Healthcare Data Management *(pp. 16, 17)*
**HIMSS** Healthcare Information and Management Systems Society *(pp. 17, 18)*
**HISs** Healthcare Information Systems *(pp. 15, 16, 18)*
**HL7** Health Level Seven International *(pp. xii, 6, 19–21, 73–76, 79, 80, 124, 125)*
**HLF** Hyperledger Fabric *(pp. 35, 55, 95, 97, 121)*
**HSSP** Healthcare Services Specification Project *(p. 20)*

**ICD** International Classification of Diseases *(pp. 19, 21, 72, 79, 80)*
**IoT** Internet of Things *(pp. 3, 6, 15, 16, 24, 25, 43, 46, 62, 76, 89, 123, 125)*
**IPFS** InterPlanetary File System *(pp. xiii, 34, 35, 46, 89–95, 97, 100, 125)*
**IS** Information Systems *(pp. 50, 73)*
**IT** Information Technology *(pp. 73, 82, 83)*

**JWT** JSON Web Token *(p. 78)*

**ML** Machine Learning *(p. 71)*

**NFTs** Non-fungible Tokens *(pp. 32–34, 98–101)*

**pBFT** Practical Byzantine Fault Tolerance *(p. 31)*
**PDR** Pedestrian Dead Reckoning *(p. 26)*
**PoS** Proof of Stake *(p. 31)*
**PoW** Proof of Work *(p. 31)*

**REST** Representational State Transfer *(pp. 21, 72)*
**RIM** Reference Information Model *(p. 20)*
**RM** Reference Model *(pp. 22, 23)*

**SWOT** Strengths, Weaknesses, Opportunities, and Threats *(pp. 11–13, 61, 82, 87, 89, 96)*

**TPS** Transactions per Second *(pp. 58–61, 85, 107)*

**WHO** World Health Organization *(pp. 21, 76)*

# Part I

# Introduction and Research Design

# 1

# Introduction and Research Design

Healthcare institutions are constantly being defied to improve clinical quality of care and patient safety, lower costs, reduce medical errors and provide more patient-centred service and evidence-based practice. Misallocation of resources and unsupported decision-making can quickly reduce the quality of care, and the evidence for this is sharply increasing (Strome & Liefer, 2013).

The constant flow of new data accumulating at unprecedented rates presents significant challenges in analyses and subsequent applications to a practical clinical environment. (Sun & Reddy, 2013) Just as the enormity and complexity of data collected and stored has changed, so too has the velocity at which it is generated, which is necessary for retrieving, analyzing, comparing and making decisions based on the output.

Resolute by binding requirements and the potential to improve the quality of healthcare delivery while reducing costs, these large amounts of heterogeneous medical data, available in various healthcare organizations (payers, providers, exams, reports, pharmaceuticals), hold the promise of supporting a wide range of medical and healthcare functions, including clinical decision support, disease surveillance, and population health management, enabling resource for deriving insights for improving care delivery and reducing waste. (Raghupathi & Raghupathi, 2014)

Furthermore, prior to the effective utilization of available information for enhancing healthcare towards more preventive, predictive, and personalized models, thus yielding improved patient outcomes, the fundamental necessity lies in developing more robust and secure data storage and exchange methods.

Adopting blockchain-based systems emerges as a viable solution for addressing these growing challenges. By their inherent design, such systems maintain a permanent and tamper-resistant ledger of transactional data, thereby rendering the data immutable. This characteristic ensures that the data cannot be altered or corrupted.

The research is in accordance with the particular needs and challenges identified in collaboration with the Hospital de Santo António in Porto. This hospital has been a pioneer in deploying cutting-edge technologies and open standards for the advancement of healthcare data management and interoperability. As a result of this collaboration, it was possible to discuss the solutions with healthcare professionals, from IT to practitioners, and implement and test or plan the developed solutions, frameworks, and architectures

in real-world healthcare scenarios.

## 1.1 Background and Motivation

The efficient management of healthcare data is critical in delivering healthcare services, as it helps preserve the validity, safety, and accessibility of patient information to offer the best healthcare possible. Recently, blockchain technology has emerged as an effective tool for solving these challenges due to its ability to advance, enhance, and optimise healthcare information management.

This thesis seeks to explore and establish ways emerging technologies such as blockchain or Internet of Things (IoT) can or could be used within healthcare to address some of its important gaps and needs, supporting such demands with real-life use cases.

Healthcare information systems demand improvement and change, specifically data management, as a response to changing necessities and existing and/or emerging problems. This section discusses the general background and motivation of the work and provides information on how the research was structured and the core research questions.

This thesis presents, analyses and discusses seven distinct contributions, each detailing a solution, framework, or architecture to improve healthcare data flow, enhance data value and integrity, and ultimately ensure better patient care. These explore how emerging technologies and methodologies can assert greater patient data ownership, enable more informed decision-making, and provide better conditions for medical research. They tackle relevant aspects of data management to reduce the delivery cost and enhance efficiency, improving patient care and the healthcare system.

## 1.2 Challenges in Healthcare Data Management

Hospital inpatient care relies on constant monitoring and reliable real-time data. There is a need for continuous improvement, adaptability, and integration of state-of-the-art technologies, which are critical for improving efficiency, productivity, and readiness; however, the challenges in healthcare data management are evident. Some of those challenges are presented below:

- Data Veracity and Integrity: Safeguarding confidential patient information from unauthorized access and breaches is paramount.
- Data Security and Privacy: Protecting sensitive patient information from unauthorized access and breaches is paramount.
- Interoperability: Many distinct distributed Healthcare information systems from different vendors, where data can be found in various file formats and databases, creating numerous islands of information and often resulting in severe data interoperability problems.

- Real-Time Data: Real-time data is essential for efficient and optimal diagnosis and patient treatment. Healthcare workers should have real-time data to make informed judgments and actions.

Blockchain technology has tremendous potential in healthcare because of the sensitive nature of data being processed and managed. It ensures that the information is tamper-proof and cannot be altered in any way, that healthcare data can be securely and immutably stored, and that data accessibility and real-time updates are guaranteed. Blockchain technology research and employment in healthcare are increasing. Current trends in blockchain research in healthcare indicate that it is mainly used for data sharing, health records, and access control but rarely for other scenarios, such as supply chain or drug prescription management. Therefore, the potential for blockchain is still unexploited (Hölbl et al., 2018a).

This thesis is driven by the critical need to address healthcare data management difficulties by studying the integration of emerging technologies. By combining insights from real-world use cases and research topics, this study seeks to understand their possible benefits, limitations, and considerations in healthcare settings. It also aims to contribute to advancing healthcare data management practices, ensuring the highest standards of data veracity, integrity, and security in patient care.

## 1.3 Research Phases

The thesis is divided into research phases that align closely to the major research objectives.

### Phase A - Bibliographic Revision of the State-of-Art

Phase A entails conducting exhaustive literature research to acquire insight into the present state of healthcare data management. This phase identifies the sector's difficulties, trends, constraints, and current frameworks, providing basic knowledge for later phases.

### Phase B - Review processes in a hospital environment and identify flows that can benefit from the results of the work

Phase B focuses on examining processes within hospital environments and identifying data flows vulnerable to issues of accuracy and integrity. The research explores how blockchain technology can address these challenges, taking into account the requirements of healthcare professionals.

### Phase C - Research on Alternative and Emergent Solutions and Frameworks

In phase C, various blockchain solutions and frameworks are evaluated to determine their suitability for ensuring data accuracy and integrity. This phase also considers the trade-offs between permissioned and permissionless blockchain implementations and explores the integration of data standards like FHIR, HL7, and OpenEHR with blockchain for improved healthcare data flows.

### Phase D - Experimental Setting and Prototypes

Phase D involves practical experimentation, including analyzing metrics for evaluating blockchain implementations and creating prototypes to simulate their impact. This phase assesses the benefits and drawbacks of selected blockchain solutions and their effects on data sharing, privacy, security, scalability, and sustainability.

The above research phases provide a structured approach to understanding the issues related to managing healthcare data. These stages align with the core and specific research goals, striving to continuously improve healthcare services and patient care.

## 1.4 Research Questions and Objectives

The main Research Question is:

**How to improve the veracity and value of healthcare data flows?**

Several objectives and subsequent RQs were formulated for each phase to help define the research topics. These objectives and questions are key in the research as they help organize and present the work and, therefore, hope to enhance the Veracity and Value of healthcare data flows.

### Phase A: Bibliographic Revision of the State-of-Art

**Objective A1:** Recognize the existing practices and standards in healthcare data management, followed by their data integrity, security, and interoperability challenges.

A1-R1: What are the current challenges and trends in managing healthcare data to improve the value and integrity of electronic health records?

**Objective A2:** Explore emerging information technologies that could help advance healthcare data flows, leading to enhanced patient outcomes.

A2-R2: What emerging approaches and technologies have the potential to enhance the quality, security and privacy concerns of healthcare data flows?

A2-R3: What is known about these technologies, and how does each of them apply to different scenarios in the healthcare sector?

A2-R4: What does the recent literature review state regarding the limitations and challenges of these technologies within healthcare?

## Phase B: Review processes in a hospital environment and identify flows that can benefit from the results of the work

**Objective B1:** Review hospital data management processes to recognize those at risk against integrity and security.

B1-R1: Which hospital data management processes are the most vulnerable to integrity threats?

B1-R2: How will technology assist in specific healthcare data management tasks and patient care challenges?

**Objective B2:** Identify key areas where technology can enhance decision-making, reduce medical errors, and improve data sharing for research purposes while ensuring patient privacy and compliance with regulations.

B2-R3: How can healthcare systems promote decision-making processes and reduce medical errors?

B2-R4: How can medical data be shared more effectively for research benefit, and what measures are necessary to promote the patient's willingness to share or provide such information?

## Phase C: Research on Alternative and Emergent Solutions and Frameworks

**Objective C1:** Compare and evaluate blockchain frameworks and other emergent technologies to establish their effectiveness in enhancing the value and integrity of healthcare data.

C1-R1: What are the most suitable blockchain solutions and frameworks to cover the needs of data integrity and veracity identified in phase B?

C1-R2: What are the trade-offs across different blockchain architectures regarding data accessibility, security, privacy and resource concerns?

C1-R3: How can blockchain, IoT or other implementations be tailored to specific processes identified in phase B to improve data management in healthcare?

C1-R4: What technologies, systems and approaches can complement existing healthcare management systems and enhance patient ownership and control of their health data?

**Objective C2:** Describe how healthcare data standards such as Fast Healthcare Interoperability Resources (FHIR), HL7 or OpenEHR can be combined with blockchain technology.

C2-R5: How can current data standards for interoperability and storage (FHIR, HL7 and OpenEHR) be effectively integrated with blockchain?

C2-R6: What possible risks and limitations must still be addressed concerning the use of a blockchain within healthcare data standards?

### Phase D: Experimental Setting and Prototypes

**Objective D1:** Study prototypes that simulate how the integration of emergent technologies such as blockchain can impact healthcare data flows.

D1-R1: How can prototypes be developed to simulate and assess the impact of blockchain integration on identified data flows in Phase B?

D1-R2: What real-world problems may prevent the implementation of decentralized data storage systems in clinic practices?

D1-R3: How do the chosen solutions impact data sharing, privacy, and security in the experimental healthcare setting?

**Objective D2:** Test the performance of such prototypes using relevant performance metrics to assess their scalability and sustainability in the long term.

D2-R4: What are the most relevant metrics and criteria that can stand in for evaluating the performance and impact of blockchain implementations in healthcare?

D2-R5: How can healthcare data management solutions and their scalability and long-term sustainability be effectively ascertained in an experimental environment?

## 1.5 Thesis Structure

This section sets forth to design and explore emergent technologies such as IoT and blockchain in the context of healthcare data management. The chapter also reviews in detail why the study was undertaken, the methods used, and the available literature in the field that forms the basis of the study. This includes exploring data in healthcare, its challenges, such as lack of interoperability, and its opportunities, such as the integration of data standards and emergent technologies.

This thesis presents several contributions that depict how the veracity and value of data can be supported in varying areas of healthcare. These contributions explore different aspects, from how to store and analyse Electronic Health Records to the real-time management of logs, addressing the practical issues and barriers related to the application of various technologies in many healthcare fields.

Finally, it summarises the work, starting with an overview of the research, the identified trends and patterns throughout the contributions and guidance on future work, suggesting directions for future research in this rapidly evolving domain.

# Part II

# Methodologies and Methods

# 2

# Understanding Methodologies and Methods

Research methodologies encompass the various strategies, techniques, and processes researchers use to conduct investigations and explore complex issues systematically and scientifically. These methodologies provide the frameworks that guide the entire research process, including gathering, analysing, and interpreting data. The choice of methodology significantly impacts the research findings' reliability, validity, and generalizability.

Broadly, research methodologies fall into two primary categories: qualitative and quantitative. Qualitative methodologies focus on understanding human behaviour and the reasons that govern such behaviour. They emphasize subjective assessment of attitudes, opinions, and behaviour. In contrast, quantitative methodologies seek to quantify the problem by generating numerical data or data that can be transformed into usable statistics.

Furthermore, mixed-methods research incorporates qualitative and quantitative research approaches for broader analysis. Each of these methodologies has tools and techniques, including surveys, interviews, case studies, and many others, depending on the research question and objectives.

The choice of a research methodology is driven by the research question, the researcher's philosophical orientation, and the research's practicalities. Researchers must understand the strengths and limitations of each methodology to choose the most appropriate approach for their research objectives.

In summary, case Study Methodology encompass the broader framework or approach that guides the entire research process, including the underlying philosophy, strategies, and rationale behind the choice of research methods. Methodology shapes the study's overall design, defining how research questions are formulated, how data is interpreted, and how results are validated.

## Description of the Methodologies and Methods

The pursuit of knowledge is not just about finding answers but about asking the right questions and choosing the appropriate methodologies to explore them. This chapter delves into a pivotal research methodology that have shaped contemporary research in healthcare information systems: Design Science Research (DSR); also, a research Method: SWOT analysis.

## 2.1 Design Science Research (DSR)

DSR is a methodological framework utilized predominantly within information systems, software engineering, and technology development. Its primary aim is to address complex issues by conceiving and scrutinizing innovative artifacts. DSR distinguishes itself by a purpose-driven approach to research, focusing on developing pragmatic solutions tailored to specific, tangible challenges.

DSR is underpinned by a solid theoretical foundation, leveraging existing theories, models, and empirical findings to guide the development process. This ensures that the artifacts contribute significantly to the advancement of theory and have practical applications. The methodology's core lies in its iterative and cyclical research process, emphasizing continuous refinement and adaptation. This process initiates with the precise identification of a problem, followed by the articulation of the solution's objectives. The design and development phase then brings the conceptualized artifact into being.

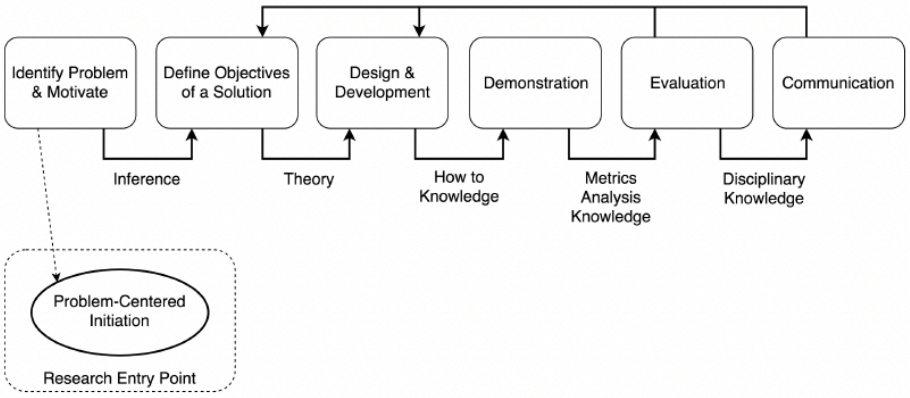



Figure 1: Main Research Methodology: Design Science Research. Adapted from: (Hevner et al., 2004).

1. **Problem Identification and Motivation:** Clearly delineate the problem to be addressed.
2. **Define Objectives for a Solution:** Define what the artifact aims to achieve.
3. **Design and Development:** The phase where the artifact is conceptualized and created.
4. **Demonstration:** Showcasing the artifact in a scenario where it solves the identified problem.
5. **Evaluation:** Rigorously assessing the artifact's effectiveness and efficiency in solving the problem.
6. **Communication:** Documenting and sharing the research findings with both the academic and practitioner communities.

DSR results in the creation of various artifacts, including constructs (conceptual vocabularies and symbols), models (system representations or blueprints), methods (algorithms and processes), and instantiations (real-world applications demonstrating feasibility and utility).

Those artifacts are rigorously demonstrated and evaluated for utility, quality, and efficacy. The methodology seeks a balance between innovation, rigor, and relevance, facing challenges in ensuring artifact generalizability and integrating multidisciplinary perspectives.

DSR contributes to theoretical advancements by extending or creating new theories and models. Practically, it offers innovative solutions to real-world problems. Methodologically, it introduces new methods or approaches for conducting research. As technological and societal needs evolve, DSR remains a pivotal and dynamic methodology for fostering innovation and addressing contemporary challenges.

## Research Process

Each methodology, with its unique focus and application, contributes significantly to the advancement of knowledge across disciplines. The choice of methodology ultimately depends on the research questions, objectives, and the specific context of the study. As the landscape of research evolves, these methodologies will continue to play a pivotal role in fostering innovation, strategic decision-making, and a deeper understanding of complex phenomena.

DSR guided the overall structure of the research, from problem identification to Demonstration and Evaluation.

| **DSR Focus** | **Research Phases** |
|---|---|
| Problem Identification and Motivation: Literature review to identify challenges and gaps in healthcare data management. | Phase A: Bibliographic Revision of the State-of-the-Art |
| Define Objectives for a Solution: Focus on specific hospital data management processes and identifying key problem areas. | Phase B: Review Processes in a Hospital Environment and Identify Beneficial Flows |
| Design and Development: Development of blockchain systems, frameworks, and data models to address identified issues. | Phase C: Research on Different Solutions and Frameworks |
| Demonstration and Evaluation: Assess solutions in real-world environments and collecting data for iterative refinement. | Phase D: Experimental Setting and Prototypes |

Table 1: DSR Focus and Research Phases

## 2.2 SWOT

Strengths, Weaknesses, Opportunities, and Threats (SWOT) Analysis is a comprehensive framework employed to evaluate the strategic position of a business entity or project. It facilitates the identification of internal and external factors that are favorable and unfavorable to achieving an objective.

It is instrumental in strategic planning, offering insights that aid in decision-making processes for businesses, projects, and personal career planning. By assessing both internal and external environments, stakeholders can formulate strategies that leverage strengths, mitigate weaknesses, capitalize on opportunities, and defend against threats.

## Components of SWOT Analysis

1. **Strengths:** Attributes of the organization that are helpful to achieving the objective. These are internal factors that include resources, capabilities, and positive situational aspects.

2. **Weaknesses:** Attributes of the organization that are harmful to achieving the objective. These are internal factors that include deficiencies in resources, capabilities, and negative situational aspects.

3. **Opportunities:** External conditions that are favorable to achieving the objective. These include trends, market dynamics, and external factors that can be exploited.

4. **Threats:** External conditions that could damage the business's performance. These include environmental challenges, competitors, and adverse market dynamics.

## Conducting a SWOT Analysis

To effectively conduct a SWOT Analysis, the process typically involves several key steps:

1. Gather a diverse team to ensure multiple perspectives.

2. Define the objective clearly to focus the analysis.

3. Identify and list the strengths, weaknesses, opportunities, and threats relevant to the objective.

4. Analyze and prioritize the SWOT factors in terms of their potential impact on the objective.

5. Develop strategic actions that leverage strengths and opportunities, address weaknesses, and mitigate threats.

SWOT Analysis is widely applied in strategic planning, marketing, competitive analysis, and personal career development. While it provides valuable insights, its effectiveness can be limited by factors such as biases in the assessment process, the dynamic nature of business environments, and the complexity of external factors.

## Research Process

In this thesis, the SWOT analysis has been used throughout the case studies to evaluate the proposed solutions, frameworks, and architectures in a more organized and succinct way. Using SWOT in the study helped the researchers present the advantages of the solutions and uncover areas that needed improvement. It helped to identify opportunities for broader application of the solutions in the healthcare system and the associated threats, which made it possible to comprehend the practical implications of the solutions more deeply.

# Part III

# Literature Review

# 3

# Healthcare Information Systems

Healthcare Information Systems (HISs) are crucial in modern healthcare and refer to systems that are used to process data, information, and knowledge in healthcare environments, enabling the management, processing, and sharing of medical data within and across healthcare organizations. They were developed to increase the efficiency and effectiveness of healthcare delivery, ensuring that patient data is accurately recorded, securely stored, and readily accessible to Healthcare workers. The incorporation of HISs into healthcare practices was implemented to enhance patient outcomes, optimize administrative procedures, allow research feasibility, and facilitate decision-making across all levels of care. (Ngafeeson, 2015)

HISs plays a vital role in the advancement of digital health innovation projects in hospitals since it offers the required support for managing EHRs and other digital data. Strong leadership and the involvement of top management are crucial to encourage widespread adoption and usage of these systems. They are usually more reliant on first addressing organizational and environmental challenges than technology to ensure their effective use in diverse healthcare settings.

The health industry has become more complex and has increasingly newer needs, which, throughout the years, has led to the creation of multiple systems and platforms, each with multiple data formats and standards tailored to them without any standardization. (Cuevas-González et al., 2022)

One of the main challenges this frenetic growth generated within HISs is interoperability. The lack of interoperability between health information systems reduces patient care quality and wastes resources. Accordingly, there is an urgent need to develop and implement integration mechanisms, such as data standards, to ensure integration and operational efficiency between the diverse HISs (Canova-Barrios & Machuca-Contreras, 2022; Torab-Miandoab et al., 2023).

Security and privacy while exchanging biomedical and healthcare information are also recurring themes and new approaches are being studied and implemented to ensure it, like blockchain technology (Soni & Singh, 2021). This technology is being rapidly adopted across multiple healthcare sectors to address data trust, traceability, and immutability issues.

Real-time transactional and monitoring data is also a recurring trend in HISs, allowing an increase in medical response and consequently improving patient care and diagnostics. To that, IoT has had a revolutionary impact on many facets of the healthcare industry, allowing for distinct solutions in different

areas to be developed with significant impact (Arunsankar et al., 2023; Robinson et al., 2021).

## 3.1 Healthcare data flows

Healthcare data flows refer to the transferring or sharing of all the data within HISs, from patient information and clinical data to other relevant data across various systems, departments, and organizations. Effective management of these data flows is vital to ensuring continuity of care. This leads to enhanced patient outcomes, optimization of operational efficiency, and reduction of costs.

In modern healthcare settings, data flows encompass a wide range of activities, including sharing EHRs, real-time patient monitoring, and advanced analytics for decision support. (Blanken et al., 2022; Silan et al., 2020).

Proactive risk management of healthcare data is essential and can only be achieved by adequately structuring and handling data flows. This will enable healthcare providers to anticipate and mitigate potential issues before they could impact patient care delivery.

Technologies like Blockchain, IoT and Artificial Antelligence (AI) are bridging this gap by aiming to improve healthcare data flows' security, trust, value, efficiency, and scalability. This offers promising solutions that balance valuable data access and communication, and data protection (Jadon & Kumar, 2023; Misra et al., 2023).

Healthcare data flows are a critical component of the healthcare information system, underpinning the ability to deliver high-quality, patient-centered care while meeting the demands of an increasingly data-driven healthcare landscape. (Meshkov et al., 2020; Vezyridis & Timmons, 2017).

## 3.2 Healthcare Data Management

Healthcare Data Management (HDM) is the comprehensive and systematic approach to managing health-related data. It encompasses collecting, storing, organising, analysing, and sharing data generated by healthcare providers, patients, and health systems. The primary objective of HDM is to ensure that accurate and timely information is available to support clinical decision-making, enhance patient care, and improve operational efficiency.

Healthcare data can include a variety of data types, such as:

- **EHRs**: Data generated by one or more encounters in any care delivery setting. This information includes patient demographics, progress notes, problems, medications, vital signs, past medical history, immunizations, laboratory data, and radiology reports. The EHR automates and streamlines the clinician's workflow (Seymour et al., 2012);
- **Administrative Data**: Data collected for administrative tasks like scheduling and communication with patients and billing purposes (Vardasca & Martins, 2011);

- **Health/Patient Surveys**: Data collected from patients or healthcare workers concerning their experience, quality of service, health status, current diseases and outcomes (Anhang Price et al., 2014; McHorney & Tarlov, 1995);

- **Clinical Trials Data**: Data collected to test the efficacy of a specific treatment or intervention in a group of patients/subjects. It can involve one or multiple clinical centres (McFadden, 2007).

The key processes in HDM include data extraction and collection from multiple data sources, data organization and storage, data analysis and sharing. Each of these processes is essential for an efficient HDM that aims to improve the support for clinical practice, patient care, and operational efficiency within healthcare organizations.

A well-designed and implemented HDM ensures data quality, reliability, and availability, which ultimately enhances operational Efficiency, support for research and innovation, and cost reduction, which can be materialized in better decision-making and improved patient care.

The following sections provide a closer examination of several crucial aspects of healthcare data management. It begins with the concept of interoperability, emphasizing its significance and the challenges of achieving seamless data exchange across diverse healthcare systems. This is followed by an exploration of **data standards**, highlighting essential frameworks and protocols for accurately and securely managing healthcare data. The final section addresses **data repositories**, focusing on the different types used for storing and managing healthcare data and their importance in facilitating efficient data retrieval and analysis. These sections collectively offer a comprehensive overview of the critical components of effective healthcare data management.

## 3.3 Interoperability

Several definitions for Interoperability in healthcare can be found in the literature. Gathering and somewhat merging the definitions by IBM, in (IBM, 2024), and by the Healthcare Information and Management Systems Society (HIMSS), in (HIMSS, 2024), different information systems, devices and applications/systems essentially can access, exchange, integrate and cooperatively use data in a coordinated manner, to provide timely and seamless portability of information so that it can be used to optimize health outcomes for individuals and populations. Adding to the definition, IBM, in (IBM, 2022), also stated that "Lack of interoperability can lead to an insufficient picture of the health needs of an individual or population, which can result in lower outcomes and higher costs."

Interoperability in healthcare is essential since it allows for seamless data exchange of health information without compromising the patient's privacy and security. It has the potential to reduce medical errors, improve collaboration between healthcare providers, reduce the cost of healthcare, and dramatically improve the delivery and quality of healthcare.

The constant growth of HISs has generated an enormous amount of information relating to the diagnosis, testing, monitoring, treatment and health management of patients, billing for healthcare services and asset management of healthcare resources. This information is likely generated by heterogeneous distributed HISs in different file formats and databases, creating numerous islands of information and often resulting in severe data interoperability problems. This information needs to interact and be accessed by healthcare practitioners uniformly, as required by the patient's treatment path. Healthcare providers must exchange information, such as clinical notes, observations, laboratory tests, diagnostic imaging reports, treatments, therapies, drugs administered, allergies and letters, x-rays, and bills (d'Aliberti & Clark, 2022; Iroju et al., 2013).

Numerous solutions have been proposed to achieve total interoperability in healthcare with degrees of success. These include the use of standards, archetypes, web services, a healthcare service bus, interface engines, and ontologies (Ryan, 2006).

In (HIMSS, 2024), HIMSS divides interoperability into four components:

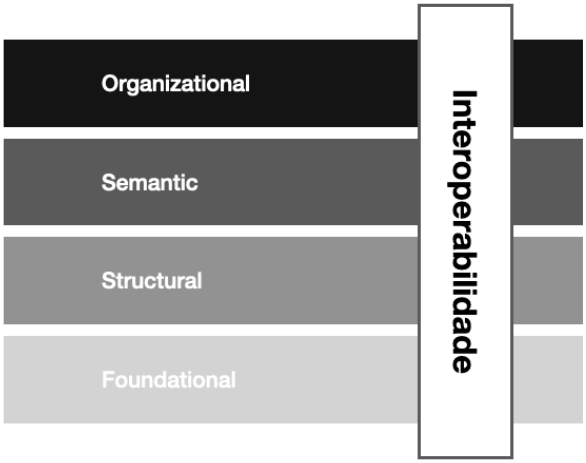



Figure 2: Pyramid of Interoperability, adapted from (IMPRIVATA, 2019)

**Foundational interoperability (Level 1) :** Defines the essential requirements for one system or application to exchange data with and receive data from another securely. It does not require the receiving technology to interpret the data.

**Structural interoperability (Level 2) :** Defines the structure, syntax and organization of data exchange, including the interpretation of individual data elements.

**Semantic interoperability (Level 3) :** Provides for common underlying models and codification of the data, including using data elements with standardized definitions from publicly available value sets and coding vocabularies. By creating a common vocabulary for accurate and reliable system communication, this fosters a shared understanding and meaning for the user.

**Organizational interoperability (Level 4):** This is the newest proposed tier. It includes governance, policy, social, legal, and organizational factors to promote secure, seamless, and timely data communication and use both within and between organizations, entities, and individuals. HIMSS, justified

the addition of the 4th level of interoperability to facilitate the establishment of shared consent, trust, and seamless integration of processes and workflows for end-users.

Interoperability benefits include improved care coordination, enhanced performance through data analysis, and better overall experiences for healthcare professionals and patients. It enables healthcare entities to work together, access comprehensive patient information, make data-driven improvements, and streamline administrative processes, ultimately contributing to better healthcare delivery and outcomes.

## 3.4 Data Standards

Data standards play a fundamental role in the contemporary health informatics ecosystem. They were created to ensure that all parties involved in a given process take the same approach to developing, sharing, storing, or interpreting data. They aim to establish an efficient, accurate, and secure exchange of medical information across various healthcare systems and platforms. They form the basis for implementing interoperability. (Richesson & Krischer, 2007; Schulz et al., 2019).

The primary objective of healthcare data standards is to ensure that medical information is consistent and interpretable by different systems. Health systems must be able to exchange medical data regardless of the software domain or vendor. This standardization is essential, from clinical decision-making and healthcare delivery to research and public health monitoring. Healthcare data standards comprise formats for structuring data, terminologies for describing clinical conditions and treatments, and protocols for secure data exchange.

HL7, International Classification of Diseases (ICD), FHIR, and openEHR are some examples of healthcare data standards currently used in Healthcare institutions.

Contributions presented in this thesis relied on or used some of the standards presented in the following subsections: HL7 and FHIR for interoperability (exchange of messages) between the different partners; ICD-10 for disease diagnosis/classification, Findability, Accessibility, Interoperability, and Reuse (FAIR) for providing and updating the data and openEHR.

### Health Level Seven International (HL7)

HL7 is a standards-setting not-for-profit organization accredited by the American National Standards Institute (ANSI), focused on developing standards for exchanging, integrating, sharing, and managing health information. These standards facilitate interoperability among healthcare systems (Dolin et al., 2001).

Some of the key standards and broader healthcare interoperability efforts of HL7 rely on:

- *Messaging Standards*: Defining the format and sequence of data exchanged between healthcare applications. These specifications are unified by shared reference models of the health care and technical domains (e.g., HL7 2.x, HL7 v3 and FHIR).

- *Document Standards*: Specifications like the Clinical Document Architecture (CDA) for the structure and semantics of clinical documents (e.g., discharge summaries and progress notes).

- *Healthcare Services Specification Project (HSSP)*: Collaborating on service-oriented architecture standards in healthcare. HSSP provides interface specifications for healthcare services, not the implementation guidelines.

The HL7 messaging standard is sent as a collection of one or more messages, each transmitting one record (such as a patient record, lab record, or billing information) or item of health-related information (Soceanu et al., 2013).

HL7 has several versions. However, v2.x is still the most commonly used approach to exchange data in the clinical domain and has grown from 2.1 since 1981 to 2.8.2 in 2016 (Dhayne et al., 2018).

The main building block of a message in HL7 v2.x is a segment. A segment always begins with a three-character designation (e.g. PID - Patient identification, OBX - Observation result, AL1 - Patient Allergy Information and DG1 - diagnosis) that indicates the segment type. Each HL7 segment includes one or more elements (or fields). A pipe | character separates one data element from another (Dhayne et al., 2018).

An example message of an admission is illustrated in the figure 3. The Admission generated an A04 event that signals that the patient has arrived or checked in as a one-time or recurring outpatient and is not assigned to a bed (HL7 International, 2024b).

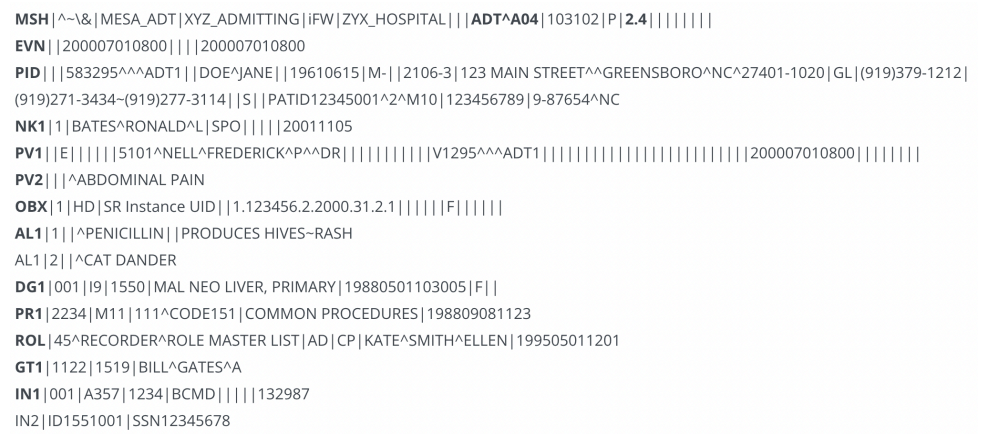



Figure 3: Example HL7 message - ADT A04 . Adapted from (HL7International, 2022).

Currently, HL7 is in version 3. The central aspect of this version is the Reference Information Model (RIM), which supports healthcare workflows following a model-driven methodology (HL7 International, 2024a).

The FHIR specification is the most recent messaging standard from HL7, aiming to overcome the complexity of V3 while maintaining compatibility (HL7 International, 2024a).

## Fast Healthcare Interoperability Resources (FHIR)

FHIR is a messaging standard by HL7 introduced in 2011, and its main idea was to build a set of resources, a generic definition of common healthcare concepts (e.g., patient, observation, practitioner, device and condition), which define the content and structure of information and can refer to each other using reference mechanisms. (Ayaz et al., 2021).

FHIR is based on previous HL7 standards (HL7 v2.x, v3 and CDA) and combines their advantages with established modern web technologies such as a Representational State Transfer (REST) architecture; APIs, XML, and JSON formats; and authorization tools (Open Authorization) (Vorisek et al., 2022).

Since the first day of its introduction, FHIR has gained popularity and has been increasingly adopted by the healthcare industry.

## The International Classification of Diseases (ICD)

ICD is a globally used standard for classifying and coding diseases and various signs, symptoms, abnormal findings, complaints, and external causes of injury or disease. It is maintained by the World Health Organization (WHO) and promotes international comparability in collecting, classifying, processing, and presenting mortality statistics (DiSantostefano, 2009).

The use of ICD is diverse and widespread; what is known about the extent, causes, and consequences of human disease worldwide rests on data classified according to the ICD. Clinical modifications of ICD are the main basis for statistics on disease that underlie crucial functions such as payment systems, service planning, administration of quality and safety and health services research.

This essential infrastructure for health information has now been revised for the 11th time in 2019. The 11th revision was more extensive and has significantly more implications for what can be done with the ICD, and how, than any revision since the 6th, in 1948.

The changes in this latest revision are substantial: ICD-11 is not just ICD-10 with some new categories but a different and more robust health information standard based on formal ontology, designed to be implemented in modern information technology infrastructures, and flexible enough for future modification and use with other classifications and terminologies. ICD-11-encoded data was intended to be comparable with data coded to ICD-10 (Harrison et al., 2021).

With ICD-10 a disease or health condition is given a unique code of three to seven characters. The first three elements represent a single category or disease; the second three digits describe subcategories: the aetiology, anatomical location, severity, and other vital details. At the same time, the seventh character - or span - specifies an episode of care for injuries, poisonings, and other conditions with external causes (World Health Organization, 2019).

## FAIR

Data sharing has been demonstrated to be essential in industries like healthcare when responding to emergencies like infectious disease epidemics.

FAIR stands for Findable, Accessible, Interoperable and Reusable and is a set of guidelines that strives to enable scientific data to be discovered, used appropriately, connected with other data and reused. This is the philosophy scientists aspire to implement in managing scientific data. These principles were first introduced in 2016 to address data availability and reusability issues, especially in the era of open science (M. D. Wilkinson et al., 2018; Wilkinson et al., 2016).

According to the FAIR Principles, research data must be:

- **Findable**: The information must be specifically and permanently recognizable. The information needs to be accessible to other researchers;
- **Accessible**: Both humans and machines should be able to understand the terms under which the data may be utilized;
- **Interoperable**: Data should be machine-readable and interoperable by using industry-standard terminologies, vocabularies, and ontologies;
- **Reusable**: Data must adhere to the requirements and be sufficiently well-described with metadata and provenance information to link or integrate with other data sources and proper citation.

## openEHR

OpenEHR an open-source, vendor-neutral standard for storing, retrieving, and exchanging interoperable EHR components. This system was developed in 2000 by a consortium of international health informatics experts to create a shared EHR model for different healthcare settings and countries. The OpenEHR approach is based on archetypes and flexible and reusable templates for capturing clinical information. These archetypes can be combined and modified to create specific EHR instances that meet the needs of different healthcare organisations and individual patients (openEHR, n.d.).

OpenEHR is designed to overcome the limitations of traditional EHR systems, which are often sealed, proprietary, and challenging to customise. The openEHR approach is multi-level single-source modelling within a service-oriented software framework. It is a promising approach to facilitate the interoperation of EHR systems, based on the fact that a complete EHR dataset can be fully represented using sharable archetypes. The OpenEHR approach aims to achieve interoperability between EHR systems by constraining the information model through structuring archetypes that represent clinical concepts (Beale & Heard, 2007; Hak et al., 2020; Wulff et al., 2018).

The openEHR approach has three central pillars: Reference Model (RM), Archetype Model (AM), and terminology. The RM is a stable and formal information model that focuses on the logical structures of an

EHR and defines the basic structures and attributes needed to express EHR data instances, including data types, data structures, and components. The AM consists of archetypes and templates. Archetypes are the formal and semantic artifacts that facilitate collecting, storing, retrieving, representing, communicating and analyzing clinical data, which clinical professionals and health informatics experts can model by constraining RM. Meanwhile, each archetype is designed towards reuse so it should be agreed upon and shared to contribute to semantic interoperability among EHR systems (Min et al., 2018).

**Key Features of openEHR**

- *Archetypes and Templates*: openEHR uses archetypes for reusable, formal models of clinical concepts. Templates are collections of archetypes for specific clinical use cases.
- *Multilingual and Cross-Cultural Support*: This allows more than one language and cultural context and, consequently, to be used globally.
- *Interoperability*: Eases data exchange between healthcare and healthcare-related systems and applications.
- *Clinician-Led Design*: Development of archetypes is often clinician-led, hence its usefulness in practice.
- *EHR System Independence*: Supports the development of EHR systems not tied to any particular vendor
- *Support for Clinical Decision Support*: Standardizing data representation enhances the chances of integration with clinical decision support systems.

One of OpenEHR's main objectives is the universal use of the same data structure based on archetypes by distinct systems. Given this, the standard provides OpenEHR Clinical Knowledge Management (CKM), an open repository that provides free access, management, and interaction of archetypes and templates selected and modelled with a clinical purpose (Hak et al., 2020).

## 3.5 Data Repositories

A Data Repository is a generic infrastructure that stores segmented data for analysis or reporting. These infrastructures are highly valued because they enable businesses to make decisions supported by more reliable information than gut feeling (Uzwyshyn & Raymond, 2016). A data repository increases the speed of data access and sharing and the preservation and archiving of sensitive data. On the other hand, inherent weaknesses must be addressed, such as the repository's potential behaviour as the data expands or the possibility of a system failure necessitating more frequent backups (Austin et al., 2016). Therefore, these are legitimate risks, but the data repository management team can be aware of and plan for them.

### Data Warehouse

In 1995, Inmon defined a Data Warehouse as "a subject-oriented, integrated, time-variant, and nonvolatile collection of data in support of management's decision-making process" (Inmon, 1995). This definition suggests that a data warehouse is a centralized repository that stores large volumes of data from multiple sources, organizing, analyzing, reporting, and supporting decision-making activities. Unlike a data mart and a data lake, Dta warehouse covers multiple subjects and is already filtered, cleaned and designated for a specific use (Inmon, 1996).

In short, this structure stores structured data, which is used mainly by data visualization or Business Intelligence (BI) reporting platforms since the data present here is ready to be used. The data typically comes from relational databases and internal or external systems or platforms. The typical data warehouse architecture is the Star Schema, devised by Ralph Kimball in 1996. It consists of a central table called the fact table surrounded by several dimension tables.(Golfarelli & Rizzi, 2018).

### Data Mart

A data mart is a storage system designed to provide specific data to a specific user for a particular application. This type of repository is focused on a single subject. Therefore, for this structure, only extremely well-structured data is considered and more detailed than in a data warehouse (Ghezzi, 2001). A data mart serves as the front-end element for the data of a department in a company. Although they are often "subsets" of a data warehouse, they can be independent. However, their management is substantially complicated as it multiplies the work of the database manager (Inmon, 1996).

### Data Lake

In contrast to a data mart, a data lake is a data storage facility that contains raw, unstructured data. It does not store information in files and folders. Instead, it stores raw data in a flat hierarchy in a massive storage. Data lakes store different types of raw information, including text documents, images, videos, and audio. In short, this storage system accepts indiscriminate data (unstructured, semi-structured, structured) and is widely used for big data archives and storage systems. The data is not ready for immediate use as it typically comes from non-relational databases, IoT devices, email, and images. (Miloslavskaya & Tolstoy, 2016).

## 3.6 Internet of Things

The IoT permits the interconnection of the physical world with the ability to integrate and understand greater amounts of information and make actions based on this information with the help of communication and information sharing.

IoT technology makes it easy to enhance traditional objects into smart objects by using their basic functionalities, which include embedded devices, communication, sensor networks, and internet protocols applications.

Concerning healthcare applications of IoT, it means the medical instruments, sensors, and applications used in healthcare systems integration. This includes a variety of devices such as internet-enabled weight loss wristbands, health-improving accessories, inhalers, glucose monitoring devices, smart beds, remote monitoring devices, and many more. This integration enables more personalized care by providing constant data flows and accessibility of information regarding a patient. This expedites the monitoring of individuals and allows for a more effective management, sharing and use of information on diagnosis and treatment, logistics, and drugs.

Due to the rapid increase in population and consequent surge in people resorting to health institutions, IoT can be used as a way to reduce hospital stays and readmissions by enabling remote monitoring and telemedicine. It enhances operational efficiency by automating routine tasks and improving resource management. In IoT medical sensors and wearable devices can capture essential health signs for health monitoring that can capture pressure level, glucose, weight, Electrocardiogram (ECG) signal and heart rate. Also, they can be used to observe paralyzed and elderly persons (Debnath et al., 2022).

## Context Awareness Through IoT

Systems are context-aware if they use context to provide relevant information and services to the user, where a person depends on the user's task (Abowd et al., 1999). Wireless sensor networks enable and enhance many ubiquitous computing applications in homes, offices, production, and vehicles. (Gaur, 2015). Ubiquitous computing refers to the construction of a global computing environment in which continuous and invisible access to computing resources is provided to users. It deals with acquiring context knowledge of the environment and provides dynamic, proactive, and context-aware services to users (Singh et al., 2006).

In ubiquitous computing, the user's context is constantly changing. When using applications in these settings, effectively utilizing the detected context can significantly benefit the user because it enables the application's behaviour to be personalized based on its current location (Abowd et al., 1999).

Traditional location-based services determine the specific location of an object by using GPS via a wireless communication/Internet-enabled device. Tracking implies determining the trajectory of an entity in an environment where network or IoT coverage is available (Ramnath et al., 2017). Localization-based services were also included in this pool of applications.

Localization and tracking are the foundations of many applications, including efficient security monitoring, surveillance, patient monitoring, and mobile device tracking. The main features that should be considered when selecting the appropriate short-range wireless technology are as follows.

- Power consumption: Many use cases require batteries or energy-harvesting technologies as power sources (Research, 2013).
- Ease-of-use: It must be easy to associate a device with a network or internet service.
- Security: Wireless technology must adequately support authentication and encryption; end-to-end security (from sensors to web services) is occasionally required.
- Available ecosystem: The possibility of connecting to smartphones, tablets, PCs and home gateways is essential; this requirement also drives volumes and has a meaningful impact on costs.
- Range: It is necessary to have the capability to cover enough of a range or to have some capabilities to extend the coverage (repeaters, routers, etc.) without having an excessive impact on the system cost (Collotta & Pau, 2015).
- Cost: Affordable solutions are more likely to be implemented in more institutions.

Depending on the purpose, certain techniques can be used to estimate indoor position. Typical methods for measuring indoor position include Wi-Fi, Pedestrian Dead Reckoning (PDR), and Bluetooth low-energy (BLE) beacon-based methods.

**Wi-Fi-based Positioning System** uses the RSSI values from each Access Point (AP) and does not require additional resources when the AP is already installed. However, this system can produce significant errors in RSSI values owing to external obstacle factors and can cause a cost burden when a Wi-Fi network is not installed.

**PDR-based Positioning Systems** are widely used in car navigation. This system estimates the position of the following from the previous position by measuring speed and direction using sensors. This system uses a smartphone and other sensors to assess the indoor user position from the absolute location by using the number of steps, stride length, and pedestrian direction (Ramnath et al., 2017).

**BLE Beacon Positioning System** resorts to BLE to determine the location of mobile devices with relatively low distance error by placing beacons scattered across a room or multiple rooms. Using the RSSI value, the BLE beacon-based positioning system calculates the distance between beacons and devices. A beacon can transmit the RSSI value to multiple smartphones using an advertisement function (Ramnath et al., 2017)(Faragher & Harle, 2015).

The PDR-based Indoor Positioning System requires initial calibration, is not easy to deploy, and may include errors in estimating movements from variables such as step length and uncounted movement. Research also indicates that hand position could be better for this system, which is not ideal (Zhao et al., 2019). A Wireless Local Area Network requires expensive implementation when it is not already present. Also, BLE beacons are more easily deployed, don't need to provide uniform communications coverage and require a lower power draw than a Wi-Fi-based positioning system (Ramnath et al., 2017)(Faragher & Harle,

2015). Among the above solutions, BLE beacons were chosen because they are relatively inexpensive, lighter, and easier to deploy.

# 4

# Blockchain

Firstly outlined by Nakamoto in 2008, (Nakamoto, 2008), Blockchain is a distributed database (ledger) that maintains a permanent and tamper-proof record of transactional data. It relies on a peer-to-peer network, where each network node maintains a copy of the ledger to prevent a single point of failure. All copies are updated and validated simultaneously. The ledger is composed of blocks, each containing information about recent transactions. Each block is connected to the previous block and verified by a distributed network of computers (Nofer et al., 2017).

Blockchain technology can be considered a breakthrough since it provides a safe way of conducting and validating transactions that can be applied to various industries. Simply put, it enables a community of users to record transactions in a shared ledger within that community. Under regular blockchain network operation, no transaction can be changed once published (Yaga et al., 2019). This technology has recently become popular for its potential to improve and provide information security, especially in industries where data security and privacy are vital Rastogi and Srivastava, 2020. For emphasis, blockchain is compared by some authors to the invention of the internet and its impact on the entire industry (Beck & Müller-Bloch, 2017).

The emergence of new blockchain technologies inspires new possibilities for their application in various fields. Whether improving the security of important data or enabling clearer and more efficient economic operations, this technology is undoubtedly meant to be evolutional in concept and infrastructure. Blockchain has been promoting developmental creativity and improving business processes when employed in other sectors, which makes it one of the central breakthroughs in technology in the present day.

Today, many studies on the use of the blockchain show that it can be applied in several areas to securely store and manage a distributed database and register digital transactions of any kind (Hammi et al., 2018).

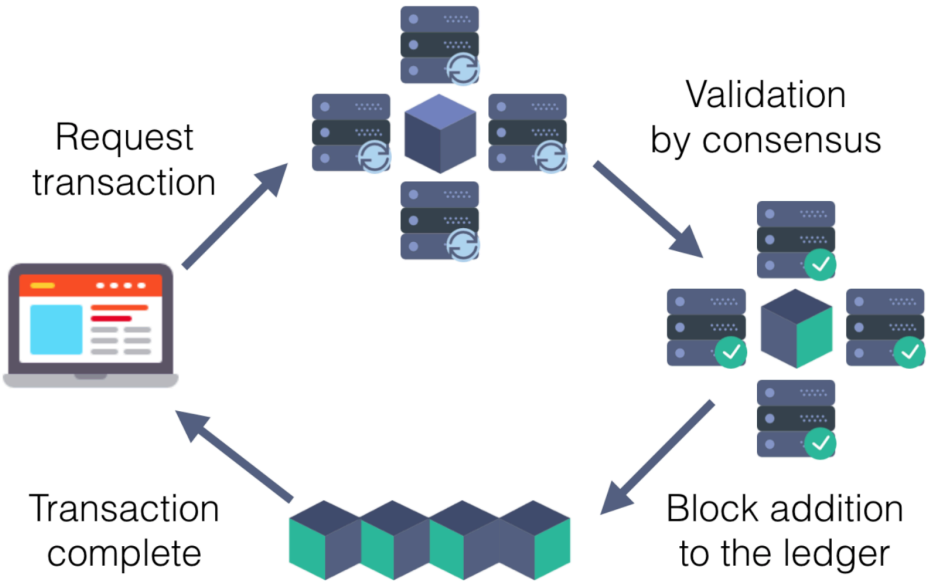



Figure 4: Blockchain process of Validation

A blockchain network has the following key characteristics (K. Kim & Hong, 2017; Laurence, 2017):

- **Consensus-based and transactional:** All relevant network participants must agree that a transaction is valid. This is achieved by consensus algorithms. Each blockchain network can establish the conditions under which a transaction or asset exchange can occur.
- **Orchestrated and flexible:** Business rules and smart contracts (that execute based on one or more conditions) can be built into the platform, blockchain business networks can evolve as they mature to support end-to-end business processes and a wide range of activities;
- **Immutability:** No participant can tamper with a transaction after it has been recorded to the ledger. If a transaction is in error, a new transaction must be used to reverse the error, and both transactions are then visible;
- **Tighter security:** Blockchain's security features protect against tampering, fraud, and cybercrime. If a network is permissioned, it enables the creation of a members-only network with proof that members are who they say they are and that goods or assets traded are exactly as represented.

## 4.1 Privacy and Confidentiality

Broadly, there are two main categories of blockchain networks: permissionless (or public) and permissioned. Permissioned blockchains can be divided into private and consortium.

In a permissionless or public blockchain, anyone can participate without a specific identity. Anyone can join the network, participate in consensus, and verify transactions. This lack of confidentiality and

control can be challenging for many enterprise solutions where not all data is desirable to be viewed by everyone. (Androulaki, Barger, Bortnikov, et al., 2018a)

Data can be encrypted to provide confidentiality; however, given enough time and computational resources, the encryption could be broken. For many enterprise use cases, the idea that their information could be accessible or leaked is unacceptable ("Hyperledger Fabric Docs release 2.2", 2020).

Permissioned blockchains have emerged as a viable alternative to address the privacy and confidentiality challenges, as they run a blockchain among a set of known, identified participants (Guimarães, Silva, et al., 2020).

A public blockchain is, by definition, very transparent and open and cannot be restricted in terms of who can use and participate in the process. Its ledgers are visible for anyone on the internet to check and add a block of transactions to the blockchain as long as they follow previously defined rules.

In the case of private blockchains, there is no unregulated or public access, as only the approved parties can access, see, or make any transaction. Such designs prevent unauthorized individuals from illicitly accessing sensitive information, as only those authorized to have the information will have access to it. Also, due to this limited access and lesser number of users, private blockchains may perform and scale better (Beck & Müller-Bloch, 2017; Mohan, 2017; Mohanta et al., 2019; Sheth & Dattani, 2019)

Consortium blockchains exist as a hybrid model between public and private blockchains. In private blockchains, a single entity controls the entire network. In public blockchains, the network is fully decentralized; anyone can join the network, participate in the consensus process, and access the data. In this model, a group of known organizations collaboratively manages the blockchain, enabling collaborative governance while maintaining some level of decentralization. These blockchains offer a middle ground between private and public by only enabling a limited set of participants to access sensitive data without relying on a central administrator. They are typically used in industries where multiple organizations need to collaborate but still require control over their data, such as banking, supply chain management, logistics, and shipping (Y. Chen et al., 2020; Dib et al., 2018)

*Hyperledger Fabric* is among the most popular permissioned blockchains, either private or consortium. Because the nodes' identities are known in private settings, most blockchains adopt one of the protocols from the vast literature on distributed consensus. The Raft and PBFT are the most popular protocols. (Dinh et al., 2018; Dubovitskaya et al., 2017; Guimarães, Silva, et al., 2020).

## 4.2 Consensus Algorithms

Consensus algorithms are crucial in blockchain technology because they determine the network's security, fault tolerance, and scalability. Consensus is the collaborative process that the members of a blockchain business network use to agree that a transaction is valid and to keep the ledger consistently synchronized. Consensus mechanisms lower the risk of fraudulent transactions because tampering with transactions added to the ledger would have to occur across many places simultaneously. There are many mechanisms

to validate blocks. However, the main focus here is going to be on the three main ones: Proof of Work (PoW), Proof of Stake (PoS), RAFT, and Practical Byzantine Fault Tolerance (pBFT) (Hammi et al., 2018).

## Proof-of-work (PoW)

In a decentralized network, someone must be selected to record the transactions. The easiest way is random selection. However, random selection is vulnerable to attacks. So, if a node wants to publish a block of transactions, much work has to be done to prove that the node is not likely to attack the network. Generally, the work means computer calculations. In PoW, each network node calculates a hash value of the block header. The consensus requires that the calculated value be equal to or smaller than a certain given value. When one node reaches the target value, it broadcasts the block to other nodes, and all other nodes must mutually confirm the correctness of the hash value. Nodes that calculate the hash values are called miners, and the PoW procedure is called mining in Bitcoin (Sloane Brakeville, 2018).

## Proof-of-stake (PoS)

PoS attempts to solve the energy expenditure problem created by PoW. To do so, PoS replaces PoW's competition by randomly selecting stakeholders to append to the blockchain. These stakeholders, however, must prove their ownership of the amount of currency. As a result, many solutions are proposed, using a combination of stake sizes to decide which one to forge the next block. The leader is elected with a probability proportional to the stake it owns in the system. In the simplest case, the stake is the amount of currency, but it can also be (for example) the age of the coin that a miner holds (Hammi et al., 2018; F. Saleh, 2018).

## Practical Byzantine Fault Tolerance (pBFT)

In the context of distributed systems, Byzantine Fault Tolerance is the ability of a distributed computer network to function as desired and correctly reach a sufficient consensus despite malicious components (nodes) of the system failing or propagating incorrect information to other peers. The objective is to defend against catastrophic system failures by mitigating the influence these malicious nodes have on the correct function of the network and the right consensus reached by the honest nodes in the system. pBFT is one of these optimizations and has been implemented in several modern distributed computer systems, including some popular blockchain platforms (Curran, 2018).

## RAFT

RAFT is a consensus-based algorithm that enables the management of replicated logs across different servers in a distributed environment. It mainly operates by ensuring data is moved from one node to another whenever an update is made in any of the other nodes. RAFT normally functions by assigning

the role of a leader to handle the functions related to log replication. The leader is in charge, keeps track of all the log entries, and is responsible for their distribution across the cluster and applying them to the state machine.

RAFT offers a way to ensure that at any time, only one leader is in charge of coordinating the log replication to avoid inconsistency. In a normal Raft operation, there is exactly one leader at any time, and all the other nodes are followers. To enforce that the leader's authority is still recognized, the leader has to send out a heartbeat to all his followers after a certain period. The leader will collect all transactions. Each transaction is added as an entry in the node's ledger. After the leader receives feedback from most followers who have written the entry, the leader notifies the followers that this entry is committed. This procedure is called ledger replication. (Huang et al., 2020)

## 4.3 Smart Contracts and Chaincodes

A distributed ledger can record a very simple contract, commonly called a smart contract, which executes once certain conditions are fulfilled (Prathyusha et al., 2018). Smart contracts are crucial in managing transactions on the ledger since they allow the network members to conduct transactions automatically. It is also worth mentioning that the transaction's signing confirms the trust rule. Once the terms are agreed upon by both parties and recorded on the ledger, the transaction is validated, and the data is recorded. In the case of transferring funds, they are automatically transferred upon receipt of the item.

In Hyperledger Fabric, smart contracts are referred as chaincodes, often used interchangeably. Chaincode in Hyperledger Fabric is code, typically written in Go, that defines the network assets and the transaction instructions for modifying these assets. A member with proper authorization installs and instantiates it into a channel. In that channel where a transaction is carried out, chain code functions are called to make changes and obtain data from the ledger. (Sloane Brakeville, 2018).

## 4.4 Blockchain-related concepts, tools and technologies

### Web3

Web3 is frequently cited as the next generation of the internet. It aims to decentralize the web, making people more active and participative. The expected result of this decentralization is to overturn the dominating power of big tech corporations, which would fundamentally change how people interact with the global economy through platforms (Wan et al., 2023).

Web3 incorporates blockchain, decentralization, transaction transparency, and user control. Web3 aims at putting the ownership of data and people's digital identities back in their hands, away from the centralized governance systems of Web2 (Ray, 2023).

The creation of Decentralized Applications (DApps), Decentralized finance (DeFi), Non-fungible Tokens (NFTs), Decentralized Autonomous Organizations (DAOs), and supply chain management systems gains

from the decentralization that Web3 promotes. These applications can leverage certain principles of Web3 to make it safer, transparent and efficient (Ray, 2023).

Additionally, Web3's infrastructure backs the idea of self-sovereign identities, enabling the secure exchange of money and data while providing citizens more control over their personal information (Bambacht & Pouwelse, 2022). The technology utilizes Distributed Ledger Technology (DLT) to allow interactions with content, services and applications without revealing real identities (H. Xu et al., 2023).

Web3, however, is not without its problems; it has issues such as scalability, interoperability, compliance and energy consumption. Nevertheless, its capacity to disrupt the Internet and the economy at large is evident (Sadowski & Beegle, 2023).

## Decentralized Finance (Defi)

Through a blockchain-based service delivery model, DeFi has transformed the provision of financial services. DeFi applications are not reliant on institutions such as banks to issue loans or facilitate the trading of assets but rather use blockchain technologies and smart contracts to render such services. Such change in the norms of financial processes is intended to increase access to the financial services market and potentially alter the existing landscape. (H. Kim et al., 2022; Schueffel, 2021)

Due to their open-source and transparency features, decentralized protocols are available for anyone (Karim et al., 2022). This enables users and developers on the network to develop financial products that are not controlled by any organization. Possible DeFi products and services include prediction markets, loans and stablecoins (Zimmermann, 2021).

Such services can be offered to anybody worldwide who can access the internet regardless of their geographical region and economic status (Nakamoto, 2008). Thus, it helps create economic and social circumstances that will enable the less privileged or those marginalized in society to have opportunities that are out of their reach with ordinary financial services.

DeFi, although offering financial services, is more concerned with the management and usage of various forms of assets in a decentralized way. In this regard, NFTs are crucial in portraying distinct and valuable digital objects which are embedded within these assets. Its technological infrastructure offers avenues for users to participate in monetary transactions and also to own, trade or utilize a wide range of digital assets, which provides a new framework for asset governance outside traditional finance.

## Non-Fungible Tokens (NFTs)

NFTs is a digital property proving an owner's possession of a unique item kept on the blockchain. NFTs are defined by their uniqueness, guaranteed through the blockchain. Every NFT contains certain information or metadata that makes it different from any other tokens. Such non-fungibility gives NFTs their worth and usefulness as a medium that conveys ownership of individual assets (Q. Wang et al., 2021).

NFTs play a significant role within the DeFi sector. They bring in new forms of asset management as well as collateralization. For example, DeFi can serve as loan collateral, be further traded in decentralized exchanges, and, in general, be included in financial products. This integration enhances liquidity and provides more opportunities for users to leverage their digital assets.

DeFi are unique, indivisible, irreplaceable, and verifiable tokens representing a given digital or physical asset on a blockchain. This property renders NFTs a valuable way of representing ownership for assets like digital arts, collectables, virtual lands, in-game assets, and even tangible assets in their digitized form.

The use of NFTs in the art sector has exponentially increased, providing more opportunities for digital creators to showcase their limited-edition digital artwork. In gaming, assets such as NFTs allow users to own and sell virtual items. They are also explored in real estate for fractional ownership and music for exclusive rights or access to exclusive content.

Lack of regulation in the crypto space has led to fraud and unauthorized sales of NFTs. The market is also very speculative and unstable, with prices fluctuating frequently.

NFTs now serve a different purpose in the DeFi sector as tools for representing unique digital assets. They allow for new methods of managing non-fungible assets, leading to the creation of a wider variety and scope of opportunities.

### Decentralized Autonomous Organizations (DAOs)

DAOs are organizations whose operational processes are articulated by smart contracts deployed on a blockchain. They enable transparent and autonomous decision-making without central authority. DAOs use a system where stakeholders vote on proposals using tokens, bringing community involvement to the decision-making process.

The idea became more popular in 2016 with ‘The DAO’ designed to be a distributed capital raising mechanism but had various security issues, leading to a significant financial loss (Ethereum Foundation, 2016). Despite this setback, modern DAOs have developed into a form of management organized around the management of several decentralized applications, DeFi protocols, or blockchain governance, providing opportunities for transparency and cost reduction (Smith & Doe, 2021). Nevertheless, challenges such as legal recognition and the security of smart contracts still exist (Johnson & Wang, 2020).

DAOs can be seen as a revolution in organizational design. They hold the potential to change the way digital entities engage with and coordinate with one another in the digital economy.

## InterPlanetary File System (IPFS)

The IPFS is a set of composable, peer-to-peer protocols for addressing, routing, and transferring content-addressed data in a decentralized file system. It synthesizes successful ideas from previous peer-to-peer systems, including BitTorret, Git and Kademlia (Benet, 2014; Maymounkov & Mazières, 2002)

IPFS uses content-based file identification with a distributed hash table (DHT) for file storage management on different nodes. When uploaded to IPFS, a file is divided into smaller chunks, each given a

cryptographic hash. These hashes are used to create a Merkle Directed Acyclic Graph (DAG), which is used to rebuild the original file. This approach provides an effective manner in recognition and verification of files, and at the same time, allowing for their smooth exchange. (Psaras & Dias, 2020).

Incorporating IPFS into various blockchains enhances storage capabilities by allowing big data files to be stored off-chain, with only their cryptographic hash retained on-chain. By employing this method, blockchain storage is improved by exploiting the strong data distribution and retrieval capabilities of IPFS (Muralidharan & Ko, 2019; H. Wang et al., 2018). The convergence of these technologies presents a practical solution for requiring decentralised applications in which data within the entire network can be both available and persistent, enabling greater data availability and immutability across the network.

## Hyperledger

Hyperledger is a collective effort to advance cross-industry blockchain technologies. As an initiative of The Linux Foundation, it embraces international collaborators from finance, banking, Internet of Things, supply chains, manufacturing and technology. The project aims to create a commercial-grade, open-source, extensible framework for distributed ledgers. This seeks to develop an open architecture for distributed ledgers that would transform how businesses and transactions could operate globally. (Cachin, 2016).

## Hyperledger Fabric (HLF)

Hyperledger Fabric (HLF) is an open-source enterprise-grade permissioned open-source DLT platform maintained mainly by IBM and Linux Foundation, designed for use in enterprise contexts. It represents an implementation of a distributed ledger platform designed for running smart contracts and incorporates familiar and proven technologies with a modular architecture, allowing for various pluggable functions. As part of the Hyperledger Project incubation, HLF operates on a peer-run distributed ledger protocol. It distinguishes between validating and non-validating peers, with validating peers executing the consensus algorithm and non-validating peers serving as proxies to connect clients to validating peers. This platform, geared towards business use, is open-source, standards-based, and features robust security and identity mechanisms (Cachin, 2016; Sankar et al., 2017).

HLF has a highly modular and configurable architecture, enabling innovation, versatility, and optimization for a broad range of industry use cases, including healthcare, which is the core theme of this thesis. (Shalaby et al., 2020) (“Hyperledger Fabric Docs release 2.2”, 2020)

Fabric is the first distributed ledger platform to support smart contracts authored in general-purpose programming languages such as Java, Go and Node.js rather than constrained domain-specific languages (DSL).

Fabric can leverage consensus protocols that do not require a native cryptocurrency to incentivise costly mining or fuel smart contract execution. The absence of cryptographic mining operations means

that the platform can be deployed with roughly the same operational cost as any other distributed system. (“Hyperledger Fabric Docs release 2.2”, 2020)

HLF is structured based on some main nodes/components and core concepts relevant to this work: Submitting client, Peer, Orderer, Certificate Authority (CA), Chaincode and Consensus. (“Hyperledger Fabric Docs release 2.2”, 2020)

**Client** represents the entity that acts on behalf of an end-user and can submit transaction invocation to the endorsers and broadcast transaction proposals to the ordering service. (“Hyperledger Fabric Docs release 2.2”, 2020) (J. Sousa et al., 2018)(Androulaki, Barger, Bortnikov, et al., 2018a)

**Peer**, a node that commits transactions and maintains the state and a copy of the ledger. A peer receives ordered state updates in the form of blocks from the ordering service and maintains the state and the ledger. Peers can additionally take up the special role of an endorser. The special function of an endorser is to a particular chaincode, which consists of endorsing a transaction before it is committed. (“Hyperledger Fabric Docs release 2.2”, 2020)

**Orderer or Ordering Service Nodes,** are the nodes that collectively form the ordering service. It provides a shared communication channel to clients and peers, offering a broadcast service for transaction messages. Clients connect to the channel and may broadcast messages on the channel, which are then delivered to all peers. The communicated messages are the candidate transactions for inclusion in the blockchain state. Orderers are entirely unaware of the application state and do not participate in the execution or validation of transactions. This design choice renders consensus in Fabric as modular as possible and simplifies the replacement of consensus protocols in Fabric. (“Hyperledger Fabric Docs release 2.2”, 2020)(Androulaki, Barger, Bortnikov, et al., 2018a)

**Hyperledger Fabric CA**, is the default Certificate Authority component, which issues PKI-based certificates to network member organizations and their users. The CA issues one root certificate to each member and one enrollment certificate to each authorized user. (“Hyperledger Fabric Docs release 2.2”, 2020)

**Chaincode** is the business logic of a blockchain application and functions as a trusted distributed application that bases its trust on the blockchain and the underlying consensus among the peers. A chaincode implements the application logic and runs during the execution phase. (Androulaki, Barger, Bortnikov, et al., 2018a)

**Consensus** implies a process in which the members of a blockchain network agree on whether a transaction is valid and to keep consistency in ledger synchronization, lowering the risk of malicious transactions.

HLF presents a pluggable consensus approach. Transaction ordering is delegated to a modular component (ordering service) for consensus, which is logically decoupled from the peers that execute transactions and maintain the ledger. Since consensus is modular, its implementation can be tailored to the trust assumption of a particular deployment or solution

## Hyperledger Explorer

Also part of the Hyperledger project, Hyperledger Explorer is an open-source tool that creates transparency in the operations of the blockchain network. It is easy-to-use open-source software that allows users to retrieve, navigate, and control blockchain information, enhancing disclosure and information quality across various applications.

This observation management system, first created to be employed in conjunction with Hyperledger Fabric, allows for real-time monitoring of blockchain networks and gives detailed analytics concerning the network by visualizing data such as blocks, transactions, and associated metadata. This kind of monitoring is very important to stakeholders who need to comprehend how the blockchain operates and the level at which it performs. (Pal et al., 2023; Supriadi & Andarsyah, 2023).

The architecture of Hyperledger Explorer is designed to be modular and extensible. It integrates seamlessly with Hyperledger Fabric, leveraging the Fabric SDK to interact with the blockchain network. The backend server processes requests from the frontend interface, retrieves data from the blockchain, and presents it in a readable format to the user (The Linux Foundation, 2020).

Hyperledger Explorer is utilized in various industries for blockchain management and monitoring. From financial services to supply chain management, it provides valuable insights into the operation of blockchain networks. It is essential for those who must perform audits, monitor network performance, and manage blockchain operations efficiently (Androulaki, Barger, Bortnikov, et al., 2018b; L. Xu et al., 2019).

In some of the forthcoming use cases, Hyperledger Explorer was initially employed to monitor and manage the blockchain network. However, it was officially discontinued and moved to End-of-Life (EOL) status on May 12, 2022. It became imperative to develop a custom solution to fulfil this essential role. This bespoke solution was designed based on the foundational principles of Hyperledger Explorer, ensuring continuity in functionality while allowing for customized enhancements to better meet the specific requirements of the projects. This transition enabled the continued provision of robust network monitoring and management capabilities without interruption and is presented in the use cases section.

## Hyperledger Caliper

Hyperledger Caliper is a tool for benchmarking efficiency of blockchain systems. Caliper is designed to assess the performance of blockchain implementations through different user-end simulations, giving a proper evaluation in scenarios resembling real-life usage. The reports produced by Caliper also cover typical performance parameters like transaction latencies, transaction throughput, and resource consumption, which are critical in exploratory research and development of the tested blockchain solutions. (Choi & Hong, 2021).

Hyperledger Caliper helps users compare blockchains in similar environments, offering a benchmarking tool that assesses the success of blockchain implementations against predefined use cases (Ampel

et al., 2019). Designed for extensibility, Caliper can work with popular monitoring and infrastructure solutions, generating reports with performance metrics such as throughput, latency, performance rate, and CPU/memory resource utilization by listening for transaction timestamps and measuring metrics from them ("Hyperledger Caliper Architecture", 2024; The Linux Foundation, 2024).

## Prometheus

Prometheus is an open-source solution for monitoring and alerting, released by SoundCloud in 2012. Since its release, Prometheus has been widely embraced across several businesses and organizations, resulting in a thriving community of developers and users. The system has grown into a standalone project, independent of any organization and is currently under the Cloud Native Computing Foundation (CNCF) since 2016 ("Cloud Native Computing Foundation", 2024; Prometheus, 2024).

With expanding capabilities, Prometheus is used in application and infrastructure operational health (monitoring of resources such as servers, databases, and their performance), application performance monitoring (request rates, error response rates, time taken to respond to requests, etc.), and monitoring of microservices (monitoring of metrics to assess if the application is working and performing well).

Prometheus features a powerful data model and a flexible query language that enable detailed analysis of application and infrastructure performance (Brazil, 2018). The core features of Prometheus include a multi-dimensional data model with time series data identified by metric names and key/value pairs; PromQL, a flexible query language; self-contained single server nodes with no need for distributed storage; and data collection using a pull model over HTTP (Prometheus, 2024). Prometheus also supports pushing time series through an intermediate gateway, discovering targets via service discovery or static configuration, and various graphing and dashboarding modes.

## Integrating Prometheus with Hyperledger Caliper

Hyperledger Caliper, in combination with Prometheus, efficiently monitors and benchmarks blockchain networks. It enhances the performance analysis done by Caliper by using Prometheus's strong data collection and alerting features.

Prometheus can scrape metrics exposed by Hyperledger Caliper during benchmarking tests. These metrics include transaction throughput, latency, and resource utilization. By collecting these metrics, Prometheus enables real-time monitoring and historical analysis of blockchain performance ("Prometheus Documentation", 2024; "Prometheus Integration with Hyperledger Caliper", 2024).

The integration of Prometheus and Hyperledger Caliper also offers advantages for the following use cases:

- **Performance Benchmarking**: The performance of blockchain networks can be assessed persistently under different loads and configurations.

- **Resource Optimization**: Metrics of resource optimization can be used to efficiently deploy and scale blockchain node resources.
- **Alerting and Incident Response**: Establish alerts for parameter limits that exceed healthy ranges to prevent excessive escalation and enable a prompt response.

The Fusion of Prometheus with Hyperledger Caliper brings the best tools to monitor and benchmark blockchain networks effectively. This combination improves the collection, analysis, and visualization of these performance metrics and is an added advantage for those developing and researching in blockchain technology.

### Grafana

Grafana is gaining rapid popularity as an open-source software for monitoring and analyzing data. Grafana was originally developed in 2014 by Torkel Ödegaarde. Today it is a very flexible and useful tool that many people in organizations use across the globe to monitor and visually represent data from different sources: metrics, logs and traces.

Grafana's main purpose is to build an environment for designing, analyzing, and distributing interactive and management dashboards and applications. Thanks to its clean interface and rich set of plugins, Grafana can be linked to numerous types of data, including time series databases, log management services, cloud platforms, and more.

Visualization is one of the critical aspects of Grafana, along with effective data source integration, templating and variables management, notification management and alerting and, more importantly, active user and contribution community and ecosystem.

As the implementation of cloud-native style architecture is becoming more widespread and the use of distributed systems is rising, Grafana has proved to be extremely helpful in enabling observability and insights into complex environments. By providing a flexible, customizable, and extensible platform for monitoring and visualization, users can obtain the information necessary for making decisions regarding the systems and applications they are using.(Brattstrom & Morreale, 2017; Chakraborty & Kundan, 2021; Leppänen, 2021).

## 4.5 Blockchain Analytics

The first purpose of blockchain technology was to serve as a transaction storage system. The growing range of offered database systems has also resulted in the desire to perform analytics in these systems (Vo et al., 2018). Data scientists spend around 80% of their time collecting, preparing, cleaning, and organizing data for analysis. In blockchain, the data has already been identified, collected, prepared, and organized, which provides a rich storehouse of information for analysis. The data that is stored is valuable in helping to meet the demands of the organization which, in most cases, are expressed in terms

of specific aggregate queries and descriptive analytics. Some examples of such queries include trend analysis, time series and time-space, top N queries, and aggregations. The creation of analytics starts with providing a dashboard or a data visualization, called descriptive analytics, which can evolve into more advanced analytics. Machine learning models can be built when sufficient historical data exists. Using this model makes it possible to find implicit patterns in the data that help answer questions about future events or trends in an organization. Analysing healthcare data organizations' data can provide helpful information for scientific research, commercial applications, and services. Thus, blockchain analytics is critical for Blockchain-enabled medical organizations to be efficient and innovative as it can contribute largely towards medical advancement and, therefore, better healthcare.

Blockchain basically presents lengthy, structurally presentable, reliable and unchangeable ways to store or relay information, and these can be utilized to enhance the analytical capabilities of the organization (Dillenberger et al., 2019).

## 4.6 Blockchain for Healthcare Data Management

Blockchain is considered a general-purpose technology with presence and relevance in several areas, among which we can highlight Healthcare (Agbo et al., 2019).

Data in healthcare is, in its essence, highly diverse and complex, sensitive and private. So, healthcare represents an area where there are several opportunities for applying this concept due to the wide variety of problems that can be solved through the features and properties offered by blockchain (Agbo & Mahmoud, 2020; Bell et al., 2018).

Patient Records Management is a vital part of healthcare. Nonetheless, there are usually many inherent problems in patient records management strategies, including data security, accessibility, and interoperability. These challenges are a major hindrance towards providing timely and efficient decision-making, compromise patient privacy, and hinder seamless collaboration among healthcare providers.

In this regard, a number of researchers have proposed using blockchain technology to handle these constant challenges in managing patient information. Given the special features and opportunities that the blockchain system presents, the management, storage, and sharing of health information could be completely changed.

Blockchain technology can enhance the data integrity, accessibility and seamless interoperability of different healthcare systems by applying encryption methods, transparency, and consensus procedures (Tandon et al., 2020). The sensitive patient data saved on the blockchain is protected by cryptographic methods like hashing and encryption, offering strong security safeguards (Azaria et al., 2016a; Zhang et al., 2022).

Blockchain can also improve accessibility by facilitating safe, permissioned data transfer between accredited healthcare providers. In the same way, modifying and accessing collaborative patients' records can be done by those who possess the proper authorization due to the automated and open access control

using smart contracts on the blockchain (Shahnaz et al., 2019). This more straightforward approach avoids intermediaries and thus improves patient care outcomes and fosters operational cooperation.

## Applications of Blockchain Technology in Healthcare

Due to its significant potential and practical applicability in healthcare, researchers are exploring various use cases for blockchain technology in this sector. The following are some of its applications found in the literature:

### Electronic Medical Records

One of the distinct applications of blockchain in healthcare is the management of EHRs. Blockchain helps gather, store, or manage patient information (Bell et al., 2018; T. Kumar et al., 2018; Kuo et al., 2017a).

An application of the blockchain for electronic medical records has been developed in the form of a decentralized blockchain-based system called MedRec (Azaria et al., 2016b). MedRec lets patients view and control their medical data in real-time as they move across different services. It allows patients to manage and protect their records, allowing them to determine who can retrieve them. Integrating local data storage with blockchain technology ensures a level of user authentication, confidentiality and data sharing that is beneficial for doctor-patient interactions.

### Global Data Sharing

Global data sharing is essential when patients want to travel to foreign countries or seek healthcare from international professionals. In such situations, healthcare providers would need to use the patients' medical information to ensure quality healthcare services (Bell et al., 2018; T. Kumar et al., 2018; Kuo et al., 2017a).

Health Wizz serves as an example of how further developments of blockchain technology can help in sharing data on a global scale ("About - HealthWIzz", 2024). Utilizing blockchain technology makes it possible to store and exchange health data worldwide while maintaining its security and confidentiality. The user can add any necessary health records, such as previous illnesses, tests, and treatments, and they can all be kept as unchangeable and secure documents that guarantee the information's trustworthiness.

### Biomedical Research and Education

Incorporating blockchain adds value to clinical trials by ensuring transparency, audit tracking, and accountability. It prevents the fabrication of clinical trials and any underreporting of trial results by preserving

the reliability of data. The technology's transparency also supports seamless replication of research findings (Bell et al., 2018; T. Kumar et al., 2018; Kuo et al., 2017a).

The Shivom Project aims to revolutionise genomics and healthcare using blockchain and genomic data technologies. It creates a global ecosystem for securely storing, sharing, and monetising genetic information. By leveraging large genomic datasets, Shivom promotes medical research and new treatments while allowing individuals to control access to their genetic data ("Shivom - Crunchbase Company Profile & Funding", 2024).

### Pharmaceutical Supply Chain

The organizational use of blockchain technology extends to the medical healthcare supply chain, especially the drug supply chain in the pharmaceutical sector. It helps fight the supply of fake or pirated medications, a problem that affects the densely populated, poorly equipped areas of healthcare (Bell et al., 2018; T. Kumar et al., 2018; Kuo et al., 2017a).

Several companies, such as IBM, have collaborated with manufacturers, distributors, and hospitals to carry out pilot projects to test the viability of encompassing blockchain solutions to enhance pharmaceutical supply chain management systems. Internal and external factors drive collaboration among supply chain participants to implement blockchain effectively. IBM Blockchain for Pharmaceuticals addresses critical traceability and cost-effectiveness in pharmaceutical supply chains (Ghadge et al., 2023).

### Equipment tracking

Medical organizations spend less when using blockchain to track items. Any records regarding the location of these assets are permanent and cannot be modified due to the encryption of cryptography technology, which is essential in knowing where the expensive medical assets have been. This method assists in dealing with the increasing problem of theft of medical devices, which has become a multimillion-dollar problem (Bell et al., 2018; T. Kumar et al., 2018; Kuo et al., 2017a).

The Chronicled Blockchain ("Chronicled", 2024), is a product verification, traceability and authenticity verification platform. It's a product development platform which implements blockchain technology and allows businesses to register and monitor products moving through its systems. This makes it possible to create permanent electronic records that are open to all parties, and a history of each item is available for examination at any time.

### Health Data Analysis and integration with AI

Implementing blockchain technology transforms healthcare systems and offers the chance to integrate emerging technologies like machine learning and artificial intelligence. This combination facilitates

predictive analysis of health data, advancing precision medicine (Bell et al., 2018; T. Kumar et al., 2018; Kuo et al., 2017a).

Nebula Genomics revolutionises the genomic data market by building the Nebula Network on blockchain. It creates a marketplace where sequencing facilities, drug companies, and health organisations can purchase genetic information. Individuals pay to learn about their genetic variants and disease predispositions, and they are compensated by allowing their data to be shared with third parties (Ozercan et al., 2018).

Also, (Jabarulla & Lee, 2021) integrated blockchain and AI to create a decentralized, patient-centric healthcare system that enhances data interoperability, secures patient records, enables privacy-preserving AI-driven diagnosis, and supports collaborative learning across hospitals for improved COVID-19 management.

### Permissioned Data Management

The implementation of blockchain can be used to improve the management of permissioned data by ensuring that such information is shared securely and transparently. It cannot be altered, yet access rights must remain controlled, the data is secured, and the intended users cooperate productively. For example, (Saha et al., 2020) highlights the use of blockchain for secure data transmission in IoT-enabled healthcare applications.

Also, (Ismail et al., 2021) discusses a patient-centric view for multiple stakeholders by addressing security and privacy concerns through blockchain's decentralization and data protection features, while cloud computing improves scalability and efficiency.

### Privacy Preservation

Implementing private blockchain technology within the healthcare system helps manage user data privacy more efficiently by offering a safe space in which defined individuals can access patient information. Additional mechanisms can be coupled to encrypt the information so that, even when access is granted, it is not immediately open and available, grating an extra layer of privacy.

Given that, multiple works could be found in the literature: The work presented on (Liu et al., 2023) significantly aids permissioned data management by utilizing different encryptions to ensure fine-grained access control of encrypted Electronic health records.

In (A. Kumar et al., 2022), by allowing only authorized users to access sensitive medical information, the architecture ensures that healthcare data is protected from unauthorized tampering and cyberattacks, improving the overall security of permissioned data systems.

Also, the work of (Ali et al., 2023) combines blockchain with homomorphic encryption to protect patient data in IoT healthcare systems. The solution ensures that only authorized parties can access

and process encrypted data without revealing sensitive information, preserving privacy while maintaining efficient and secure data management.

# Part IV

# Contributions

# 5

# Understanding the contributions

In this chapter, contributions will be presented, each highlighting a distinct technology usage in healthcare. These include, among others, context-aware EHRs, real-time log management, and advanced analytics for clinical data integration.

Each contribution chapter is organised to present the implementation of the identified challenge, the outcomes, and the challenges faced. The knowledge acquired is essential for understanding what encompasses technology today and how much more can be done with it in future health systems. This analysis is meant to enhance the ongoing debates and inform future developments.

Such diverse contributions aim to examine emergent technologies in healthcare and explore their applications, ranging from permissioned blockchains like Hyperledger Fabric to decentralized systems incorporating IPFS, IoT, and Web3. This confirms that such technologies have a wide range of applications in the health sector.

The table below summarizes these contributions, providing the assigned titles and a summary.

Table 2: Contributions Overview

| ID | Title | Context |
|---|---|---|
| **C1** | Context-aware electronic health record-an IoT and blockchain approach | Integration of IoT and blockchain to improve user experience and data accuracy in hospital settings |
| **C2** | Blockchain Analytics - Real-time Log Management in Healthcare | Implementation of a private blockchain for secure and real-time log management in healthcare environments |
| **C3** | Leveraging Standardized Real-Time Data Repositories and Blockchain to Enhance an AI-driven Healthcare Decisions | A real-time data repository using blockchain for research purposes and analytics |
| **C4** | The Role of Blockchain Technology in Ensuring Security and Immutability of Open Data in Healthcare | Use of Blockchain and openEHR to enhance data security and integrity in Healthcare settings |
| **C5** | IPFS and Hyperledger Fabric: Integrity of Data in Healthcare | Combining IPFS and Hyperledger Fabric to securely store and manage sensitive healthcare documents |

Table 2: Contributions Overview (continued)

| ID | Title | Context |
|---|---|---|
| **C6** | Decentralized Healthcare Marketplace | Decentralized platform to encourage health data exchange for research purposes and to empower patients ownership and monetization through NFTs and Web3 related technologies |
| **C7** | Scalable and Sustainable Blockchain: Architecting Infrastructure and Developing a Platform for Management and Exploration | Benchmarking Blockchain Architectures and Presenting a Platform for Blockchain Management and Exploration |

Table 3 helps map out how each specified contribution answers the research questions identified and addressed within the document. This table has been designed in a way that shows the correspondence between the identified challenges and the solutions that have been proposed to solve them.

Table 3: Cross-Reference Table Between Contributions and Research Questions

| RQ | C1 | C2 | C3 | C4 | C6 | C7 | C8 |
|---|---|---|---|---|---|---|---|
| **Phase A** | | | | | | | |
| **A1-R1** | X | X | X | X | X | X | X |
| **A2-R2** | X | X | X | X | X | X | X |
| **A2-R3** | X | X | X | X | X | X | X |
| **A2-R4** | X | X | X | X | X | X | X |
| **Phase B** | | | | | | | |
| **B1-R1** | X | X | X | X | X | X | |
| **B1-R2** | X | X | X | X | X | X | X |
| **B2-R3** | X | | X | X | | X | X |
| **B2-R4** | | | X | | | X | |
| **Phase C** | | | | | | | |
| **C1-R1** | X | X | X | X | X | X | X |
| **C1-R2** | | X | | | X | X | X |
| **C1-R3** | X | X | X | X | X | X | X |
| **C1-R4** | | | | X | | | X |
| **C2-R5** | | | X | X | | | |
| **C2-R6** | | | X | X | | | |
| **Phase D** | | | | | | | |
| **D1-R1** | X | X | X | X | X | X | X |
| **D1-R2** | | | | | X | X | |
| **D1-R3** | X | | X | X | X | X | X |
| **D2-R4** | X | | | X | X | | X |
| **D2-R5** | X | | X | | X | | X |

The subsequent sections will present the contributions. Each section will specify a particular solution,

framework, or architecture designed to resolve central challenges of healthcare data management. All these contributions aspire to simplify the data flow process, increase data value, assist decision-making in healthcare settings and explore new and emerging technologies.

# 6

# C1 - Context-aware electronic health record-an IoT and blockchain approach

Hospital inpatient care relies on constant monitoring and reliable real-time data. Continuous improvement, adaptability, and state-of-the-art technologies are critical for ongoing growth in efficiency, productivity, and readiness.

When appropriately used, technologies, such as Blockchain and IoT-enabled devices, can change the practice of medicine and ensure that it is performed based on correct assumptions and reliable data.

The proposed EHR can obtain context information from beacons, change the user interface of medical devices according to their location, and provide a more user-friendly interface. The data generated and associated with the location of the beacons and devices were stored in Hyperledger Fabric, a permissioned distributed ledger technology.

Overall, by prompting and adjusting the user interface to context- and location-specific information while ensuring the immutability and value of the data, this solution targets a decrease in medical errors and an increase in the efficiency of healthcare inpatient care by improving user experience and ease of access to data by health professionals.

Moreover, considering auditing, accountability, and governance needs, we must ensure when, if, and by whom the data are accessed.

## 6.1 Introduction

Health is one of the most concerning issues in human society. Health reflects the social, economic, political, and cultural circumstances in which individuals live, directly influencing their quality of life (Skinner, 2007). There is a need to continuously improve healthcare quality.

Healthcare has been confronted with many challenges, including high costs of practice, growing incidence of medical errors, inadequate staffing, and increased effort in administrative work by practitioners. Owing to limited financial and human resources, healthcare workers are under increasing pressure to provide more efficient services.

Access to reliable and accurate real-time data and the maintenance and pervasiveness of patients' are vital for good practice. The information included in these records can vary from progress notes, problems, medications, vital signs, and medical history to laboratory data and radiology reports. The usability of an EHR is crucial for achieving success and guaranteeing a safe and effective patient-care system. Therefore, care providers require their EHR to be practical, prompt, and effortlessly available (Pereira et al., 2012).

The solution presented here aims to increase the efficiency of clinical practice and reduce medical errors by seeking to increase the usability and ease of access to data by health professionals, where and when needed. In addition, with auditing, liability, and accountability present, assure the reliability and immutability of if and when sensitive data are accessed and by whom it concerns when needed.

## 6.2 Research Methodology

For the conceptualization and development of this solution, DSR was the methodology chosen to drive the development of the solution. DSR is a research methodology that analyzes the usability and performance of artifacts developed to understand, elucidate, and improve the behavior of certain aspects of Information Systems (IS). Thus, in this methodology, the knowledge, understanding, and solution of a problem are acquired as artifacts designed to solve a specific problem (Lacerda et al., 2013).

This research methodology comprises six phases designed to help guide the best way to answer a problem, starting with problem identification and motivation, defining the objectives of a solution, and the design and development of the actual artifact. The steps mentioned in the research methodology include demonstrating the efficacy of the artifact in solving the problem, followed by its evaluation and communication (Peffers et al., 2007).

## 6.3 Objectives

Establishing a clear goal in designing and implementing a well-functioning and functional Electronic Health Record (EHR) system is very important because it addresses the most pressing issues and expectations of the modern healthcare system. Expansion of the EHR system proposed solution aims to utilize implementation of technology such as Bluetooth beacons and also blockchain system to improve usability and dependability of the EHR system. The following objectives provide the primary targets of this work:

- **Context-aware Interface:** Create an adaptive EHR computer interface, which makes use of a real-time location system powered by Bluetooth beacons, to make patient information more useful and understandable to the users.
- **Ubiquitous Data Access:** Provide intuitive patient data information systems within the walls of the healthcare establishment in such a way that healthcare users can always get and work on information from any site.

- **Enhanced Medical Efficiency:** Provide a quick, context-based reach of generally hard to obtain compressed and coherent information on patient-related issues in relation to clinical decision making.
- **Data Security and Integrity:** Safeguard the security, integrity, and reliability of the EHR System by protecting every interaction with the system in a way that ensures that the data is unchangeable, is traceable and cannot be tampered with or altered by unauthorized parties.
- **Data Auditing and Tracking Optimization:** Develop and implement rigorous data audit systems to ensure that all interactions with data are accountable and efficient by concentrating efforts on movement tracking of healthcare professionals while maximizing their productivity and minimizing superfluous actions.
- **System Performance and Scalability:** Enhance the EHR system to efficiently perform enterprises-level engagements with quick responsiveness, reliable performance even in varying loads.

## 6.4 Design and Development

The overall goals set out earlier are the basis of designing and developing the proposed EHR – a context sensitive, safe and productive system that will efficiently fulfill the need of health workers in the changing environment. The approach mainly centres on the use of Bluetooth beacons for real-time context implementation, mobile application development, and proper data logging. In order to provide a more cohesive integration of a pervasive and context-aware EHR system, these activities have been organized into different phases .

### Pervasive and Context-Aware EHR

When treating a patient, healthcare workers need as much information as possible regarding their medical history, current state, requested examinations, and results. Although many solutions currently used in hospitals can provide information on patients, achieving this is cumbersome and not immediate.

By providing an app designed to run on mobile devices or tablets that respond to its environment and adapt its interface to the context in which it is inserted, the goal is to decrease the number of steps needed so that the EHR becomes easily usable, available, pervasive, and, therefore, more useful.

By interoperating with the hospital information system, vital sign monitors, and third-party vendor records, practitioners can access all the information they may need, where needed, so that the best care is provided to the patients.

This implementation aims to increase the ease of access and usability of EHR for physicians by gathering all patient information as doctors walk by their beds.

So to achieve this objective, the development was divided into 3 phases:

1) Phase A – Find the location of the users;

2) Phase B – Development of a Mobile EHR app;

3) Phase C – Maintain an immutable log of the data generated.

Subsequently, the development was followed by experimentation and discussion phases, as presented later in this document.

### Phase A

The implementation of a location system in a hospital care setting has several requirements and limitations. Therefore, they must be precise, reliable, durable, inexpensive, and easy to implement. Uncomplying with these requirements may lead to discrediting their implementation, future use, and growth.

Therefore, BLE beacons were believed to be the best choice for this study. The implementation was performed using the Estimote BLE beacons for ease of implementation, good documentation, and developer support.

Bluetooth low-energy beacons are small devices that other Bluetooth devices, such as smartphones or tablets, use for context-aware applications. Beacons advertise continuously and smartphones can use the received advertisements to estimate their proximity to the beacon (Zhao et al., 2019). Location is one of the most critical prospective applications of BLE beacons. GPS, which has revolutionized outdoor localization, has proven ineffective in indoor environments (Jeon et al., 2018).

Several third-party beacons, such as Estimote, were available for purchase and chosen for this project. These beacons ensure certain properties, such as

- Reliable enter/exit events.
- Fully configurable.
- Waterproof enclosure.
- Long battery life.
- Short lead time.

As presented in Figure 5, a Mobile background tracking app was developed, in React Native, whose sole purpose is to listen to proximity beacons and broadcast through Web sockets to any “Client” app that may require that information, such as our context-aware EHR.

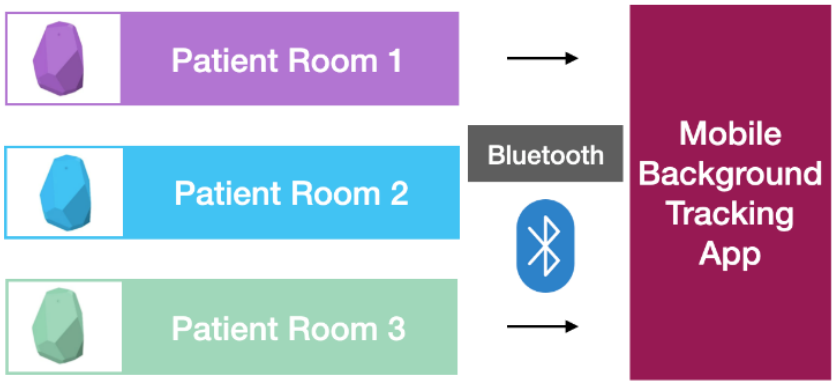



Figure 5: Context-Aware EHR - Communication between entities – Phase A

In this study, a mobile app that automatically adjusts the context in which a smartphone is inserted was developed. In the hospital context, the objective is to automatically change the interface of the mobile app when entering or leaving a room. In this experiment, four beacons were divided into four rooms.

When a healthcare professional holding a smartphone enters a room, the latter detects a Bluetooth beacon that informs the server, which automatically calls the information of hospitalized patients in that room. Subsequently, the patient's information was displayed in the application.

All beacons were set to have a range of 2.5 meters so that they did not conflict with each other when a user was inside one of the rooms where the beacons were allocated.

Therefore, they must be placed at least five meters far from others to provide good usage for health care professionals.

In Figure 6, an example of a hospital subsection floor plan with four rooms, where the four beacons are allocated:

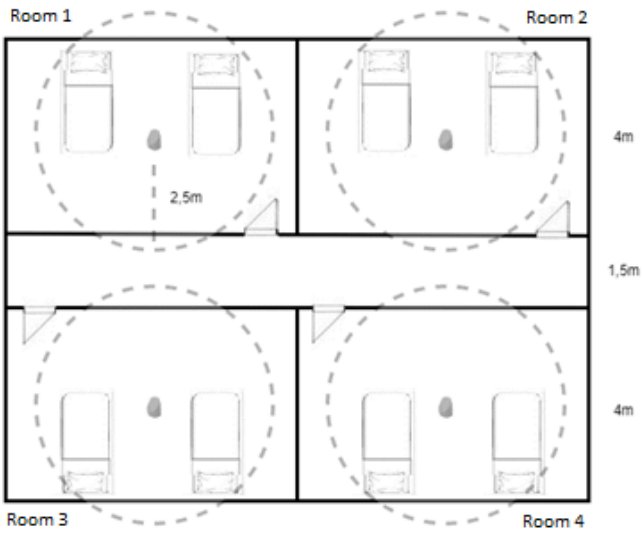



Figure 6: Simulated Hospital Floor Plan with Bluetooth Beacons

**Phase B**

This phase comprises the development of the mobile interface for the EHR.

By separating the gathering of device locations from the apps intended for physicians, the development of both mobile and web frameworks is an option.

The creation of this background-tracking app allows the decoupling of these functions from the many applications that can use it. The tracking functionalities are made available to "Client" apps or websites operating simultaneously or other authorized apps with various intents and purposes.

The solution architecture that encapsulates this concept is presented in Figure 7.

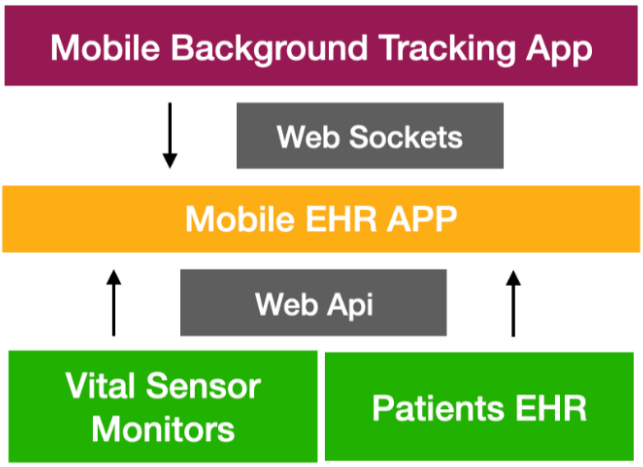



Figure 7: Context-Aware EHR - Architecture – Phase B

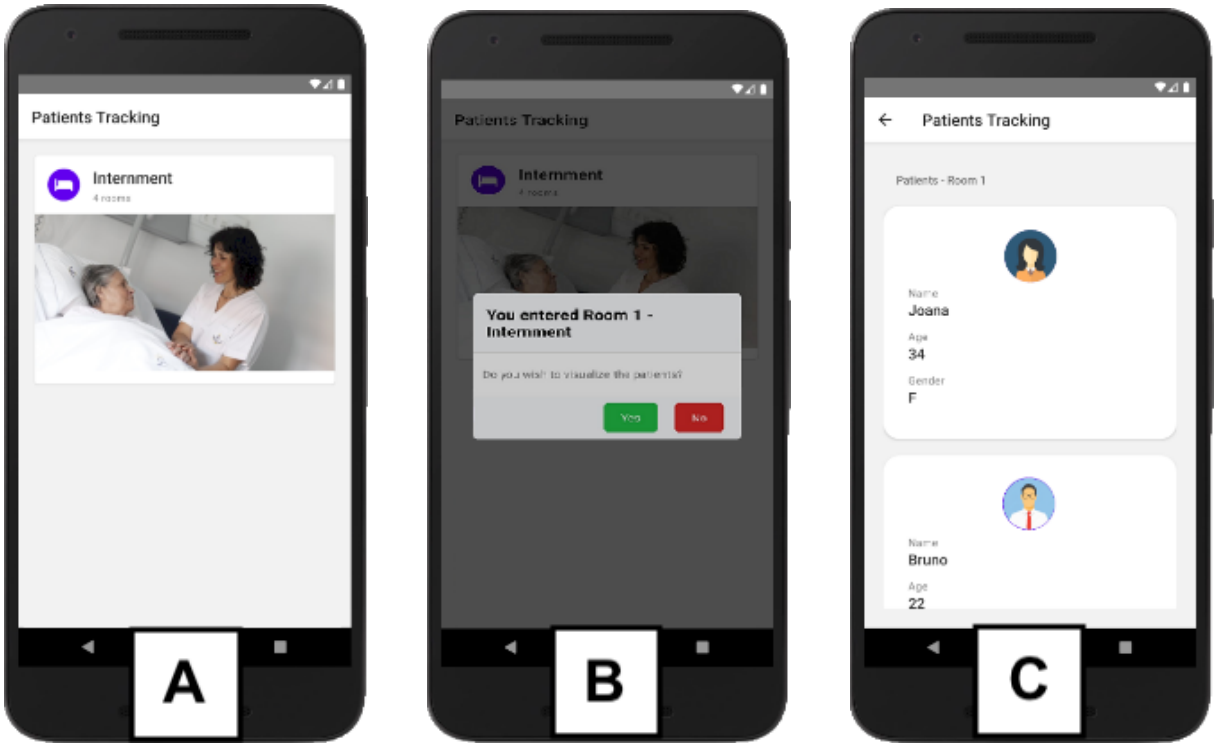
The Mobile App listens to web sockets from the background-tracking app and adjusts its interface accordingly. Knowledge of its location allows the app to present EHR records and vital sign live data from patients in the nearest bed (Figure 8).

A quick example of usage can be seen in the following steps:

A. A healthcare professional opens the application and is redirected to the home screen. In this prototype, the app was designed to allocate patient information to four rooms in the internment area.

B. Subsequently, the healthcare professional enters room number one and the smartphone detects a beacon. Automatically, an alert is shown in the app informing the healthcare professional that entered this room and asking if they wanted to visualize the information of the patients there.

C. Finally, if the healthcare professional presses the option "Yes," it is sent to a screen where all the patients' profiles are listed. Only patients who had received hospital treatment in a specific room are shown on the screen.




(a) Context-Aware EHR - Home Screen

(b) Context-Aware EHR - Beacon detection

(c) Context-Aware EHR - Patients' screen

Figure 8: Context-Aware EHR - Mobile Application Screens

### Phase C

Assuring the value and reliability of the location data is vital. Private blockchain presents a solution that not only assures the value and veracity of data within this context but also grants privacy and confidentiality to its users, making it possible to provide administrators and auditors with private and secure access to what physicians consulted the patient's data and when. This auditing functionality permits the auditing of work and performance analysis, and enables the argument for possible needs for further human resources to be employed.

HLF consists of two distinct parts that significantly benefit the solution: the world state and blockchain. The first is a distributed database across peers using CouchDB that preserves the current values of the attributes of an object. This allows programs to directly access the value of an object without navigating the entire blockchain. The second is the blockchain transaction log, which stores the history of the changes that have led to the most recent value in the world state collected in blocks (Faria et al., 2020).

These components not only allow this solution to be more efficient in retrieving the latest location of the device but also the complete history of data changes for the device.

In Figure 9, the general architecture for Phase C is presented. It displays communication with both apps and the blockchain, and within the blockchain itself. The latter focuses on the components of the Ledger and the Middleware that communicate with it. The transaction flow of information between these

two parts, adapted from (Guimarães, Moreira, et al., 2020), is as follows:

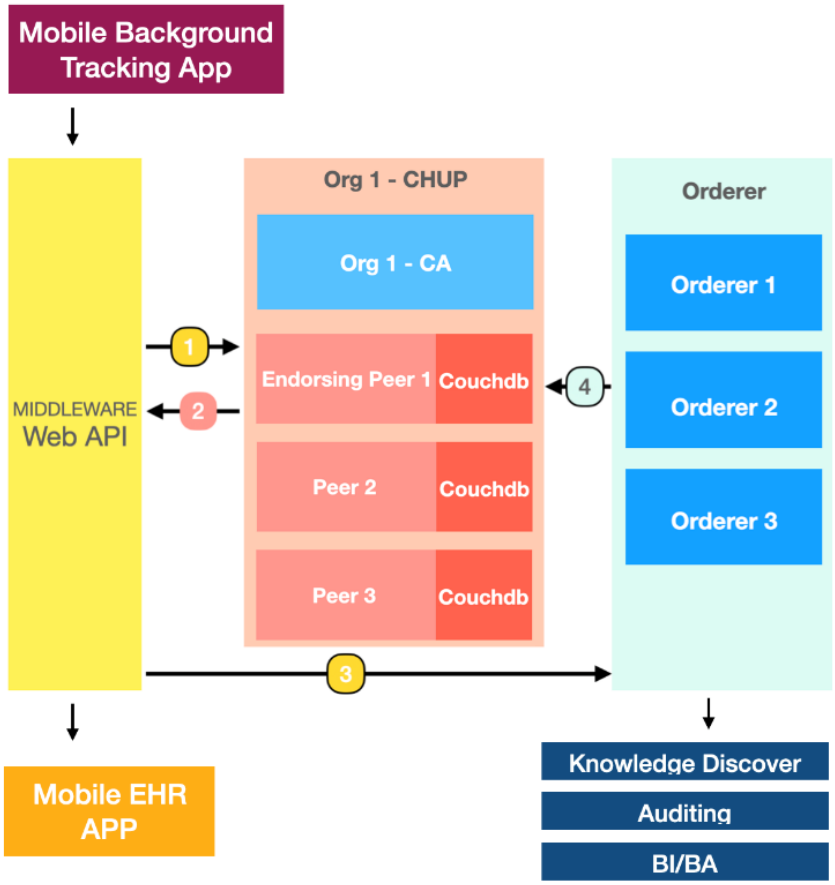



Figure 9: Context-Aware EHR - Architecture – Phase C

1. The middleware web API initiates a transaction through a request from the Tracking App.
2. Each endorsing peer checks if the proposal is well structured, if the application does not attempt to duplicate an existing transaction, if the signature of the issuer is valid, and if the issuer is allowed to perform the proposed operation. Each endorser executes the chain code individually, generates a transaction response based on the execution results, and then signs a response. Signed transaction proposal responses are sent to the application.
3. Orderers receive the endorsed transaction proposal responses from the clients.
4. The ordering service delivers a transaction to peers connected to it, whereas other peers eventually receive the block by gossiping. Each peer has an identical copy of the ledger (Shalaby et al., 2020)(Guimarães, Moreira, et al., 2020)(J. Sousa et al., 2018).

The blockchain is intended as the record of the following associations:

- Beacons and their location;

- The device and its location (Mediated through the Background tracking app);
- The physician and the device (anytime a physician logs in and out of the device).
- Physicians and rooms (mediated through the Background tracking application);
- Physicians and patients (any time a physician consults a patient record within the application). This record is anonymous, and only anonymous ids are recorded in the ledger.
- Authorized auditors, Business Intelligence and Analytics applications can consult the entire history of transactions in the blockchain within any of the smart contracts stated above.

The private Hyperledger Fabric blockchain was employed in a Linux Ubuntu virtual machine. A smart contract was created to define the data structure and functions required for the prototype. For instance, a struct named MedicalDevice was created in the smart contract to define the medical device data structure that will be stored in the tracking process. In the same line of thought, CreateMedicalDevice was developed to create the medical device asset and its insertion into the blockchain. Various functions for asset creation and state change were developed for this prototype. As presented in Table 4, we specified each function with its purpose.

longtable [table,xcdraw]xcolor

Table 4: Smart contract functions and API

| **Purpose** | **Function Name** |
|---|---|
| Create a Beacon | createBeacon |
| Create a Doctor | createMedico |
| Create a Medical Device | createDispMedico |
| Create a Patient | createDoente |
| Change the Room of a Beacon | changeBeaconSala |
| Change the Room of a Patient | changeDoenteSala |
| Change the Doctor of a Medical Device | changeDispMedMedico |
| Change the Room of a Medical Device | changeDispMedSala |
| Change the Patient of a Medical Device | changeDispMedDoente |
| Get the state history of a certain asset | getHistoryForAsset |

This structure allows asset creation, asset state updates, and viewing of the asset state history, which helps in the tracking process. For instance, one can check which rooms a given patient has been in,

which doctors have access to a medical device, and which patient information they consulted at a certain time.

Figure 10 shows a post request made to the API to create a medical device in the blockchain.

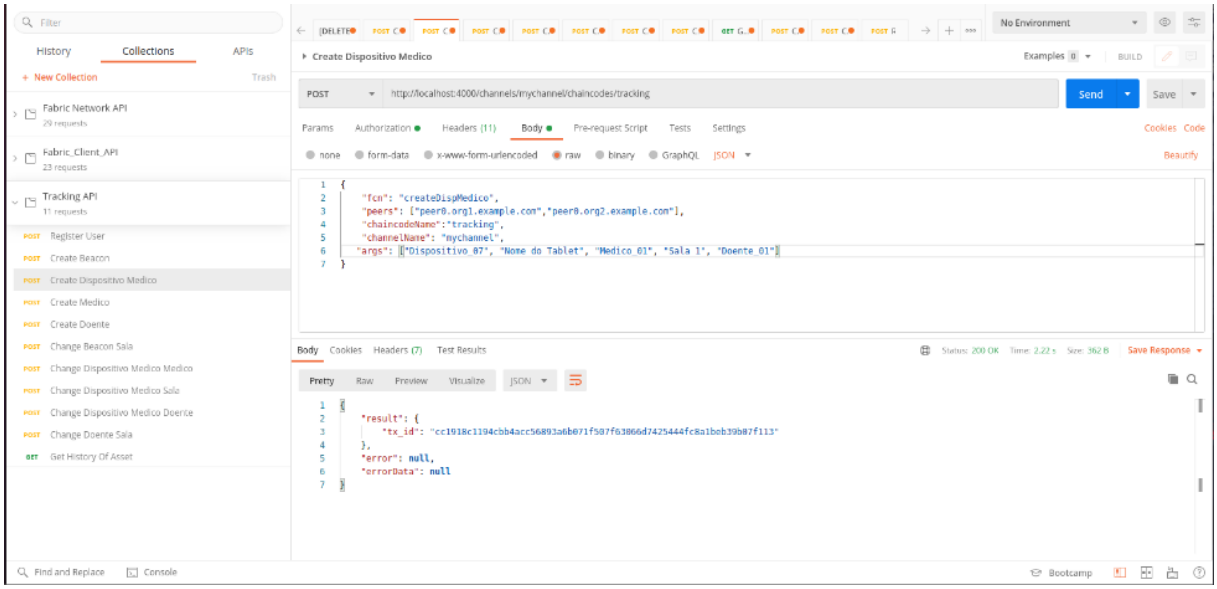



Figure 10: API call to Create Medical Device in the Blockchain

## 6.5 Experimentation

Several experiments were carried out to analyze the performance of the proposed blockchain solution, namely, to analyze the transaction latencies and success rates for 1k transactions and 10k transactions at 40 Transactions per Second (TPS) and for 100 transactions at 100, 1k, and 10k TPS. A benchmarking tool is essential to conduct such experiments. *Hyperledger Caliper* was used for this purpose.

*Hyperledger Caliper* is a blockchain-benchmarking tool that allows users to assess the performance of blockchain implementations against a set of predefined use cases.

In the first experiment, two benchmarks were performed with a transmission rate of 40 transactions/s. First, 1000 transactions for each function created were committed to the network to evaluate the performance of each function. In the second benchmark, 10000 transactions for each function. Note that the first function, *Create beacon*, is missing. This is because the first transaction of the benchmark requires substantially more time than the remaining transactions, making the variation between the function metrics more difficult to visualize. However, the performance of the first function exhibited the same behavior as that of the other functions for both benchmarks.

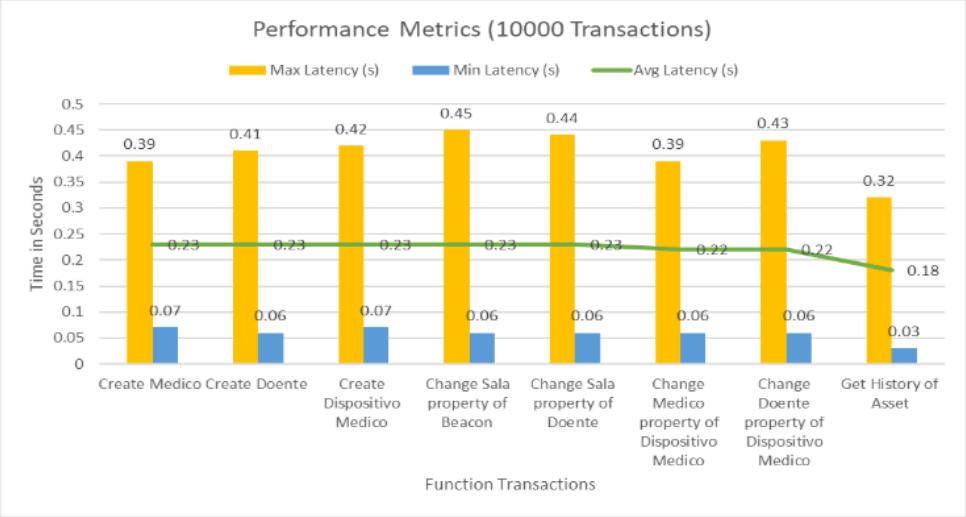



Figure 11: Blockchain Performance Metrics (10k Transactions per function)

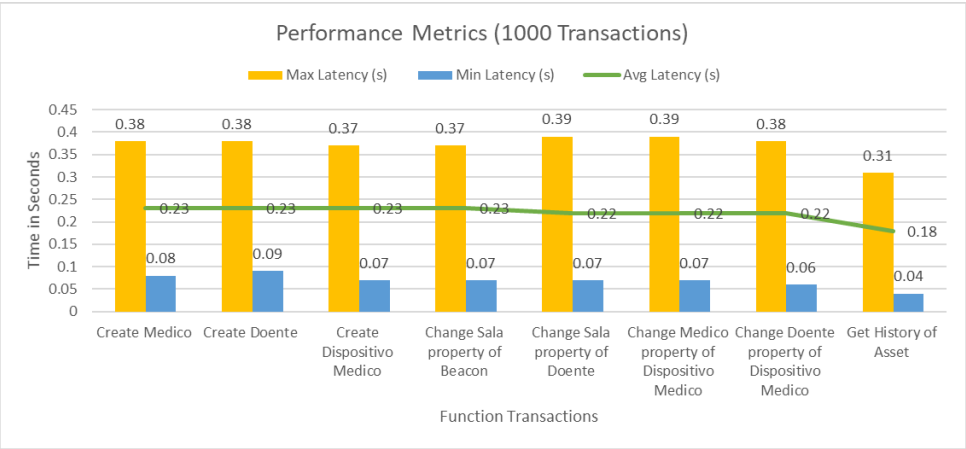



Figure 12: Blockchain Performance Metrics (1k Transactions per function)

From Figure 11 and 12, we can see that moving from 1k transactions to 10k transactions resulted in a slight increase in the transaction's maximum latency, but the average latency remained almost the same. This may be because the second benchmark environment applies more transactions; therefore, there is a greater chance that one of these transactions takes more time, thereby increasing the maximum latency value. It can be stated that the number of transactions has almost no impact on blockchain performance. The *Get History of Asset* is a query function that is significantly faster than its counterparts, and has the lowest maximum, minimum, and average latencies. From this result, it can be concluded that overall, query functions are faster in terms of latency than asset creation and state-change functions.

For the second experiment, three benchmarks were carried out for 100 transactions per function with 100, 1k, and 10k TPS, respectively, to analyze the send rate, throughput, and latency of the proposed solution. After concluding the three benchmarks, because Hyperledger Caliper outputs the send rate and

throughput of every function, we calculated the average of both metrics to obtain a better view of performance, thereby reaching a more significant conclusion. Figure (**fig:Average Send Rate vs. Throughput**) illustrates this analysis.

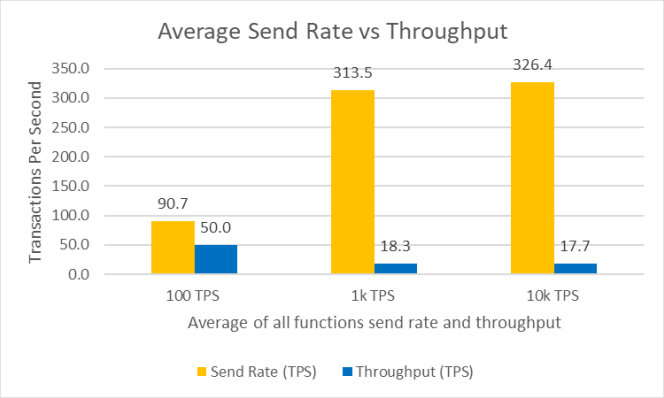



Figure 13: Blockchain Benchmarking - Average Send Rate vs. Throughput

Figure 13 shows that the average sending rate increases as TPS increases, as expected. Furthermore, the throughput decreased significantly with an increase in TPS. This happens because the blockchain system cannot handle the high number of transactions being sent in a second and fails to commit the transaction Figure 14 illustrates the average of transactions that failed per benchmark, which justifies the previous statement.

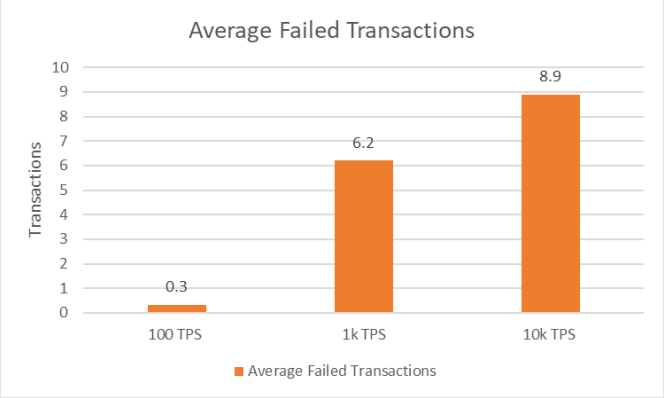



Figure 14: Blockchain Benchmarking - Average Failed Transactions

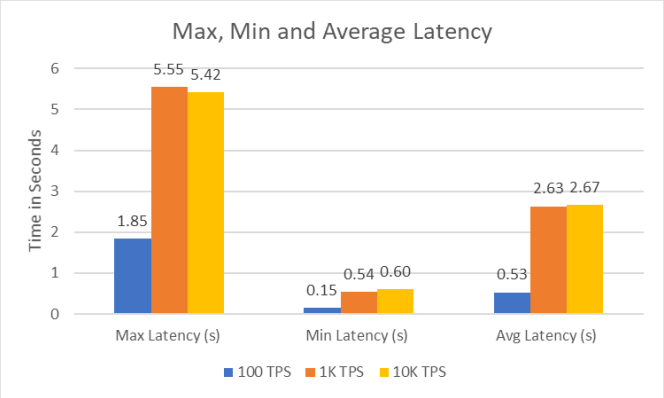



Figure 15: Blockchain Benchmarking - Latencies

As shown in Figure 15, the average latency increases substantially from 100 to 1k TPS and a very slight increase from 1k to 10k TPS.

The scalability of a system is directly affected by the number of transactions sent and the processing power of the machine running the system.

## 6.6 Discussion

Building on the findings from the experimentation phase, a SWOT analysis was conducted to provide a comprehensive evaluation of the proposed IoT/blockchain-based EHR system. This analysis aims to critically assess the system's performance, identifying key strengths and opportunities that highlight its potential benefits, while also addressing any weaknesses and threats that could impact its effectiveness and adoption.

By examining these factors, the discussion will offer a balanced perspective on the system's overall viability and readiness for deployment in healthcare environments. The SWOT analysis will also guide future improvements, ensuring that the system can be optimized to meet the evolving needs of healthcare professionals and institutions.

### Strenghts

S1. Less time spent on data insertion on the EHR;

S2. Less time spent on record analysis;

S3. Level of awareness;

S4. Ease of access to information;

S5. Ease of portability and multitasking;

S6. High precision in the location of the devices and patients;

S7. Effective interoperability is achieved by collecting information from various sources and numerous datasets in order to empower advanced analytics.

S8. Controlled and supervised access to data;

S9. Logs Users' iterations within the app;

S10.Ensures the veracity and authenticity of the data generated.

### Weaknesses

W1. Requires a connection to the hospital network;

W2. Requires investment in Beacons and Mobile devices;

W3. Demand for a correct association between patients and beds. Although correct, incorrect associations must be promptly detected and corrected.

W4. Requires a correct association between the device and the doctor using it;

W5. Complex infrastructure comprises many possible points of failure.

### Opportinities

O1. Urging need to increase efficiency in healthcare;

O2. Mobile pervasiveness and ubiquity;

O3. Mobile technology is increasingly powerful and fast;

O4. RGDP legislation requires logs for access to Health data

### Threats

T1. Low adoption by healthcare professionals;

T2. Due to portability, mobile devices can be lost or broken easily;

T3. Lack of investment in healthcare unities due to restrictive governmental policies;

T4. Battery life of mobile devices.

## 6.7 Related Work

Some examples of context-aware frameworks using various IoT-enabled devices have been documented in the literature. These include:

In (Baig & Jilani, 2018), the authors presented a context-aware solution by identifying health conditions and tracking patients using BLE Beacons in real-time. Context awareness of this solution is intended to

send alert notifications to the nearest rescue medics or emergency centers, including patient locations in critical medical conditions.

In (Sykes, 2020), the authors presented a context-aware system that uses mobile applications and beacons to track the security guard rounds. This system was intended to reduce missed zones and provide opportunities for rich data analysis and report generation.

In (Adame et al., 2018), the authors presented CUIDATS, an RFID–WSN hybrid monitoring system that provides location, status, and tracking of patients and assets. Although many architectures, systems, and frameworks have been reported in literature, the authors of this study were unable to find any information related to the research focus.

## 6.8 Summarize

This solution contains various elements that occur during the three stages of development. It aims at delivering the optimal solutions for healthcare providers, patients and managing services, the key focus being providing physicians with ease of obtaining all required information on a patient at the time and place needed.

The intent is to optimize hospital inpatient care, which can be cumbersome and laborious, by using state-of-the-art technologies.

Recent data access regulations have ensured that institutions must guarantee high accountability for unauthorized access to patient data.

When testing and evaluating an architecture, it is crucial to understand and analyze the level of satisfaction of the target audience. Therefore, it is pertinent to evaluate and instantiate the qualitative and quantitative variables of the technology acceptance model. A panel of experts measured the qualitative variables S3, S4, S5, and T1. On the other hand, quantitative variables such as S1, S2, S6, S7, S8, and S10 can be measured by a comprehensive analysis of the platform's data.

Future research may pursue several paths. Further analyses are required to obtain solutions with multiple beacons per room, including the feasibility of having one beacon per bed instead of per room and the minimum acceptable distances between each bed. Thus, even inside a room, a healthcare professional can obtain information about a patient who is closer to him.

In the prototype, patient information was basic. Further studies are required to improve the data provided by the EHR applications. Data related to a patient's problem/disease, medication schedules, and perhaps, real-time data related to vital signs can be included.

# 7

# C2 - Blockchain Analytics - Real-time Log Management in Healthcare

As healthcare organizations increasingly rely on information technologies, ensuring data security becomes essential due to the sensitive nature of the information involved. To meet this need, a system was created featuring a private blockchain network specifically designed to record hospital logs, accompanied by an interface for facilitating data analysis. This use case details the development of a private blockchain solution and a web platform. Additionally, web technologies such as WebSockets, were integrated to enable real-time log interfacing. The primary goal of this solution is to provide real-time visualization of logs, allowing for the application of various analysis methods.

## 7.1 Introduction

Health is one of the most concerning issues in human society. From a very early age, mankind began to be concerned with diseases since these factors have been present throughout evolution. The concept of health reflects the social, economic, political, and cultural circumstances in which an individual is inserted, directly influencing his/her quality of life (Skinner, 2007). In this sense, the need to improve healthcare quality arises. For this purpose, it is necessary to ensure accurate and concrete information so that the decision-making process is useful and provides value to the patient (AbouZahr & Boerma, 2005; Haux, 2006; Lippeveld et al., 2000). The management and availability of confidential and sensitive data, such as healthcare data, requires special attention and a set of specific rules to ensure its authenticity, privacy, and security. Several healthcare systems present this problem in that they do not guarantee the immutability of the data (Angraal et al., 2017) and therefore represent a threat to the privacy and security of the patients (M. L. Sousa, 2017). Blockchain technology offers a solution to this problem, as it guarantees a chronological order of data as well as its authenticity, privacy, and security (Angraal et al., 2017).

## 7.2 Objectives

The objectives of this study can be classified into four major objectives that tackle certain problems in data management and decision making in health care. The objectives are:

**Enhance Data Security**

- Develop a system to protect the integrity and confidentiality of sensitive healthcare data.
- Address the need for secure data handling in healthcare due to the sensitive nature of the information gathered.

**Implement a Private Blockchain Network**

- Create a blockchain infrastructure using Hyperledger technologies for secure data management.
- Employ technology that ensures safety and helps manage health-related data.

**Facilitate Real-Time Data Analysis**

- Provide an interface with real-time elements for efficient data visualization and better patient care.

**Improve Decision-Making Process**

- Apply various analytic methods to real-time data for informed healthcare management.

## 7.3 Design and Development

Incorporating the blockchain technology in applying the health concepts may provide a better aspect towards the availability, security, and dependability of confidential information. Here, the development of a real-time logging system for the healthcare environment has been proposed. This system uses a private blockchain network to make sure the logs of the hospital are tamper-proof and can be tracked, which in turn aids in data analysis and decision making. The use of Hyperledger Fabric as the underlying technology, provides the solution with the highest level of security, scalability and, reliability, especially in managing data within the healthcare sector. As the solution advanced from theoretical to physical application, the design-and-development processes are presented, pointing on major factors and strategies used to complete project tasks.

## Real-time Log Management in Healthcare

A private Blockchain network based on permissions using the Hyperledger Fabric technology was built with the purpose of storing hospital logs in a safe and immutable way for further analysis and the consultation of the data when needed. In order to make this possible, a Chaincode was created using Go, which is running in the blockchain network that, with the rest of the configured settings that were also made, allows the proper function of the proper function of the network and the register of the hospital logs. To complement the blockchain network it was developed a web interface with the intention of analysing and comprehending the data stored.

## Solution Architecture

This solution works in accordance with the ledger of the Hyperledger Fabric with the help of the Chaincode created for the purpose and the CouchDB that stores the data as it is at that specific moment. Additionally, a web interface was developed, with the data stored on the network updated in real-time by using socket.io. The following image represents the architecture developed to achieve the final solution.

Hyperledger Fabric was chosen due to its modular architecture, which allows for the flexible implementation of different functions, including smart contracts, access control, and data confidentiality mechanisms (Cachin et al., 2016). The system integrates a CouchDB database for data storage, ensuring that all records are consistent with the state of the blockchain at any given time.

A custom Chaincode, developed in Go, handles transaction validation and data storage logic, ensuring that only authorized actions are recorded in the blockchain ledger (X. Xu et al., 2019).

With the data stored on the network, the web interface is updated in real-time using WebSockets, namely socket.io. This enables real-time updates and data visualization, allowing healthcare professionals to monitor logs and analyze data instantly.

The architecture enhances data security and auditability while providing a scalable and efficient approach to managing sensitive healthcare information. Utilizing blockchain technology's properties ensures that every transaction and data entry is securely recorded and can be monitored for any unauthorized alterations. This level of security is considered important in healthcare, where maintaining the integrity of patient records is necessary for protecting privacy and meeting regulatory standards.

The system's design allows for scalability and efficiency, supporting the management of large volumes of real-time data within a hospital setting. Hyperledger Fabric's modular nature facilitates the addition of new nodes or integration with other healthcare systems, enabling the solution to grow in line with institutional needs without significantly affecting performance. Using smart contracts helps automate data management processes, reducing the potential for human error and promoting consistency in operations.

This architecture is intended to meet the current requirements of healthcare data management and has been developed with future adaptability in mind. The combination of security, auditability, scalability, and efficiency is expected to offer a reliable solution for managing healthcare information in various settings.

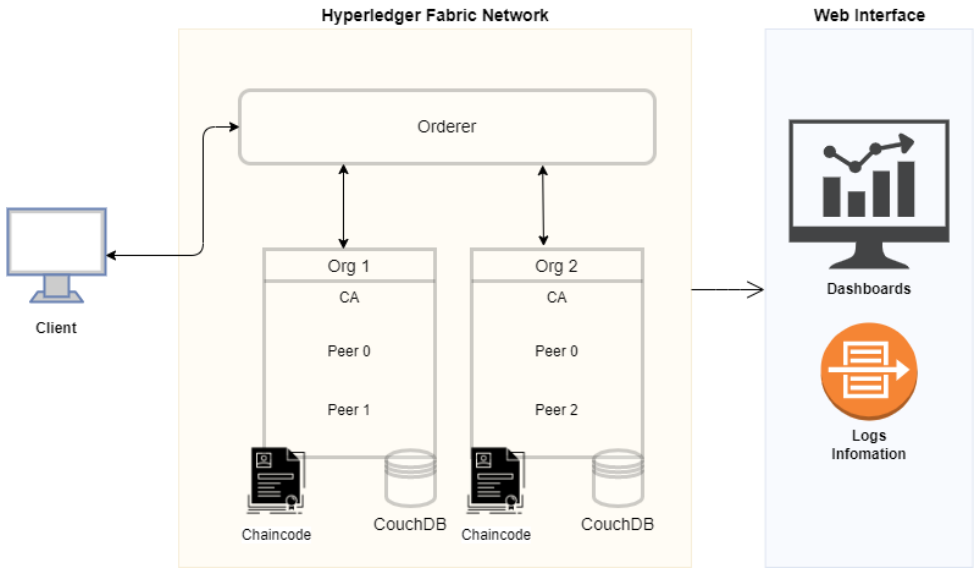



Figure 16: Real-time Log Management - Architecture

## Web Interface

The web interface consists of two areas for consultation and analysis of the data stored in the blockchain.

In the consulting area, it is possible to check every log registered in the blockchain in real-time, so it is easier to see the movements happening at that moment and find some anomaly or something that shouldn't be happening. Furthermore, it is still possible to know how many users have logged in that day on the platform and what the most accessible application in the system is. In the analyses' area, it is possible to search for any log in the blockchain, see every attribute, and access some graphics for the logs' analysis. The graphs show the number of logs recorded over time on a monthly scale, the total number of logs and the comparison between each application inherent to the system. In images 17 and 18, it is possible to observe some visuals present in the two mentioned areas.

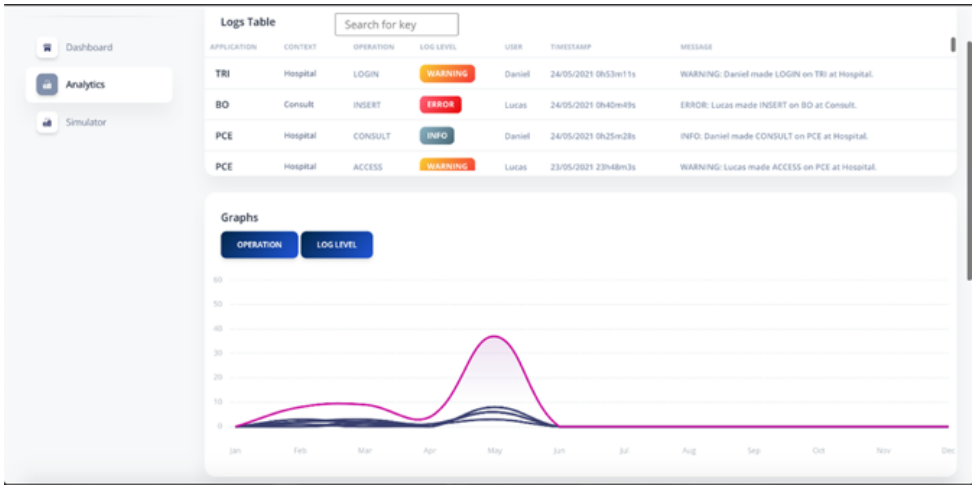



Figure 17: Real-time Log Management - Log Data Consult

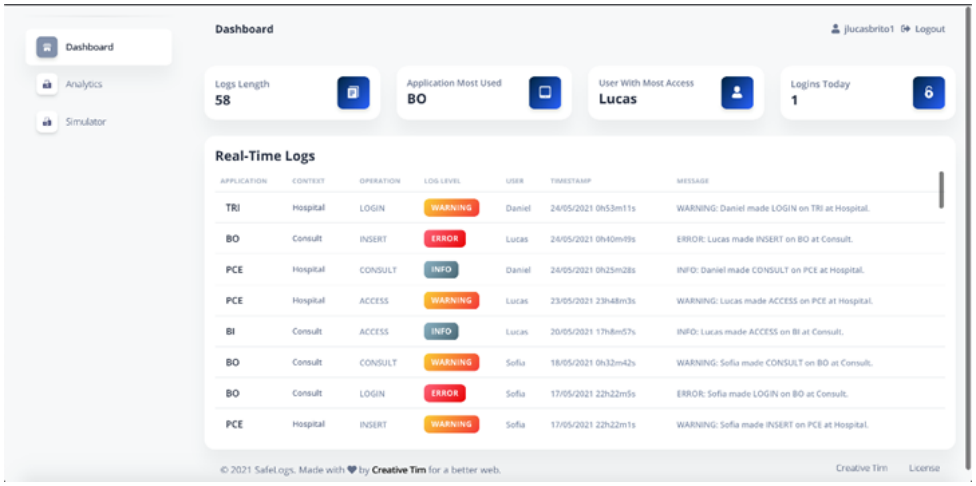



Figure 18: Real-time Log Management - Log Data Analysis

## 7.4 Summarize

The constant evolution of data management solutions has enabled growth in efficiency and reliability and in the confidentiality and privacy of patient data. When developing a platform to support a healthcare institution, it is essential to ensure the veracity and value of the data used. Over the long run, understanding the data and being able to use it correctly will lead to faster decisions with fewer human or medical errors. For vital areas, such as healthcare, being able to understand data while respecting patient privacy will lead to a more sustainable and truthful practice. The implementation of Blockchain technology provides health benefits such as integrity, security, immutability, verifiability, and resistance to breaches of sensitive medical data. The enumerated benefits facilitate the data management process for the most diverse actors present in the area and also ensure accountability for improper consultations of private data or

patient confidences. In this context, it becomes an adequate solution with the potential to improve this sensitive and critical area, such as health.

Through the Blockchain application developed, it is possible to maintain a database with the current data, where analysis methods are applied to the logs registered in the blockchain network. With this process, an important step was taken to maintain a fully functional network. However, it is not enough just to store the data; it is essential to perform an analysis of them to find patterns and anomalies that avoid both human and network errors. In addition, with increasing documentation, evolution, and contributions, and by supporting smart contracts created in general-purpose programming languages, the learning curve for its implementation is reduced when compared to other solutions.

# 8

# C3 - Leveraging Standardized Real-Time Data Repositories and Blockchain to Enhance an AI-driven Healthcare Decisions

As healthcare systems have been embracing technology, the processes of clinical examination, health records and various other healthcare processes are continuously providing real time data to every organization. This data has tremendous potential, and with advanced analytics and machine learning, it can lead to better patient diagnosis and personalized treatment plans. However, this potential requires a comprehensive architecture for integration and analysis of real-time data that is also able to focus on ethics, privacy, and security. Patient data is sensitive, and its use must comply with privacy regulations, respect informed consent, honour their agreement on the use of their data, and explain the policies on the acquisition, use, and release of such data.

To address these concerns, this study proposes a secure and scalable solution to data storage that allow real time patients' data integration from different health facilities employing health data standards like HL7. In order to maintain the integrity and security of data, a blockchain layer based on Hyperledger Fabric will act to provide an immutable and auditable record of all transactions performed while ensuring that there is no unauthorized access and tampering with the contents of this record.

The designed architecture also aims to enhance the interoperability and scalability of data in use in different health sectors in order to allow for improved data sharing and collaboration. In addition, it will adhere with the FAIR principles (Findability, Accessibility, Interoperability, and Reusability), taking into consideration some strategies and considerations. The FAIR principles are indispensable as they aim at improving the administration, distribution, and application of data which is extremely relevant in the health sector where data has to be kept safe yet be available for research, treatments, and other medical decisions. This will enable more comprehensive data analysis, improve decision-making, and support research initiatives. The purpose of this research is to enable a broader adoption for more practical and real-time healthcare supported data initiatives while ensuring a strict adherence to ethical, privacy, and security standards.

So, this study aims to answer can a real-time data repository, strengthened by advanced analytics and blockchain security, improve patient outcomes and personalized treatment based on machine learning models while addressing the ethical, privacy, and security challenges following the FAIR principles in healthcare?

## 8.1 Introduction

Lack of evidence on pathogenic organisms, risk prediction, insufficient resources, and ineffective therapeutic options often violate the evidence-based medicine premise (D. Oliveira, Ferreira, et al., 2021; Vijayvargiya et al., 2020). Consequently, traditional methods have been replaced by AI, Machine Learning (ML), and even applied statistics. However, developing and deploying AI and ML systems requires massive data sets. Access to medical data, such as EHRs, is sometimes restricted by legislation designed to protect patient privacy. These restrictions make reproducing existing results based on private health data difficult and delay progress and studies (Cornock, 2018; Duan et al., 2019). Typically, this problem is solved by using synthetically generated health data, which protects privacy while allowing researchers to analyze and inform decisions. Indeed, this is an enormous temptation compared to the time and resources required to gather and categorize datasets containing millions of pieces retrieved from the actual world. Nevertheless, these contain simplified, generated data based on actual data (R. J. Chen, Lu, et al., 2021). The goal is for the synthetic data to represent the original data accurately. However, the problem of providing realistic data without exposing private information is recognized (F. S. Saleh et al., 2018). Alternatively, if the synthetic data is insufficiently accurate, it will not reflect the essential patterns of the training or test data. Modelling efforts based on implausible data cannot produce useful insights (F. S. Saleh et al., 2018).

Data processing methods, such as anonymization, are noteworthy. They allow the anonymization of real health data and provide valuable information about patient visits to health units. This results in a time series dataset influenced by protected attributes like age, gender, and location. When entering the universe of data from the patient's medical record, the amount of data to be processed increases exponentially (Langarizadeh et al., 2018b). Millions of people produce valuable medical data records daily to feed information systems such as those used for forecasting or decision support. They require preprocessed and normalized data to improve their performance sequentially.

This is precisely the stated flaw: the absence of real-time updated data repositories containing data collected in the field. Thus, many EHR-based research papers lack follow-up data, challenging further study and validation. Depending on clinical analysis results, providing a standardized and real-time data repository based on interoperability technologies would be highly beneficial to improve healthcare delivery, especially in supporting professionals in tracking disease progression, assessing risks and other tasks. After a health crisis comparable to that caused by COVID-19, all these benefits can be highlighted (D. Oliveira, Miranda, et al., 2021; R. Sousa et al., 2021).

In addition to the inaccuracy and insufficiency of such datasets, the proposed system aims to address the escalating challenges in data security and integrity in healthcare by integrating blockchain technology into the healthcare data repository.

Traditional data management systems are increasingly vulnerable to breaches and tampering, particularly in the healthcare sector where the stakes are extraordinarily high (Shull, 2019). Sensitive patient data, if compromised, can lead to severe privacy violations, legal ramifications, and a loss of trust among patients and healthcare providers. With its inherent immutability, transparency, and decentralized trust, blockchain technology offers a robust solution to these challenges (R. J. Chen, Lu, et al., 2021). By ensuring that every transaction within the data repository is securely hashed and recorded on a permissioned blockchain, this approach provides an immutable audit trail that authorized stakeholders can independently verify. This level of security is crucial for protecting sensitive data and maintaining the accuracy and reliability of the data that drives critical healthcare decisions (Langarizadeh et al., 2018a). Without such measures, the potential for data corruption or unauthorized access could significantly undermine the effectiveness of machine learning models and other advanced analytics used to inform patient care, ultimately jeopardizing patient outcomes (Topol, 2019). Therefore, adopting a blockchain-based approach is not merely an option but a requisite for any healthcare data management system aiming to meet the highest data integrity, security, and trustworthiness standards.

As previously stated this architecture should follow the FAIR principles in order to enhance the management, sharing, and use of data, which is particularly crucial in healthcare where data must be securely handled, yet readily available for research, clinical decision-making, and personalized treatment. Following one can find how the architecture was compatible with each of the FAIR principles:

**Findability:**

The architecture encompasses an standardized metadata format and unique identifiers using uuids, thus making any data entry easily found. An exhaustive indexing system is, however, to be incorporated within the data repository, allowing workers in healthcare and clinical research to sort and retrieve the necessary data easily. This was been done by using current medical ontologies and controlled vocabularies (for example: SNOMED CT, ICD) to improve the metadata. The use of a safe and searchable blockchain distributed ledger will create a record for all transactions and modifications made to comprise a traceable history of every data entry.

**Accessibility:** The repository is open to users through standard protocols (REST API) for data access; therefore, authorized users can retrieve and use the data while maintaining security and privacy standards. It was established well-defined authentication and authorization mechanisms that are compliant to the said accessibility requirements and make sure data is accessible to all the right people and only to those people, the sensitive patient data is protected. This encompasses role based access (RBAC) and safe storage and access of information policies that are transparent and enforceable. Restricted access to the content will be ensured by end-user licenses agreements and usage terms complying with the current legislation, in this case GDPR, outlining who can access the data and under what conditions.

**Interoperability:**

The framework is compliant to the well-known general health information technology exchange standards, such as HL7 FHIR, meaning data exchange can happen smoothly to other systems and organizations. Use of common data models and standard formats e.g. JSON, XML allows to considerably minimize the preprocessing of information coming from different origin and facilitates the interoperation of distinct healthcare systems.

This architecture provides all the participants access to a Blockchain-backed ledger that registers and verifies all the transactions to promote opportunities for trust and data consistency among the various platforms.

**Reusability:**

The data repository makes sure that the data includes additional attributes and elements that define its context, and lineage dus to the fact that wherever it may be used, it will be correctly and efficiently utilized be it in patient care, studies, or development of regulations. The architecture further allows for data information management and storability whereby the aspects of the data will be systematically processed to include the changes that occur and older copies are used to perform validation or further analysis. The repository through its strong governance structure has policies which evaluate data that will be shared, access to data and the reuse of data, ensuring that data remains valuable and does not infringe ethical standards, and is usable by a wide range of stakeholders.

## 8.2 Research Methodology

Even in healthcare, IS research is primarily characterized by behavioural and design science paradigms. The former seeks to push the limits of human and organizational capabilities by developing new and innovative Information Technology (IT) artefacts broadly defined as constructs, models, and/or methods. The latter seeks to push the boundaries of human and organizational capabilities (Hevner et al., 2004). DSR methodology for IS is suited for carrying out this research procedure because the work described results in an IT item.

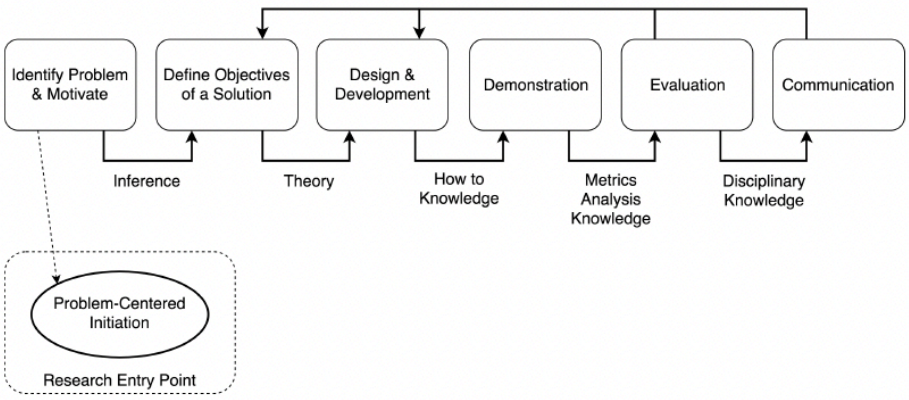



Figure 19: Main Research Methodology: Design Science Research. Adapted from: (Hevner et al., 2004).

As a result, when looking at figure 19, it becomes clear that the effort began with a problem already identified: the demand for more anonymized data updated in real-time for health research. The definition of the primary goals of the job comes after determining the gap and motivation, as shown in the figure.

## 8.3 Objectives

The main objectives that will be attained by using this strategy are the following, starting with the stated challenge:

- Analyze the data obtained through HL7 messages (Mirth Connect) in real-time;
- Sorting and processing the data gathered in the preceding point to retain just the relevant information;
- Identification of additional information of interest that should be included in the data repository but is not covered in the preceding point;
- Data availability, storage system selection and development, real-time data loading and updating using Big Data approaches;
- Ensuring integrity and reliability of the data repository;
- Validation of the data repository by health professionals.

## 8.4 Proposed Model

The proposed model architecture is designed to enhance healthcare data management by ensuring that data are efficiently integrated, securely stored, and accurately processed. This architecture supports seamless data exchange, scalable storage solutions, and robust security measures to protect data integrity. By leveraging advanced preprocessing techniques and secure access methods, the model aims to provide reliable and actionable insights, supporting effective decision-making in healthcare environments. The architecture is flexible and scalable, making it capable of adapting to the evolving demands of healthcare data management.

### Architecture

The architecture is presented in the figure 20, and its components will be detailed subsequently.

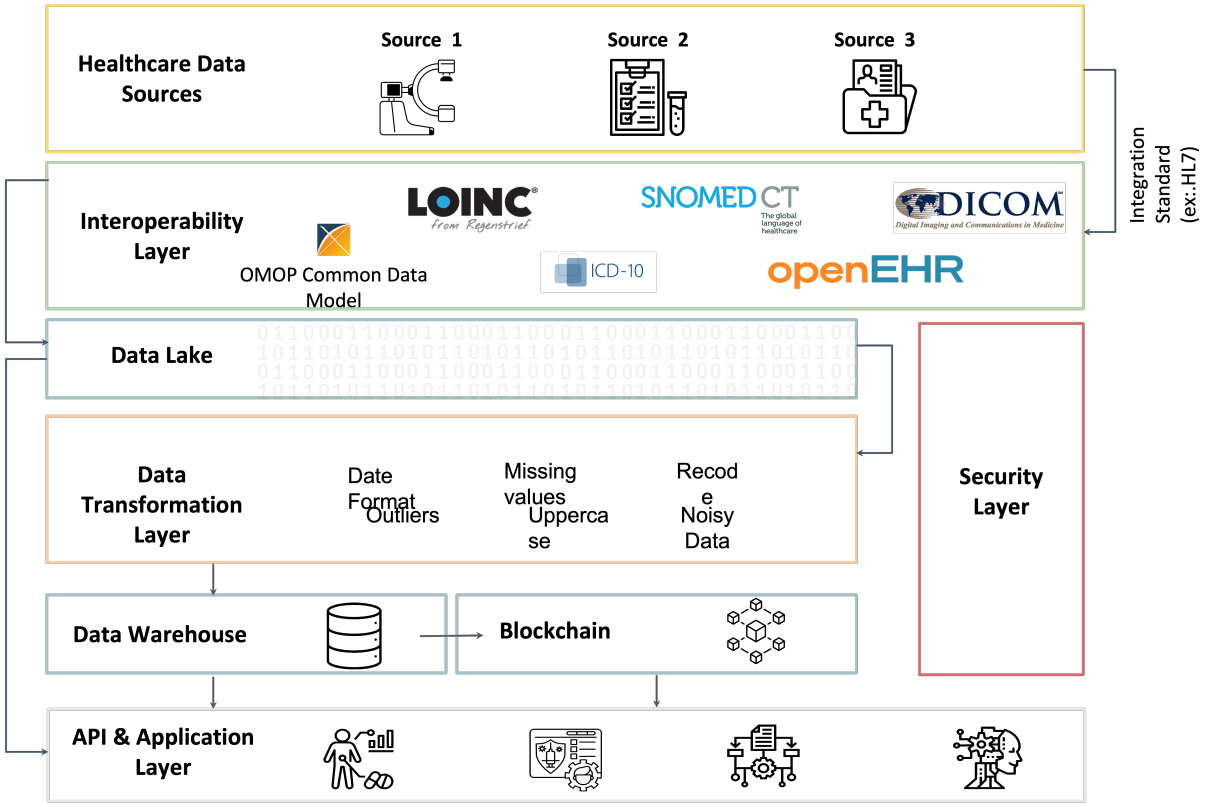



Figure 20: Proposed Architecture for the Real-time Data Repository

Data sources send information through a transport standard, such as HL7, to a central section where the data is standardized according to its type. These data are then stored in a data lake for processing, transformation, or direct consumption.

Next, a transformation layer processes the data according to specific needs, such as correcting missing values or eliminating noise. After this step, the data is stored in a data warehouse and sent to the blockchain to ensure data security and integrity.

Users can access the data through an API, choosing between data from the data lake or the data warehouse.

This architecture is designed to be highly scalable and flexible, allowing the integration of new data sources and customising data processing according to specific needs. Using blockchain ensures data integrity and security, guaranteeing the information is reliable, immutable and auditable (Levandoski et al., 2024).

This approach can be applied in various domains, including healthcare, finance, and e-commerce. With its ability to process large volumes of heterogeneous data, this architecture is a robust and efficient solution for meeting the growing demand for real-time data and actionable insights.

## Components

### Healthcare data sources

Heterogeneous data sources, such as patient databases, electronic medical records, and monitoring systems, are integrated into a single environment using transport standards like HL7. These standards allow for the exchange of information between different systems, enabling data to be easily accessed and processed on a unified platform.

Integrating heterogeneous healthcare data sources using HL7 protocols is essential for enabling real-time interaction between various systems, including wearable IoT devices and EHRs. This approach facilitates seamless data exchange and supports data standardisation across multiple platforms, enhancing the overall interoperability within healthcare environments. Studies have demonstrated the effectiveness of HL7 in integrating medical data, allowing for improved patient identification and care delivery processes (AlQudah et al., 2021).

The use of HL7 and FHIR in data integration also supports the merging of structured and unstructured data from various sources, making it possible to provide personalized decision support at the point of care. This integration ensures that healthcare providers can access accurate and timely data, critical for making informed decisions in clinical settings (Beckmann et al., 2023).

### Interoperability Layer

Standardizing healthcare data using globally recognized standards is essential for achieving interoperability across diverse healthcare systems. These standards facilitate the seamless exchange and integration of data, ensuring that healthcare information can be accessed and processed consistently, regardless of geographical location. Implementing such standards as HL7 or FHIR in healthcare systems has been recommended by the WHO to promote the secure and efficient sharing of health data across borders. (Jaffe et al., 2023; Sinaci et al., 2023).

### Data storage - Lake, Mart, warehouse

After being standardized, the data are stored in a data lake, a centralized repository for raw data storage. The data lake is highly scalable and can store large volumes of data in its original format without requiring prior structuring. This allows for large-scale exploratory analysis and machine learning algorithms (Olawoyin et al., 2021; Panwar & Bhatnagar, 2020).

After preprocessing, the data are stored in a data warehouse, a structured and organized data repository. This layer stores processed data and ensures they are available for future queries, enabling advanced analysis and extracting actionable insights (Abdelhédi et al., 2023; Sakib et al., 2022).

In addition, data marts, which are specialized subsets of the data warehouse, play a crucial role in enabling targeted analysis. These data marts are designed to focus on specific areas of healthcare data, allowing for more efficient and detailed investigations. This approach is particularly valuable in enhancing

decision support systems by providing tailored datasets that align with specific analytical needs. By improving the quality and coherence of the data available for analysis, data marts contribute significantly to the overall effectiveness of clinical decision-making and operational strategies in healthcare (Mw et al., 2001; Santosh Kumar, 2024).

### Transformation layer

The transformation layer plays a critical role in the preprocessing of raw data, preparing it for subsequent analysis and application-specific use. This layer addresses various data quality issues, including eventually correcting missing values, normalizing data, reducing noise, and categorizing data into structured formats. Each preprocessing step is essential to ensure that the data meets the necessary standards for accuracy, consistency, and usability in healthcare applications.

This layer is tailored to the application's specific requirements, allowing for flexibility and adaptability in processing diverse types of healthcare data. This customization ensures the data is optimally prepared for the intended analytical methods, whether predictive modeling, decision support, or other advanced analytics tasks.

By systematically applying these preprocessing techniques, the transformation layer improves the quality and reliability of the data and contributes significantly to the overall effectiveness of healthcare information systems. This layer ensures that the data fed into subsequent analytical processes is of the highest possible quality, thereby enhancing the validity and utility of its insights. The role of data preprocessing in ensuring high data quality is crucial, as it directly impacts the performance of machine learning models and the accuracy of the insights generated from healthcare data (M. Oliveira et al., 2016; Seker et al., 2022).

### Security Layer

The security layer is paramount in ensuring the data's integrity and veracity in the repository. The security layer's hashing techniques allow for efficient data integrity verification. Each data entry generates a hash value that acts as a fingerprint for the data. Any alteration to the data, even at the bit level, results in a completely different hash value, which can be detected immediately. (Akinola et al., 2024; Alharby, 2023).

In addition to ensuring data integrity, the security layer supports audit functions by logging all legitimate changes in a blockchain-based ledger. This capability is crucial for regulatory compliance, providing a transparent and immutable record of all data transactions. Such audit trails are invaluable for verifying the authenticity of data over time, particularly in environments that require stringent adherence to privacy and security standards (Sairam et al., 2023; Sarkar et al., 2023).

This ensures that stakeholders can have confidence in the data's integrity, security, and accessibility, which are essential for effective decision-making and patient care.

## API Implementation and Functionality

An API is a set of guidelines, computer code, and standards that enable software programs to communicate with one another. APIs are essential in modern software development, facilitating the interaction between different systems and applications. The API created for this project was developed using the NodeJS programming language, a popular choice due to its efficiency and scalability in handling asynchronous events. Furthermore, the documentation for this API was automatically generated using Swagger, a tool that creates interactive and easy-to-navigate API documentation.

The following are a few key methods provided by the API for data retrieval:

- **authentication** - This method generates a JSON Web Token (JWT) for authorization across all other routes. The token is securely generated from a combination of the user's email and password, ensuring that only authorized users can access the API's functionalities.
- **getSample** - This method returns the last 100 values entered in the repository, allowing for a quick overview of recent data entries.
- **getPatientResults** - Given an exam number and patient ID, this method retrieves all test results associated with the patient, providing a comprehensive view of their medical history.
- **getResults** - This method returns all results for all tests associated with a specific patient, identified by their unique patient ID. It is useful for aggregating a patient's complete set of test results.
- **getLastResult** - This method returns the date of the most recent examination performed based on the analysis code and the patient's ID. It is particularly useful for tracking the timeline of a patient's tests.
- **getResultsAge** - Given a specific analysis type and an age range, this method returns the minimum, average, and maximum values, which can be used for statistical analysis and comparison across different age groups.
- **getModDiag** - This method, based on the diagnosis code (ICD10), returns the most frequently performed analyses, helping understand trends in diagnostic practices.

Each API route is designed to return a JSON object, with the most recent exam result listed at the top. The schema documentation, necessary inputs, and expected API responses are fully documented and accessible through Swagger, providing a user-friendly interface for developers and users.

In addition to the core functionalities, this API was enhanced by integrating blockchain-based hash validation mechanisms to ensure data integrity and security across all transactions. This addition guarantees that all data interactions are secure and auditable, significantly bolstering the system's reliability and trustworthiness.

The hash validation process is set to run automatically on a scheduled basis to ensure regular integrity checks without compromising system performance. However, the API also allows users to trigger on-demand hash validation. While this provides immediate verification, it may result in longer response times, especially for complex queries or large datasets, as the system validates real-time data integrity.

## 8.5 Summarize

Through identifying risk factors, implementing targeted interventions, and optimising resource allocation, the use of data-driven approaches in healthcare can enhance patient outcomes and lower costs, according to a systematic review published in the Journal of Medical Internet Research (Lin et al., 2017). By making it possible to create tailored medicine, forecast disease outbreaks, and improve healthcare delivery, data analytics and machine learning techniques have the potential to revolutionize the healthcare industry (Topol, 2019). Data is, therefore, one of the most valuable resources in the world, both in the commercial and intellectual arenas. Creating authentic and reliable data repositories in the healthcare industry is crucial.

The first benefit is that it enables the storage and organization of massive volumes of data, such as medical records, trial data, and research findings. This facilitates the availability and analysis of the data by healthcare professionals, which can enhance decision-making and patient care (C. Oliveira et al., 2022). Second, data repositories can promote data collaboration and sharing across institutions, academics, and healthcare practitioners.

Building on the robust foundation established by developing an API-accessible real-time data repository, integrating a blockchain layer can further enhance the stored data's security, integrity, and trustworthiness.

This solution was created following the FAIR principles, making it Findable (each record has a unique key), Accessible (generic usage guidelines), Interoperable (use of internationally recognized and adopted terminologies), and Reusable (API developed with several endpoints available and dynamically documented).

This can result in the creation of novel cures and treatments and the discovery of patterns and trends in health data that can guide practice and policy.

The main contributions of this work are:

- The development of an API-accessible real-time data repository for clinical test findings.
- The incorporation of HL7 messages from many sources enables the creation of a consistent and orderly data structure that complies with global standards, including HL7, ICD-10 and FAIR.
- The data can be used to anticipate and enhance patient care by feeding dashboards and machine or deep learning models;

- The proposed addition of a blockchain layer using a permissioned Hyperledger Fabric network ensures data integrity, protects against tampering, and allows for the independent verification of data authenticity;
- The potential for this repository to be a useful tool for healthcare organizations, empowering them to make decisions based on data and progressively raise the standard of care given to patients.

In the future, efforts will be focused on integrating HL7 v2 with FHIR and incorporating ICD-10 with ICD-11 (the most recent version of the classification system). Additionally, a website application is being developed to allow for the real-time visualization of clinical test results based on factors such as patient, examination, location, and diagnosis. Finally, there is potential to enhance the data warehouse's capabilities by incorporating additional data repositories or even data marts.

While the current integration of a blockchain layer significantly enhances the integrity of the data repository, future work could explore further applications of blockchain technology in healthcare data management. This includes the potential development of smart contracts for automating data access control, patient consent management, and more sophisticated real-time auditing processes.

Additionally, evaluating the blockchain's performance and scalability under varying data loads will ensure its long-term viability in large-scale healthcare systems.

# 9

# C4 - The Role of Blockchain Technology in Ensuring Security and Immutability of Open Data in Healthcare

Clinical information is highly confidential due to its sensitive content. The implementation of health information systems has sparked concerns about privacy, security and interoperability. The storage and retrieval of this information also present similar challenges. Therefore, any initiative to introduce healthcare information systems must prioritize patient data's safety, privacy, integrity, and immutability. To address these concerns, blockchain technology and the openEHR open data model have emerged to guarantee data security, system interoperability, and the accuracy of stored data queries. Two distinct architectures were developed and subjected to multiple performance tests to enhance security and immutability in open data models implemented within healthcare institutions. The findings were analyzed to determine which architecture brings greater value to a healthcare institution, followed by a discussion to draw appropriate conclusions.

The health sector is a sector that has unique requirements, and trusting the data from its activities is essential for its operations (Onik et al., 2019), (Hasselgren et al., 2020). With the growing amount of data generated, some problems arise, including unauthorised sharing, invasions, and theft of confidential data. These propensities lead to people's suspicions and doubts about the trust veracity of these institutions (Hasselgren et al., 2020), (Gamal et al., 2021). It is essential to consider alternative approaches, like blockchain technology, to address these issues. Given its nature and characteristics, it offers a solution to the needs demanded by the sector (Hölbl et al., 2018b), (Prokofieva & Miah, 2019). Allied with this technology comes the open data structure, openEHR. It enables reliable structuring, management, storage, and integration of patient data across healthcare organisations. The main idea is to standardise concepts related to health used in databases or EHR systems in a set of libraries called archetypes (Ribeiro et al., 2019).

## 9.1 Why openEHR with blockchain in healthcare?

OpenEHR is a standard for EHR systems that allows for creating interoperable and vendor-neutral health data. Blockchain technology can enhance the security, privacy, and interoperability of OpenEHR by providing a decentralised and tamper-resistant platform for storing and sharing health data. By combining OpenEHR with blockchain, healthcare providers can create a secure and transparent environment for managing patient health data, improving patient outcomes, and reducing costs. Furthermore, blockchain technology can also support creating a patient-centric healthcare system, where patients can control their health data and choose who can access it (Azaria et al., 2016a; Kuo et al., 2017b; openEHR, n.d.).

A SWOT analysis based on the publications of various authors was conducted to understand the Strengths, Weaknesses, Opportunities, and Threats of combining openEHR with blockchain in healthcare.

The **strengths** highlighted by the authors are that OpenEHR provides a structured data model based on standards that can improve interoperability and data integration in healthcare (Kalra et al., 2005). Blockchain can enhance the security and privacy of healthcare data, ensuring that only authorised individuals can access sensitive information. The combination of OpenEHR with blockchain can provide an open, decentralised, and trustworthy solution for managing health data (Azaria et al., 2016a), and the combination of OpenEHR with blockchain technology can enhance the security of electronic health records, protecting patient data from breaches and unauthorised access (Cunha et al., 2022).

The **weaknesses** highlighted by the authors are that implementing OpenEHR and blockchain in healthcare may be expensive and require a high investment in IT infrastructure and resources (Benchoufi et al., 2018). Implementing OpenEHR requires a certain level of technical expertise and may be complex for end users (openEHR, n.d.). The use of blockchain has yet to be widely adopted in the healthcare industry, still facing significant challenges for its implementation, which may limit its effectiveness in certain areas (Soltanisehat et al., 2020).

The **opportunities** highlighted by the authors include the integration of OpenEHR with blockchain, which can provide a technical foundation for decentralised healthcare applications, such as digital health wallets and health tracking apps (Fekih & Lahami, 2020), (Khezr et al., 2019). Blockchain-based solutions can increase public trust in digital health systems and promote wider adoption of digital health technologies (Hasselgren et al., 2020). The growing demand for health data security and privacy protection may drive the adoption of more advanced technologies, such as OpenEHR with blockchain (Angraal et al., 2017).

The **threats** highlighted by the authors include that data privacy may be compromised if blockchain technology is not implemented correctly or privacy policies are insufficient (Soltanisehat et al., 2020). Resistance to change by healthcare professionals and patients may limit the adoption of digital health technologies, including solutions based on blockchain and openEHR (T. Kumar et al., 2018), and the adoption of emerging technologies such as OpenEHR with blockchain may face regulatory and compliance challenges (Soltanisehat et al., 2020).

Combining OpenEHR with blockchain technology can offer numerous benefits to the healthcare industry, including the security of electronic medical records, the protection of patient data against violations

and unauthorised access, patient control over their health data, and improvements in clinical research and population health. While adopting this technology may require a sophisticated IT infrastructure and changes in organisational culture, the growing demand for health data security and privacy protection can drive its implementation in the healthcare industry (Cunha et al., 2022), (Dagher et al., 2018).

## 9.2 Objectives

The objectives of this research can be grouped into four categories, focusing on enhancing healthcare data management. These objectives are:

**Objective 1: Enhance Data Security and immutability**

- Use measures to safeguard and maintain the secrecy and privacy of the health information.
- Manage the risks of data leakage and unauthorized access to the healthcare data management system

**Objective 2: Improve Data Interoperability**

- Enable interoperability between health information systems for efficient systems communication and reliable patient data access.

**Objective 3: Implement Blockchain and openEHR Technologies**

- Leverage blockchain technology to provide audit trails and data immutability.
- Incorporate the openEHR data model for managing health information.

**Objective 4: Assess System Architecture**

- Design and assess secure privacy frameworks for health information.
- Evaluate structural efficiency and performance in the health care settings.

## 9.3 Architecture

By integrating Blockchain technology with the open data model, openEHR, it is possible to ensure data interoperability and standardisation of all EHRs while maintaining data integrity, privacy, and security. In our case study, two scenarios were considered: Scenario 1, as represented in Figure 21, and Scenario 2, as represented in Figure 22.

Analysing the flow of Scenario 1, as depicted in the following figure, begins with the insertion of information and data about patients. These inputs are then transformed into EHRs and sequentially processed and analysed based on the specifications modelled in the open data model, openEHR, at the APIs layer through the gateway. Hyperledger Caliper was utilised to perform a series of insertions in the blockchain. Subsequently, the blockchain stores all the transactions in a secure, immutable, and

private manner for future consultation. Finally, Hyperledger Caliper evaluates the transactions in terms of success, speed, the maximum, minimum, and average time to send and receive a response, and the average number of transactions processed per second. These metrics are presented on an HTML page.

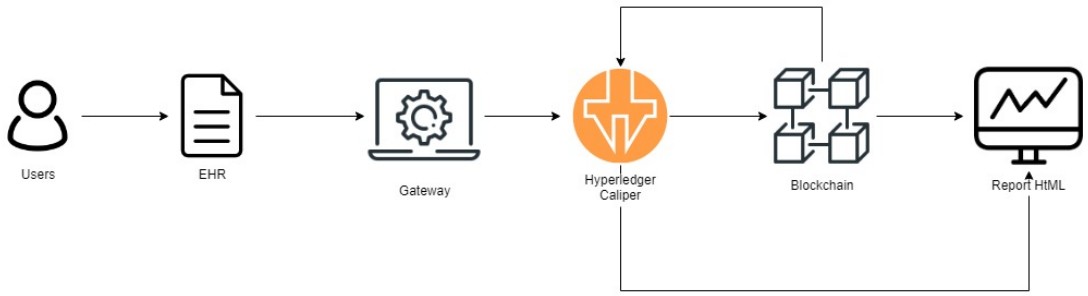



Figure 21: Blockchain Technology and Open Data - First Scenario

Initiating the analysis of Scenario 2, as illustrated in the figure below, the flow begins similarly to the scenario described above. It commences with inserting clinical information for patients into the systems used by the institution. These inputs are then transformed into EHRs and sequentially processed and analysed based on the specifications modelled in the open data model, openEHR, at the APIs layer through the gateway. Continuing with the flow, a fork is observed. Following the upper arrow in the flow, the data is stored in the hospital's database, where it can be further processed and transformed as per the needs of the hospital's stakeholders.

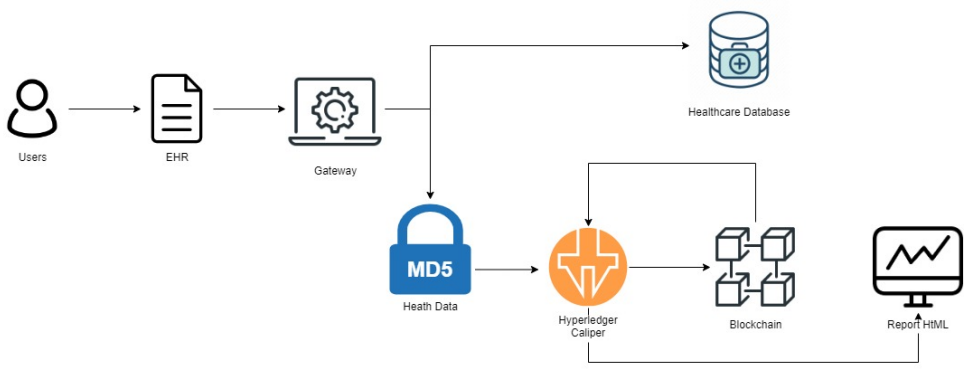



Figure 22: Blockchain Technology and Open Data - Second Scenario

On the other hand, the lower path involves creating a hash block for each object through the encoding process. An object ID is associated with the block to identify the person to whom the data pertains. The main objective of this technique is to validate if there has been any intrusion or alteration to the data, thus providing enhanced security. If any changes are made to the data in the object, the md5 will be updated, and the updated block will be stored on the blockchain. Proceeding with the flow, Hyperledger Caliper triggers the entries of the hashed objects into the blockchain. However, in this case, the constitution of the object changes, and it becomes just an ID and the hash. Next, the blockchain stores the transactions and plays a crucial role in verifying whether the recorded hash matches the updated hash. Finally, Hyperledger Caliper utilises metrics to measure performance, which are presented on an HTML page.

## 9.4 Results and Discussion

In this chapter, a visual demonstration of the network's performance obtained in the various stress tests will be carried out. Thus, it will be possible to measure and understand whether the objective of increasing the security and immutability of implementing open data models in a hospital environment has been achieved. This income statement performed two tests, one for the first and the other for the second. At each test, two types of graphs are shown. One evaluates the performance of the network in the gradual submission of people. The other considers the total amount of memory that the network uses.

### Insertion of data into the blockchain with 20000 records, Scenario 1 and Scenario 2

Four insertions of 20000 people were performed on the blockchain for this test. Initially, the container was restarted. As the insertions were performed, the processing capacity of the network decreased, gradually increasing the average latency. This phenomenon is explained by the increasing amount of data stored in the blockchain. It is noteworthy that the processing speed was 5TPS. Adding this to the physical capacity of the machine used for testing, the processing time increased considerably. A positive aspect that goes against speed stability corresponds to the absence of failures.

In this test, it is possible to see a growing increase in processing time and memory usage in both scenarios. As mentioned, the amount of data entered is twenty thousand in each of the four iterations, thus pushing the blockchain's capacity to the limit. As the iterations were carried out, the network performance naturally decreased, which caused an increase in processing time. The same occurred with memory usage, where it is possible to conclude that as the volume of data increases, the memory used by the system also increases, which will cause a slower system.

Upon analysing the two scenarios, as evidenced in Table 5, it is possible to deduce that Scenario 2 stands out with shorter processing times and memory usage in each iteration performed. Moreover, this scenario adds a layer of data security and better aligns with the internal requirements of the hospital. Considering the minimal impact on the existing implementation in the hospital setting, Scenario 2 is identified as the optimal choice. It is less resource-intensive, provides the desired benefits, and avoids disruptions. Further tests were conducted for this scenario, which will be presented in the subsequent chapters.

Table 5: Blockchain Technology and Open Data - Analise between two Scenarios

| | | 1st Interaction | 2nd Interaction | 3rd Interaction | 4th Interaction |
|---|---|---|---|---|---|
| Process Time | Test – Scenario 1 | 583,74 | 688,3 | 768,45 | 1035,24 |
| | Test – Scenario 2 | 60,33 | 312,37 | 442,89 | 763,4 |
| Memory Usage | Test – Scenario 1 | 1679,55 | 2025,88 | 2231,38 | 2566,96 |
| | Test – Scenario 2 | 529,39 | 752,26 | 1289,7 | 1631,93 |

## Additional Test for Scenario 2

For the second test of scenario 2, a different configuration was performed, where the network defined the send rate automatically. Initially, the containers were cleared and then 1000, 5000, 10000, and 20000 people were inserted into the network. With the change made, a considerable variation in latency was observed compared to the previous tests. The achieved latency times show an improved, constant, and consistent speed. This occurs because the change allowed the system to choose the rate it could support.

Additionally, it is possible to observe that the sending speed decreases with each insertion. This evolution is expected as the network's capacity decreases as more data is inserted. It is possible to observe that memory increases progressively. There is more significant variation in memory because each iteration involves a different number of insertions, which justifies that memory is inconsistent and growing. For the third test of scenario 2, the same configuration as test 2 was performed, where the network defined the send rate automatically. Initially, the containers were cleared, and then four insertions of 20000 people were performed each time in the network. With the changes made, considerable alterations were observed regarding latency times. The latency times increased and presented an improved, constant, and consistent speed because the change allowed the system to choose the rate it could support. Additionally, it is possible to observe that the sending speed decreased as the 20000 people were inserted. This happens because the network's capacity decreases with the continuous insertion of data, causing an overload of the network.

Regarding memory, it is possible to observe that it increases progressively. In this case, memory increased consistently because the number of insertions was constant, meaning that the amount of processing by peers and orderers was practically the same, and the only thing that increased was the size of the databases. This increase is considered regular, constant, and growing because the number of records also increases. The results for both tests are visible in the following table.

Table 6: Blockchain Technology and Open Data - Additional tests for Scenario 2

| | | 1st Interaction | 2nd Interaction | 3rd Interaction | 4th Interaction |
|---|---|---|---|---|---|
| Insertions | Scenario 2 – Test 2 | 1000 | 5000 | 10000 | 20000 |
| | Scenario 2 – Test 3 | 20000 | 20000 | 20000 | 20000 |
| Process Time | Scenario 2 – Test 2 | 3,87 | 3,9 | 4,7 | 4,79 |
| | Scenario 2 – Test 3 | 5,16 | 5,4 | 5,14 | 6,38 |
| TPS | Scenario 2 – Test 2 | 17,6 | 17,5 | 14,6 | 14,5 |
| | Scenario 2 – Test 3 | 13,4 | 12,9 | 13,6 | 11,3 |
| Memory Usage | Scenario 2 – Test 2 | 689,25 | 997 | 1139,45 | 1314,39 |
| | Scenario 2 – Test 3 | 1566,44 | 1909,07 | 2267,47 | 2323,48 |

## 9.5 Summarize

Every solution requires a thorough and truthful evaluation, and engaging in discussion about its effectiveness is essential. To do so, it is helpful to utilize technology assessment methodologies like a SWOT analysis. A SWOT analysis is a tool commonly used by organisations for managing their strategies and objectives. This tool assesses internal and external factors affecting the organisation, with SW factors being internal and OT factors being external attributes. By performing this analysis, one can determine the feasibility of implementing a given solution. The SWOT analysis yields qualitative and quantitative metrics, which can serve as indicators of the technology acceptance model as perceived by practitioners.

**Strengths:**

- Structured clinical data.
- Interoperability between all systems.
- Availability of data for better development of Business Intelligence and decision support systems.
- Reduction of obsolete data and poorly inserted records without clinical value and clean information analysis.

**Weakness:**

- Scalability and storage and processing capacity.
- Application with a real-time data update.
- Dynamics of OpenEHR structures and their versioning.
- Efficiency regarding processing time and resources.

- Relationship between OpenEHR structures and Multidimensional structures that support analytical processes considering analysis axes that cut across several patients or certain variables/ characteristics of the same patient.

**Opportunities:**

- Standardisation of clinical records on a large scale.
- Training and integration of clinical modelling of these structures in training healthcare professionals and/or higher healthcare courses.
- Centralised data for analysis.

**Threats:**

- User resistance to adopting a new system by healthcare professionals.
- Negative aspects of the environment with the potential to compromise the proposed solution.
- External development of more efficient solutions.
- The emergence of a new standard with better conditions.

Integrating these technologies and methodologies in the health area is important for evolution in terms of patient care speed and service quality. However, the importance of OpenEHR interoperability for better communication between services and BI integration must not be forgotten.

OpenEHR models provide a disruptive way of storing data within healthcare and are primarily focused on standardising and managing clinical data, including capturing and storing structured and unstructured health information. It is not explicitly designed for data analysis or business intelligence purposes, so current BI solutions must adapt and adjust how data is consulted efficiently.

According to my research, this integration between OpenEHR and BI has yet to be adequately investigated, so a gap in this area can be used for research. Future research work will be the realisation of artefacts to adopt a BI system generically to the OpenEHR model and the study of the creation of a layer of Extract, Transform, and Load (ETL) that efficiently analyses data from the models.

# 10

# C5 - IPFS and Hyperledger Fabric: Integrity of Data in Healthcare

Since the arrival of the IoT, one of the main problems encountered daily is data breaches and data integrity. Now more than ever, the expertise needed to develop an attack is decreasing. Developers are creating software that does the same thing as an expert, requiring less knowledge from the attacker. Also, ill-intended professionals within the institutions can compromise and access information without authorization.

Healthcare Information Technologies must be aware of and proactive about this problem within each sector. With this in mind, researchers and developers must propose and study solutions and architectures to store and query sensitive files and information more securely.

When considering security, there are more dimensions to think of other than the technology itself, but it does remove some constraints. This contribution presents an architecture that relies on Blockchain through HyperLedger Fabric and IPFS to securely host sensitive documents such as contracts within Healthcare.

## 10.1 Introduction

The healthcare industry handles vast amounts of sensitive information, from patient records and contracts to clinical trial data. As such, ensuring the security of this data is crucial. This work aims to propose a solution for securely storing sensitive information in the healthcare industry (Cunha et al., 2022), based on permissions.

Previous research has emphasized the importance of secure data storage in healthcare, but there are gaps in the literature regarding the use of combined centralized and decentralized mechanisms for this purpose. This combines a master node and slave nodes for managing communications between containers, an ordering node for message production in the hyperledger channel, and a local network of IPFS peers for file storage and hash generation. A SWOT analysis was conducted to assess the feasibility and potential benefits of this proposed solution. Strengths include the use of both centralized and

decentralized mechanisms, as well as permissions-based access control. Weaknesses include the need for a secure authentication system to manage permissions and potential compatibility issues with existing healthcare infrastructure. Opportunities include the potential to enhance data security and streamline data management processes. Threats include potential resistance to change and the need for additional resources to implement the proposed solution. In conclusion, this solution offers a potential solution for securely storing sensitive information in the healthcare industry based on permissions. By utilizing a combination of centralized and decentralized mechanisms, as well as permissions-based access control, it is able to ensure data integrity and increase security.

## 10.2 Related Works

To provide a clear understanding of the potential applications of this technology, several relevant projects have been compiled and categorized, including those managed by well-established organizations. This categorization highlights individual technologies and demonstrates how these technologies can be effectively integrated. This approach enhances comprehension and showcases the versatility and potential of these technological solutions.

**IPFS** The following is a list of significant IPFS-related projects found in the literature:

- Arbore (MichaelMure, 2018) - IPFS application for storing files in a decentralized way.
- FileNation (Alexsicart, 2018) - Filenation lets you send files as a link to an email. The files cannot be censored as they are sent, stored, and transmitted decentralised because they use the IPFS.
- Snapshot (“Snapshot”, 2023) - Web3 project that enables the user to vote in proposals. Normally, these votes are saved in a public blockchain (Tapscott & Tapscott, 2018) like ethereum (Tikhomirov, 2018), but this project is more cost-effective because, instead of saving the data on a public chain, it is stored on the Hyperledger fabric, which does not require gas fees.
- Berty.tech (“bertyTech”, 2023) - Non-required mobile internet messaging system, this project has the objective to exchange messages between mobile phones that will be able to run their IPFS nodes locally without internet, using any proximity protocol like Bluetooth.

**Hyper Ledger Fabric** The following is a list of Hyperledger Fabric-related projects found in the literature:

- IBM Food Trust (Nguyen et al., 2018) - In this project, IBM ensures the quality of the food and the chain itself by creating a network of connecting growers, processors, distributors, and retailers through a permissioned, permanent and shared record of food system data.

- NIIT Technologies: Chain-m Blockchain ("NIIT Technologies Introduces Chain-m, a Blockchain Powered Solution for Airlines and Its Partners", 2018) - Project to airlines to keep track of the number of tickets sold to fare amounts, commissions, taxes collected and more.
- Hitachi Streamlines and Secures Procurement (Fabric, 2022) - Project that uses Hyper Ledger Fabric to process contracts.

**Both**

- Starling Project("Starling", 2023) - This is a social media project that uses multiple decentralized technologies, including IPFS, GUN, Hyperledger Fabric, and Hedera Hashgraph, throughout its process. It uses IPFS for storing images and files and uses HyperLedger Fabric to store those hashs, which can also be stored in Hedera Hashgraph (Public blockchain).
- Decentralized Data Access with IPFS and Smart Contract Permission Management for Electronic Health Records(Verdonck & Poels, 2020) - This article examines the use of smart contracts in blockchain for EHR permission management. Benefits include traceability, transparency, and improved security. However, EHRs are still stored locally despite decentralized permission management, allowing undetected queries within hospital infrastructure. Smart contracts pose challenges for verifying actor identity and handling lost or stolen private keys. Our proposal integrates blockchain technology with the IPFS for decentralized EHR storage. IPFS ensures peer-to-peer distributed network storage, enhancing security and availability. A governing body is introduced to handle public key governance and identity verification. Our solution combines blockchain, decentralized storage, and robust identity verification to enhance EHR permission management.

## 10.3 Objectives

This work presents a model for the safe storage of sensitive healthcare documents that leverages HyperLedger Fabric Blockchain and IPFS. The targets aim to improve security, utilize modern technologies, and be preemptive in the challenges of healthcare data management.

**Improve Data Security and Integrity**

- Decrease the risk of data breaches in the healthcare sector.
- Protect and preserve critical and sensitive healthcare information

**Implement Advanced Technologies for Secure Data Management**

- Use HyperLedger Fabric to build up a secure and compliant healthcare ecosystem solely based on blockchain technology for data sharing.

- Host confidential healthcare-related documents such as contracts and health records using decentralized IPFS in a more secure manner.

## 10.4 Architecture

### Basic Explanation

To explain the concept, a basic layer representation was created, which includes the technology from the lowest to the highest level. According to this approach, the structure consists of the operating system, multiple containers, CA Authority for authenticating communication with the components, Hyperledger, IPFS, Kubernetes, the API, and finally, the front office in React.




Figure 23: IPFS and Hyperledger Fabric - Layered Architecture

### Node composition

Given the presence of multiple machines, this describes the composition of a single node. This is a Master node responsible for orchestrating all the nodes in the network, while the slave nodes will have the same composition, with the only difference being that the Master node commands them. IPFS will not be placed in a container on every node to maximize resource usage because it does not make sense to confine it within a container.

### Global representation

For example purposes, this is the overall conception of the system, which will consist of multiple nodes, each serving three different functions. The first node will be responsible for ordering the information shared

among all the nodes. The second will orchestrate the slave nodes, and the third will act as a slave node. It is important to note that the network administrator, who has access to the Master node, will be responsible for maintaining Hyperledger Fabric, IPFS, and the Kubernetes Network.

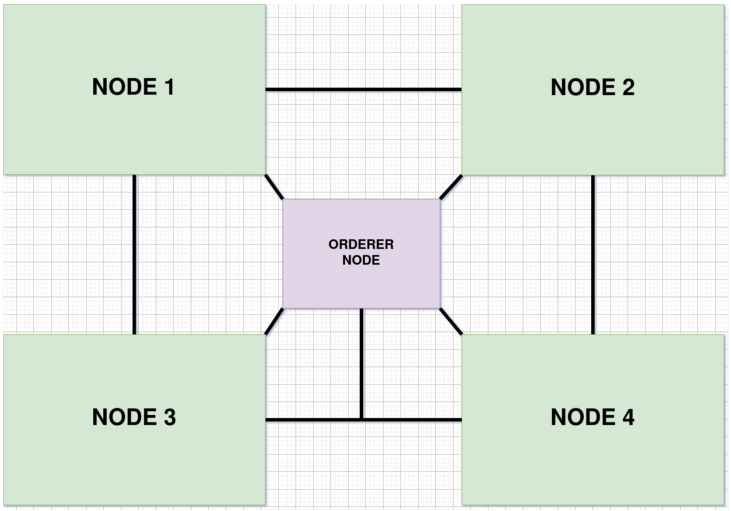



Figure 24: Master Node

Hyperledger is a peer-to-peer, role-based system typically implemented for collaboration between multiple organizations. However, in this context, the focus is on a single hospital environment. Rather than involving multiple organizations, the approach envisions representing different departments within the hospital as separate entities within the network.

Despite the current focus on a single hospital setup, the network structure is designed to be adaptable and can be extended to link with other organizations if needed. At present, the approach is centred around a partnership model within the hospital, with each department functioning as an independent entity within the network. However, this can evolve into a more expansive structure, enabling seamless integration with external entities in the future.

In line with standard implementation practices, each peer in the network is represented as a container. In this context, however, each container corresponds to a specific department within the hospital rather than a distinct organization.

Similarly, different departments within the hospital can have their own dedicated channels within the network, allowing for secure and isolated communication between departments while maintaining the system's overall integrity.

Every machine or peer within the network can be assigned specific roles based on the certificate authentication of the individuals using them. This role-based approach ensures that authorized personnel have the appropriate permissions and access levels corresponding to their assigned roles.

The flexible network design also supports connections to various nodes within the network, facilitating seamless communication and collaboration between peers. This enhances the overall efficiency of data sharing and interaction within the hospital environment.

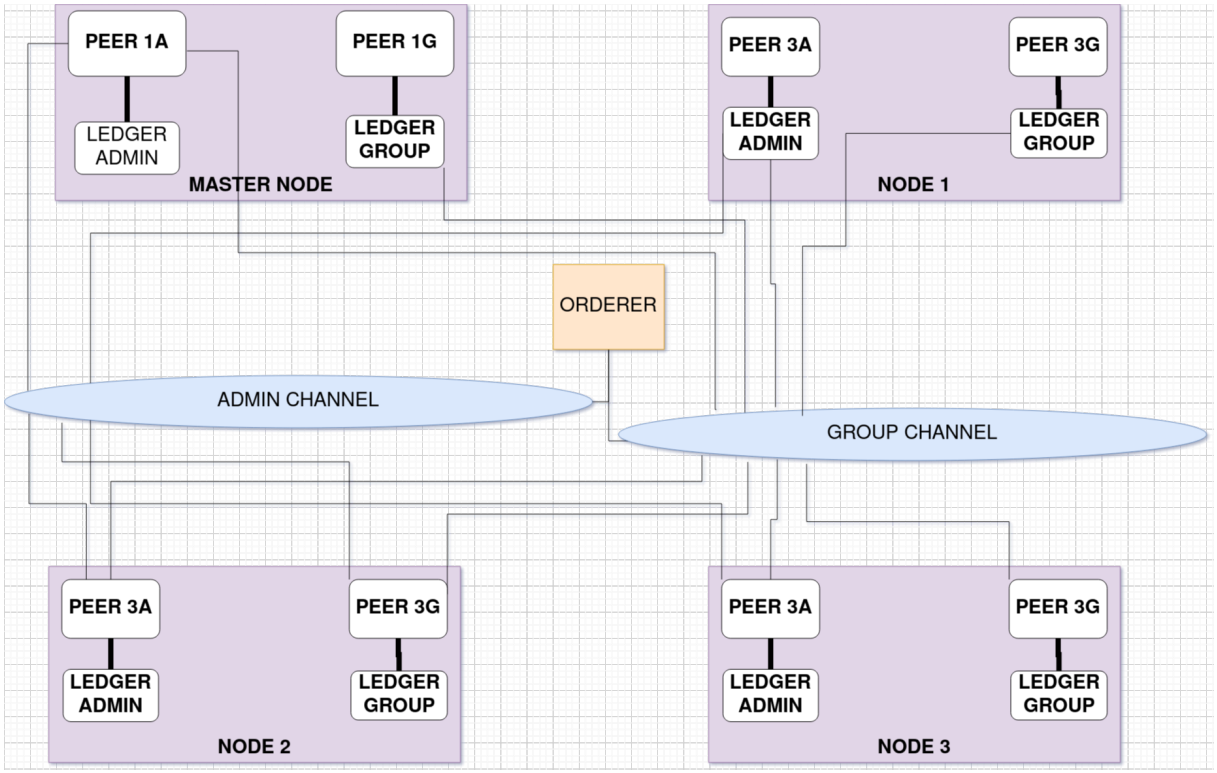



Figure 25: IPFS and Hyperledger Fabric: Network design

## Security Measures

Various measures can strengthen the security of storing files in IPFS. Storing the file's hash and its versions in a Hyperledger Fabric network provides additional security and transparency. Managing interactions using certificates, maintaining logs of every operation performed by certificates, conducting regular analysis of sensitive files and corresponding logs, and leveraging Kubernetes for network management and high availability further enhance the system's overall security.

By storing a file's hash and its versions in a Hyperledger Fabric network, it is established a tamper-evident record of the file's integrity and version history. This ensures that any modifications or updates to the file can be traced and audited. The Hyperledger Fabric network provides a trusted and immutable ledger that securely stores the file hashes, adding an extra layer of security and facilitating regulatory compliance and dispute resolution.

Managing interactions using certificates is crucial for securing the system. Certificates, issued by a trusted CA, validate the identity of network participants and ensure secure communication. By utilizing certificates, it is possible to authenticate and authorize users, preventing unauthorized access and ensuring that only trusted entities can interact with the system. Furthermore, maintaining logs of every operation performed by certificates provides an audit trail for accountability and forensic analysis, enabling the tracking and investigation of any suspicious activities.

Regular analysis of sensitive files and their corresponding logs is essential to identify unexpected

behaviour and potential security threats. By conducting periodic reviews of the logs and analyzing the activities related to sensitive files, it is possible to detect any unusual patterns, unauthorized access attempts, or data breaches. This proactive approach allows a prompt response to security incidents and mitigates potential risks before they escalate.

Managing the network using Kubernetes brings additional security benefits. Kubernetes is a container orchestration platform that provides robust management capabilities, including workload isolation, automatic scaling, and service discovery. By leveraging Kubernetes, it is possible to ensure that the network components running IPFS, HLF, and other related services are deployed in a controlled and scalable manner. Additionally, Kubernetes offers high availability features, such as automatic failover and load balancing, which help mitigate the impact of potential failures or disruptions, ensuring the continued availability and reliability of the file storage system.

By combining these security measures, including storing file hashes in Hyperledger Fabric, managing interactions with certificates, maintaining comprehensive logs, analyzing sensitive files and logs regularly, and leveraging Kubernetes for network management and high availability, you establish a robust and secure environment for storing files in IPFS. These measures enhance the stored files' integrity, confidentiality, and availability, protecting them from unauthorized access, tampering, and potential system failures.

## Workflow

The process begins when a doctor logs into the system using their unique credentials and digital certificate. This initial authentication ensures the doctor's identity and authorization. Once logged in, the doctor proceeds to upload, for example, a file related to a contract he wishes to store.

At this point, a Rest Service comes into play. It validates the provided credentials and certificate, ensuring the doctor's identity and authenticity. With successful validation, the Rest Service takes the uploaded file and saves it into the IPFS. IPFS provides a decentralized and secure storage solution for files.

After saving the file, IPFS generates a unique hash that acts as a digital fingerprint representing the content of the file. This hash ensures the integrity and tamper-proof nature of the stored data. The Rest Service then retrieves this hash and saves it into the HLF using a Smart Contract.

Depending on the type of operation, the workflow branches into two paths: file update or simple save. In the case of a file update, the system creates a file record and a version record with a specific sequence. However, for a simple save operation, the system creates a file record and a version record with an initial sequence set to 1. These records maintain a chronological history of file versions.

To maintain an audit trail, every transaction within the system is recorded in a dedicated logs data structure. This structure captures essential information, including the file ID, the version ID, and the data that was inserted during the transaction. These logs serve as a comprehensive record, allowing for traceability and accountability.

Once the Rest Service has completed the necessary steps, it receives confirmation that the file has been successfully stored in the system. This confirmation ensures that the storage process has been completed without any issues. Simultaneously, the doctor who initiated the file storage receives confirmation as well, ensuring they are aware of the successful operation.

This workflow follows the same principles and applies to file storage as well as other types of operations. Whether Creating, Reading, Updating, or Deleting (CRUD) files, the workflow remains consistent, with the variation lying in the nature of the operations performed.

## 10.5 Discussion

A SWOT analysis was developed to better understand the implications of such implementation:

Table 7: SWOT Analysis

| STRENGTHS | WEAKNESSES |
|---|---|
| • Recent and emergent Technology<br>• It can escalate easily<br>• Provides data immutability<br>• Provides Version and Access Control<br>• Provides Control | • If the local certificate authority becomes compromised, the system also becomes compromised<br>• Complex implementation and management<br>• It requires multiple local machines.<br>• Data duplication |
| **OPPORTUNITIES** | **THREATS** |
| • It can be expanded to a public blockchain<br>• You can easily add features as you go<br>• You can link multiple hospitals to the network and make data flow more secure and easy<br>• You can extend the technology for your supply chain | • Acceptance from the hospital team<br>• Motivation from the stakeholders<br>• The costs<br>• The availability of those machines<br>• Cheaper conceptions<br>• The relation between cost and needs<br>• Some stakeholders still rely on paperwork |

## 10.6 Summarize

In summary, the use of IPFS and HLF in the hospital environment is a promising solution to address data security, interoperability, and transparency challenges. By leveraging IPFS's distributed nature and Hyperledger Fabric's blockchain technology, hospitals can create a secure, tamper-proof, and decentralized system for storing, sharing, and accessing sensitive patient data.

However, to assess this system's effectiveness, measuring its performance and comparing it with centralized solutions is necessary. This will require further research and testing to determine data throughput, scalability, and latency factors.

Overall, this combination can revolutionise how hospitals handle patient and staff data and improve the quality of patient care. Further exploration and experimentation will be essential to validate these claims and ensure the system meets the healthcare industry's unique needs.

# 11

# C6 - Decentralized Healthcare Marketplace

This contriibution introduces the idea of creating a decentralized marketplace for healthcare where patients are able to sell their medical data in the form of NFTs to researchers in a completely anonymous manner. The platform is designed to integrate NFTs, and a DeFi, with the management of patients' medical records, giving power to patients, increasing research scope, and improving healthcare through the power of blockchain. The methodology employed for this research includes field research and discussions with professionals, ensuring credible and valuable insights. The article concludes that blockchain technology offers a transformative solution for healthcare record management, addressing data security, privacy, interoperability, and transparency issues. The article concludes that the use of blockchain and web3 technology in storing and managing healthcare records offers a solid way to empower patients to be participating stakeholders of the healthcare ecosystem, assuring that the issues of security, privacy, and transparency are effectively addressed.

## 11.1 Introduction

This work aims to offer a solution for patients to be incentivised to provide their health data for research purposes, addressing critical challenges in healthcare data management, such as data security vulnerabilities, limited accessibility, and interoperability issues. By creating a system that encourages patient participation, this work seeks to improve the flow of valuable health information while maintaining the privacy and security of sensitive data, ultimately enhancing collaboration among healthcare providers and advancing medical research. The work presents an innovative solution that harnesses the combined potential of NFTs and DeFi. By integrating NFTs and DeFi into patient data management. The decentralized nature of DeFi reduces reliance on central authorities, mitigating the risk of data breaches and unauthorized access. Furthermore, NFTs provide a unique tokenization mechanism for patient records, enabling easy verification, tracking, and transferability across various healthcare systems. It aims to reach a little closer to a stage where healthcare data is secure, accessible, and seamlessly integrated, allowing healthcare practitioners to make informed decisions and redefine patient care. This future can be made achievable by investigating the creative and fresh uses of these technologies.

## 11.2 Objectives

Thanks to the collaboration between decentralized finance and NFT-based data exchange, patients can become participating stakeholders of the healthcare ecosystem. The following objectives are structured to reflect the goals for this decentralised marketplace of health care with a particular focus on empowering patients to own their data and to have options on what to do with it, improving data availability, research and healthcare outcomes for the long term.

**Empower Patients and Expand Research Opportunities**

- Enable patients to anonymously sell their health data as NFTs, empowering them with control over their information.
- Expand research opportunities by providing researchers with access to valuable, consensually provided patient data.

**Explore web3 subjects to enhance Healthcare Outcomes**

- Use web3-related technology to secure the patient‘s data while also solving the problems of lack of interoperability, access do reliable data and transparency within healthcare data systems and research.

## 11.3 Decentralized Clinical Data-sharing Platform

This data-sharing platform rises from the search for novel approaches, mainly to increase clinical data offering for research and the use of web3-based technologies. This project integrates the principles of decentralized technology and the need for innovative and secure sharing and management of health data.

Management of the patient's medical records is associated with certain issues of traditional systems, such as data ownership, privacy, and data security. Research on blockchain technology suggests that this technological innovation has the disruptive capability to address these concerns and transform the healthcare ecosystem.

This platform strives to give individuals autonomy over their health information and motivate them to share information in a safe environment. It presents a groundbreaking approach to managing health records using blockchain technology and Web3-related technologies and concepts. This approach focuses on data ownership and confidentiality through web3 and blockchain attributes, such as decentralization, encryption, and immutability.

Following the main features and a description of the distinct platform roles of this proposed platform will be presented.

## Main features

***Patient Data Control*:** Patients must always have full ownership of their data, as NFTs, with what purpose they may allow others, such as researchers, healthcare centres or others who are participants in medical studies, to access certain data. This shift of power in decision-making from the authorities to the patients allows them the choice of who and when to grant access to their information, thus upholding data privacy and data sovereignty.

***Data Value*:** Health data is only as reliable as its source. If the source is solely patient input, the platform incentivises only quantity over quality. As such, automatic mechanisms for automatic data retrieval from medical institutions must be assured, with the patients' full authorization. So, standardized data formats, ontologies, and protocols for seamless data integration and exchange must be assured.

***Data Variety*:** In order to promote a diverse data-sharing platform for research, data must be diverse in theme and form. NFTs are a good fit since they can assume the form of basically any entity, from input forms, clinical records or datasets (medical admissions, prescriptions...) and medical reports to medical images. These NFTs serve as verifiable and traceable representations of the underlying health data. All the data is provided in an encrypted and anonymous way.

***Descentralized Secure Storage*:** The health data NFTs are securely stored on a decentralized infrastructure, such as the IPFS. Paring this storage with Blockchain technology should ensure immutability, tamper-resistance, and data privacy. By leveraging cryptographic techniques, patient data remains confidential and protected.

***DeFi Mechanisms for Incentivization*:** Token rewards are a key feature of the platform, the aim being to encourage patients towards active participation in data sharing. Patients are to receive monetary benefits for the data they give to the platform. These are either platform-specific or cryptocurrencies, providing a tangible reward for their participation.

***Smart Contract Automation*:** Smart contracts play a pivotal role in the platform's incentivization mechanisms. They allow the automation for the allocation of Token Rewards relying on factors and parameters contained in the contract. Such criteria can be data quality or how long the user agrees to participate, ensuring equity and accountability in the reward-based system.

## Patient role

Patients are engaged in a process where their medical information can be exchanged with various researchers multiple times for compensation that the patient or the research group deems fair. The details also include the ability to view the contract on Etherscan and the type of token associated with the patient's information.

## Researcher role

Researchers can purchase data chunks related to a specific health condition, in the form of NFTs, from patients at the listed price or place bids on them. By acquiring these NFTs, researchers gain access to specific data that can be used for further research. They can also create data request pools for specific data where a fee for patients' participation is established. Patients can opt-in and receive the established amount by the researchers.

## Organization Role

As clinical data providers, medical entities, such as hospitals or healthcare organizations should play a crucial role in managing the exchange of data within the platform. These organizations should act not as the owners of the data but as mediators for data integration in the platform, provided patient consent. These organizations oversee the transactions, ensuring compliance with regulations and safeguarding data integrity. Additionally, they can audit and monitor the data exchange process, ensuring that all interactions meet the platform's privacy and security standards. Organizations also play a key role in maintaining transparency and accountability by validating the data shared and ensuring its proper use in research initiatives.

## Perceived benefits:

**Driving Political Change for Data Ownership:** Thereby intended to put the patients in control of health information, the platform encourages advocacy where the patients, not the institutions, own their medical records. This model could instigate political changes by leading to legislation meeting the legal definition of patient data ownership within the relevant healthcare facilities where data is managed.

**Active Patient Participation:** The model stimulates the patients to become initiators of the data-sharing process, as they are rewarded with tokens for their contributions. This results in a wider and richer health data pool, thus giving researchers and health organizations the upper hand in decision-making and reasoning through data.

**Data Traceability and Provenance:** The use of NFTs ensures the traceability and provenance of health data sources. Each NFT contains a unique digital fingerprint that verifies the authenticity and origin of the associated health data. This feature enhances data integrity, credibility, and trust among researchers and stakeholders.

**Enhanced Research Capabilities:** By providing researchers and healthcare organizations with access to a broader range of patient data, the platform facilitates more comprehensive studies and research efforts. The availability of diverse datasets enables the identification of patterns, trends, and correlations that can drive medical breakthroughs and advancements.

**Clinical Trials and Drug Development:** The platform's data repository can serve as a valuable resource for clinical trials and pharmaceutical research. Researchers can identify potential participants

with specific conditions, ensuring a more comprehensive and diverse pool of trial candidates. This accelerates the development of new drugs, treatments, and therapies, benefiting patients and advancing medical science.

### Perceived Weaknessess and threats

**Adoption Barriers:** The decentralized nature of the platform and the requirement for patients to tokenize their health data may pose adoption challenges for individuals who are unfamiliar with blockchain technology or have concerns about data privacy and security.

**Data Privacy and Compliance:** Compliance with evolving data privacy regulations poses a significant challenge for the platform. Ensuring that the platform meets the stringent requirements for data privacy, consent management, and legal compliance is essential to avoid regulatory penalties.

**Data Fragmentation:** The platform's success relies on a critical mass of participants and the availability of diverse and comprehensive health data. Fragmentation of data across different systems, institutions, and jurisdictions may limit the platform's effectiveness in generating meaningful insights and research outcomes.

**Security Risks:** Despite the inherent security features of blockchain, the platform may still be susceptible to new vulnerabilities.

## 11.4 Summarize

Data availability aligned with security, privacy, interoperability, and trust are some of the major issues that the integration of blockchain technology in healthcare patient records management can help solve. By embracing Web3 technologies and approaches, the healthcare sector should build a strong infrastructure that empowers patients, expands research opportunities, and increases healthcare results.

Solutions such as this, have still many challenges to solve, however its mais purpose should core in emerging Healthcare information systems. Provide platforms to ensure patients' ownership over their own data and continuously seek ways to gather research data that is available publicly. This work seeks to provide an exploratory and preliminary answer to such challenges by establishing innovative uses of these emergent technologies (Musamih et al., 2022). Healthcare organisations should address these current issues and seize future possibilities of these technologies.

The decentralized health data-sharing incentivization platform concept shows great promise, but further research and development are crucial to unlocking its full potential. Key areas for future exploration include:

**Scalability and Performance considerations:** Develop efficient consensus mechanisms, data storage solutions, and network architectures to handle large-scale data transactions and ensure real-time access to patient records.

**Regulatory Compliance and Governance:** Explore governance models and mechanisms for secure data sharing and content management, ensuring compliance with privacy regulations like General Data Protection Regulation (GDPR).

**Privacy-Preserving Technologies:** Advance privacy-preserving technologies like zero-knowledge proofs and differential privacy to protect patient data while enabling meaningful analysis.

**Ethical Considerations and Patient Empowerment:** Explore the ethical implications of data sharing, informed consent, and patient empowerment in decision-making processes.

12

# C7 - Scalable and Sustainable Blockchain: Architecting Infrastructure and Developing a Platform for Efficient Management and Exploration

The application of blockchain technology in the health and healthcare sector is disruptive, requiring trust, integrity, and data value. This document analyses the potential of permissioned blockchain, specifically Hyperledger Fabric, to improve healthcare systems' security, integrity, and efficiency. It examines ways this can be done in a manner that has both scalability and sustainability prospects in the long term. This is achieved by reaching the optimal compromise between the efficiency of resources and their ease of use, management, and upscaling. The ability to be as lightweight as possible while quickly expanding the infrastructure and seamlessly integrating new functionalities, maintaining operational efficiency. The research involves a literature review and the development of three different blockchain implementations/architectures with a practical assessment of their performance metrics. At last, it presents a management platform for permissioned blockchain networks. This platform was developed to ensure such solutions' long-term scalability and sustainability in the healthcare sector. This work seeks to improve the use of blockchain within the healthcare sector, focusing simultaneously on presently existing demands and future advances in security and efficiency.

## 12.1 Introduction

The healthcare industry has exclusive requirements where data integrity, flexibility, collaboration, and confidence are critical to its daily operations. Blockchain technology as a transformative solution arises to combat the industry's needs. In this particular sector, secure solutions are necessary to protect patients' data and enhance efficiency and collaboration. This article investigates how private blockchain technology can contribute by reinforcing the principles of data integrity, privacy, flexibility, and trust. There has been an alarming increase in data manipulation and privacy breaches, which risk the security and productivity of the healthcare sector, where data integrity is paramount. A Hyperledger Fabric network was implemented

to increase trust in health information as it enables secure and immutable transactions. Thanks to its modular architecture, it can adapt to future demands without major architectural modifications. This encourages continuous growth, scalability, and usability. In this context, scalability must be viewed from the perspectives of infrastructure and utilisation. Regarding infrastructure, the solution needs to support the accumulation of additional components or servers as the demand increases, using a platform and scripts developed to facilitate this expansion. Concerning utilisation, scalability entails the capacity to expand to new healthcare areas. Given this, the architecture should allow the implementation of new chaincodes and continuous integration of new functionalities. Considering sustainability, the platform should consider environmental and economic constraints while providing long-lasting, robust, and adaptable solutions. The key aim is to achieve maximum protection with minimum components, processing power and number of machines. Besides, the strategy must be straightforward, readily implementable and scalable to prolong its useful life span and minimise the chances of obsolescence, which will adversely affect its usefulness and effectiveness in the future. This paper explores the use of HLF in local networks using different methods. Firstly, a literature review was performed to provide a background on blockchain technology and its relevance to the healthcare system, as well as the research methodology and the tools/frameworks employed. In the subsequent practical phase, a set of architectures was implemented, upon which tests were conducted, evaluating four metrics: CPU variation and Disk, Ledger and RAM usage. Such architecture comparisons are made by looking at specific features and the described metrics to establish which architecture fits best in this case study.

In this chapter, the developed architectures will be presented, accompanied by a series of tests conducted on them, along with a detailed analysis of the results obtained.

## 12.2 Infrastructure Architectures

To understand which architecture is the best, three scenarios were developed. These architectures will be presented and described below.

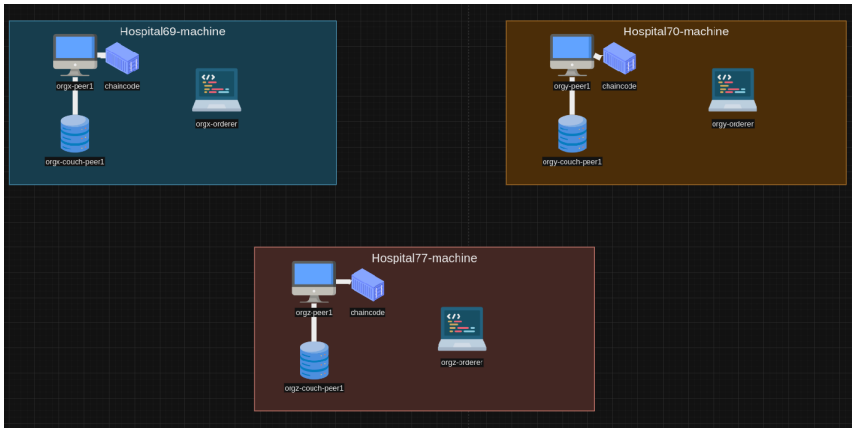



Figure 26: Scalable and Sustainable Blockchain - Proposed Architecture 1 - Docker

This network comprises several building blocks, all of which are hosted inside docker containers: Peers (one per machine), Orderer (One per machine), CouchDB (one per peer) and chaincode (one per peer). A series of scripts is created to ease the configuration and management of this type of Docker network. This approach minimises the effort necessary for network configuration and reloading, which is critical in running benchmarks and tests. It allows to repetitively run tasks, destroy and recreate Docker containers, and maintain consistent configurations for varying approaches.

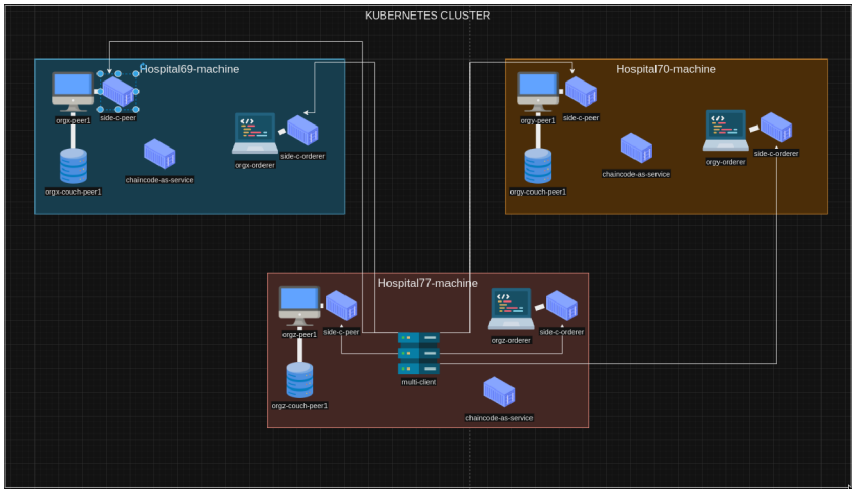



Figure 27: Scalable and Sustainable Blockchain - Proposed Architecture 2 - Kubernetes

In this project, a transition was performed to a Kubernetes-based networking configuration, which superseded the existing Docker-only configuration. This method uses Kubernetes to better manage resources, improve availability and enhance scalability. This architecture contains the same components as the Docker network; the difference is in the side containers for admin config communication, which allow access from a single point of failure (multi-client). Also, the chaincode here is a chaincode-as-service, which means it works as another micro-service. Using Jenkins, scripts, multi-client, and the Kubernetes API allows for the cleaning and creation of a new network instance for benchmarking.

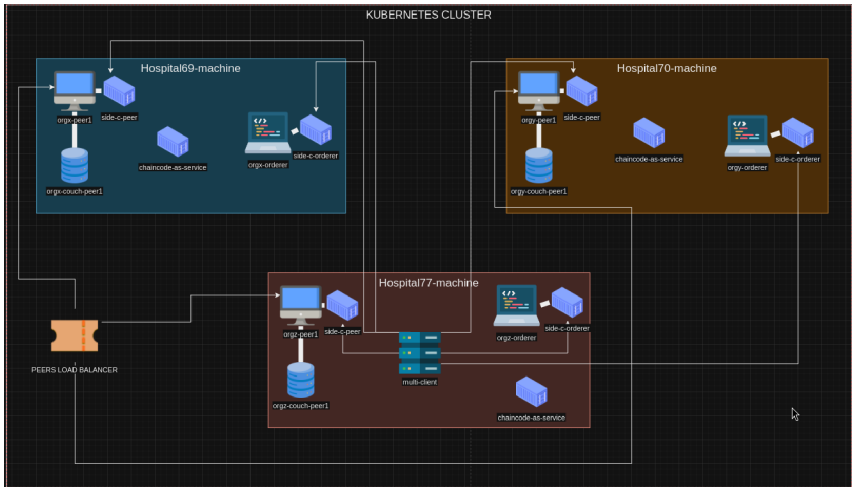



Figure 28: Scalable and Sustainable Blockchain - Proposed Architecture 3 - Kubernetes with Load Balancer

This architecture is similar to Figure 2, differing in access. Instead of communicating individually with each component, it is carried out only with the single point of failure that loads the balance evenly between the pairs.

This project uses a NodePort service or a more advanced solution such as MetalLB to achieve load balancing for peers. When using a NodePort, services can be exposed to specific nodes. Still, it has limitations: customisation of the load balancer type is not allowed, and the IPs must be 30000-32767, which prevents defining a common IP or port such as port 80. This can be impractical, as it requires specifying the exact machine where the component will run.

There are also benefits to MetalLB, such as being more flexible in how load balancers can be deployed either in Layer 2 (L2) mode or BGP mode. MetalLB can mmap a group of sequentially allocated IP addresses and along with this mask, allocate one port, for instance, port 80, which provides a much more predictable setup. This method eliminates the randomness typical of NodePort since load balancing is not concerned with allocating any particular node.

Nonetheless, a few aspects still need to be tested, mainly how the system operates when a channel, although present in one of the peers behind the load balancer, is not searched for in that peer. Providing a distinct address for each channel might be necessary if the system fails in such a scenario. This would not be ideal as the cluster was designed with the assumption that all peers participate in the same channel. This design tends towards handling components in a consensus fashion across different organisations, which is the primary purpose of a blockchain.

Although this version of the system is designed with a scenario where several organisations participate in the consensus, in theory, it is possible to constitute a cluster that would include elements of this organisation and elements of others. This approach is valid for implementation but would require further consideration and planning.

## 12.3 Evaluation

Four key metrics were evaluated to understand/evaluate which of the presented architectures is the best for the case study: CPU, RAM, DISK, and LEDGER variation. A load environment in a hospital context was simulated for each test, with 10820 insertions carried out at a throughput of 45 TPS over 23 periods. During this process, the errors recorded in this step were considered negligible for a reason: out of 10820 insertions performed per test, only one case was observed, which was insubstantial for a sound comparative analysis. Therefore, their comparison was ruled out.

The results will be distinguished between Architecture 1, Docker, and the subsequent Architectures with Kubernetes. The two technologies (Docker and Kubernetes) are differentiated based on their usage, which depends on the network size, scale and complexity.

## Evaluation: Architecture 1

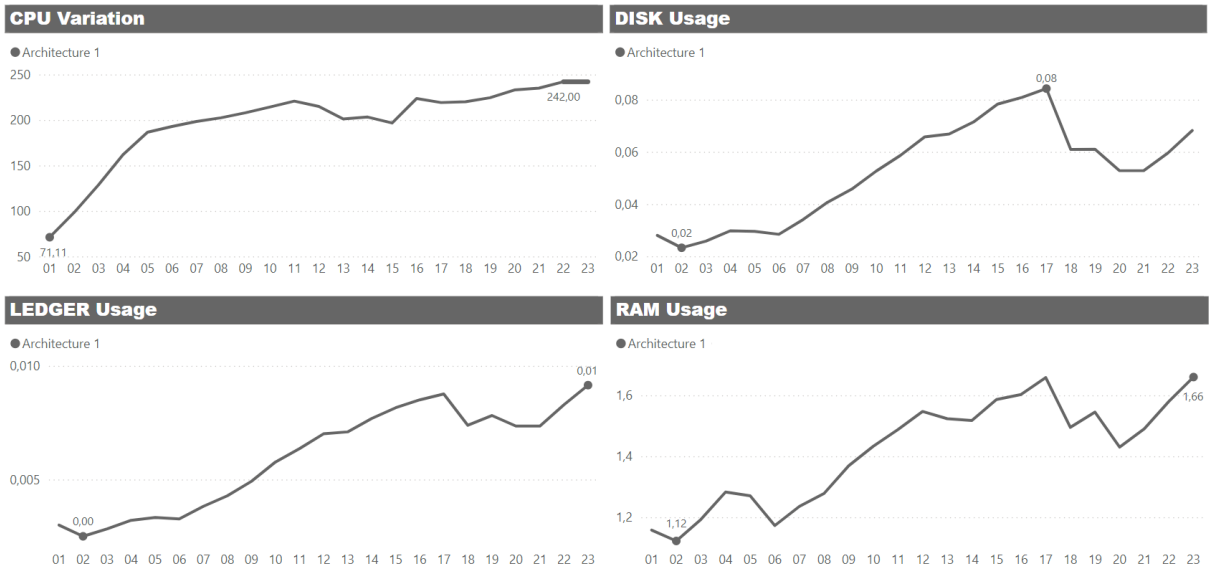



Figure 29: Scalable and Sustainable Blockchain - Performance metrics - Architecture 1

In image 29 it is possible to observe the results of the metrics analysed for architecture 1. Starting the analysis with the CPU variation shows a sharp initial growth, followed by oscillations and a slight drop before growing again until the end when it reaches the peak with a value of 242.0.

Disk usage on this architecture starts low and shows steady growth until it peaks at 0.08 GB. After this, there is a slight reduction before growing again at the end of the period.

Analysing the metric, the use of the ledger grows gradually over time, with some fluctuations, until it reaches a maximum value of 0.01 at the end of the period.

Finally, analysing the use of RAM shows several fluctuations. Specific variations can be observed in the graph, but the trend is for growth over time, reaching its maximum peak at the end of the period with a value of 1.66 GB.

## Evaluation: Architecture 2 and 3

Figure 30 shows the results of the metrics analysed in both architectures. The analysis is carried out comparatively between them because they both use Kubernetes. They differ: While Architecture 2 uses Kubernetes, Architecture 3 uses Kubernetes with peer load balancing. In this way, a comparative analysis is carried out between them.

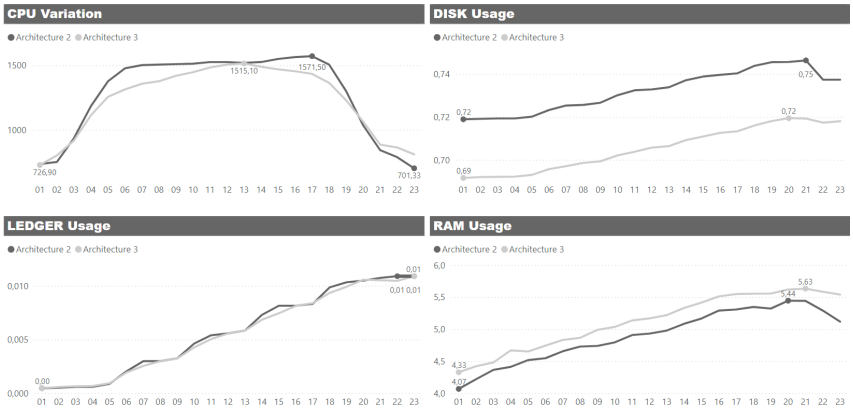



Figure 30: Scalable and Sustainable Blockchain - Performance metrics - Architecture 2 and 3

In Figure 30, it is possible to observe that architecture 2 shows a sharp increase in CPU variation, reaching higher peaks, with a maximum value of 1571.50 while architecture 3 presents a maximum peak of 1515.10.

When analyzing disk usage, both grow consistently. However, architecture 2 has a higher disk usage with a peak of 0.75 GB compared to architecture 3, which has a peak of 0.72 GB. At the end of the analysis period, both showed a decline and stabilised.

The use of the ledger in both architectures is practically identical throughout the analysis. Both follow a similar growth trajectory, with a maximum peak of 0.01 GB.

Finally, in relation to the RAM usage metric, both grow consistently. However, architecture 3 has slightly higher RAM usage than architecture 2 throughout the analysis period, reaching its peak at 5.63 GB.

## 12.4 Discussion

This section will discuss the distinct architectures, considering the test results regarding scalability and sustainability. First, the results obtained from the benchmarking presented in Table 8 will be evaluated.

| Architecture | CPU (Max Variation) | DISK (Peak Usage (GB)) | LEDGER (Peak Usage (GB)) | RAM (Peak Usage (GB)) |
|---|---|---|---|---|
| **Architecture 1** | 242.00 | 0.08 | 0.01 | 1.66 |
| **Architecture 2** | 1571.50 | 0.75 | 0.01 | 5.44 |
| **Architecture 3** | 1515.10 | 0.72 | 0.01 | 5.63 |

Table 8: Max/peak values of Performance metrics

Based on the results, Docker performs better due to the small size of the environment. Since it is lightweight and its structural composition is quite basic, it is useful when performance and resource consumption are geared towards efficiency. Its less abstract nature simplifies the learning curve and relatively fast deployment, which is good for the present structure.

There are, however, quite a few benefits with Kubernetes that contributed as the driving forces of the platform developed during the project. Due to such advanced API management in Kubernetes, it is much simpler to connect and manage the components, thus allowing the system to include or exclude such components without changing the underlying platform. This flexibility is also essential in preserving the effectiveness and dependability of the UI tool while improving and enhancing it throughout the project.

There are several differences between deploying applications with pure Docker and using a Kubernetes-oriented solution. There are cases where a simple implementation of a docker is also enough. However, it changes when the complexity and dimensions of the environments increase, and this is the point at which Kubernetes shines. It is built to easily handle complex and scalable deployment of applications, providing features like resource load-balancing, management, and orchestration API. Owing to these, Kubernetes is highly effective in scenarios requiring seamless application deployment that must be highly available, easily scalable and distributed over several nodes.

Table 9 presents some main characteristics and distinctions between the two solutions.

| Characteristic | Docker | Kubernetes |
|---|---|---|
| More performance for smaller environments | x | |
| Less abstract and easier to learn | x | |
| Incorporated load balancer | | x |
| Resource management | | x |
| More abstract | | x |
| Harder to learn | | x |
| Robust API for managing the networks' resources | | x |
| High availability | | x |
| Built-in mechanism for horizontal scaling | | x |
| Higher resource overhead | | x |

Table 9: Characteristics Comparison between Docker and Kubernetes

While Kubernetes has a steeper learning curve and a higher resource overhead, these complexities are justified in larger, more complex environments. In this case, the smaller environment favours Docker for its performance and ease of use. However, as the project expands and the environment scales, Kubernetes will likely become more beneficial due to its advanced features and ability to handle larger workloads.

Regarding the comparison between Architecture 2 and 3, even though the implementation of a load balancer had only residual benefits in some of the metrics and its implementation may introduce complexity to the development of the network, it provides several advantages that, in the long-term, can be very beneficial. It can ensure better scalability, reliability, resource allocation and performance, contributing to the solution's sustainability over time (Ganesh et al., 2023; Ranjan et al., 2023).

In summary, Docker has proven to be the more performant solution for the current, smaller environment. Yet, this project relies on Kubernetes for specific aspects, such as the UI tool, due to its powerful API and management capabilities. As growth is anticipated, Kubernetes' robust management and high

availability by deploying a load balancer will become increasingly valuable, making it the preferred choice in larger, more complex deployments.

### Chosen Architecture for Healthcare

The chosen architecture for this use case was the one with Kubernetes with load balancer. Here, the architecture is presented with additional components that are essential to a production environment. With this in mind besides the core components we also have: prometheus (for fetching the data from all the cadvisors and also components of the network), cadvisor (measures collector for prometheus), cpp-rest-service (to wrap the data from prometheus and serve it to the admin web server; it is a good practise to not expose entirely the prometheus API), keycloak (for users management), blockexplorerlistener (a developed implementation of a block explorer listener to grab the data from events and store it on a database), postgresql-block-explorer (database for the blockexplorer listener) and quarkus rest for serving this blockexplorer data to the admin web server. Note that the multi-client now serves the admin web server.

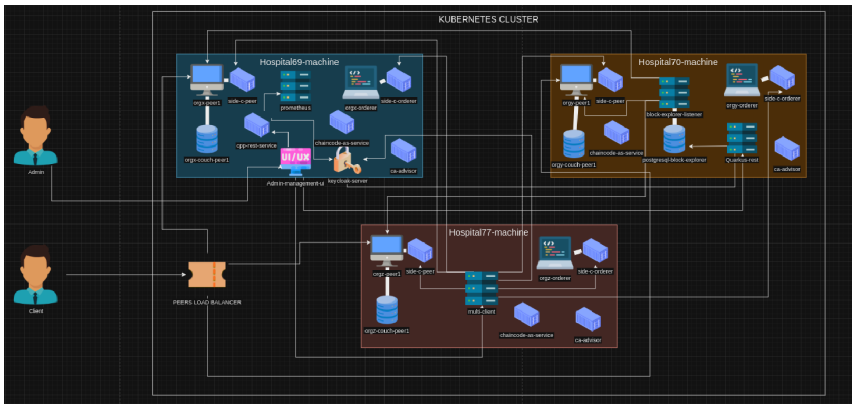



Figure 31: Chosen Architecture - Kubernetes with Load Balancer

## 12.5 Platform for Efficient Blockchain Management and Exploration

Throughout this section, all components related to the developed platform will be presented and described. The platform is divided into four main components: Block Explorer, General Network, Order, and Peer Configuration. Each of these four components will be presented along with their features.

### Block Explorer

The first main component designed was the Block Explorer, which monitors and manages network transactions. It collects and stores data through a custom implementation that captures all relevant details

from the network. This data is securely stored in a database, granting easy access and analysis. Later, a backend architecture processes it and makes it available to the administrative web interface.

This system allows administrators to perform a number of administrative functions over most parts of the Blockchain. These include viewing the network activities by channel, the network's performance in considerable detail, and the inspection of blocks, transactions, and other related network objects. It also enables the supervision and administration of the components and the channels they form part of, necessary for the network to operate.

The dashboard allows the supply of in-depth statistics for the registered blocks, the transactions, the nodes, the chaincodes, and the peers in the system. It further offers information on what percentage of the total number of transactions falls under each organisation, making it easier to visualise the distribution of the activities. There is also a block list which provides the details of the blocks in the order of their incorporation timelines within the blocks. All of this is organised by channel, allowing the patients to proceed to the relevant data of each channel without wasting time.

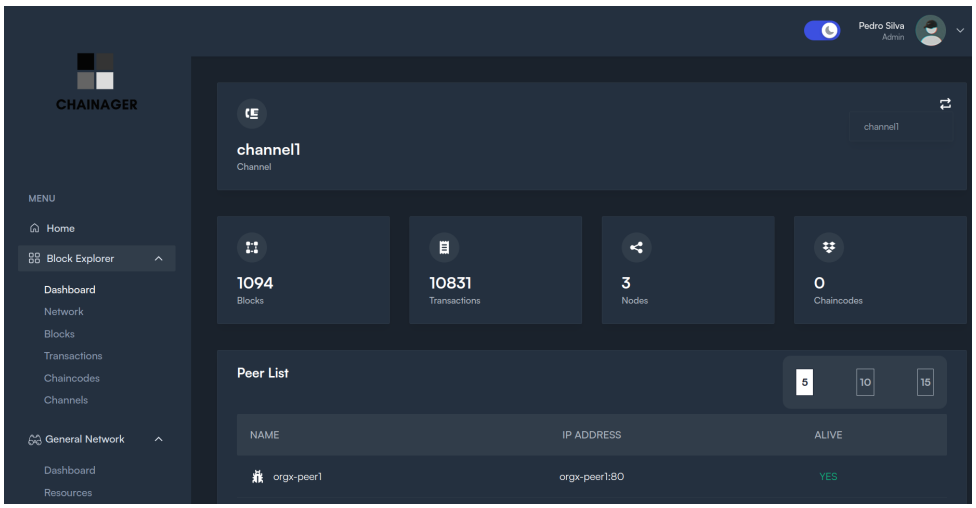



Figure 32: Block Explorer - Dashboard

In the network section, users can check on all the active nodes in the channel. The structure of this list differs from the one that can be viewed in the dashboard since this one is more detailed about every peer. For example, this includes the peer's IP address, type, Membership Service Provider (MSP), the number of transactions it has processed, the number of chaincodes it supports, and its current status (whether it is active or not). As for the dashboard, all this information is aggregated by channel to help the user narrow down to the specific channels when needed.

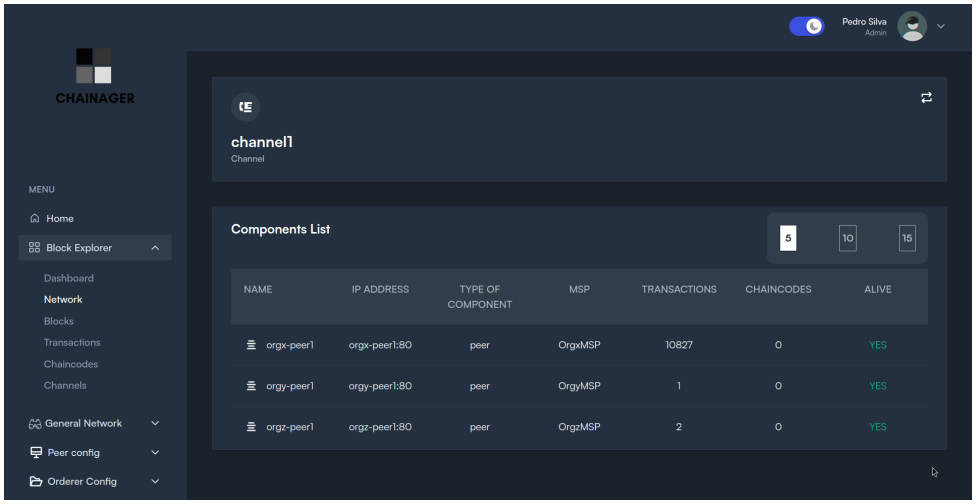



Figure 33: Block Explorer - Network

The blocks section provides detailed information about each block, including the channel it belongs to (which is evident since it is possible to select the channel to inspect), its data hash, the number of transactions it contains and its size within the ledger.

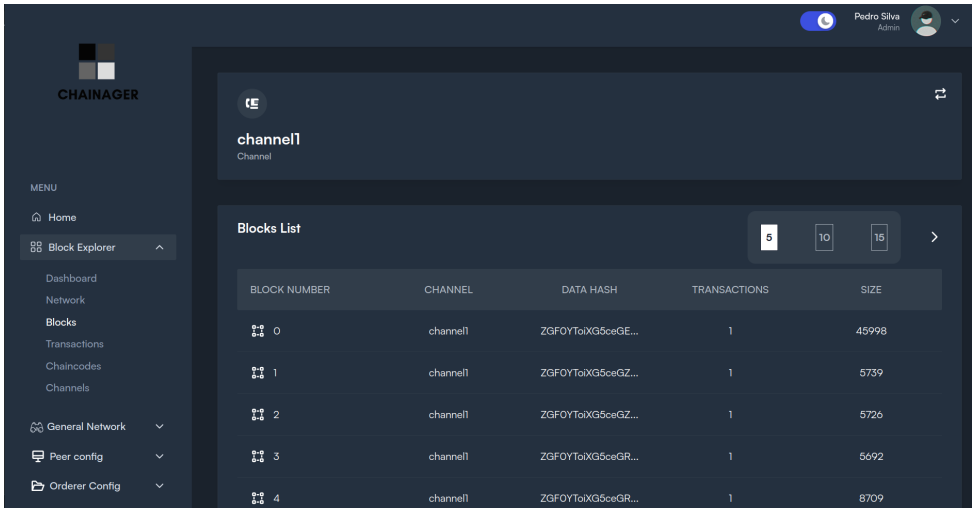



Figure 34: Block Explorer - Blocks

In the Transactions section, users can find a complete listing of the transactions performed along with their information, in chronological order, arranged by channel. These encompass the individual creating the transaction, the name of the channel where the transaction was made, the transaction ID for unique identification, the transaction type performed, the invocation of the chaincode, and the specific time the transaction was carried out. This analysis is done in a channel-specific manner, allowing the users to analyse and track each transaction, ensuring complete transparency and traceability within the system.

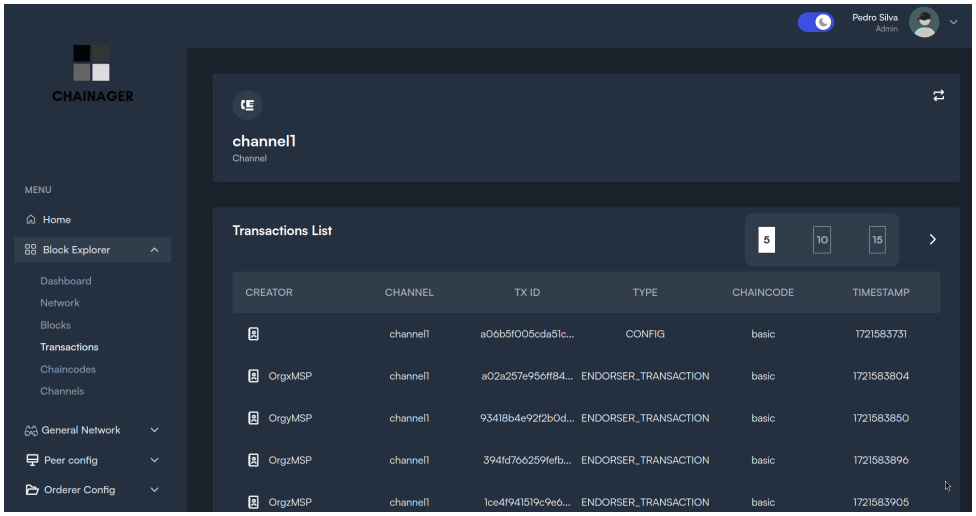



Figure 35: Block Explorer - Transactions

In the Chaincodes section, users can view chaincode details for each channel, including chaincode name, channel name, chaincode transaction count and chaincode version.

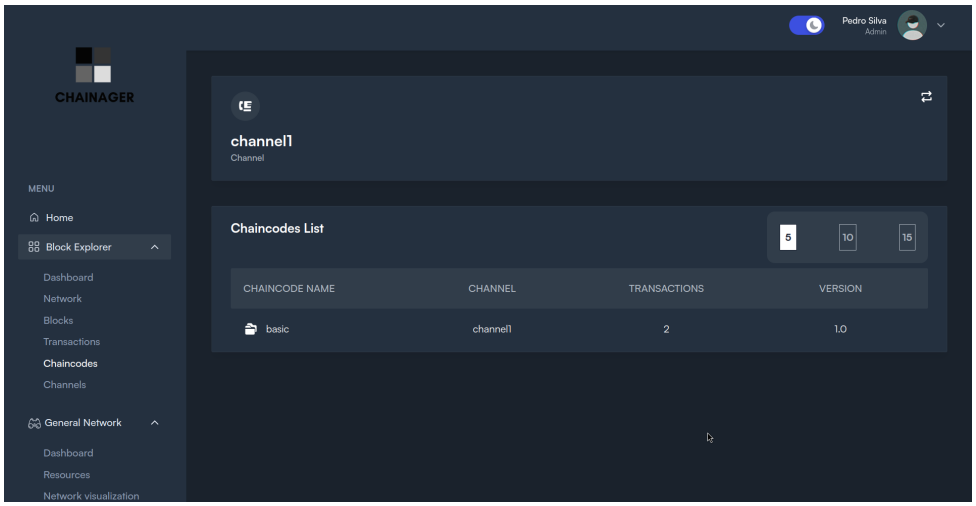



Figure 36: Block Explorer - Chaincodes

In the Channels section, detailed features of every channel are available to the users, including the chaincode information within the channel, the number of transactions, the version, and the timestamp of creation.

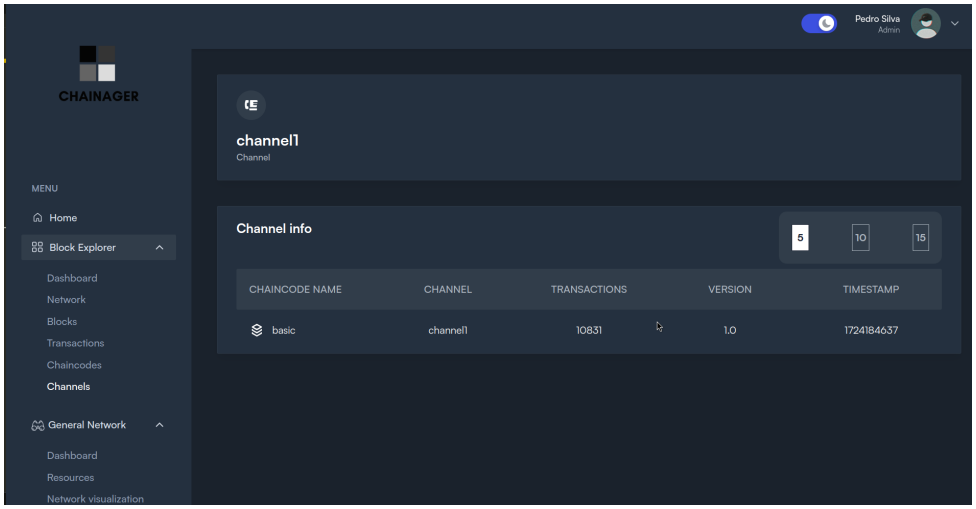



Figure 37: Block Explorer - Channels

## General Network Overview

This part analyses the network's resource utilisation. It monitors several performance metrics: CPU, RAM, disk usage, ledger activity, I/O operations, and network performance. Also, it presents the resources within each cluster, a graphical representation of the network's structure, and allows for an examination of their configurations and how they are organized within each component's directory.

In the "Dashboard" section, it is possible to have a glance at the network, such as checking the number of nodes, alive nodes, dead nodes, CPU variation %, Disk usage per machine GB, Disk usage machine %, RAM per machine GB, and RAM per machine %.

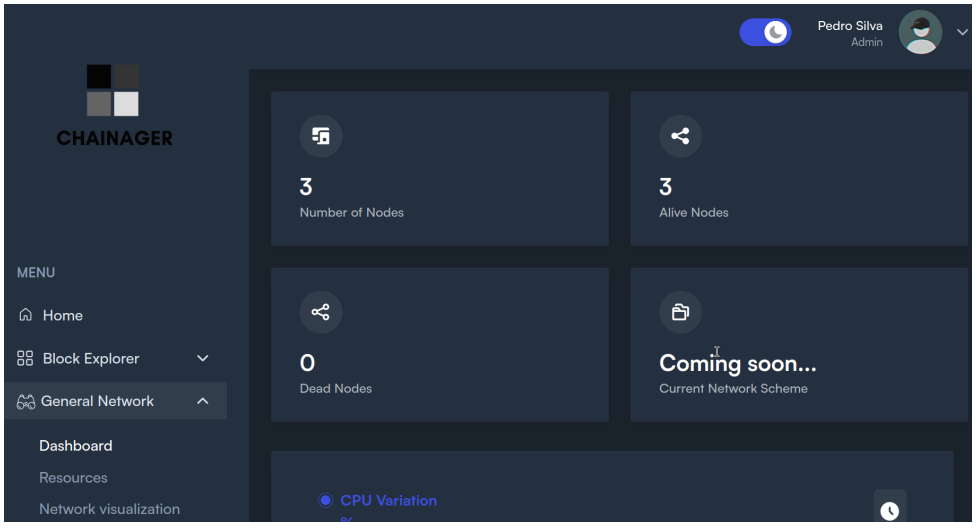



Figure 38: General Network Overview - Dashboard

The "Resources" section provides a list of the services residing in that cluster, each corresponding to the DNS name of that service.

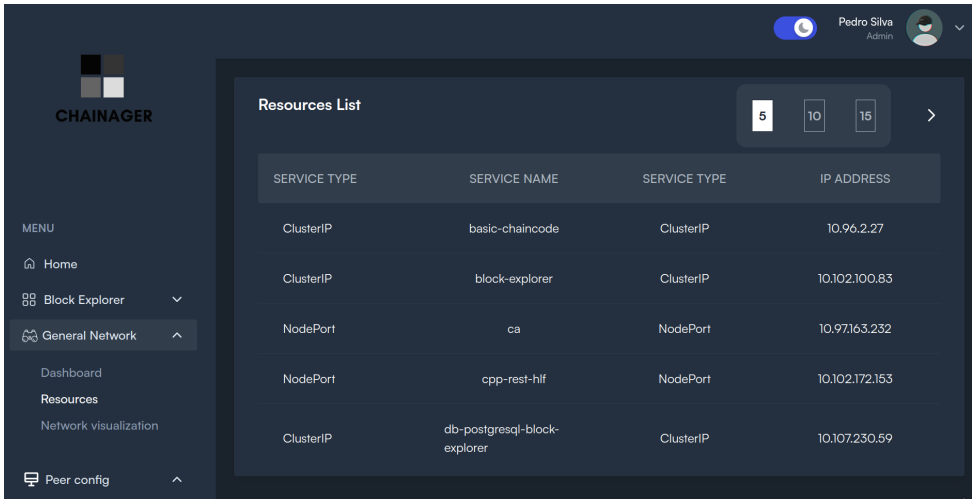



Figure 39: General Network Overview - Resources

The “Network Visualization” section includes a cluster-oriented representation of the current components. This is cluster-oriented, as it groups resources according to what is in the cluster and not to any particular network channel. If it were based on a network channel, the visualisation could include components outside the cluster.

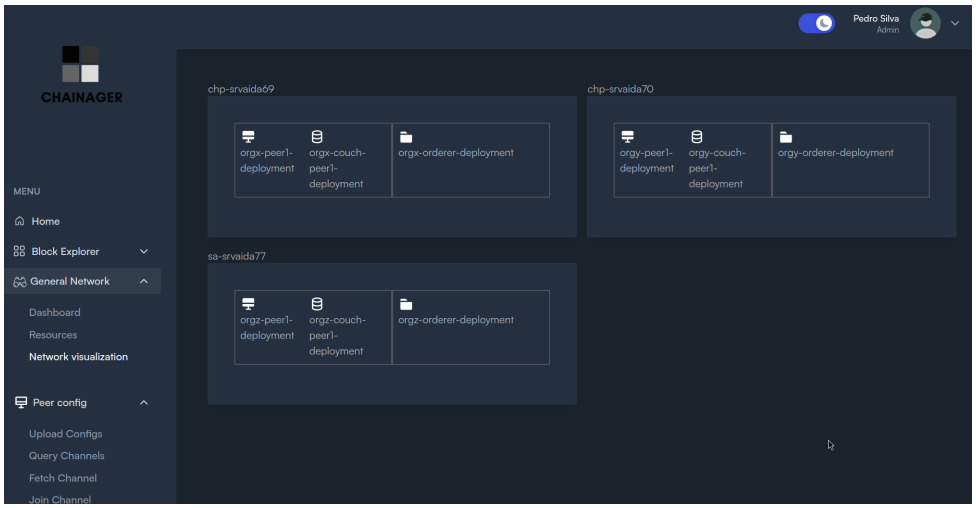



Figure 40: General Network Overview - Network Visualization

## Peer Config

This section deals with peer management and provides a comprehensive user interface for performing all standard peer operations, like: uploading configurations, querying, fetching and joining channels, installing, querying, aproving and committing chaincode, checking chaincode approvals, invoking chaincode for testing, and executing custom commands for more advanced operations.

The following images present some of these operations, namely:

**"Upload Configs"**, where peer configurations can be uploaded, such as the chaincode package for installation.

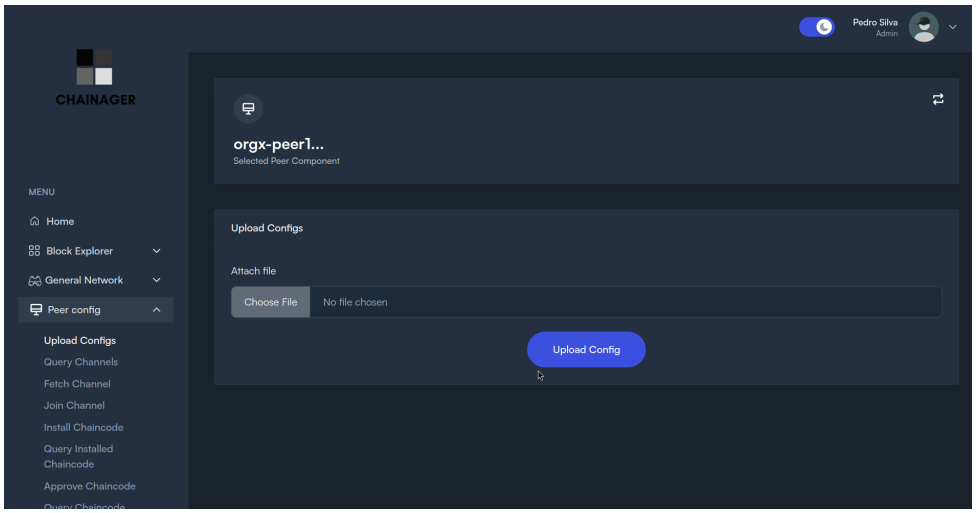



Figure 41: Peer Config - Upload Configs

**"Fetch Channels"**, lets the user fetch a channel from the orderer. To achieve this, they must provide the channel name, the TLS CA file path, the certificate file path, the key file path, and the IP address of the orderer from which they want to fetch the channel.

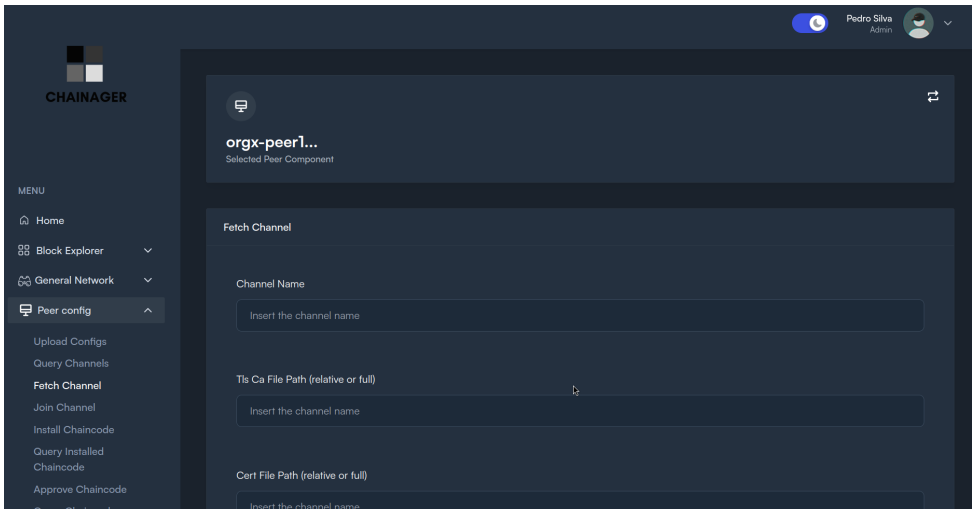



Figure 42: Peer Config - Fetch Channels

**"Install Chaincode"**, after uploading files via the "Upload Configs" section, the files list is shown, and thus, the user can find the right .tar.gz file needed for the installation conveniently.

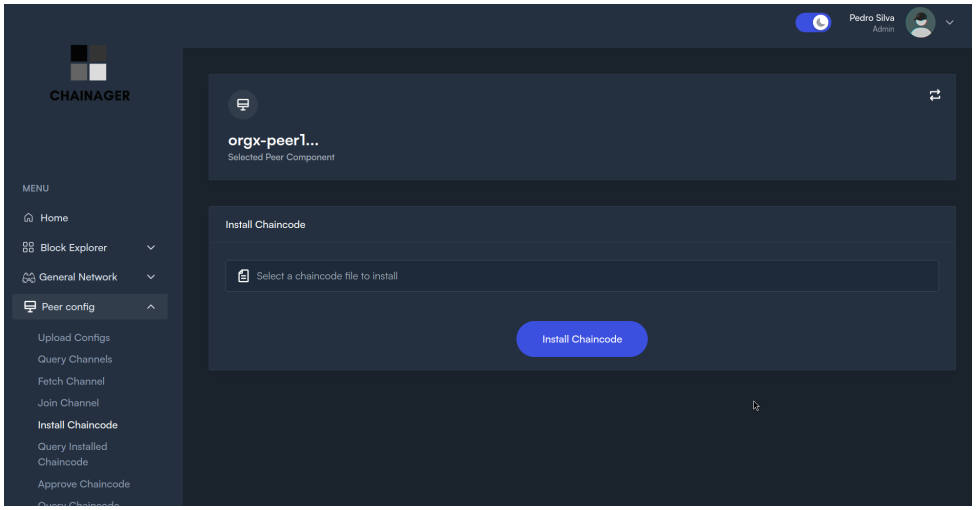



Figure 43: Peer Config - Install Chaincode

**"Custom Commands"**, gives the user the control and all the resources needed to run a specific command to assign to a peer.

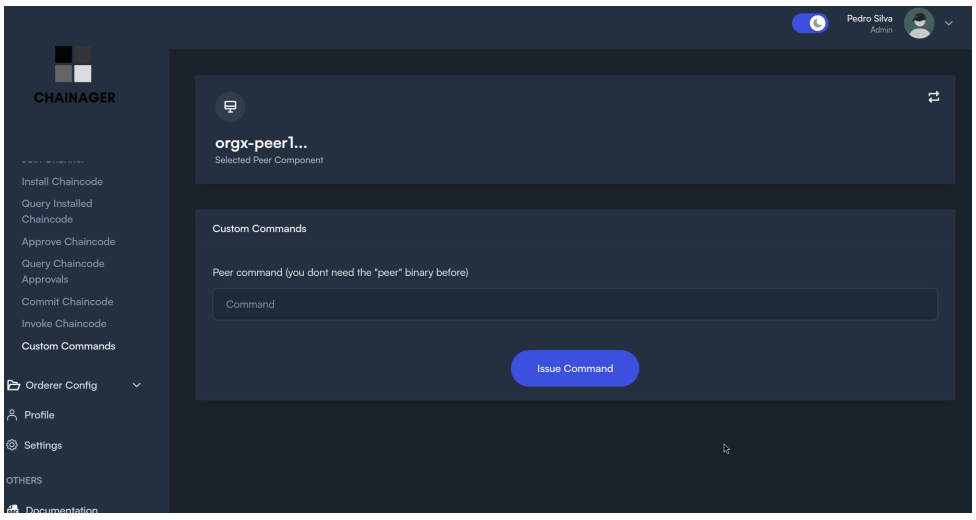



Figure 44: Peer Config - Custom Commands

## Orderer Config

This section focuses on the orderer's management and offers a fairly detailed set of tools for effectively accomplishing all routine tasks. Users can create new channels, join previously created ones, and perform custom actions for further extension.

The following images present some of these operations, namely:

**"Creating Channel"**, allows the user to create a channel for a chosen orderer. In this case, they must select an orderer, upload a channel configuration file, fill in a channel name, and send a request.

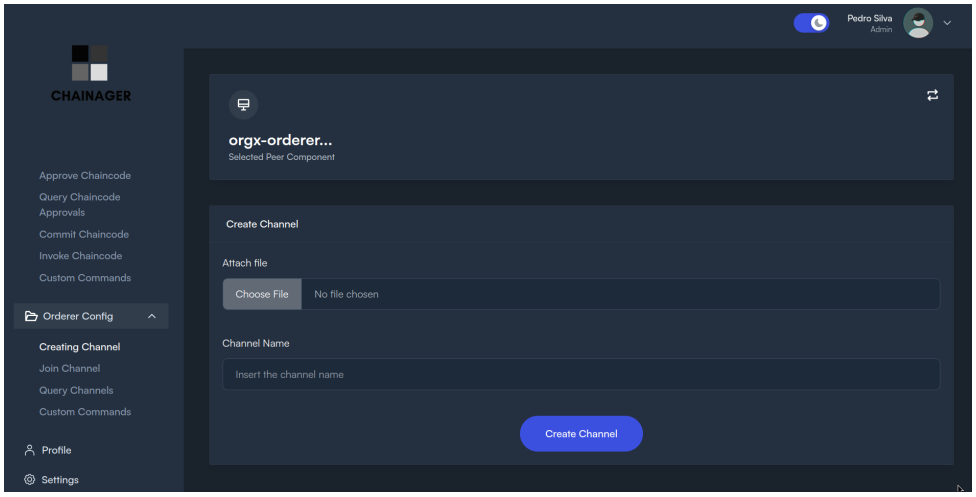



Figure 45: Orderer Config - Creating Channel

**"Query Channel"**, where channels associated with a given orderer can be queried. To perform the query, the user must provide the orderer IP, TLS CA path, client key path, and client certificate path.

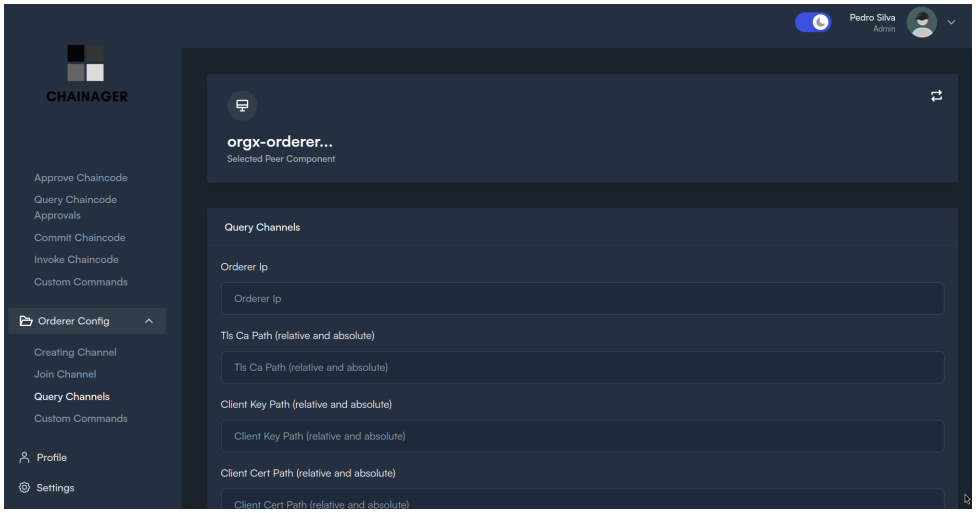



Figure 46: Orderer Config - Query Channel

**"Custom Commands"**, where the user can run custom commands in the orderer component when custom interactions are needed with the networks' orderer.

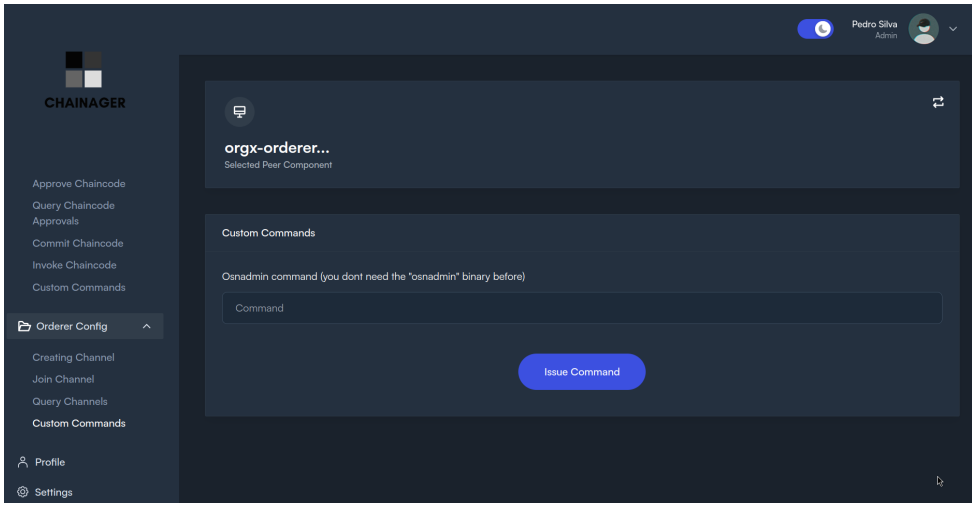



Figure 47: Orderer Config - Custom commands

## 12.6 Summarize

To summarise, three Infrastructures were developed during the project: one using Docker, the other using Kubernetes and the third using Kubernetes alongside a load balancer for interaction with the network. These implementations evolved as we developed further in time, aiming to firstly create the most basic network (docker) and, secondly, to present a more robust architecture that could also be used to manage better an infrastructure that could evolve in many components with time (Kubernetes) and lastly to an infrastructure where we could balance traffic within a same channel contained in a certain number of components (Kubernetes with load balancing). Docker is suitable for small businesses due to its greater simplicity and ease of use. However, there is more work overhead around setting how components must communicate. At the same time, Kubernetes is better for treating components as simple resources designed for larger, more complex environments and is more scalable, incremental, and more manageable to maintain architectures. This work also benefited from features provided by the Kubernetes API, which was used to obtain information about concrete resources employed to create analysis tools. With Kubernetes, regardless of the number of components we have, we can use this analysis tool without further configurations than the resource itself. The Kubernetes with a load balancer (K8 with LB) approach was chosen. This makes sense because of all of the characteristics mentioned so far that are very suited for an infrastructure for the healthcare industry. This sector demands an extensive, resilient infrastructure and advanced features to manage and monitor the network for its administrators, aligning with the primary goal.

Regarding the developed platform, it not only replicates but also improves the functionality of previous solutions. It allows administrators to perform a wide range of tasks with greater efficiency and precision in one place, reducing errors as common network tasks are successfully automated and monitoring is

provided. More concretely, the system provides more than basic network management. It offers information about resource utilisation, peer management and orderer operations. It also provides a user-friendly interface to efficiently handle complex tasks such as monitoring network activity, managing resources or adjusting settings. This is a solution that offers everything that an administrator needs to control its network.

Regarding future work, this project still requires development to achieve broad acceptance in the target environment. Given its potential use in critical industries, it is crucial to continue automating the Network Component Generation, creating Recovery Plans for HLF Components, improving the documentation practices, and continuing to improve the current User interface and User Experience.

# Part V

# Conclusion

# 13

# Improve the Veracity and Value of Healthcare Data Flows

Veracity is a measure of the quality, reliability, and trustworthiness of data managed in processes such as data analysis, sharing, and integration. For these reasons, data veracity is crucial in most, if not all, business domains but especially in healthcare where its absence or presence will affect the decision-making process, the results of patient care, and the health system's culture.

In the healthcare context, the value of data resides in its ability to increase the quality of patient care, address health problems, and enhance healthcare processes. That value is evident in how it can affect clinical choices, increase operational efficiency, and ultimately improve healthcare. In the healthcare sector, the implications of data value creation mean ensuring the accuracy of the data and its practical use within workflows and decision-making processes aimed at addressing important health issues.

Due to the complexity of managing the extensive amounts of information control that the healthcare industry bears, emerging trends like Blockchain Technology and the IoT have become potential solutions to improve the veracity and value of healthcare data flows. This thesis examined the issues of patient data security, privacy, and integrity of health data records concerning such technologies. Through the integration of these technologies, this thesis aims to highlight the need to enhance healthcare data usability by ensuring it is accurate, relevant, valuable, and utilized effectively in the provision of healthcare services.

## 13.1 Overview of the Research

In this thesis, the research aims at solving the core problems of managing and optimizing the flow and management of data in healthcare systems. With healthcare systems moving towards the implementation of data-based patient care, diagnostics, and operational efficiency, data veracity and value have become essential.

In light of this, the following research question arose as the main guiding principle of the workflow.

**How to improve the veracity and value of healthcare data flows?**

The framing of this question not only directed the to study of available and existing technologies and methodologies but also led to the development of new approaches to healthcare designed to meet the specific riding needs of the healthcare industry. Along this recurrent theme, the research produced practical conclusions and recommendations that can be implemented to enhance the current state of healthcare data flows.

In the first instance, such information gaps were identified about the present degree of healthcare data flow analysis, focusing primarily on data validation, data reliability, and data trustworthiness. The research began with an analysis of the available literature and technologies for managing data in healthcare in order to identify existing problems that required solutions. Such issues apply to data collection, processing, integration, and sharing with other healthcare platforms or stakeholders. Besides, factors such as inconsistent standards, problems associated with protecting data across healthcare systems, and ensuring secure data access and auditing remained unresolved. Such literature analysis guided the selection of the areas within the different contributions.

Subsequently, specific frameworks and models were designed to be used within healthcare systems so that the data would remain accurate and valuable over its entire lifecycle. More specifically, emphasis was put on identifying techniques that could potentially and practically be implemented in a real-life healthcare setting, focusing on scalability and adaptability to different healthcare environments.

The research affirmed the importance of developing versatile solutions that can evolve and adapt to new challenges as they arise without compromising data access and integrity.

The study pointed out that technologies such as blockchain, web3, and IoT, which are currently in the developmental phase, can potentially improve the quality, safety, and efficiency of health data. However, it further confirmed that there are obstacles to the uptake of these technologies in terms of their scalability, the amount of infrastructure required, and how they can be integrated into existing ones.

From this perspective, this work has pinpointed one of the most critical issues in healthcare information management: the problem of interoperability. Showcasing innovative approaches to traditional healthcare standards such as HL7 and OpenEHR is essential to ensuring efficient data flow and promoting consistency of data operations. Also, the study supported the necessity to use secure data-sharing methods effective in clinical and research collaboration while preserving privacy and supporting data sharing.

The analysis concerned the ability of each presented contribution to impact data trust and value in specific and distinct ways within data healthcare management. These demonstrated what was possible in making such leaps and what obstacles remained in including emerging technologies such as blockchain, IoT, and decentralized storage systems in healthcare.

The effects of this work should contribute to the basis for further scientific and practical studies and implementations regarding the management of healthcare data. The findings offer several contributions to the ongoing efforts to optimize healthcare systems through better data practices.

## Identified Trends and patterns

Throughout this research, various ideas and consistent elements appear recurrently. When such events are spotted and such details are collated, they present an understanding of the essentials affecting the management of healthcare data and the application of other technologies in this area.

**Emerging technologies integration** such as blockchain, IoT, Web3 solutions and decentralized storage like IPFS improve the performance of healthcare data management significantly and also ensure that the data is secure. These technologies will then provide new means of healthcare data management and protection, consequently enhancing the results and efficiency of operations within the firm.

**Data security and integrity** emerged as the most critical issue: accuracy, reliability, and protection of health information on healthcare systems were emphasized.

**Patient privacy and control**, regarding how much information can be accessed and how it is essential to protect the patient's information and the ownership of the personal health data. This is essential for developing trust in healthcare systems and compliance with the regulations.

**Interoperability and standardization** is considered integral in managing healthcare data. The implementation of these standards, such as HL7, FHIR or OpenEHR, is essential to an efficient and comprehensive exchange and integration of data across diverse systems. This is vital for improved care and operations coordination in the healthcare sector.

The research also pointed out the importance of **scalability and sustainability** in the adoption of the new technologies. It is equally important to deal with the issues of scaling up the technologies across different healthcare scenarios and ensuring their lasting relevance over time to ensure they are successfully adopted, integrated and maintained.

**Enhanced decision-making:** The introduction of new data management tools and technologies into daily operations is helping the making of both managerial and clinical decisions, facilitating procedures and lessening errors.

Lastly, the research focused on **patient-centered care**. There is a growing need for the use of technologies and frameworks that enable a paradigm shift in healthcare delivery, in which data is used to help provide better healthcare delivery by enhancing the approach to patients. This ensures that healthcare delivery focuses on the needs of the patients, resulting in better care and higher levels of satisfaction experienced by the patients.

## 13.2 Future Directions

Research shows that the findings and developments discussed in this study offer great prospects in handling data in healthcare systems and, to be more specific, improving the veracity and value of data flows. Several key areas have emerged as promising directions for assessing exploration:

**Delivering Efficient, Scalable and Flexibilities Solutions:**

To address this need, it's imperative to have a clear strategy for exploring solutions that will not only cater to immediate needs but also develop solutions that can be used more broadly and expand functionalities and infrastructure. Research should ensure that the frameworks are both increasingly effective and adaptable to changes over time.

**Further Investigation on emerging Technologies:**

The technology landscape is dynamic, undergoing improvements within and between its boundaries. Further research should not be static; it should assess new avenues continually emerging in the age of technology and merge new technologies into the management of healthcare data. This means healthcare systems can sustain their functionality by answering new, unique problems and taking advantage of new possibilities as they arise.

**Simplifying Data Exploration and Network Administration:**

New and existing open-source Blockchain data and network management exploration interfaces and tools must be enhanced or developed. It is crucial to automate and simplify the process of blockchain implementation and management. Improve existing documentation and develop tools to decrease the steep learning curve and difficulty finding and training knowledgeable Infrastructure and network administrators. This would significantly improve the adoption and sustainability of developed solutions in the long term.

**Simplifying Chaincode Development:**

It is technically challenging to create and deploy chaincode, which is how to interact with the network and update the blockchain ledger. Future work should focus on simplifying the creation and management of chaincode by developing frameworks, processes and tools. This might include visual programming environments, templates, and tools that assist in writing, testing and deploying chaincode without much manual intervention. Such changes would help overcome the challenges, and more healthcare institutions would implement blockchain technology to engage in safe, self-executing contract transactions and reduce operational and development costs.

**Further research Blockchain ETL and Analytics:**

To achieve a broader acceptance of the technology, many challenges concerning Blockchain Analytics (BA) and ETL processes need to be addressed. Advanced tools and methodologies suitable for blockchain data should be developed to improve the efficiency and efficacy of analysing, extracting meaningful insights, and integrating them into existing healthcare data systems. Healthcare institutions can leverage the improvement of these processes to make more data-centric decisions, hence improving the quality of healthcare practices and patient care.

**Blockchain and AI integration:**

Further studies may help determine how to combine blockchain with AI to improve healthcare data management accuracy, security, and efficiency. This would allow more intelligent data analysis and automation of decision-making and modelling while preserving data security. It would also contribute to simplifying the implementation, growth, and continuous management of Blockchain solutions.

Those directions provide proper ways to progress in managing healthcare data, using emerging technologies to improve patient care, data security, and healthcare system management.

# Bibliography


Abbate, S., Centobelli, P., Cerchione, R., Oropallo, E., & Riccio, E. (2022). Blockchain design in health data management. *2022 IEEE TEMS Conference on Europe (TEMSCON Europe)*, 1–6. https://doi.org/10.1109/temsconeurope54743.2022.9801918

Abdelhédi, F., Jemmali, R., & Zurfluh, G. (2023). Medical data lake query assistance. *2023 IEEE/ACS 20th International Conference on Computer Systems and Applications (AICCSA)*. https://doi.org/10.1109/AICCSA59173.2023.10479336

About - healthwizz [Accessed: Jan. 25, 2024]. (2024). https://healthwizz.com/about/

AbouZahr, C., & Boerma, T. (2005). Health information systems: The foundations of public health. *Bull. World Health Organ.*, *83*(8), 578–583.

Abowd, G. D., Dey, A. K., Brown, P. J., Davies, N., Smith, M., & Steggles, P. (1999). Towards a better understanding of context and context-awareness. *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, *1707*, 304–307.

Abu-elezz, I., Hassan, A., Nazeemudeen, A., Househ, M., & Abd-alrazaq, A. (2020). The benefits and threats of blockchain technology in healthcare: A scoping review. *International Journal of Medical Informatics*, *142*. https://doi.org/10.1016/j.ijmedinf.2020.104246

Adame, T., Bel, A., Carreras, A., Melià-Seguí, J., Oliver, M., & Pous, R. (2018). Cuidats: An rfid–wsn hybrid monitoring system for smart health care environments. *Futur. Gener. Comput. Syst.*, *78*, 602–615.

Agbo, C. C., & Mahmoud, Q. H. (2020). Blockchain in healthcare opportunities, challenges, and possible solutions. *Int. J. Healthc. Inf. Syst. Informatics*, *15*(3), 82–97.

Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019). Blockchain technology in healthcare: A systematic review. *Healthc.*, *7*(2). https://doi.org/10.3390/healthcare7020056

Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., & Amaba, B. (2017). Blockchain technology innovations. *2017 IEEE Technol. Eng. Manag. Soc. Conf. TEMSCON 2017*, 137–141.

Aimedis. (2023). Aimedis whitepaper.

Akinola, O., Akinola, A., Oyekan, B., Oyerinde, O., Adebiyi, H. F., & Sulaimon, B. (2024). Blockchain-enabled security solutions for medical device integrity and provenance in cloud environments.

*International Journal of Information Security Research and Technology*. https://doi.org/10.38124/ijisrt/ijisrt24apr225

Aktas, F., Ceken, C., & Erdemli, Y. E. (2018). Iot-based healthcare framework for biomedical applications. *J. Med. Biol. Eng.*, *38*(6), 966–979.

Alertmanager documentation [Accessed: 2023-09-22]. (2023). https://prometheus.io/docs/alerting/latest/alertmanager/

Alexsicart. (2018). Filenation [Last access: 21-04-2023]. https://github.com/FileNation/FileNation

Alharby, M. (2023). Blockchain-based system for secure storage and sharing of diabetics healthcare records. *2023 IEEE International Conference on Artificial Intelligence and Smart Computing (ICAISC)*. https://doi.org/10.1109/ICAISC56366.2023.10085169

Ali, A., Al-rimy, B., Alsubaei, F. S., Almazroi, A., & Almazroi, A. A. (2023). Healthlock: Blockchain-based privacy preservation using homomorphic encryption in internet of things healthcare applications. *Sensors*, *23*(15), 6762. https://doi.org/10.3390/s23156762

Ali, O., et al. (2019). Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives. *Journal of Medical Systems*.

Alkhateeb, A., Catal, C., Kar, G., & Mishra, A. (2022). Hybrid blockchain platforms for the internet of things (iot): A systematic literature review. *Sensors*. https://doi.org/10.3390/s22041304

AlQudah, A., Al-Emran, M., & Shaalan, K. (2021). Medical data integration using hl7 standards for patient's early identification. *PLOS ONE*. https://doi.org/10.1371/journal.pone.0262067

Altarawneh, H., & Tarawneh, M. (2023). Business intelligence and information system management: A conceptual view. *Journal of Strategic Management Studies*. https://doi.org/10.33168/jsms.2023.0203

Ampel, B., Patton, M., & Chen, H. (2019). Performance modeling of hyperledger sawtooth blockchain. *2019 IEEE Int. Conf. Intell. Secur. Informatics, ISI 2019*, 59–61.

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., & Muralidharan, S. (2018a). Hyperledger fabric: A distributed operating system for permissioned blockchains. *Proceedings of the thirteenth EuroSys conference*, 1–15.

Androulaki, E., Barger, A., Bortnikov, V., et al. (2018b). Hyperledger fabric: A distributed operating system for permissioned blockchains. *Proceedings of the Thirteenth EuroSys Conference*.

androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., Caro, A. D., Enyart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolić, M., ... Yellick, J. (2018). Hyperledger fabric: A distributed operating system for permissioned blockchains.

Angraal, S., Krumholz, H. M., & Schulz, W. L. (2017). Blockchain technology: Applications in health care. *Circ. Cardiovasc. Qual. Outcomes*, *10*(9), 1–4. https://doi.org/10.1161/CIRCOUTCOMES.117.003800

Anhang Price, R., Elliott, M. N., Zaslavsky, A. M., Hays, R. D., Lehrman, W. G., Rybowski, L., Edgman-Levitan, S., & Cleary, P. D. (2014). Examining the role of patient experience surveys in measuring health care quality. *Medical Care Research and Review*, *71*(5), 522–554.

Aronson, S., Babb, L., Ames, D. C., Gibbs, R., Venner, E., Connelly, J. J., Marsolo, K. A., Weng, C., Williams, M. S., Hartzler, A., Liang, W. H., Ralston, J., Devine, E., Murphy, S., Chute, C., Caraballo, P., Kullo, I., Freimuth, R., Rasmussen, L., ... eMERGE Network Ehri Working Group. (2018). Empowering genomic medicine by establishing critical sequencing result data flows: The emerge example. *Journal of the American Medical Informatics Association*. https://doi.org/10.1093/jamia/ocy051

Arunsankar, G., Gopi, B., Sampathrajan, R., Sasikala, S., Vanathi, A., & Srinivasan, C. (2023). Iot controlled device to manage the emg signals of the patient and alert in real time. *2023 Second International Conference On Smart Technologies For Smart Nation (SmartTechCon)*, 1365–1370.

Ashraf, E., Areed, N., Salem, H., Abdelhay, E. H., & Farouk, A. (2022). Fidchain: Federated intrusion detection system for blockchain-enabled iot healthcare applications. *Healthcare*, *10*(6), 1110. https://doi.org/10.3390/healthcare10061110

Austin, C. C., Brown, S., Fong, N., Humphrey, C., Leahey, A., & Webster, P. (2016). Research data repositories: Review of current features, gap analysis, and recommendations for minimum requirements. *IASSIST Quarterly*, *39*(4), 24–24.

Ayaz, M., Pasha, M. F., Alzahrani, M. Y., Budiarto, R., & Stiawan, D. (2021). The fast health interoperability resources (fhir) standard: Systematic literature review of implementations, applications, challenges and opportunities. *JMIR medical informatics*, *9*(7), e21929.

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016a). Medrec: Using blockchain for medical data access and permission management. *Proceedings - 2016 2nd International Conference on Open and Big Data, OBD 2016*, 25–30. https://doi.org/10.1109/OBD.2016.11

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016b). Medrec: Using blockchain for medical data access and permission management. *2016 2nd International Conference on Open and Big Data (OBD)*, 25–30.

Bai, P., Kumar, S., Kumar, K., Kaiwartya, O., Mahmud, M., & Lloret, J. (2022). Gdpr compliant data storage and sharing in smart healthcare system: A blockchain-based solution. *Electronics*. https://doi.org/10.3390/electronics11203311

Baig, M. M. B., & Jilani, M. T. (2018). An ibeacon based real-time context-aware e-healthcare system. *2017 1st Int. Conf. Latest Trends Electr. Eng. Comput. Technol. INTELLECT 2017*, *2018-January*, 1–5.

Balatska, V., Poberezhnyk, V., Petriv, P., & Opirskyy, I. (2024). Blockchain application concept in sso technology context. *Proceedings of the International Conference on Current Progress in IT Security (CPITS)*. https://dblp.org/rec/conf/cpits/BalatskaPPO24.html

Bamakan, S. M. H., Moghaddam, S. G., & Manshadi, S. D. (2021). Blockchain-enabled pharmaceutical cold chain: Applications, key challenges, and future trends. *Journal of Cleaner Production*, *302*, 127021. https://doi.org/10.1016/j.jclepro.2021.127021

Bambacht, J., & Pouwelse, J. (2022). Web3: A decentralized societal infrastructure for identity, trust, money, and data. *arXiv preprint arXiv:2203.00398*.

Beale, T., & Heard, S. (2007). *Architecture overview, openehr* (tech. rep.). openEHR Foundation.

Beck, R., & Müller-Bloch, C. (2017). Blockchain as radical innovation: A framework for engaging with distributed ledgers. *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, *2017-Janua*, 5390–5399.

Beckmann, C. L., Keuchel, D., Soleman, W. O. I. A., Nürnberg, S., & Böckmann, B. (2023). Semantic integration of bpmn models and fhir data to enable personalized decision support for malignant melanoma. *Information*. https://doi.org/10.3390/info14120649

Bell, L., Buchanan, W. J., Cameron, J., & Lo, O. (2018). Applications of blockchain within healthcare. *Blockchain Healthc. Today*, *1*, 1–7.

Benchoufi, M., Porcher, R., & Ravaud, P. (2018). Blockchain protocols in clinical trials: Transparency and traceability of consent. *F1000Research*, *6*, 66.

Benet, J. (2014a). Ipfs - content addressed, versioned, p2p file system.

Benet, J. (2014b). Ipfs - content addressed, versioned, p2p file system. *arXiv preprint arXiv:1407.3561*.

Benet, J. (2015). Ipfs: The distributed, permanent web. *Protocol Labs*. https://ipfs.io/ipfs/QmR7GSQM93Cx5eAg6a6fNYyqNV3g8niKzZK7AZ2k9G8Mn1

Benson, T. (2012). *Principles of health interoperability hl7 and snomed*. Springer Science & Business Media.

Benson, T., & Grieve, G. (2021). Principles of health interoperability. *Cham: Springer International*, 21–40.

Bertytech [Last access: 21-04-2023]. (2023). https://berty.tech/

Blanken, M., Mathijssen, J., van Nieuwenhuizen, C., Raab, J., & van Oers, H. V. (2022). Intersectoral collaboration at a decentralized level: Information flows in child welfare and healthcare networks. *BMC Health Services Research*. https://doi.org/10.1186/s12913-022-07810-z

Borycz, J. D. (2021). Implementing data management workflows in research groups through integrated library consultancy. *Data Science Journal*, *20*, 1–9. https://doi.org/10.5334/dsj-2021-009

Brattstrom, M., & Morreale, P. (2017). Scalable agentless cloud network monitoring. *Proc. - 4th IEEE Int. Conf. Cyber Secur. Cloud Comput. CSCloud 2017 3rd IEEE Int. Conf. Scalable Smart Cloud, SSC 2017*, 171–176. https://doi.org/10.1109/CSCloud.2017.11

Brazil, B. (2018). *Prometheus: Up & running: Infrastructure and application performance monitoring*. "O'Reilly Media, Inc."

Bucknall, T. K. (2010). Medical error and decision making: Learning from the past and present in intensive care. *Australian critical care*, *23*, 150–156.

Buterin, V. (2014). *A next generation smart contract & decentralized application platform*.

Cachin, C. (2016a). Architecture of the hyperledger blockchain fabric. *Workshop on Distributed Cryptocurrencies and Consensus Ledgers*, *310*.

Cachin, C., Schubert, S., & Vukolić, M. (2016). Architecture of the hyperledger blockchain fabric. *Leibniz Int. Proc. Informatics, LIPIcs*, *70*, 24.1–24.16.

Cachin, C. (2016b). Architecture of the hyperledger blockchain fabric. *Workshop on Distributed Cryptocurrencies and Consensus Ledgers*.

Canova-Barrios, C., & Machuca-Contreras, F. (2022). Interoperability standards in health information systems: Systematic review. *MW Salud*. https://doi.org/10.56294/mw20227

Cardoso, L., Marins, F., Portela, F., Santos, M., Abelha, A., & Machado, J. (2014). The next generation of interoperability agents in healthcare. *International journal of environmental research and public health*, *11*(5), 5349–5371.

Castanheira, A., Peixoto, H., & Machado, J. (2020). Overcoming challenges in healthcare interoperability regulatory compliance. *International Symposium on Ambient Intelligence*, 44–53.

Chakraborty, M., & Kundan, A. P. (2021). *Monitoring cloud-native applications: Lead agile operations confidently using open source software*. Springer. https://doi.org/10.1007/978-1-4842-6888-9

Chen, R. J., Lu, M. Y., Chen, T. Y., Williamson, D. F., & Mahmood, F. (2021). Synthetic data in machine learning for medicine and healthcare. *Nature Biomedical Engineering*, *5*(6), 493–497.

Chen, R. J., Lu, M. N., Chen, T. Y., Williamson, D. F., & Mahmood, F. (2021). Synthetic data in machine learning for medicine and healthcare. *Nature Biomedical Engineering*, *5*(6), 493–497.

Chen, Y., Chen, S., Liang, J., Feagan, L. W., Han, W., Huang, S., & Wang, X. S. (2020). Decentralized data access control over consortium blockchains. *Information Systems*, *94*, 101590.

Choi, W., & Hong, J. W.-K. (2021). Performance evaluation of ethereum private and testnet networks using hyperledger caliper. *2021 22nd Asia-Pacific Network Operations and Management Symposium (APNOMS)*, 325–329. https://doi.org/10.23919/APNOMS52696.2021.9562684

Chronicled [Accessed: Jan. 25, 2024]. (2024). https://www.chronicled.com/

Cloud native computing foundation [Accessed: 2024-03-06]. (2024). https://www.cncf.io

Collotta, M., & Pau, G. (2015). A solution based on bluetooth low energy for smart home energy management. *Energies*, *8*(10), 11916–11938.

Cornock, M. (2018). General data protection regulation (gdpr) and implications for research. *Maturitas*, *111*, A1–A2.

Cuevas-González, D., García-Vázquez, J.-P., Bravo-Zanoguera, M., López-Avitia, R., Reyna, M., Zermeño-Campos, N. A., & González-Ramírez, M. L. (2022). Ecg standards and formats for interoperability between mhealth and healthcare information systems: A scoping review. *International Journal of Environmental Research and Public Health*. https://doi.org/10.3390/ijerph191911941

Cunha, J., Duarte, R., Guimarães, T., Quintas, C., & Santos, M. F. (2022). Blockchain analytics in healthcare: An overview. *Procedia Comput. Sci.*, *201*(100), 708–713. https://doi.org/10.1016/j.procs.2022.03.095

Cunha, J., Duarte, R., Guimarães, T., & Santos, M. F. (2022). Permissioned blockchain approach using open data in healthcare. *Procedia Comput. Sci.*, *210*, 242–247.

Curran, B. (2018). What is practical byzantine fault tolerance? complete beginner's guide [Last access: 21-04-2023]. https://blockonomi.com/practical-byzantine-fault-tolerance/

Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustain. cities Soc.*, *39*, 283–297.

d'Aliberti, O. G., & Clark, M. A. (2022). Preserving patient privacy during computation over shared electronic health record data. *Journal of Medical Systems*, *46*(12), 1–8.

De Donno, M., Tange, K., & Dragoni, N. (2019). Foundations and evolution of modern computing paradigms: Cloud, iot, edge, and fog. *IEEE Access*, *7*, 103771–103781. https://doi.org/10.1109/ACCESS.2019.2947652

Debnath, P., Mahmud, A., Hossain, A. K., & Rahman, S. I. (2022). Design and application of iot-based real-time patient telemonitoring system using biomedical sensor network. *SN Computer Science*, *4*(2), 94.

Dhayne, H., Kilany, R., Haque, R., & Taher, Y. (2018). Sedie: A semantic-driven engine for integration of healthcare data. *2018 IEEE International Conference on Bioinformatics and Biomedicine (BIBM)*, 617–622.

Dib, O., Brousmiche, K.-L., Durand, A., Thea, E., & Hamida, E. B. (2018). Consortium blockchains: Overview, applications and challenges. *Int. J. Adv. Telecommun*, *11*(1), 51–64.

Dillenberger, D. N., et al. (2019). Blockchain analytics and artificial intelligence. *IBM J. Res. Dev.*, *63*(2).

Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C., & Wang, J. (2018). Untangling blockchain: A data processing view of blockchain systems. *IEEE Trans. Knowl. Data Eng.*, *30*(7), 1366–1385.

DiSantostefano, J. (2009). International classification of diseases 10th revision (icd-10). *The Journal for Nurse Practitioners*, *5*(1), 56–57.

Dolin, R. H., Alschuler, L., Beebe, C., Biron, P. V., Boyer, S. L., Essin, D., Kimber, E., Lincoln, T., & Mattison, J. E. (2001). The hl7 clinical document architecture. *Journal of the American Medical Informatics Association*, *8*(6), 552–569.

Drescher, D. (2017). *Blockchain basics: A non-technical introduction in 25 steps*. Apress.

Duan, Y., Edwards, J. S., & Dwivedi, Y. K. (2019a). Artificial intelligence for decision making in the era of big data–evolution, challenges and research agenda. *International journal of information management*, *48*, 63–71.

Duan, Y., Edwards, J. S., & Dwivedi, Y. K. (2019b). Artificial intelligence for decision making in the era of big data–evolution, challenges and research agenda. *International journal of information management*, *48*, 63–71.

Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., & Wang, F. (2017). Secure and trustable electronic medical records sharing using blockchain. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5977675/

Dubovitskaya, A., Baig, F., Xu, Z., Shukla, R., Zambani, P. S., Swaminathan, A., Jahangir, M., Chowdhry, K., Lachhani, R., Idnani, N., Schumacher, M., Aberer, K., Stoller, S., Ryu, S., & Wang, F. (2020). Action-ehr: Patient-centric blockchain-based electronic health record data management for cancer care. *Journal of Medical Internet Research*. https://doi.org/10.2196/13598

Dubovitskaya, M., Xu, Z., Ryu, S.-H., Schumacher, M., & Wang, F.-Y. (2017). Secure and trustful electronic medical records sharing using blockchain. *AMIA Annual Symposium Proceedings*, *2017*, 650.

Ebardo, R. A., & Tuazon, J. B. D. (2019). Identifying healthcare information systems enablers in a developing economy. *2019 International Conference on Engineering, Technology and Innovation (ICE/ITMC)*. https://doi.org/10.1109/ICETAS48360.2019.9117421

Ehrsam, F. (2017). Regulating healthcare with blockchain technology. *Health Informatics Journal*, *23*(3), 133–141.

Engelhardt, M. A. (2017). Hitching healthcare to the chain: An introduction to blockchain technology in the healthcare sector. *Technology Innovation Management Review*, *7*(10), 22–34.

Espín, R. A., León, K. P., & Espín, J. A. (2019). The case study methodology: A guide for research. *EDULEARN19 Proceedings*, 8783–8783.

Ethereum Foundation. (2016). The dao [https://ethereum.org/en/dao/].

Fabric, H. L. (2022). Case study hitachi streamlines and secures procurement with hyperledger fabric.

Faragher, R., & Harle, R. (2015). Location fingerprinting with bluetooth low energy beacons. *IEEE J. Sel. Areas Commun.*, *33*(11), 2418–2428.

Faria, S., Oliveira, D., Abelha, A., & Machado, J. (2020). Intelligent support system for the provision of inpatient care. *Adv. Intell. Syst. Comput.*, *1137*, 364–374.

Fekih, R. B., & Lahami, M. (2020). Application of blockchain technology in healthcare: A comprehensive study. *The Impact of Digital Technologies on Public Health in Developed and Developing Countries: 18th International Conference, ICOST 2020*, 268–276.

Foschini, L., Gavagna, A., Martuscelli, G., & Montanari, R. (2020). Hyperledger fabric blockchain: Chaincode performance analysis. *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, 1–6.

Foundation, L. (2018a). Hyperledger architecture, volume 2: Smart contracts.

Foundation, L. (2018b). Hyperledger architecture, volume 2: Smart contracts.

Foundation, L. (2018c). An introduction to hyperledger.

Gamal, A., Barakat, S., & Rezk, A. (2021a). Standardised electronic health record data modeling and persistence: A comparative review. *J. Biomed. Inform.*, *114*, 103670. https://doi.org/10.1016/j.jbi.2020.103670

Gamal, A., Barakat, S., & Rezk, A. (2021b). Standardized electronic health record data modeling and persistence: A comparative review. *J. Biomed. Inform.*, *114*(December 2020), 103670.

Ganesh, A., Ramakrishnan, R., Sekar, A. K., & Logeshwaran, J. (2023). A load balancing architecture to improve the security of cloud computing in the disease management centers. *2023 Second International Conference On Smart Technologies For Smart Nation (SmartTechCon)*, 1299–1305. https://doi.org/10.1109/SmartTechCon57526.2023.10391528

Gaur, S. (2015). Bringing context awareness to iot-based wireless sensor networks. *2015 IEEE Int. Conf. Pervasive Comput. Commun. Work. PerCom Work. 2015*, 228–229.

Ghadge, A., Bourlakis, M., Kamble, S., & Seuring, S. (2023). Blockchain implementation in pharmaceutical supply chains: A review and conceptual framework. *International Journal of Production Research*, *61*(19), 6633–6651. https://doi.org/10.1080/00207543.2022.2125595

Ghezzi, C. (2001). Designing data marts for data warehouses. *ACM Transactions on Software Engineering and Methodology (TOSEM)*, *10*(4), 452–483.

Gohil, K., Gohil, A., Gupta, R., Jadav, N., & Tanwar, S. (2023). Proxy-based verification of smart contracts for healthcare domain in blockchain environment. *2023 International Conference on Computational Intelligence, Security & IoT (ICCISIoT)*, 256–261. https://doi.org/10.1109/ICCCIS60361.2023.10425319

Golfarelli, M., & Rizzi, S. (2018). From star schemas to big data: 20+ years of data warehouse research. *A comprehensive guide through the Italian database research over the last 25 years*, 93–107.

Gordon, W. J., & Catalini, C. (2018). Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability. https://www.sciencedirect.com/science/article/pii/S20010370 1830028X#bb0030

Gorenflo, C., Lee, S., Golab, L., & Keshav, S. (2019). Fastfabric: Scaling hyperledger fabric to 20,000 transactions per second. *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 455–463. https://doi.org/10.1109/ICBC.2019.00067

Grafana integration with prometheus [Accessed: 2024-05-07]. (2024). https://grafana.com/docs/grafana/latest/datasources/prometheus/

Guimarães, T., Moreira, A., Peixoto, H., & Santos, M. (2020). Icu data management - a permissioned blockchain approach. *Procedia Comput. Sci.*, *177*, 546–551.

Guimarães, T., Silva, H., Peixoto, H., & Santos, M. (2020). Modular blockchain implementation in intensive medicine. *Procedia Comput. Sci.*, *170*, 1059–1064.

Gulati, K., Khare, A., Sumathy, B., Mamgain, P., Arnoldovich, S. A., & Arkadyevna, Z. E. (2021). Using blockchain integration patterns to ensure data integrity in the health care industry. *Journal of Pharmaceutical Research International*. https://doi.org/10.9734/jpri/2021/v33i64a35364

Guo, W., & He, Y. (2022). Optimized wayfinding signage positioning in hospital built environment through medical data and flows simulations. *Buildings*. https://doi.org/10.3390/buildings12091426

Guziołowski, R. (2006). Design and implementation of fully configurable interpreter and generator of hl7 standard protocol messages. *Poznan University of Technology technical report no. RA-xxx/06*.

Hak, F., Oliveira, D., Abreu, N., Leuschner, P., Abelha, A., & Santos, M. (2020). An openehr adoption in a portuguese healthcare facility. *Procedia Computer Science*, *170*, 1047–1052.

Hammi, M. T., Hammi, B., Bellot, P., & Serhrouchni, A. (2018). Bubbles of trust: A decentralized blockchain-based authentication system for iot. *Computers & Security*, *78*, 126–142.

Hammond, W. E. (2005). The making and adoption of health data standards. *Health affairs*, *24*(5), 1205–1213.

Harrison, J. E., Weber, S., Jakob, R., & Chute, C. G. (2021). Icd-11: An international classification of diseases for the twenty-first century. *BMC medical informatics and decision making*, *21*, 1–10.

Hasselgren, A., Kralevska, K., Gligoroski, D., Pedersen, S. A., & Faxvaag, A. (2020). Blockchain in healthcare and health sciences—a scoping review. *Int. J. Med. Inform.*, *134*(May 2019), 104040. https://doi.org/10.1016/j.ijmedinf.2019.104040

Haux, R. (2006). Health information systems - past, present, future. *Int. J. Med. Inform.*, *75*(3-4 SPEC. ISS.), 268–281.

Helwig, A. (2013, October). Ehr certification criteria for snomed ct help transition to icd-10. https://www.healthit.gov/buzz-blog/electronic-health-and-medical-records/ehr-certification-criteria-snomed-ct-%5C%5Cdoctors-transition-icd10

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS quarterly*, 75–105.

HIMSS. (2024). *Interoperability in healthcare* [Accessed on '05/07/2024]. https://www.himss.org/resources/interoperability-healthcare

HL7 International. (2024a). Hl7 reference information model (rim) [Accessed: 2024-09-04]. https://www.hl7.org/implement/standards/rim.cfm

HL7 International. (2024b). Hl7 v2.7.1 adt_a04 - patient registration event [Accessed: 2024-09-04]. https://hl7-definition.caristix.com/v2/HL7v2.7.1/TriggerEvents/ADT_A04

HL7International. (2022a). Health level seven international. https://www.hl7.org/about/index.cfm?ref=nav

HL7International. (2022b). Hl7-definition v2. https://hl7-definition.caristix.com/v2/

Hölbl, M., Kompara, M., Kamišalić, A., & Zlatolas, L. N. (2018a). A systematic review of the use of blockchain in healthcare. *Symmetry (Basel).*, *10*(10).

Hölbl, M., Kompara, M., Kamišalić, A., & Zlatolas, L. N. (2018b). A systematic review of the use of blockchain in healthcare. *Symmetry (Basel).*, *10*(10). https://doi.org/10.3390/sym10100470

Huang, D., Ma, X., & Zhang, S. (2020). Performance analysis of the raft consensus algorithm for private blockchains. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *50*(1), 172–181. https://doi.org/10.1109/TSMC.2019.2895471

Hyperledger [Accessed: 2023-10-21]. (2023). https://www.hyperledger.org/About

Hyperledger. (2020). *Hyperledger fabric docs release 2.2* [Last access: 25-06-2023]. https://hyperledger-fabric.readthedocs.io/en/release-2.2/

Hyperledger caliper architecture [Last access: 25-07-2024]. (2024). https://hyperledger.github.io/caliper/vNext/getting-started/

Hyperledger caliper documentation [Accessed: 2023-09-22]. (2023). https://hyperledger.github.io/caliper/

Hyperledger caliper overview [Accessed: 2023-09-22]. (2023). https://www.hyperledger.org/use/caliper

*Hyperledger fabric docs release 2.2*. (2020). https://hyperledger-fabric.readthedocs.io/en/release-2.2/

IBM. (2022). Interoperability in healthcare. https://www.ibm.com/topics/interoperability-in-healthcare

IBM. (2024). *Interoperability in healthcare* [Accessed on 2024-02-05]. https://www.ibm.com/topics/interoperability-in-healthcare

IMPRIVATA. (2019). *Himss proposes a new interoperability definition in healthcare* [Accessed on '05/07/2024]. https://www.imprivata.com/uk/node/99796

Inastrilla, C. R. A. (2022). Big data in health information systems. *MW Salud*. https://doi.org/10.56294/mw20226

Inmon, W. H. (1996). The data warehouse and data mining. *Communications of the ACM*, *39*(11), 49–51.

Inmon, W. H. (1995). What is a data warehouse. *Prism Tech Topic*, *1*(1), 1–5.

Ipfs documentation [Accessed: 2024-08-07]. (2024). https://docs.ipfs.tech

Iroju, O., Soriyan, A., Gambo, I., Olaleke, J., et al. (2013). Interoperability in healthcare: Benefits, challenges and resolutions. *International Journal of Innovation and Applied Studies*, *3*(1), 262–270.

Ismail, L., Materwala, H., & Hennebelle, A. (2021). A scoping review of integrated blockchain-cloud (bcc) architecture for healthcare: Applications, challenges and solutions. *Sensors*, *21*(11), 3753. https://doi.org/10.3390/s21113753

Jabarulla, M. Y., & Lee, H.-n. (2021). A blockchain and artificial intelligence-based, patient-centric healthcare system for combating the covid-19 pandemic: Opportunities and applications. *Healthcare*, *9*(8), 1019. https://doi.org/10.3390/healthcare9081019

Jadon, A., & Kumar, S. (2023). Leveraging generative ai models for synthetic data generation in healthcare: Balancing research and privacy. *2023 International Conference on Smart Applications, Communications and Networking (SmartNets)*, 1–4.

Jaffe, C., Vreeman, D., Kaminker, D., & Nguyen, V. (2023). Implementing hl7 fhir. *Journal of Healthcare Management Systems*. https://doi.org/10.4018/jhms.316144

Jalghoum, Y., Tahtamouni, A., Khasawneh, S., & Al-Madadha, A. (2019). Challenges to healthcare information systems development: The case of jordan. *International Journal of Healthcare Management*. https://doi.org/10.1080/20479700.2019.1658159

Jeon, K. E., She, J., Soonsawad, P., & Ng, P. C. (2018). Ble beacons for internet of things applications: Survey, challenges, and opportunities. *IEEE Internet Things J.*, *5*(2), 811–828.

Johnson, E., & Wang, L. (2020). Challenges and opportunities in decentralized autonomous organizations [https://example.com/dao-challenges]. *Journal of Blockchain Research*, *4*, 45–56.

Kalra, D., Beale, T., & Heard, S. (2005). The openehr foundation. *Stud. Health Technol. Inform.*, *115*, 153–173.

Karim, S., Lucey, B. M., Naeem, M. A., & Uddin, G. S. (2022). Examining the interrelatedness of nfts, defi tokens and cryptocurrencies. *Financ Res Lett*, *47*. https://doi.org/10.1016/j.frl.2022.102696

Keating, P., Murray, J., Schenkel, K., Merson, L., & Seale, A. (2021). Electronic data collection, management and analysis tools used for outbreak response in low- and middle-income countries: A systematic review and stakeholder survey. *BMC Public Health*, *21*, 1–14. https://doi.org/10.1186/s12889-021-11790-w

Khan, W. A., Salah, K., Arshad, J., Yaqoob, I., & Jayaraman, R. (2018). Blockchain technology in the healthcare ecosystem: A systematic review. *IEEE Access*, *6*, 40411–40421.

Khanna, A., & Kaur, S. (2019). Evolution of internet of things (iot) and its significant impact in the field of precision agriculture. *Computers and Electronics in Agriculture*, *157*, 218–231. https://doi.org/10.1016/j.compag.2018.12.039

Khezr, S., Moniruzzaman, M., Yassine, A., & Benlamri, R. (2019). Blockchain technology in healthcare: A comprehensive review and directions for future research. *Appl. Sci.*, *9*(9), 1736.

Kim, H., Kim, H. S., & Park, Y. S. (2022). Perpetual contract nft as collateral for defi composability. *IEEE Access*. https://doi.org/10.1109/access.2022.3225884

Kim, H., Kim, H.-S., & Park, Y.-S. (2022). Perpetual contract nft as collateral for defi composability. *IEEE Access*, *10*, 126802–126814.

Kim, K., & Hong, S. (2017). A trusted sharing model for patient records based on permissioned blockchain. *18*(6), 75–84.

Kulkov, I., Tsvetkova, A., & Ivanova-Gongne, M. (2021). Identifying institutional barriers when implementing new technologies in the healthcare industry. *European Journal of Innovation Management*. https://doi.org/10.1108/ejim-02-2021-0093

Kumar, A., Singh, A. K., Ahmad, I., Singh, P. K., Anushree, Verma, P., Alissa, K. A., Bajaj, M., ur Rehman, A., & Tag-eldin, E. (2022). A novel decentralized blockchain architecture for the preservation of privacy and data security against cyberattacks in healthcare. *Sensors*, *22*(15), 5921. https://doi.org/10.3390/s22155921

Kumar, M., Verma, S., Bhattacharya, P., Ghimire, D., Kim, S.-h., & Hosen, A. (2023). Healthcare internet of things (h-iot): Current trends, future prospects, applications, challenges, and security issues. *Electronics*, *12*(9), 2050. https://doi.org/10.3390/electronics12092050

Kumar, S., Bharti, A. K., & Amin, R. (2021). Decentralized secure storage of medical records using blockchain and ipfs: A comparative analysis with future directions.

Kumar, T., Ramani, V., Ahmad, I., Braeken, A., Harjula, E., & Ylianttila, M. (2018). Blockchain utilisation in healthcare: Key requirements and challenges. *2018 IEEE 20th Int. Conf. e-Health Networking, Appl. Serv. Heal. 2018*, 1–7. https://doi.org/10.1109/HealthCom.2018.8531136

Kuo, T. T., Kim, H. E., & Ohno-Machado, L. (2017a). Blockchain distributed ledger technologies for biomedical and health care applications. *J. Am. Med. Informatics Assoc.*, *24*(6), 1211–1220.

Kuo, T. T., Kim, H. E., & Ohno-Machado, L. (2017b). Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association*, *24*(6), 1211–1220. https://doi.org/10.1093/jamia/ocx068

Kuo, T.-T., Kim, H.-E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. *J. Am. Med. Informatics Assoc.*, *24*(6), 1211–1220.

Lacerda, D. P., Dresch, A., Proença, A., & Júnior, J. A. V. A. (2013). Design science research: A research method to production engineering. *Gest. e Prod.*, *20*(4), 741–761.

Langarizadeh, M., Orooji, A., Sheikhtaheri, A., & Hayn, D. (2018a). Effectiveness of anonymization methods in preserving patients' privacy: A systematic literature review. *eHealth*, *248*, 80–87.

Langarizadeh, M., Orooji, A., Sheikhtaheri, A., & Hayn, D. (2018b). Effectiveness of anonymization methods in preserving patients' privacy: A systematic literature review. *eHealth*, *248*, 80–87.

Laurence, T. (2017). *Blockchain for dummies*. John Wiley & Sons.

Leppänen, T. (2021). Data visualization and monitoring with grafana and prometheus [p. 49].

Levandoski, J. J., Casto, G., Deng, M., Desai, R., Edara, P., Hottelier, T., Hormati, A., Johnson, A., Johnson, J., Kurzyniec, D., McVeety, S., Ramanathan, P., Saxena, G., Shanmugan, V., & Volobuev, Y. (2024). Biglake: Bigquery's evolution toward a multi-cloud lakehouse. *Proceedings of the ACM International Conference on Management of Data*. https://doi.org/10.1145/3626246.3653388

Lin, C.-C., Huang, H.-Y., Chen, W.-C., Tsai, C.-H., Chen, C.-H., Cheng, T.-C., Chen, H.-C., Lee, H.-H., Lai, M.-F., & Chen, T.-H. (2017). Data-driven approaches in healthcare: A systematic review. *Journal of Medical Internet Research*, *19*(9), e269. https://doi.org/10.2196/jmir.7254

Lintern, G., & Motavalli, A. (2018). Healthcare information systems: The cognitive challenge. *BMC Medical Informatics and Decision Making*. https://doi.org/10.1186/s12911-018-0584-z

Lippeveld, T., Sauerborn, R., & Bodart, C. (2000). *Design and implementation of health information systems*.

Liu, J., Fan, Y., Sun, R., Liu, L., Wu, C., & Mumtaz, S. (2023). Blockchain-aided privacy-preserving medical data sharing scheme for e-healthcare system. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2023.3287636

Lourenço, J. M. (2021). *The NOVAthesis LaTeX Template User's Manual*. NOVA University Lisbon. https://github.com/joaomlourenco/novathesis/raw/main/template.pdf

Mani, V., 2, P. M., Alotaibi, Y., Alghamdi, S., & Khalaf, O. I. (2021). Hyperledger healthchain: Patient-centric ipfs-based storage of health records.

Marks, M., Lal, S., Brindle, H., Gsell, P., MacGregor, M. E., Stott, C., van de Rijdt, M., Almazor, G. G., Golia, S., Watson, C., et al. (2021). Electronic data management for vaccine trials in low resource settings: Upgrades, scalability, and impact of odk. *Frontiers in Public Health*, *9*, 665584. https://doi.org/10.3389/fpubh.2021.665584

Maymounkov, P., & Mazières, D. (2002a). Kademlia: A peer-to-peer information system based on the xor metric.

Maymounkov, P., & Mazières, D. (2002b). *Kademlia: A peer-to-peer information system based on the xor metric*.

Mayo. (2022). Loinc®. https://www.mayocliniclabs.com/test-catalog/appendix/LOINC-Codes

McDonald, C. J., Huff, S. M., Suico, J. G., Hill, G., Leavelle, D., Aller, R., Forrey, A., Mercer, K., DeMoor, G., Hook, J., et al. (2003). Loinc, a universal standard for identifying laboratory observations: A 5-year update. *Clinical chemistry*, *49*(4), 624–633.

McFadden, E. (2007). *Management of data in clinical trials*. John Wiley & Sons.

McGhin, T., Choo, K. K. R., Liu, C. Z., & He, D. (2019). Blockchain in healthcare applications: Research challenges and opportunities. *J. Netw. Comput. Appl.*, *135*(January), 62–75.

McHorney, C. A., & Tarlov, A. R. (1995). Individual-patient monitoring in clinical practice: Are available health status surveys adequate? *Quality of life research*, *4*(4), 293–307.

MedicalChain. (2018). *Whitepaper 2.1*.

Meshkov, D., Bezmelnitsyna, L., & Cherkasov, S. (2020). A data management model for proactive risk management in healthcare. *Automation and Remote Control*. https://doi.org/10.25728/ASSA.2020.20.1.864

Mettler, M. (2016). Blockchain technology in healthcare: The revolution starts here. *2016 IEEE 18th international conference on e-health networking, applications and services (Healthcom)*, 1–3.

Mettler, T. (2016a). Blockchain technology in healthcare: The revolution starts here. *IEEE Pulse*, *7*(3), 22–26. https://doi.org/10.1109/MPUL.2016.2520537

Mettler, T. (2016b). Blockchain technology in healthcare: The revolution starts here. *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)*, 1–3.

MichaelMure. (2018). Arbore [Last access: 21-04-2023]. https://github.com/MichaelMure/Arbore

Miers, C., Koslovski, G., Pillon, M., & Marques, M. (2020). Blockchains com hyperledger: Conceitos, instalação, configuração e uso. *Minicursos da XVIII Esc. Reg. Redes Comput.*, 16–41.

Miloslavskaya, N., & Tolstoy, A. (2016). Big data, fast data and data lake concepts. *Procedia Computer Science*, *88*, 300–305.

Min, L., Tian, Q., Lu, X., & Duan, H. (2018). Modeling ehr with the openehr approach: An exploratory study in china. *BMC medical informatics and decision making*, *18*, 1–15.

Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei, W., & Qijun, C. (2017). A review on consensus algorithm of blockchain. *2017 IEEE international conference on systems, man, and cybernetics (SMC)*, 2567–2572.

Misra, S., Pal, S., Ahmed, N., & Mukherjee, A. (2023). Sdn-controlled resource-tailored analytics for healthcare iot system. *IEEE Systems Journal*. https://doi.org/10.1109/JSYST.2023.3245816

Mohammed, B. G., & Hasan, D. (2023). Smart healthcare monitoring system using iot. *International Journal of Interactive Mobile Technologies*, *17*(1), 34675. https://doi.org/10.3991/ijim.v17i01.34675

Mohan, C. (2017). Blockchains and databases. *Proceedings of the 2017 ACM International Conference on Management of Data*, 1733–1734. https://doi.org/10.14778/3137765.3137830

Mohanta, B. K., Jena, D., Panda, S. S., & Sobhanayak, S. (2019). Blockchain technology: A survey on applications and security privacy challenges. *Internet of Things (Netherlands)*, *8*.

Muralidharan, S., & Ko, H. (2019). An interplanetary file system (ipfs) based iot framework. *IEEE International Conference on Consumer Electronics (ICCE)*. https://doi.org/10.1109/ICCE.2019.8662002

Musamih, A., Salah, K., Jayaraman, R., Yaqoob, I., Puthal, D., & Ellahham, S. (2022). Nfts in healthcare: Vision, opportunities, and challenges. *IEEE Consumer Electronics Magazine*. https://doi.org/10.1109/MCE.2022.3196480

Musen, M. A., Middleton, B., & Greenes, R. A. (2014). Clinical decision-support systems. In *Biomedical informatics* (pp. 643–674). Springer.

Mw, I., Sj, L., & West, M. (2001). A data mart for operations analysis. *Journal of Healthcare Information Management*. https://pubmed.ncbi.nlm.nih.gov/11452576

Nabila, M., Alzami, F., Megantara, R. A., Tananto, F. F., Syafrudin, H. A., Handoko, L., & Umam, C. (2023). Implementation of a supply chain management system blockchain-based in red onion farming. *JIM*. https://doi.org/10.24843/jim.2023.v11.i01.p02

Nadarajah, T. (2020). Exploring the adoption of ipfs for nfts: Benefits and challenges. *Blockchain Research*.

Nærland, K., Beck, R., Müller-Bloch, C., & Palmund, S. (2018). Blockchain to rule the waves - nascent design principles for reducing risk and uncertainty in decentralized environments. *ICIS 2017 Transform. Soc. with Digit. Innov.*, 1–16.

Nakamoto, S. (2008a). Bitcoin: A peer-to-peer electronic cash system.

Nakamoto, S. (2008b). *Bitcoin: A peer-to-peer electronic cash system*.

Neudecker, T., & Hartenstein, H. (2019). Network layer aspects of permissionless blockchains. *IEEE Communications Surveys & Tutorials*, *21*(1), 838–857. https://doi.org/10.1109/COMST.2018.2852480

Ngafeeson, M. N. (2015). Healthcare information systems opportunities and challenges. *Encyclopedia of Information Science and Technology, Third Edition*, 3387–3395.

Nguyen, G., & Kim, K. (2018). A survey about consensus algorithms used in blockchain. *Journal of Information Processing Systems*, *14*(1), 101–128. http://myweb.jnu.ac.kr/~kbkim/papers/%5B2018%20JIPS%5DA%20Survey%20about%20Consensus%20Algorithms%20Used%20in%20Blockchain.pdf

Nguyen, Ha, Do, & Linh. (2018). The adoption of blockchain in food retail supply chain : Case : Ibm food trust blockchain and the food retail supply chain in malta.

Niit technologies introduces chain-m, a blockchain powered solution for airlines and its partners [Last access: 21-04-2023]. (2018). https://www.prnewswire.com/in/news-releases/niit-technologies-introduces-chain-m-a-blockchain-powered-solution-for-airlines-and-its-partners-693610061.html

Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business & information systems engineering*, *59*, 183–187.

Odeh, A., Keshta, I., & Al-Haija, Q. A. (2022). Analysis of blockchain in the healthcare sector: Application and issues. *Symmetry*, *14*(9), 1760. https://doi.org/10.3390/sym14091760

Olawoyin, A. M., Leung, C., & Cuzzocrea, A. (2021). Open data lake to support machine learning on arctic big data. *2021 IEEE International Conference on Big Data (Big Data)*. https://doi.org/10.1109/BigData52589.2021.9671453

Oliveira, C., Sousa, R., Peixoto, H., & Machado, J. (2022). Improving the effectiveness of heart disease diagnosis with machine learning. *International Conference on Practical Applications of Agents and Multi-Agent Systems*, 222–231.

Oliveira, D., Duarte, J., Abelha, A., & Machado, J. (2017). Improving nursing practice through interoperability and intelligence. *Proc. - 2017 5th Int. Conf. Futur. Internet Things Cloud Work. W-FiCloud 2017*, *2017-January*, 194–199.

Oliveira, D., Duarte, J., Abelha, A., & Machado, J. (2018). Step towards interoperability in nursing practice. *Int. J. Public Heal. Manag. Ethics*, *3*(1), 26–37.

Oliveira, D., Ferreira, D., Abreu, N., Leuschner, P., Abelha, A., & Machado, J. (2021). Prediction of covid-19 diagnosis based on openehr artefacts.

Oliveira, D., Miranda, R., Leuschner, P., Abreu, N., Santos, M. F., Abelha, A., & Machado, J. (2021). Openehr modeling: Improving clinical records during the covid-19 pandemic. *Health and Technology*, *11*(5), 1109–1118.

Oliveira, M., Janela, F., Martins, H., & Ferrão, J. (2016). Preprocessing structured clinical data for predictive modeling and decision support. *Applied Clinical Informatics*. https://doi.org/10.4338/ACI-2016-03-SOA-0035

Onik, M. M. H., Aich, S., Yang, J., Kim, C.-S., & Kim, H.-C. (2019). *Blockchain in healthcare: Challenges and solutions*. Elsevier Inc. https://doi.org/10.1016/b978-0-12-818146-1.00008-8

openEHR. (n.d.). *What is openehr?* https://www.openehr.org/about/what%5C_is%5C_openehr

Ozercan, H. I., Ileri, A. M., Ayday, E., & Alkan, C. (2018). Realizing the potential of blockchain technologies in genomics. *Genome Research*, *28*(9), 1255–1263. https://doi.org/10.1101/gr.207464.116

Pal, P. K., Khanna, S., Shukla, S., & Shukla, V. (2023). Securing and visualizing sensor data on private blockchain. *InCACCT*. https://doi.org/10.1109/InCACCT57535.2023.10141766

Panwar, A., & Bhatnagar, V. (2020). Scrutinize the idea of hadoop-based data lake for big data storage. In *Lecture notes in networks and systems*. https://doi.org/10.1007/978-981-15-3357-0_24

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *J. Manag. Inf. Syst.*, *24*(3), 45–77.

Peixoto, H., Guimarães, T., & Santos, M. F. (2020). A new architecture for intelligent clinical decision support for intensive medicine. *Procedia Computer Science*, *170*, 1035–1040.

Peixoto, H., Santos, M., Abelha, A., & Machado, J. (2012). Intelligence in interoperability with aida. *International Symposium on Methodologies for Intelligent Systems*, 264–273.

Pereira, R., Duarte, J., Salazar, M., Santos, M., Abelha, A., & Machado, J. (2012). Usability of an electronic health record. *IEEE Int. Conf. Ind. Eng. Eng. Manag.*, 1568–1572.

Prathyusha, T., Kavya, M., & Akshita, P. S. L. (2018). Block chain technology.

Prokofieva, M., & Miah, S. J. (2019). Blockchain in healthcare. *Australas. J. Inf. Syst.*, *23*, 1–22. https://doi.org/10.3127/ajis.v23i0.2203

Prometheus. (2024). Overview | prometheus [Last access: 25-07-2024]. https://prometheus.io/docs/introduction/overview/

Prometheus architecture [Accessed: 2024-03-06]. (2024). https://prometheus.io/docs/introduction/overview/#architecture

Prometheus documentation [Accessed: 2024-03-06]. (2024). https://prometheus.io/docs/introduction/overview/

Prometheus exporters [Accessed: 2023-09-22]. (2023). https://prometheus.io/docs/instrumenting/exporters/

Prometheus integration with hyperledger caliper [Accessed: 2024-04-15]. (2024). https://hyperledger.github.io/caliper/vNext/caliper-monitors/#prometheus-monitor

Prometheus query language (promql) documentation [Accessed: 2024-03-06]. (2024). https://prometheus.io/docs/prometheus/latest/querying/basics/

Prometheus use cases [Accessed: 2023-09-22]. (2023). https://prometheus.io/docs/introduction/overview/#use-cases

Psaras, Y., & Dias, D. (2020). The interplanetary file system and the filecoin network. *IEEE/IFIP International Conference on Dependable Systems and Networks-Supplemental Volume (DSN-S)*. https://doi.org/10.1109/DSN-S50200.2020.00043

Qasse, I. A., Talib, M. A., & Nassif, A. B. (2018). Performance analysis of hyperledger fabric platforms.

Raghupathi, W., & Raghupathi, V. (2014). Big data analytics in healthcare: Promise and potential. *Health Information Science and Systems*, *2*(1), 3.

Rahim, M., Rahman, M. A., Rahman, M. M., Asyhari, A., Bhuiyan, M. Z. A., & Ramasamy, D. (2020). Evolution of iot-enabled connectivity and applications in automotive industry: A review. *Vehicular Communications*, *23*, 100285. https://doi.org/10.1016/j.vehcom.2020.100285

Ramnath, S., Javali, A., Narang, B., Mishra, P., & Routray, S. K. (2017). Iot based localization and tracking. *IEEE Int. Conf. IoT its Appl. ICIOT 2017*.

Ranaldo, A. (2022). *Non-fungible tokens*. https://ssrn.com/abstract=4274986

Ranjan, N., et al. (2023). Optimizing cloud computing applications with a data center load balancing algorithm. *International Journal on Recent and Innovation Trends in Computing and Communication*, *11*(10), 320–331. https://doi.org/10.17762/ijritcc.v11i10.8495

Rastogi, A., & Srivastava, S. (2020). Blockchain: Its importance in healthcare, education, agriculture. *SSRN*. https://doi.org/10.2139/ssrn.3645880

Ray, P. P. (2023). Web3: A comprehensive review on background, technologies, applications, zero-trust architectures, challenges and future directions. *Internet of Things and Cyber-Physical Systems*, *3*, 213–248.

Rehman, W., e Zainab, H., Imran, J., & Bawany, N. Z. (2021). Nfts: Applications and challenges.

Rejeb, A., Rejeb, K., Treiblmaier, H., Appolloni, A., Alghamdi, S., Alhasawi, Y., & Iranmanesh, M. (2023). The internet of things (iot) in healthcare: Taking stock and moving forward. *Internet of Things*, *25*, 100721. https://doi.org/10.1016/j.iot.2023.100721

Research, L. (2013). *An introduction to the internet of things (iot)*.

Ribeiro, T., Oliveira, S., Portela, C., & Santos, M. (2019). Clinical workflows based on openehr using bpm. *ICT4AWE 2019 - Proc. 5th Int. Conf. Inf. Commun. Technol. Ageing Well e-Health*, 352–358. https://doi.org/10.5220/0007878203520358

Richesson, R. L., & Krischer, J. (2007). Data standards in clinical research: Gaps, overlaps, challenges and future directions. *Journal of the American Medical Informatics Association*, *14*(6), 687–696.

Robinson, Y. H., Krishnan, R., & Raja, S. (2021). A comprehensive study for security mechanisms in healthcare information systems using internet of things. *Lecture Notes in Computer Science*. https://doi.org/10.1007/978-3-030-39119-5_15

Ryan, A. (2006). Towards semantic interoperability in healthcare: Ontology mapping from snomed-ct to hl 7 version 3. *ACM International Conference Proceeding Series*, *238*, 69–74.

Sadowski, J., & Beegle, K. (2023). Expansive and extractive networks of web3. *Big Data and Society*, *10*(1), 20539517231159629.

Saha, S., Sutrala, A. K., Das, A., Kumar, N., & Rodrigues, J. (2020). On the design of blockchain-based access control protocol for iot-enabled healthcare applications. *2020 IEEE International Conference on Communications (ICC)*, 1–6. https://doi.org/10.1109/ICC40277.2020.9148915

Sairam, G. V., Kumar, S., Gupta, S., & Haider, S. S. (2023). Healthcare management system using blockchain. *International Journal of Recent Advances in Engineering and Technology*. https://doi.org/10.22214/ijraset.2023.51153

Sakib, N., Jamil, S., & Mukta, S. H. (2022). A novel approach on machine learning based data warehousing for intelligent healthcare services. *2022 IEEE Region 10 Symposium (TENSYMP)*. https://doi.org/10.1109/TENSYMP54529.2022.9864564

Saleh, F. (2018). Blockchain without waste: Proof-of-stake.

Saleh, F. S., Aliakbarian, M. S., Salzmann, M., Petersson, L., & Alvarez, J. M. (2018). Effective use of synthetic data for urban scene semantic segmentation. *Proceedings of the European Conference on Computer Vision (ECCV)*, 84–100.

Salesforce. (2022). Customer expectations [Accessed on [November 2022]]. https://www.salesforce.com/resources/articles/customer-expectations/?sfdc-redirect=369

Sankar, L. S., Sindhu, M., & Sethumadhavan, M. (2017). Survey of consensus protocols on blockchain applications. *Advanced Computing and Communication Systems (ICACCS), 2017 4th International Conference on*, 1–5.

Santosh Kumar, S. S. I. (2024). Advanced framework for multi-modal healthcare data integration: Leveraging hpc with gpu computing and cnn architecture in cdss. *Journal of Healthcare Information Management*. https://doi.org/10.52783/jes.874

Sarkar, A., Maitra, T., & Neogy, S. (2023). Blockchain in healthcare system: Security issues, attacks and challenges. In *Handbook of blockchain for healthcare*. https://doi.org/10.1007/978-3-030-69395-4_7

Schueffel, P. (2021). Defi: Decentralized finance-an introduction and overview. *Journal of Innovation Management*, *9*(3), I–XI.

Schulz, S., Stegwee, R., & Chronaki, C. (2019). Standards in healthcare data. *Fundamentals of Clinical Data Science*, 19–36.

Seker, E., Talburt, J., & Greer, M. (2022). Preprocessing to address bias in healthcare data. *2022 Studies in Health Technology and Informatics*. https://doi.org/10.3233/SHTI220468

Selvanayagi, A., Ramya, K., Shivani, S., & Suwathika, K. (2024). A comprehensive analysis on blockchain based healthcare data security. *2024 5th International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*, 700–703.

Seymour, T., Frantsvog, D., & Graeber, T. (2012). Electronic health records (ehr). *American Journal of Health Sciences*, *3*(3), 201.

Shahnaz, A., Qamar, U., & Khalid, A. (2019). Using blockchain for electronic health records. *IEEE Access*, *7*, 147782–147795. https://doi.org/10.1109/ACCESS.2019.2946373

Shalaby, S., Abdellatif, A. A., Al-Ali, A., Mohamed, A., Erbad, A., & Guizani, M. (2020). Performance evaluation of hyperledger fabric. *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*, 608–613. https://doi.org/10.1109/ICIoT48696.2020.9089614

Sharma, P., Namasudra, S., Crespo, R. G., Fuente, J. P., & Trivedi, M. (2023). Ehdhe: Enhancing security of healthcare documents in iot-enabled digital healthcare ecosystems using blockchain. *Information Sciences*, *623*, 202–217. https://doi.org/10.1016/j.ins.2023.01.148

Sheth, H., & Dattani, J. (2019). Overview of blockchain technology. *Asian J. Converg. Technol.*, *05*(01), 1–4.

Shivom - crunchbase company profile & funding [Accessed: Jan. 25, 2024]. (2024). https://www.crunchbase.com/organization/project-shivom

Shull & Germaine, J. (2019). Digital health and the state of interoperable electronic health records. *JMIR medical informatics*, *7*(4), e12712.

Shull, J. G. (2019). Digital health and the state of interoperable electronic health records. *JMIR medical informatics*, *7*(4), e12712.

Silan, M., Signorin, G., Ferracin, E., Listorti, E., Spadea, T., Costa, G., & Boccuzzo, G. (2020). Construction of a frailty indicator with partially ordered sets: A multiple-outcome proposal based on administrative healthcare data. *Social Indicators Research*. https://doi.org/10.1007/s11205-020-02512-7

Simborg & W, D. (1988). The case for the hl7 standard. *Computers in Healthcare*, *9*(1), 39–40.

Sinaci, A., Gencturk, M., Teoman, H. A., Erturkmen, G. B. L., Álvarez-Romero, C., Martínez-García, A., Poblador-Plou, B., Carmona-Pírez, J., Löbe, M., & Parra-Calderón, C. (2023). A data transformation methodology to create findable, accessible, interoperable, and reusable health data: Software design, development, and evaluation study. *Journal of Medical Internet Research*. https://doi.org/10.2196/42822

Singh, S., Puradkar, S., & Lee, Y. (2006). Ubiquitous computing: Connecting pervasive computing through semantic web. *Inf. Syst. E-bus. Manag.*, *4*(4), 421–439.

Singh, Y., Jabbar, M. A., Shandilya, S. K., Vovk, O., & Hnatiuk, Y. (2023). Exploring applications of blockchain in healthcare: Road map and future directions. *Frontiers in Public Health*, *11*, 1229386. https://doi.org/10.3389/fpubh.2023.1229386

Singhal, B., Dhameja, G., & Panda, P. S. (2018). *Beginning blockchain*.

Skinner, P. E. M. B. F. (2007). História do conceito de saúde. *17*(1), 29–41.

Sloane Brakeville, B. P. (2018). Blockchain basics: Glossary and use cases [Last access: 25-06-2023]. https://developer.ibm.com/tutorials/cl-blockchain-basics-glossary-bluemix-trs

Smith, J., & Doe, J. (2021). Modern daos: Decentralized governance for the digital age [https://example.com/modern-dao]. *Blockchain Innovations*, *5*, 123–130.

Snapshot [Last access: 21-04-2023]. (2023). https://snapshot.org/

Soceanu, A., Egner, A., & Moldoveanu, F. (2013). Towards interoperability of ehealth system networked components. *2013 19th International Conference on Control Systems and Computer Science*, 147–154.

Soltanisehat, L., Alizadeh, R., Hao, H., & Choo, K.-K. R. (2020). Technical, temporal, and spatial research challenges and opportunities in blockchain-based healthcare: A systematic literature review. *IEEE Trans. Eng. Manag.*

Soni, M., & Singh, D. (2021). Blockchain-based security & privacy for biomedical and healthcare information exchange systems. *Materials Today: Proceedings*. https://doi.org/10.1016/J.MATPR.2021.02.094

Sousa, J., Bessani, A., & Vukolic, M. (2018). A byzantine fault-tolerant ordering service for the hyperledger fabric blockchain platform. *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 51–58. https://doi.org/10.1109/DSN.2018.00018

Sousa, M. L. (2017). *Openehr como solução para o regulamento geral de proteção de dados na área da saúde* [Master's thesis].

Sousa, R., Lima, T., Abelha, A., & Machado, J. (2021). Hierarchical temporal memory theory approach to stock market time series forecasting. *Electronics*, *10*(14), 1630.

Sousa, R., Miranda, R., Moreira, A., Alves, C., Lori, N., & Machado, J. (2021). Software tools for conducting real-time information processing and visualization in industry: An up-to-date review. *Applied Sciences*, *11*(11), 4800.

Stackpole, T. (2022). What is web3. *Harvard Business Review*, *10*.

Starling [Last access: 21-04-2023]. (2023). https://hedera.com/users/starling

Steichen, M., Fiz, B., Norvill, R., Shbair, W., & State, R. (2018). Blockchain-based, decentralized access control for ipfs. *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 1499–1506. https://doi.org/10.1109/Cybermatics_2018.2018.00253

Strome, T. L., & Liefer, A. (2013). *Healthcare analytics for quality and performance improvement*. Wiley Hoboken.

Sun, J., & Reddy, C. K. (2013). Big data analytics for healthcare. *Proceedings of the 19th ACM SIGKDD international conference on Knowledge discovery and data mining*, 1525.

Supriadi, M. R., & Andarsyah, R. (2023). Integritas data private blockchain hyperledger fabric menggunakan metode practical byzantine fault tolerance dan proof of authority. *Semantik*. https://doi.org/10.55679/semantik.v9i2.42584

Swan, M. (2015). *Blockchain: Blueprint for a new economy*. O'Reilly Media, Inc.

Sykes, E. R. (2020). A context-aware system using mobile applications and beacons for on-premise security environments. *J. Ambient Intell. Humaniz. Comput.*, *11*(11), 5487–5511.

Tandon, A., Dhir, A., Islam, N., & Mäntymäki, M. (2020). Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda. *Comput Ind*, *122*. https://doi.org/10.1016/j.compind.2020.103290

Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world*. Penguin.

Tapscott, D., & Tapscott, A. (2018). Blockchain revolution: How the technology behind bitcoin and other cryptocurrencies is changing the world, 432.

The Linux Foundation. (2024). Hyperledger caliper – hyperledger [Last access: 25-07-2024]. https://www.hyperledger.org/use/caliper

The Linux Foundation. (2020a). Hyperledger explorer [Last access: 25-06-2023]. https://www.hyperledger.org/use/explorer

The Linux Foundation. (2020b). Hyperledger fabric - hyperledger [Last access: 25-06-2023]. https://www.hyperledger.org/use/fabric

Tikhomirov, S. (2018). Ethereum: State of knowledge and research perspectives.

Topol, E. (2019). High-performance medicine: The convergence of human and artificial intelligence. *Nature Medicine*, *25*(1), 44–56. https://doi.org/10.1038/s41591-018-0268-4

Torab-Miandoab, A., Samad-Soltani, T., Jodati, A., & Rezaei-Hachesu, P. (2023). Interoperability of heterogeneous health information systems: A systematic literature review. *BMC Medical Informatics and Decision Making*, *23*(1), 18.

Underwood, S. (2016a). Blockchain beyond bitcoin. *Communications of the ACM*, *59*(11), 15–17. https://doi.org/10.1145/2994581

Underwood, S. (2016b). Blockchain beyond bitcoin. *Communications of the ACM*, *59*(11), 15–17.

Uzwyshyn & Raymond. (2016). Research data repositories: The what, when, why and how. *Computers in Libraries*, *36*(3), 8–21.

Vardasca, T. R., & Martins, H. (2011). Patient relationship management in public healthcare settings. *2011 IEEE International Conference on Communications (ICC)*, 1–4.

Verdonck, M., & Poels, G. (2020). Decentralized data access with ipfs and smart contract permission management for electronic health records.

Vezyridis, P., & Timmons, S. (2017). Understanding the care.data conundrum: New information flows for economic growth. *Big Data and Society*. https://doi.org/10.1177/2053951716688490

Vijayvargiya, P., Garrigos, Z. E., Almeida, N. E. C., Gurram, P. R., Stevens, R. W., & Razonable, R. R. (2020). Treatment considerations for covid-19: A critical review of the evidence (or lack thereof). *Mayo Clinic Proceedings*, *95*, 1454–1466.

Vinola, C., Premi, G., Solainayagi, P., Srinivasan, C., & Kuppusamy, P. G. (2023). Data privacy and confidentiality in healthcare applications of iot-enabled wireless sensor networks. *SmartTechCon 2023*, 1–6. https://doi.org/10.1109/SmartTechCon57526.2023.10391743

Vo, H. T., Kundu, A., & Mohania, M. (2018). Research directions in blockchain data management and analytics. *Adv. Database Technol. - EDBT*, *2018-March*, 445–448.

Vorisek, C. N., Lehne, M., Klopfenstein, S. A. I., Mayer, P. J., Bartschke, A., Haese, T., & Thun, S. (2022). Fast healthcare interoperability resources (fhir) for interoperability in health research: Systematic review. *JMIR medical informatics*, *10*(7), e35724.

Vuković, J., Ivanković, D., Habl, C., & Dimnjaković, J. (2022). Enablers and barriers to the secondary use of health data in europe: General data protection regulation perspective. *Archives of Public Health*, *80*, 1–10. https://doi.org/10.1186/s13690-022-00866-7

Wadmann, S., Hartlev, M., & Hoeyer, K. (2022). The life and death of confidentiality: A historical analysis of the flows of patient information. *BioSocieties*. https://doi.org/10.1057/s41292-021-00269-x

Wadud, M. A. H., Bhuiyan, T. M. A.-U.-H., Uddin, M., & Rahman, M. M. (2020). A patient centric agent assisted private blockchain on hyperledger fabric for managing remote patient monitoring. *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 1–7. https://doi.org/10.1109/ICECE51571.2020.9393124

Wan, S., Lin, H., Gan, W., Chen, J., & Yu, P. S. (2023). Web3: The next internet revolution. *arXiv preprint arXiv:2304.06111*.

Wang, H., et al. (2018). Blockchain, iot and ipfs based electronic health record sharing and storage. *arXiv preprint arXiv:1802.10203*.

Wang, J., Lim, M., Wang, C., & Tseng, M. (2021). The evolution of the internet of things (iot) over the past 20 years. *Computers & Industrial Engineering*, *158*, 107174. https://doi.org/10.1016/J.CIE.2021.107174

Wang, Q., Li, R., Wang, Q., & Chen, S. (2021). *Non-fungible token (nft): Overview, evaluation, opportunities and challenges*. http://arxiv.org/abs/2105.07447

Wang, Q., Li, R., Wang, Q., Chen, S., Ryan, M., & Hardjono, T. (2022). Exploring web3 from the view of blockchain. *arXiv preprint arXiv:2206.08821*.

Wazid, M., Bera, B., Mitra, A., Das, A., & Ali, R. (2020). Private blockchain-envisioned security framework for ai-enabled iot-based drone-aided healthcare services. *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 287–288. https://doi.org/10.1145/3414045.3415941

WHO. (1992). International classification of diseases. *WHO [Internet]*.

WHO. (2022). International classification of diseases (icd). https://www.who.int/classifications/classification-of-diseases

Wilkinson, D, M., Dumontier, Michel, Aalbersberg, Jan, I., Appleton, Gabrielle, Axton, Myles, Baak, Arie, Blomberg, Niklas, Boiten, Jan-Willem, da Silva Santos, Bonino, L., Bourne, E, P., et al. (2016). The fair guiding principles for scientific data management and stewardship. *Scientific data*, *3*(1), 1–9.

Wilkinson, M. D., Sansone, S.-A., Schultes, E., Doorn, P., Bonino da Silva Santos, L. O., & Dumontier, M. (2018). A design framework and exemplar metrics for fairness. *Scientific data*, *5*(1), 1–4.

World Health Organization. (2019). Icd-10: International statistical classification of diseases and related health problems, 10th revision, volume 2 [Accessed: 2024-09-04]. https://icd.who.int/browse10/Content/statichtml/ICD10Volume2_en_2019.pdf

Wulff, A., Haarbrandt, B., Tute, E., Marschollek, M., Beerbaum, P., & Jack, T. (2018). An interoperable clinical decision-support system for early detection of sirs in pediatric intensive care using openehr. *Artif. Intell. Med.*, *89*, 10–23.

Xu, H., Sun, Y., Li, Z., Sun, Y., Zhang, L., & Zhang, X. (2023). Decontroller: A web3 native cyberspace infrastructure perspective. *IEEE communications magazine*, *61*(8), 68–74.

Xu, L., et al. (2019). *Blockchain and supply chain management*. Springer.

Xu, X., Weber, I., & Staples, M. (2019). *Architecture for blockchain applications*. Springer.

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain technology overview. *arXiv preprint arXiv:1906.11078*.

Yan, T., & Kelly, K. (2022). *The year ahead for nfts*.

Yousaf, I., & Yarovaya, L. (2022). Static and dynamic connectedness between nfts, defi and other assets: Portfolio implication. *Global Finance Journal*, *53*. https://doi.org/10.1016/j.gfj.2022.100719

Yue, X., Wang, H., Jin, J., Li, M., & Jiang, W. (2016). Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. *Journal of Medical Systems*, *40*(10), 218.

Zhai, M. (2022). Research on the development of computer simulation technology in the context of blockchain. *2022 IEEE International Conference on Power, Energy, Control and Applications (ICPECA)*, 1–6. https://doi.org/10.1109/ICPECA53709.2022.9718980

Zhang, G., Yang, Z., & Liu, W. (2022). Blockchain-based privacy preserving e-health system for healthcare data in cloud. *Computer Networks*, *203*. https://doi.org/10.1016/j.comnet.2021.108586

Zhang, P., Schmidt, D. C., White, J., & Lenz, G. (2018). Blockchain technology use cases in healthcare. In *Advances in computers* (pp. 1–41, Vol. 111). Elsevier.

Zhang, W., Qamar, F., Abdali, T.-A. N., Hassan, R., Jafri, S. T. A., & Nguyen, Q. N. (2023). Blockchain technology: Security issues, healthcare applications, challenges and future trends. *Electronics*, *12*(3), 546. https://doi.org/10.3390/electronics12030546

Zhao, H., Zhang, L., Qiu, S., Wang, Z., Yang, N., & Xu, J. (2019). Pedestrian dead reckoning using pocket-worn smartphone. *IEEE Access*, *7*, 91063–91073.

Zheng, Q., Li, Y., Chen, P., & Dong, X. (2018). An innovative ipfs-based storage model for blockchain.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. *Proc. - 2017 IEEE 6th Int. Congr. Big Data, BigData Congr. 2017*, 557–564.

Zimmermann, H. (1980). Osi reference model-the iso model of architecture for open systems interconnection. *IEEE Transactions on communications*, *28*(4), 425–432.

Zimmermann, R. (2021). *Decentralized finance (defi) high potential with new rules of the game*. https://morethandigital.info/en/decentralized-finance-defi-high-potential-with-new-rules-of-the-game/

Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing privacy: Using blockchain to protect personal data. *2015 IEEE Security and Privacy Workshops*, 180–184.