A NOVEL BLOCKCHAIN-BASED INCENTIVE MECHANISM TO MITIGATE INEQUALITIES FOR PRESCRIPTION MANAGEMENT SYSTEM

A THESIS SUBMITTED TO AUCKLAND UNIVERSITY OF TECHNOLOGY
IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

Supervisors
Dr Alan T. Litchfield
Dr Brian Cusack

August, 2023

By
Arshad Khan
School of Engineering, Computer and Mathematical Sciences

Abstract

The research proposes a BlockPres framework and an incentive mechanism based on blockchain technology. The aim is to encourage participation and the use of healthcare services. The integration of advanced technologies has led to the development of a smart healthcare system, which is increasingly recognized as essential in meeting the needs of today's society. The literature review identified challenges in the Prescription Management System (PMS), an essential aspect of the healthcare system. It also found that trust, affordability, and accessibility contribute to unequal access to services. Therefore, such disparities create disadvantages in different communities when accessing healthcare services.

The BlockPres framework is created and introduced in this study as a solution to the issues in the prescription management system in New Zealand. It utilizes a novel incentive mechanism that rewards patients for actively participating and engaging with healthcare services. Tokens can be earned by patients whenever they participate and engage with the PMS, and spent on other healthcare services or for purchasing products. Tokens can also be transferred to others to assist them in obtaining additional healthcare services.

The blockchain technology incorporated into BlockPres provides immutability, decentralization, accountability, and security features, for increasing equal access and participation by easy to use authorization and authentication for healthcare providers and patients. Moreover, BlockPres empowers the under-served by providing them control and access to their records.

The researcher formulated questions and hypotheses around the problem, and the proposed solution. The study adopted and adapted Design Science Research Methodology (DSRM) to be the guiding framework for the research. DSRM consists of three primary phases: problem identification, solution design, and evaluation. In the problem identification phase, the study identified the issue and formulated research questions that led to the development of the BlockPres Artefact in the solution design phase. The evaluation phase of DSRM has validation to verify the proposed artefact and incentive mechanism.

To answer the research questions and validate the proposed solution, an evaluation of the BlockPres artefact was completed. The evaluation involved two stages. First, a simulation was performed using the Ethereum blockchain. It tested the successful completion of transactions and the performance rates, and confirmed the efficiency and effectiveness of blockchain for a prescription management system. Secondly, based on the simulation results, a BlockPres prototype was developed to evaluate the solution and incentive mechanism. The results showed that the artefact improved motivation and community engagement, trust, and perceptions of PMS and health services. However, it is recommended that industry experts test the artefact in future work to validate its effectiveness in a live environment.

Contents

List of Tables

List of Figures

Attestation of Authorship

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which to a substantial extent has been accepted for the qualification of any other degree or diploma of a university or other institution of higher learning.

Signature of candidate

Publications

1. Alan Litchfield, Arshad Khan. (2021). BlockPres: *A Novel Blockchain-Based Incentive Mechanism to Mitigate Inequalities for Prescription Management System*. Sensors, 21(15), 5035.
2. Alan Litchfield, Arshad Khan. (2019). *A Review of Issues in Healthcare Information Management Systems and Blockchain Solutions*. In International Conference on Information Resources Management (Vol. 1). Association for Information Systems (AIS).
3. Yanwei Zhou, Bo Yang,Yong Yu & Arshad Khan (2019). *Efficient Chosen-Ciphertext Secure Hybrid Encryption Scheme Tolerating Continuous Leakage Attacks*. Journal of the Chinese Institute of Engineers, 42(1), 39-47.
4. Xiuze Dong, Yunchuan Guo, Fenghua Li, Liju Dong, Arshad Khan (2019). *Combination Model of Heterogeneous Data for Security Measurement*.
5. Arshad Khan, Brian Cusack, Alan Litchfield. *A Systematic Literature Review of Prescription Management System Using Blockchain Technology* (Submission Pending).
6. Arshad Khan, Brian Cusack, Alan Litchfield. *A Concrete Construction of BlockPres Incentive Mechansim to Mitigate Inequality in Prescription Management System* (In-Progress).

Acknowledgements

First and foremost, I am expressing my gratitude to Allah, whose blessings showered upon me and provided me with the strength, patience, knowledge, and opportunity to complete my Ph.D. successfully. I am humbled to have my parent's prayers which helped me to complete this milestone.

I am deeply grateful to my current Primary supervisor, Dr. Brian, for his unwavering support, patience, and expertise in this thesis. His guidance and on-time feedback have been significant in shaping the outcome of this thesis. I want to thank my secondary supervisor Dr. Alan Litchfield for his guidance and support during the early stages of my Ph.D. research. I started my Ph.D. journey with him back in 2018, and He was an instrumental pillar in helping me shape the Ph.D. research idea from the beginning until the end. We both faced many ups and downs, and it was not less than a roller coaster ride, yet he stood firm with the research. His input and advice throughout my journey helped me push forward. I am will appreciate this for the rest of my life.

Another thank you to the sponsor company. Without the generous support of Orion Health, this research would not have been possible. They collaborated with the Auckland University of Technology and funded my Ph.D. studies for three years. I would also like to thank the Faculty and Design and Creative Technologies administration for their unwavering support throughout my student journey.

Finally, I would like to express my heartfelt appreciation to the love of my life, my partner, Komal, for her unwavering support, understanding, and encouragement throughout this journey. She understood the importance of my studies and dedication. She handled all my mood swings and supported me well while things were static. Her love, patience, guidance, and support have been the core of my success.

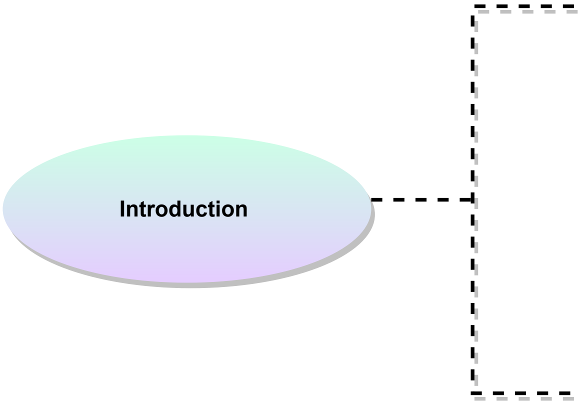
Intellectual Property Rights

This work is supported by Precision Driven Health: Ref No. 832-blockchains.

Chapter 1

Introduction

1.1 Introduction



- Introduction
- Problem Definition
- Methodology
- Research Contributions
- Thesis structure

Healthcare Information System (HIS) is the process of storing and analysing patient health records to improve patient treatment, track the causes of diseases, manufacture effective medicines, and establish prevention agendas. The start of data management includes documenting patient complaints, diagnoses, and the corresponding treatment that is manually introduced in a health record. With the development of digital data, Electronic Health Records (EHRs) came into existence (Jamie, 2019). EHRs are often required to be shared among different healthcare organisations, medical drug manufacturers, pharmacists, medical insurance providers, researchers and patients for total health care. The Healthcare Information System (HIS) consists of a range of information systems, including the Prescription Management System (PMS) (Cartwright-Smith et al., 2016).

This study focuses on the New Zealand PMS and issues related to underserved communities, in particular, the Maori and Pasifika peoples. Research indicates that under-served communities experience unequal access to HIS and, given the broad range of systems that people may interact with, this study specifically addresses the PMS. There are indications that as people experience unequal access, they also become disengaged from the services provided. Factors resulting in patients becoming disengaged include, a lack of trust, the cost of treatment and prescriptions, and the cost of transport, and distances to the healthcare providers (Cartwright-Smith et al., 2016; Howe et al., 2018; Meng et al., 2018).

The process of storing and transferring patient data across multiple entities is complicated by a heterogeneous and poorly integrated information systems standards (such as for historical prescriptions) (Cartwright-Smith et al., 2016). This is not a new problem and there have been attempts by Howe et al. (2018) at solving this problem before. The PMS environment is crucial for maintaining an accurate prescription record and mechanisms to share them across healthcare providers. In this study, the proposed system problem is addressed with blockchain technology. Blockchain technology is a distributed ledger that maintains its transaction history across a decentralised network of nodes that retain copies of the ledger. The Blockchain is updated using a one of a large range of consensus based protocols. In that sense, there is an expectation that there is no trust in the community but that all contributing members have trust in the efficacy of the consensus protocol. The ledger then provides immutable transaction logs and they are typically open to public scrutiny (Nakamoto, 2008).

This study uses Blockchain technology to enable an incentive mechanism to encourage and attract patients to participate and engage with the PMS. They receive forms of compensation that may be exchanged for the cost of future prescriptions, doctor visits and so on. The study proposes a Blockchain based PMS, named BlockPres, that addresses the issues identified and seeks to resolve the lack of trust and poor perceptions of the healthcare system by Maori and Pasifika peoples. The Healthcare Information System (HIS) involves the storage and analysis of patient health records to enhance patient treatment, track disease causes, create effective medicines, and establish a prevention agenda. Data management previously involved manually documenting patient complaints, diagnoses, and corresponding treatments in health records. However, with the advent of digital data, Electronic Health Records (EHRs) emerged (Jamie, 2019). EHRs need to be shared among various healthcare organisations, medical drug manufacturers, pharmacists, medical insurance providers, researchers, and patients, for effective healthcare. The HIS encompasses several information systems, including the Prescription Management System (PMS) (Cartwright-Smith et al., 2016), which is the focus of this study. The study specifically addresses issues related to under-served communities, particularly the Maori and Pasifika peoples, who often experience unequal access to HIS. The study suggests that unequal access leads to disengagement from healthcare services due to several factors, such as lack of trust, cost of treatment and prescriptions, distance to healthcare providers, and so on.

The challenge of storing and transferring patient data across multiple entities is complicated by a heterogeneous and poorly integrated information systems environment. Blockchain technology is a proposed solution to this problem. Blockchain technology is a distributed ledger that maintains its transaction history across a decentralised network of nodes that retain copies of the ledger. The Blockchain is updated using one of a large range of consensus-based protocols, ensuring trust in the efficacy of the consensus protocol. This study proposes the use of Blockchain technology to develop an incentive mechanism for patients to participate in the PMS and receive compensation that may be exchanged for the cost of future prescriptions and doctor visits. The study introduces a blockchain-based PMS, called BlockPres, to address the issues identified and resolves the lack of trust and poor perceptions of the healthcare system in the Maori and Pasifika communities.

The organisation of Chapter 1 is as follows: Section 1.2 provides an overview of the problem that is identified in Chapter 2. Section 1.3 describes the methodology that is adopted for this research. Section 1.4 presents the contributions of this research, and finally, Section 1.5 outlines the overall structure of the thesis chapters.

1.2 Problem Definition

A range of factors identifies a group as being an under-served community. In addition to the factors that have been identified, behaviour in under-served communities tends to exhibit disengagement from healthcare services. In this section, the factors that are related to this study and the problem area are defined. However, communities in other cultural or geographic regions may identify different sets of factors contributing to their relationships with HIS. A common factor that affects a patient's perception and trust towards the system is a personal belief held that the healthcare system treats the patient unfairly or does not provide equal access to services. This results in the patient becoming disengaged from the healthcare system. This may be because the patient sees the public health system as hostile and alienating and that may be a consequence of the patient's inability to pay the cost of treatment and prescriptions. Also a patient living in a rural area may experience high transport costs or difficulties in getting to a hospital or clinic, and others have difficulty in taking leave from family and work commitments.

There are also personal and cultural beliefs that run counter to established medical practices (Graham et al., 2020). Over the past several decades, developments in technology have seen a rapid growth of digital devices and technologies to improve HIS (Steyn et al., 2021). However, groups that are considered to be under-served have also emerged over the same period (Goslee et al., 1998). This includes under-served Maori and Pasifika groups with limited access to digital infrastructure (Graham et al., 2020). Factors that typify these groups, amongst others, are long-term medical or disability issues and cultural or language barriers. Additional problems in under-served communities arise as they often believe that the system treats them differently from what may be described as a "served" community. Consequently, lack of trust emerges and the unwillingness to make use of healthcare systems available results. In all these cases, social impacts arise when an unequal level of access to digital platforms exists, and in the current environment results in an unequal level of healthcare delivery (Collins et al., 2017).

The level of health and well-being amongst Maori populations is well documented (Colijn et al., 2017; Lawson, 2019), for example). Studies repeatedly show that there exists wellness gaps between Maori and non-Maori and that these include lifestyle factors, levels of existing health conditions and the life expectancy gap is more than eight years between the groups. Rates of smoking tobacco amongst the Maori is 50% higher than non-Maori, resulting in a mortality rate of up to 10%. Successive governments have made promises to reduce inequities over the past decades, but the problem continues to increase and healthcare systems fail to overcome equity problems in all population groups (Goodyear-Smith et al., 2019) . In addition, while recent developments and reforms in the delivery of healthcare services have been made, the problem of accessibility remains, which contributes to inefficiencies and inequalities.

1.3 Methodology

In order to design and develop a BlockPres artifact as a solution to the research problem described above, the Design Science Research (DSR) methodology is adopted (Dresch et al., 2015). This methodology framework is used because it allows the extension of boundaries in human and organisational capabilities by creating new and innovative artifacts. For this study, the DSR process is comprised of the following three phases: problem identification, solution design and evaluation, as depicted in Figure 4.1. Each phase comprises different steps (Furda et al., 2019; Wieringa et al., 2012). The design process incorporates the definition of the problem statement and the design of an Artifact as a conceptual model, which is then refined as a logical model that is evaluated in an iterative process of instantiations to determine the quality of the logical model. The primary purpose of this process is to produce an effective system in the form of a blockchain-based PMS.

1.4 Research Contribution

This Ph.D. research has made several significant contributions to the field of Blockchain analysis. The following are the contributions of this research:

- In Chapter 2, Conducting a systematic literature review to identify issues in the current healthcare system in New Zealand, including security and privacy, data heterogeneity, counterfeit drugs, prescription issues, and unequal access to the prescription system. The study aims to formulate research questions by examining unequal access to the PMS.
- In Chapter 3, a Blockchain technology-based literature review is analysed to mitigate unequal access or inequality in healthcare. The Chapter 3 explores the potential of Blockchain technology in the healthcare system and studies relevant

to healthcare. Additionally, Chapter 3 examines incentive mechanisms proposed for other purposes and how they can be applied to this study.

- In Chapter 6, proposes an incentive mechanism to encourage under-served communities to participate in the delivery of healthcare services, and potentially reducing the financial burden on them and allowing them to claim incentives for discounts, payment for medication, or other healthcare services.
- In Chapter 5, designes and developes the BlockPres framework using DSR methodology,. This provides a blockchain-based solution to the issues in the current healthcare system, and specifically the prescription management system. The proposed framework is developed based on the New Zealand healthcare system. It is designed to enhance the overall perception of Maori and Pasifika peoples towards HIS and PMS, and increase their trust levels toward healthcare providers. The Chapter 5 also includes the development of a BlockPres prototype based on the proposed framework in Chapter 5 and the incentive mechanism in Chapter 6, which is included in Appendix 1. The BlockPres framework also changes patient behavior by altering perceptions about inequality or unequal access and encourages under-served communities to participate in and use the healthcare system. The proposed patient-centric approach allows patients to control parts of their records and the authorisation process, in order to increase trust levels. Healthcare providers can only access patients' records if the patients are willing to provide access authorisation.
- In Chapter 7, the prototype is evaluated to reconcile with the theoretical findings of Chapter 2. The analysis of the evaluation of the BlockPres framework indicates that Blockchain technology can enhance the engagement and participation of Maori and Pasifika by providing security and privacy, the authority over records, improving trust levels, and offering incentive benefits.

1.5 Thesis Structure

The thesis is presented in eight chapter and are structured below:

- **Chapter 1:** Provides an overview of the thesis, including the healthcare system background, problem definition, methodology, contribution of the study, and thesis structure.
- **Chapter 2:** Presents a theoretical review of the literature, adopting a systematic literature review and PRISMA method to identify issues in the healthcare information system, such as security and privacy, counterfeit drugs, prescription problems, and unequal access. The chapter 2 focuses on unequal access to PMS and formulates research questions and hypotheses.
- **Chapter 3:** Reviews technological solutions to mitigate inequality in the prescription system, focusing on Blockchain technology, and explores research articles to study proposed systems and frameworks. It also discusses incentivisation protocols using Blockchain technology.
- **Chapter 4:** Discusses the research methodology adopted for the study, using Design Science Research Methodology as a framework to build an artifact. The chapter 4 proposes methods to evaluate the research questions.
- **Chapter 6:** Proposes a blockchain-based incentive mechanism using formal methods and cryptographic techniques to motivate Maori and Pasifika financially and engage them into the proposed system.
- **Chapter 5:** Develops BlockPres design and architecture using Archimate, an open and independent enterprise architecture modeling language that provides a visual representation and Framework for describing, analysing, and communicating

the structure, behavior, and relationships of an organisation's architecture components. Chapter 5 includes the internal and external design of the BlockPres artifact.

- **Chapter 7:** Presents an evaluation of the proposed BlockPres artifact and incentive mechanism, using the Ethereum network to test the performance of the artifact. The prototype is developed and presented in Appendix 1. Chapter 7 also evaluates the trust level of the system and reconciles the hypothesis with the findings.
- **Chapter 8:** Finally, Chapter 8 concludes the research and discusses limitations and future research to enhance the proposed BlockPres artifact.

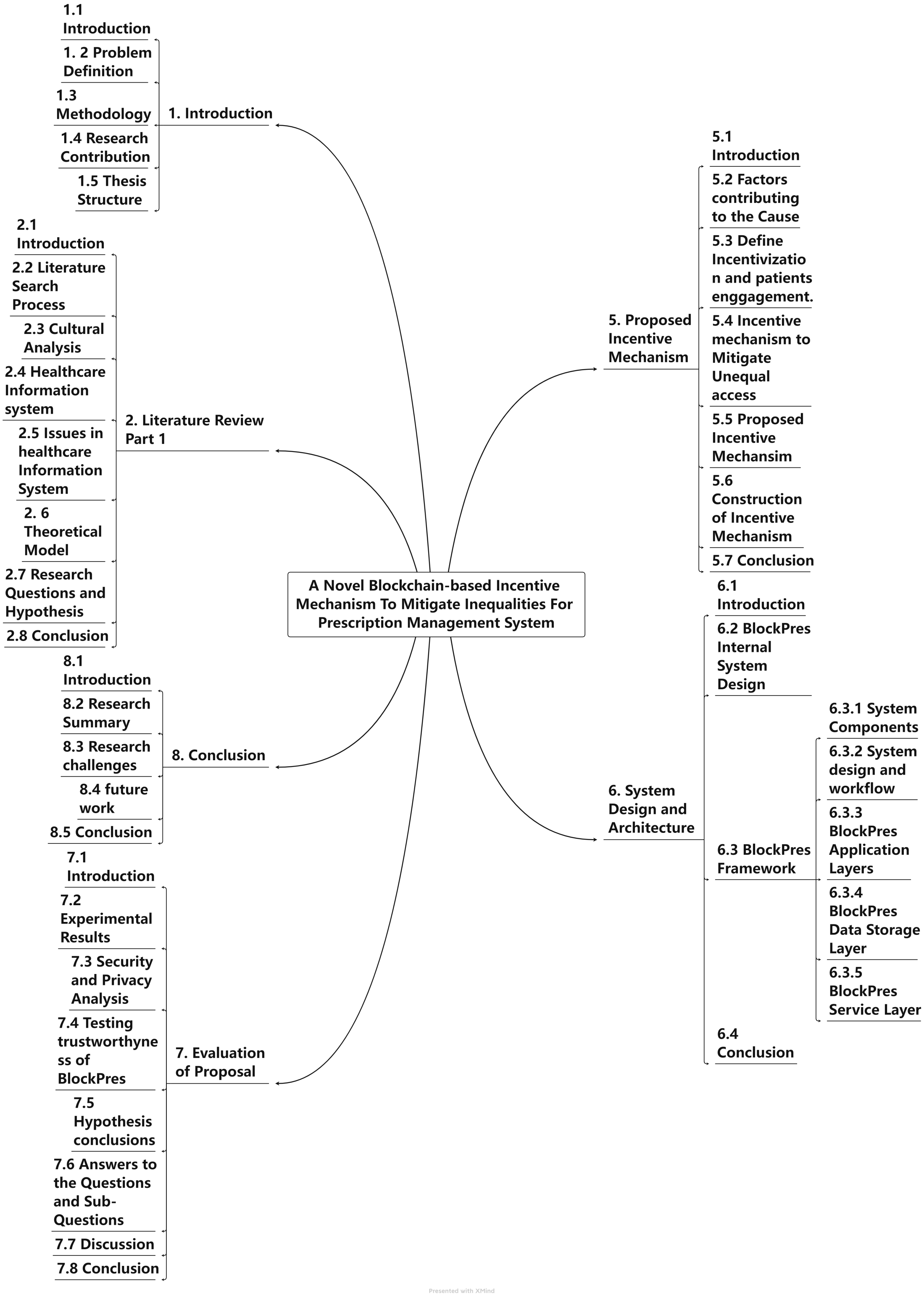
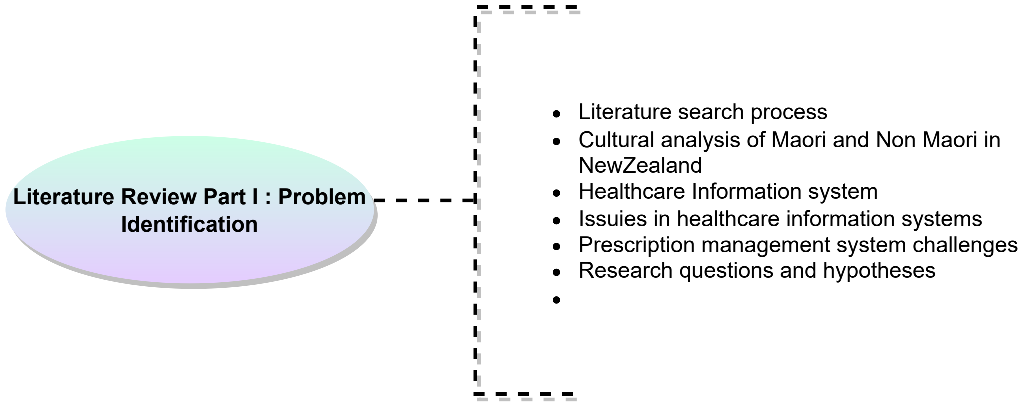


Figure 1.1: Thesis Structure

Chapter 2

Literature Review Part 1: Problem Identification

2.1 Introduction



Chapter 2 presents a systematic literature review of HIS research. A range of articles are identified covering various issues related to HIS, such as security and privacy, data transparency, data heterogeneity, counterfeit and substandard drugs, and an inequity in the prescription management system (PMS). However, the study's focus is narrowed down to unequal access to PMS, particularly among the Maori and Pasifika communities.

This lack of access is a significant cause of prescription problems, including wrong dosage, wrong medication, and prescription cloning, specifically in these communities. The Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) method was applied to establish the literature for the research. By following the PRISMA guidelines, the study was able to identify and decompose the data and identify gaps and problems within the scope of the thesis. The most relevant articles are selected by taking the research papers from higher-ranked journals and conferences.

Systematic Reviews have been widely used in healthcare research for a long time and have become increasingly popular more recently (Chitu, 2015). The PRISMA method, used by (Moher et al., 2009), is a widely accepted approach for ensuring a high level of rigor in reporting theoretical and scientific research. Many studies have adopted the PRISMA methodology in healthcare research, including (Gagnon et al., 2015; Datta et al., 2017; Agbo et al., 2019). Rezaeibagha et al. (2015) used the PRISMA method to systematically review HIS security and privacy requirements and described access control policies. Additionally, West et al. (2014) used the PRISMA method to investigate visualisation techniques on EHR data to find valuable knowledge that can increase efficiency and provide effective ways to deal with patients. Similarly, Braun et al. (2013) adopted the PRISMA method to explore the deployment and development of mobile technologies to strengthen health service delivery and the healthcare community. They also noted that mobile technology facilitates health education and improves program monitoring. These studies demonstrate the effectiveness of the PRISMA method in the healthcare field for literature selection.

This study also adopted the PRISMA method and the PRISMA protocols. The PRISMA method was modified to use in the IS domain, specifically regarding the capture and recombination of raw data. PRISMA has a 12-step process for analysing data, including: identifying protocols, establishing acceptance and rejection criteria for papers and studies, identifying sources of information, developing a search strategy, selecting studies, determining data collection methods, identifying potential variables that may affect the selection, assessing bias risks in individual studies, evaluating bias risks in the overall collection of studies, summarising study results, synthesising findings, and applying other forms of analysis.

The chapter is organised as follows: Section 2.2 covers the literature search process and the use of various online libraries to find articles related to keywords. Section 2.3 presents cultural analysis of Maori and Non-Maori in New Zealand. This section provides the differences face by Maori is discussed. Section 2.4 defines healthcare information system (HIS) and how HIS works. Section 2.5 on page 35 discusses various issues and problems in healthcare information systems. Section 2.5.5 on page 38 presents a specific research problem and conducts a comprehensive literature review. Section 2.5.5.3 on page 41 addresses system challenges related to unequal access or inequality in PMS. The research questions, objectives, and hypothesis are presented in section 4.3 on page 95.

2.2 Literature Search Process

In this section, a systematic literature search process of the research on HIS is presented. To begin, the study reviewed articles to address the following questions

- How cultural differences and other factors affect Maori health in New Zealand healthcare system?
- What are the issues and problems associated with HIS?
- What solutions blockchain technology provide to HIS?
- Does the paper present a blockchain solution or propose a proof of concept?

PRISMA is the systematic review methodology used in the study to search for articles on the above questions. The majority of the articles reviewed were from reputable journals or high-ranking conference proceedings, with a small number of patents also included. The study searched the databases from IEEE, PubMed, Springer, ACM, Elsevier, and Scopus to find high-quality research papers and used a consistent set of keywords. The literature review was divided into two phases. In the first phase, the study reviewed papers related to HIS and its issues, using keywords such as "Healthcare Information System current issues," "E-health issues," "Healthcare Information System issues," and "Electronic healthcare record." In the second phase, the study reviewed papers that discussed blockchain technology and its potential solutions for HIS, using keywords such as "blockchain technology for Healthcare Information System," "blockchain Solutions for Healthcare issues," and "blockchain technology architecture." This division of the literature review aimed to separate studies on HIS issues from those on proposed solutions and existing studies based on blockchain technology.

2.2.1 Article Inclusion and Exclusion Criteria

Initially, Figure 2.1 presents the process of retrieving articles from online libraries and screening them. A significant number of articles were eliminated due to duplication, and a majority were also excluded after reviewing the titles and abstracts. The remaining articles were then reviewed and evaluated for eligibility.

The following general inclusion criteria were applied:

1. High rank journals and conferences
2. Period range, 2000–2018
3. Articles relevant to the primary subject or theme of the study
4. Written in English.

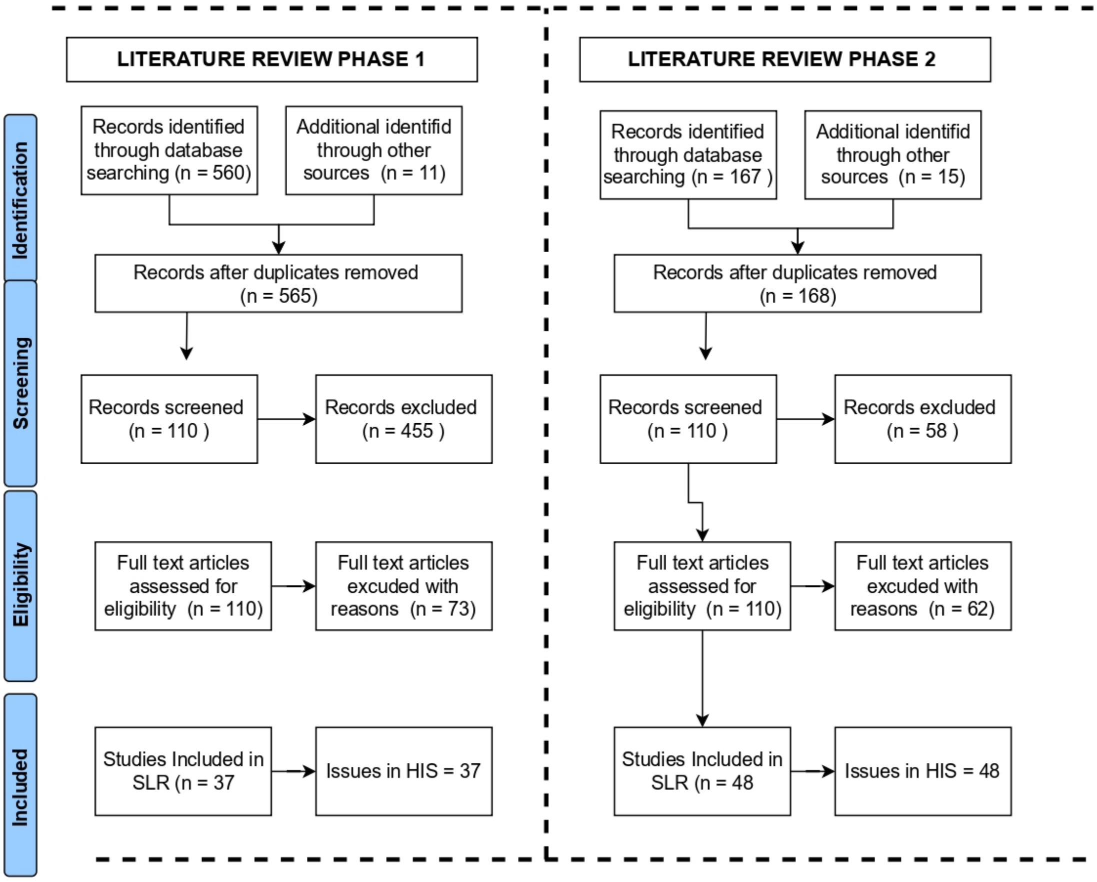


Figure 2.1: PRISMA Literature Review Chart

2.2.2 Search Analysis

The study identified 571 studies. As shown in Figure 2.2 on the next page, the most studies were obtained from online libraries such as Association for Computing Machinery (ACM), Elsevier, Springer, The Institute of Electrical and Electronics Engineers (IEEE), Scopus, and PubMed. After removing duplicate articles, 565 articles were suitable for screening. The study applied article inclusion and exclusion criteria as outlined in section 2.2.1 on the preceding page on the preceding page. As a result, 455 articles were excluded as they were not related to healthcare or Distributed Ledger Technologies. The remaining 110 articles were then classified according to subject and keyword discovery. These classifications identified problem areas in HIS such as security and privacy, data transparency, data heterogeneity, counterfeit and substandard drugs, unequal access to

HIS, and prescription issues.

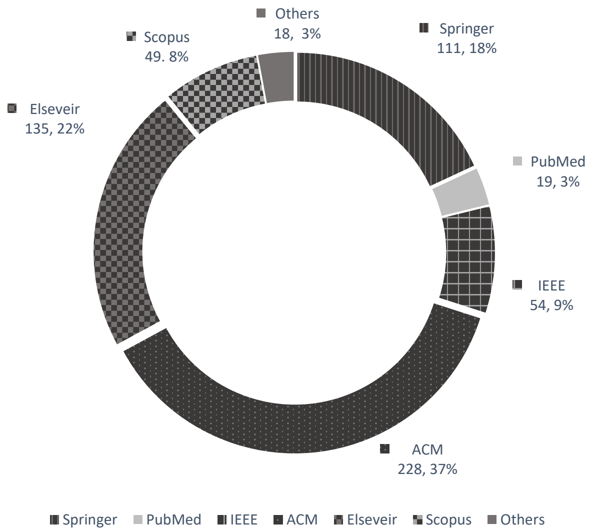


Figure 2.2: Source and Percentage of Papers

The literature review was divided into two phases. In phase 1, the study reviewed 37 papers related to research problems and issues in HIS. Several challenges were found during the literature review process, such as security and privacy, data transparency, data heterogeneity, prescription issues and unequal access in HIS with underserved people. In phase 2, the study reviewed 48 papers related to blockchain technology and how it may potentially address these issues. Many of the papers present solutions based on Smart Contracts, consensus algorithms using Proof of Work (PoW) or Proof of Stake (PoS), or other types of blockchain technology. Most approaches use Ethereum as a platform, PoW for consensus and public blockchains. It is interesting to note that researchers are considering alternative consensus algorithms for specific use cases and the number of private and hybrid DLTs is increasing.

Table 2.1 on page 18 presents the results of a review of literature that involved 85 unique highquality articles published between 2000 and 2018. Most of the publications were published in journals or in high-rank conferences proceedings. Some patents and other literature were also included and reviewed during data gathering. Table 2.1 on the following page shows that most of the publications were published in high impact factor journals and most were published recently between 2015 and 2018.

Table 2.1: Article Summary

Author, Year	**Impact Factor/Rank**	**Source**
Journal Articles		
Ichikawa et al., 2017	4.541	JMIR mHealth and uHealth
Kleinaki et al., 2018	4.148	Computational and structural biotechnology
Zhang et al., 2018a	4.148	Computational and structural biotechnology
Xia et al., 2017b	3.557	IEEE Access
Guo et al., 2018	3.557	IEEE Access
Zhang et al., 2016b	3.557	IEEE Access
Dagher et al., 2018	3.073	Sustainable Cities and Society
Roehrs et al., 2017	2.882	Journal of biomedical informatics
Zhao et al., 2018	2.493	CAAI Transactions on Intelligence Technology
Tseng et al., 2018	2.145	International journal of environmental research and public health
Kaur et al., 2018	2.098	Journal of medical systems

Continued over page/..

Author, Year	**Impact Factor/Rank**	**Source**
Griggs et al., 2018	2.098	Journal of medical systems
Yue et al., 2016	2.098	Journal of medical systems
Fan et al., 2018	2.098	Journal of medical systems
Zhou et al., 2018	2.098	Journal of medical systems
Zhang et al., 2018b	2.098	Journal of medical systems
Patel, 2018	1.833	Health informatics
ne Hussein et al., 2018	1.425	Cognitive Systems Research
Xia et al., 2017a	1.2	Information
Benkaouz et al., 2015	0.732	Procedia Computer Science
Ananth et al., 2018	0.69	Journal of Engineering Technology
Cardenas et al., 2013	1.239	IEEE Security and Privacy
Castaneda et al., 2015	0.56	Journal of Clinical Bioinformatics
Colijn et al., 2017	3.394	Computational Physiology and Medicine
Das et al., 2016	3.833	American Economic Review
Geifman et al., 2015	4.219	BMC Medicine

Continued over page/..

Author, **Year**	**Impact Factor/Rank**	**Source**
Goslee et al., 1998		Education Resources Information Center
Hartung et al., 2014	19.384	Annals of Internal Medicine
Jacobs, 2009	2.652	ACM Queue
John et al., 2012	6.125	Association for Psychological Science
Kaushal et al., 2003	47.7	JAMA Network Open
Stephen, 2000		Education Resources Information Center
Kelman et al., 2002	1.889	Australian and New Zealand Journal of Public Health
Middleton et al., 2013	3.428	Journal of the American Medical Informatics Association
Miriovsky et al., 2012	26.303	Journal of Clinical Oncology
Schatz et al., 2017	1.78	Journal of Digital Forensics, Security and Law
Schiff et al., 2009	19.989	JAMA Internal Medicine
Singh et al., 2013	19.989	JAMA Internal Medicine

Continued over page/..

Author, **Year**	**Impact Factor/Rank**	**Source**
Sinha et al., 2009	3.428	Journal of the American Medical Informatics Association
Taichman et al., 2016	19.384	Annals of Internal Medicine
Terry et al., 2000	2.56	Journal of Health law
Tsai et al., 2016	1.747	Computers Electrical Engineering, Elsevier
Viceconti et al., 2015	3.85	IEEE Journal of Biomedical and Health Informatics
Warren, 2016	79.258	the new england journal of medicine
Yin et al., 2015	9.107	Proceedings of the IEEE
McGuire et al., 2008	41.57	Nature : International journal of Science
Meng et al., 2018	3.557	IEEE Access
Cartwright-Smith et al., 2016	6.34	Vanderbilt Journal of Entertainment Technology Law
Raghupathi et al., 2014	2.75	Health Information Science and Systems, Springer

Continued over page/..

Author, Year	**Impact Factor/Rank**	**Source**
Campbell et al., 2009	4.005	Journal of General Internal Medicine, Springer
Campbell et al., 2006	4.270	Journal of the American Medical Informatics Association
Saleem et al., 2005	4.270	journal for biomedical and health informatics
Ash et al., 2007	4.270	journal for biomedical and health informatics
Horsky et al., 2005	4.270	journal for biomedical and health informatics
Chapron, 2017	41.57	Nature: International journal of Science
Friedman et al., 2009	2.957	International Journal of Medical Informatics, Elsevier
Sands, 2004	4.270	journal for biomedical and health informatics
Winthereik et al., 2005	0.725	Computer Supported Cooperative Work (CSCW), Springer
Conference proceedings		
Liang et al., 2017	A	IEEE Symposium on Personal, Indoor, and Mobile Radio Communications

Continued over page/..

Author, **Year**	**Impact Factor/Rank**	**Source**
Juneja et al., 2018	A	IEEE Biomedical & Health Informatics
Shae et al., 2017	A	IEEE Distributed Computing Systems
Dubovitskaya et al., 2017b	A	American Medical Informatics Association Annual Symposium
Zhao et al., 2017	B	IEEE Symposium on Autonomous Decentralized Systems
Omar et al., 2017	B	International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage
Azaria et al., 2016	B	IEEE Open and Big Data
Zhang et al., 2017b	B	IEEE e-Health Networking, Applications and Services
Han et al., 2018	B	International Conference on Cloud Computing and Security

Continued over page/..

Author, **Year**	**Impact Factor/Rank**	**Source**
Jiang et al., 2018	B	IEEE International Conference on Smart Computing
Liu et al., 2017	C	e-Health Networking, Applications and Services
Ekblaw et al., 2016		IEEE Open and Big Data
Mashima et al., 2012	B	USENIX Security '12
Cunningham et al., 2018		World Congress on Medical and Health Informatics
Dubovitskaya et al., 2017a		Workshop on Data Management and Analytics for Medicine and Healthcare
Patil et al., 2014	B	IEEE International Congress on Big Data
Zhang et al., 2010	B	IEEE 3rd International Conference on Cloud Computing
Other		
da Conceição et al., 2018		CoRR ArXiv
Zhang et al., 2017a		CoRR ArXiv

Continued over page/..

Author, **Year**	**Impact Factor/Rank**	**Source**
Dias et al., 2018		CoRR ArXiv
Kuo et al., 2018		CoRR Arxiv
Massi et al., 2018		e-print
Peterson et al., 2016		White paper
Bulleit et al., 2018		Patent
Reid et al., 2005		Book
Shortliffe et al., 2000		Book

2.3 Cultural Analysis of Māori and Non-Māori in New Zealand

Significant differences in health outcomes between indigenous and non-indigenous people exist in various regions (Who, 2013). According to the World Health Organisation, indigenous people are those who have a particular identity in a specific community, and the community identifies them as one of their own. These people are believed to be culturally associated with early settlers of a particular region and therefore have links to various natural resources and territories (Charters, 2019). Also, indigenous people have particular cultural beliefs that cut across their social, economic and political practices (Axelsson et al., 2016). Reid et al. (2005) states that efforts put in place for many decades to improve the health of indigenous people have been in vain, as these disparities in health have increased rather than diminish .

According to Charters (2019), increased health problems among the indigenous people is a significant issue for this century. Health among indigenous people is considered a matter that violates the rights of humans, and this is against various global principles, which include the Red Cross and Red Crescent Societies (Paine et al., 2016). According to Hobbs et al. (2019), the first and second article in the United Nations Declarations that speaks on the privileges of indigenous people, and it is clear that these people have the right to full enjoyment and the right not to be discriminated because of their origin or culture. The United Nations (UN) world congress concerning indi-genous people held in 2014 September, made a commitment that it would strive to offer non-biased psychological and general health services to indigenous people (UN, 2014).

Initially, New Zealand did not support the United Nations Declaration on the Rights of Indigenous Peoples (UNDRIP). However, three years later, the country accepted the declaration (Harris et al., 2015). Anderson et al. (2006) says that Maori is a group of people, who are known to be the early settlers of New Zealand, who arrived from Polynesia around 1000 years ago. The Treaty of Waitangi, which was a political agreement between the Maori and British Empire was signed in 1840 to protect the rights of the Maori people (Anderson et al., 2006). The population of Maori was 100,000, and this was fifty times more than the settlers who were only 2000 in number (Theunissen, 2011). The translation of treaty from English to Maori has significant variances and this led to challenges in implementing and understanding the treaty. Also, the agreements defined in the treaty were not met, and this led to Maori becoming colonised and the minority. It resulted in them losing their land and reduced food resources (Theunissen, 2011).

The Treaty of Waitangi was the only sure way that Maori people could be protected. However, the rights of Maori were not observed, and this resulted in disparities in health between the settlers and the Maori (Anderson et al., 2006). Despite efforts by the government to make sure the rights of the Maori were observed. The health disparities are still visible as the population of Maori now constituting only 14% in New Zealand. The rights of the under-served populations are often put aside in favour of populist policymaking, for example, removing the right of prisoners to vote. The largest group of prisoners are Maori, and that group is excluded from the democratic process (Theunissen, 2011). Therefore, all the factors discussed above are causes impacting Maori health. The next section discusses Maori health status.

2.3.1 Māori health status

According to the World Health Organisation, there is a correlation between colonisation of land to the health status of people who are involved (WHO, 2017). These people tend to have decreased health status as compared to their neighbours. This is not only been seen among the Maori but other communities in the world such as indigenous peoples.

In New Zealand, these health disparities exist between Maori and Pasifika (Eriksson et al., 2017). During the beginning of the seventeenth century, life expectancy is longer in Maori than for Britain (Anderson et al., 2006). However, as the original settlers of New Zealand were colonised, health disparities increased, and this resulted to the emergence of new disease among the Maori such as tuberculosis (Harris et al., 2015; Robb et al., 2017).

According to (Paine et al., 2016), poor health among Maori also resulted from British influences that curbed native languages among children in schools. Marriott et al. (2015) state that losing land by Maori was a blessing in disguise as it was noted that, various diseases did not inflict those who lost their land as compared to those who did not lose their land. Moreover, this affected children the most, with 50% of the deaths involving infants. From 1938, the health status among the Maori gradually increased, and this was attributed to national systems that were concerned about the welfare of the whole of society (Rahiri et al., 2018).

Paine et al. (2016) state that, despite the increase in life expectancy, the difference between Maori with other communities in still large. Currently, Maori lead in the prevalence of both chronic diseases such as asthma, cancer and other non-communicable diseases (Gurney et al., 2020), as compared to nonMaori, whose rates of non-communicable disease decreased (Rahiri et al., 2018). Maori experienced various challenges and access to health services was one. This resulted in the availability and affordability of healthcare. This is as a result of the cost of going to seek healthcare and lack of time to leave work and go to the hospital (Eriksson et al., 2017). It has also been identified that, as compared to non-Maori, Maori wait for a long time in hospitals, and this slows down the entire treatment process (Gurney et al., 2020). Also, there is less likelihood that healthcare providers refer Maori to a specialist as compared to non-Maori.

(Deng et al., 2020) also adds that cancer chances are higher among Maori, and there is 77% percent likelihood that a Maori would die from the disease as compared to a non-Maori. Social-economic conditions, lifestyle and availability of access for health care are significant factors that affect Maori health and some reasons for health disparities between Maori and Non-Maori (Rahiri et al., 2018). (Charters, 2019) says there is a link between racial discrimination and poor health among Maori and nonMaori. This is evident, according to (Ryks et al., 2019; Litchfield & Khan, 2021), who reported that Maori recorded the highest number of discriminatory cases from healthcare providers. They felt like their cultural understanding about healthcare is undermined, and in one way or the other, this affects their health (Rahiri et al., 2018).

2.3.2 Factors Affect Māori Health

This section highlights the factors that affect Maori health because of inequalities in the healthcare system. The factors are socio-economic, lifestyle, and the healthcare system.

2.3.2.1 Socioeconomic Factors

The disparities among the socioeconomic status of Maori and non-Maori has been said to play a considerable role in the resulting disparities in the health status of the two groups of people (Eriksson et al., 2017). In the past, Maori lost most of their resources to colonisation (Denison et al., 2018). This affected Maori education, healthcare, and employment that collectively resulted in poor health outcomes. Many studies, (Rahiri et al., 2018; Eriksson et al., 2017; Paine et al., 2016), show a link between social practices and health outcomes. In their studies, non-Maori have fewer health issues as compared to Maori, and this may play a role in explaining health disparities. Despite these studies showing a link between socioeconomic status and health, it is not the only factor that determines health, and there are many other factors which may create disparities.

2.3.2.2 Lifestyle Factors

Richardson et al. (2016) State that lifestyle factors gained more attention than socioeconomic factors. At first, since the former requires much less social and political change. However, the researcher warns that using a lifestyle approach in social policies can decontextualise behavior and encourage victim-blaming. Instead, according to Tompkins (2017) , lifestyle factors should be regarded as a result of numerous distal determinants of health (for example, social, institutional, political, legal, and cultural factors). Tobacco consumption, hazardous drinking, obesity, and poor nutrition (Collins et al., 2017; Denison et al., 2018; Theunissen, 2011; Gurney et al., 2020). Maori People in New Zealand have consistently had higher rates. Despite the fact that several public health initiatives have been implemented to reduce inequalities between these groups, Maori People keep showing trends that deviate from policy targets (Rahiri et al., 2018). Deng et al. (2020) state that people with a right level of health awareness and income appears to be sensitive to the advice of relaxation or healthy lifestyles.The government should therefore focus on implementing evidence-based policies that protect Maori, such as reducing the presence of unhealthy food outlets in areas where many Maori live. Additionally, Zawaly et al. (2019) supports this argument in the context of oral healthcare, pointing out that while the government funds other health services, individuals are often expected to pay non-subsidised premiums for dental care (Rahiri et al., 2018).

2.3.2.3 Health Care System Factors

Many deaths that could have been prevented by adequate healthcare occur among Maori and Pasifika populations, even when healthcare services are available (Al-Busaidi et al., 2018). This suggests that gaps in ethnic wellbeing continue to exist regarding accessing and utilising healthcare (Paine et al., 2016). Theodore et al. (2019) found that Maori have unmet health needs, specifically in relation to cardiovascular diseases.

Despite a relatively higher number of Maori being hospitalised due to heart disease, they receive lower levels of interventional treatment compared to non-Maori (Al-Busaidi et al., 2018). Providing elective operations is also a concern and could help improve these adverse outcomes. Similarly, while Maori and Pasifika have lower cancer survival rates than other ethnic groups, a small proportion of these health differences can be explained at diagnosis (Rahiri et al., 2018). The remaining differences can be attributed to disparities in healthcare service access, such as access to prescription management or secondary healthcare, as well as cultural safety and norms, particularly the attitudes of healthcare professionals towards Maori and the acceptability of visiting healthcare providers among ethnic minorities groups (Al-Busaidi et al., 2018).

Came et al. (2017), stated that the level of co-morbidity among each ethnic group is counted, which may have prevented treatment. As a result, they account for a portion of the observed health disparities. Theodore et al. (2019) investigate ethnic health disparities in healthcare access and quality as well. According to the researchers, Maori are twice as likely as non-Maori to disregard healthcare services due to high medication prices or living in the country side (Al-Busaidi et al., 2018; Came et al., 2017; Theodore et al., 2019). Access of healthcare system especially to PMS may have high disparities because of the Universal Health System in New Zealand, it is not free but subsidised and patients are expected to contribute to the fee and that is the problem for many low income people. It is also state that in the public system, there are significant waiting lists for non-emergency healthcare. (Deng et al., 2020).

2.4 Healthcare Information System

This section presents an overview of HIS and how HIS works and What are the key features of HIS. Significant variances exist in the definition of the term HIS (Boonstra et al., 2014; Ahern et al., 2006; Howe et al., 2018). There is no standard definition for this term worldwide but key features give meaning to the concept of HIS. The following definitions for HIS apply in the context of this doctoral research:

- HIS refers to information about a patient's health that is stored electronically in a computer system (Grandia, 2017).
- HIS contains various patient's records, including personal data, treatment details, underlying diseases, and diagnosis procedures, radiological reports, and other details, including dates of next appointment(Kohli et al., 2016).

HIS is a secured system, which means that specific healthcare workers can only access it with authorisation from the institution. According to Kombe et al. (2018) the advantages of a HIS system, among others, include offering a platform to run healthcare services, reducing the time taken for patient care at a health center, enhancing workflow, and maintaining the confidentiality of patient's information by ensuring that only the right people get access. There is significant variation in the definition of the term HIS (Boonstra et al., 2014; Ahern et al., 2006; Howe et al., 2018). However, despite the lack of a standard definition, certain key features are essential for understanding the concept of HIS. In the context of this doctoral research, the following definitions are used for HIS.

HIS refers to electronically stored information about a patient's health in a computer system (Grandia, 2017). HIS contains various patient records, including personal data, treatment details, underlying diseases, diagnosis procedures, radiological reports, and other details, such as dates of following appointments (Kohli et al., 2016). HIS is a secure system accessible only by authorised healthcare workers. According to Kombe et al. (2018), some advantages of HIS systems include providing a platform for healthcare services, reducing patient care time at a health center, improving workflow, and maintaining patient confidentiality by ensuring that only authorised individuals have access to patient information.

According to Roehrs et al. (2017), HIS is a collection of information about individuals receiving healthcare that is generated and stored electronically. The Healthcare Information and Management Systems Society (HIMSS) defines HIS as a safe, uptodate, and patient-centered source of information for healthcare workers (Fatima et al., 2018). Kohli et al. (2016) say that HIS supports healthcare providers by providing timely information that improves evidence-based healthcare decisions. Automating many aspects of healthcare such as patient care and communication, minimises errors made by healthcare teams. Incorporating HIS into other areas such as billing, disease surveillance, and quality of care improves efficiency in these areas within the healthcare setting (da Conceição et al., 2018). In summary, HIS is an electronic system that provides a platform for maintaining records and other relevant information. Securing access to this system means that it is only accessible to a few healthcare staff, reducing errors that are common in hand-written or hardcopy medical records. Some of the critical features of HIS are listed in the following sub-sections.

2.4.1 Key Features of HIS

There are four classifications of features in HIS: Clinical, functional, secure, and technological features. These features ensure the quality of the system's functions and make them useful (Nelson et al., 2016).

2.4.1.1 Clinical features:

One of the clinical features of HIS should be the ability for healthcare staff to access real-time information about health records, disease profiles, and other beneficial medical results (Howe et al., 2018). Warning signs that alert healthcare staff to a relevant event that occurs with a patient are also a clinical feature of HIS. This may include red flags that notify healthcare staff of potential issues (Ahern et al., 2006). Atanasovski

(2018) designed a general HIS architecture and discussed the clinical features and the connectivity of stakeholders with the system. Hence, clinical features take into consideration all medical inputs available in the HIS, which are meant to protect the well-being of patients.

2.4.1.2 Functional Features

Functional features ensure that HIS tasks are practical and efficient (Qi et al., 2017). Fatima et al. (2018) state that the functionality of the HIS system determines its effectiveness in helping staff and the hospital accomplish tasks quickly and in minimum time. The HIS should provide features enabling hospital staff to run tasks from remote areas, such as the bedside or hospital administration, as well as clinical departments (Gursel et al., 2016). According to Nelson et al. (2016), HIS systems use specific definitions that are consistent with international guidelines and hence consistent with other systems. Functional features provide information about patients' billing and charges and improve the effectiveness of healthcare tasks by the staff.

2.4.1.3 Security features

Patients' information is confidential and should not be accessed by unauthorised persons. Al-Dhafian et al. (2017); Chen et al. (2016) state that security features play a role in ensuring that information about a patient is only accessed in the right way, for the proper purpose, and by the right person. Additionally, security features enable the system to identify the details of the staff who access the patient's information and the date and time of access. Security features enhance the security of data in a HIS system, improving the system's effectiveness (Fatima et al., 2018).

2.4.1.4 Technological features

Technological features are components of the HIS system that include hardware, software, and a network system. These features allow information to be entered into the system effectively and shared among other organisations while maintaining the confidentiality of the information (Gursel et al., 2016). Sharma et al. (2006) discussed a core structure and network architecture that shows the technological connectivity of different entities such as hospitals, pharmacies, labs, web servers, private networks in HIS.

2.5 Issues in Healthcare Information Systems

This section discusses issues identified in the healthcare system using the PRISMA method. The study reviews the literature, selects PMS issues for further research, and finds different issues related to PMS. Other issues include: Security and Privacy, Data transparency, and Data heterogeneity. These issues are discussed in the following sub-sections.

2.5.1 Security & Privacy

HIS is often installed onto centralised systems, providing a single failure point in many attack scenarios (Patil et al., 2014; Schatz et al., 2017). Also, data reliability is lost when data are altered maliciously or accidentally. This may affect the veracity of clinical trials or negatively impact clinical decisions (Zhang et al., 2010). Furthermore, the greater the number of points of access to patient information, the increased risk of intrusion (Terry et al., 2000). For example, sensor networks for in-home patient monitoring provide data security and integrity challenges where data may be intercepted wirelessly (Shortliffe et al., 2000).

Privacy issues may arise with mobile apps and devices because they are often provided by third-party vendors. For example, privacy breaches or the unintended use of very sensitive patient data Viceconti et al. (2015). Also on selling data to other providers or big data aggregators (Cardenas et al., 2013), and data creep where new uses are found for data than what the data were originally collected for. Data in the hands of unknown providers, whose motive is likely to be profit-driven, removes effective control of personal information from the patient or authorised parties (Tsai et al., 2016). For example, recently, the approach towards data in most jurisdictions has been very loose, with few standards or statutory regulations (Cardenas et al., 2013). Consequently, the use of tracking software and cookies on websites has fallen out of favor because, for example, patients fear that insurance companies might change their coverage after discovering what online information they have accessed.

2.5.2 Data Transparency

Patients may be justifiably concerned that their information is not handled openly or transparently (Kelman et al., 2002). Patients may be equally concerned that their confidentiality may be breached without their knowledge and that decisions may be made regarding service provision or treatment without their input. When data ownership is in doubt, such concerns lead to a lack of trust in healthcare providers and systems vendors (Miriovsky et al., 2012). Doubts about who is accountable for the protection and proper management of data identify questions about staff and management capability, whether the system is fit for purpose, and whether transactions are auditable (Mashima et al., 2012). However, data owners may not be willing to provide open access for such assessments Colijn et al. (2017); Das et al. (2016), and this casts further doubt on the intentions. Furthermore, trust is an issue in publishing results of studies and clinical trials (John et al., 2012; Hartung et al., 2014), where data may be accidentally or maliciously altered or lost, and there may be a lack of redundancy or data unavailability occurs. Also, published results may vary from the intended study goals by adding bias, for example, removing or adding data or stopping the data collection at a beneficial point.

2.5.3 Data Heterogeneity

The HIS environment is heterogenous, and data exchange is difficult (Reid et al., 2005). A factor in heterogeneity is the range of systems that exist in even relatively coherent environments. However, hospitals may have hundreds of unique information systems built without regard to data sharing, thus creating problems when sharing data across organisational (Middleton et al., 2013). Heterogeneity also affects the scalability of platforms where different systems must be optimised equally well. Also, if data are to be mined effectively and if the information presented to clinicians acquires appropriate context and accuracy, a consistent data structure is required (Tsai et al., 2016). Therefore, data processing provides a range of issues, from capturing data at the right time before it loses value, to transforming data to a consistent format for analysis (Yin et al., 2015). Often, data requires significant preprocessing to make it usable, such as from imaging machines, sensor networks, and monitoring equipment.

2.5.4 Counterfeit and Substandard Drugs

Counterfeit drugs pose a significant problem for the general population, particularly in developing countries (Rebiere et al., 2017; Fadlallah et al., 2016). Julian et al. (2009) and Fenoff (2009) point out that the primary reason behind this issue is the poor condition of the drug supply chain management, which makes it easy for counterfeit drugs to be produced, distributed, and consumed on a large scale (Tim et al., 2013). These drugs are either poorly manufactured and distributed, which can lead to intoxication, or they do not contain the proper drug dosage, which is vital for treating a problem and can lead to drug resistance (Fenoff, 2009). These counterfeit drugs are sold in the drug market under the name of well-reputed drug companies (Fenoff, 2009). According to WHO (2017), these drugs may not pose a significant problem when taken in limited doses but pose a significant life-threatening risk when used to treat serious diseases. Several studies have reported that counterfeit drugs for treating health problems such as cancer, hypertension, contraception, painkillers, antibiotics, and other major prescribing drugs are creating problems and may lead to life-threatening issues (Dégardin et al., 2014; Rebiere et al., 2017; dos Santos et al., 2019).

According to WHO (2017); Beverley (2014), 1 out of 10 medical products produced in developing and under-developed countries are counterfeit and substandard. (Nayyar, 2019) says that some low-level companies produce Counterfeit and Substandard Drugs (CSDs) to make a substantial profit, and they made the factories to create those drugs. Another study reveals that most drugs are made with cheap ingredients, and some drugs include dangerous ingredients that cause health problems for patients (Dégardin et al., 2014). However, Who (2017); dos Santos et al. (2019); Dégardin et al. (2014); Nayyar (2019), state that authorities are responsible for controlling these CSDs from entering the drug supply chain process, but some dishonest suppliers and lowlevel companies find ways to enter the healthcare system.Who (2013) estimates that over 1 million deaths are recorded yearly due to counterfeit and substandard drugs. Fenoff (2009) also states that more than 0.7 million people die from tuberculosis and malaria because of CSDs.

2.5.5 Prescription Management System and Its Challenges

This section briefly defines PMS and its usage in HIS, and unequal access to PMS and the associated challenges. It also report incidents and complaints related to these issues reported by the Health and Disability Commissioner in New Zealand.

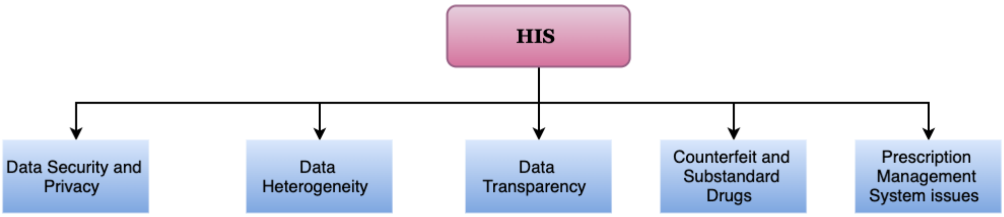


Figure 2.3: Issues in HIS

2.5.5.1 Definition of PMS

Hamlin et al. (2016) define PMS as an electronic, computerised system used by doctors, nurses, physicians, and clinicians to enter, review, modify, and prescribe medications. Keene et al. (2016) states that PMS is supported by the main Computerised Physician Order Entry (CPOE) system, which include other systems such as decision support systems and clinical support systems to share the characteristic feature of automating the ordering process for medications. CPOEs range from simple systems with a limited set of medications that can be prescribed to complex systems with various forms of decision support, including warnings and reminders for the medical doctor on various aspects of the prescribing process (Jamie, 2019).

2.5.5.2 Current Practices in PMS

Electronic prescriptions have been available in New Zealand since 2015, according to the Ministry of Health, and the number of E-prescriptions has increased dramatically in recent years. E-prescriptions have several advantages over paper prescriptions, including greater accuracy, efficiency, and security. The Ministry of Health in New Zealand manages electronic prescriptions, known as (EPS) Electronic Prescription Service. It eliminates the need for paper prescriptions and allows EPS to send the prescription directly to the pharmacies electronically. Prescribers must register to use the EPS and get access to secure online portals or software which allows for generating electronic prescriptions. It can be dispensed in the same way as paper prescriptions; once the prescription is generated, it is sent to the patient's chosen pharmacy electronically.

Additionally, in improving the prescribing and dispensing process, E-prescriptions provide many benefits for patients. Such as, patients can select the pharmacies to their prescriptions to be sent, which will further reduce the process of collecting the prescriptions from the doctor's office physically. Patients with mobility or those living in rural or rural areas can get a considerable benefit from it. Many benefits are associated with prescription management systems and can reduce the error of medications. They are not immune to errors. However, some research shows that prescription errors can be made due to these systems when used. Below are various studies confirming that prescription errors exist in New Zealand's healthcare system and have affected patients' lives.

The study of Leitch et al. (2021), conducted a retrospective review of 40,000 patient records from 54 general practices in New Zealand and identified 466 cases of medication-related harm. The study found that medication-related harm was a significant problem in New Zealand general practice, with a prevalence of 1.2% per year. The study found that medication-related harms are the most common adverse drug reactions, prescribing errors, and medication non-adherence. There are higher risks for medication-related harm to specific patients, including older adults, multiple medication in-takers, and those with chronic conditions. With regard to the factors that are related to medication-related harm, various issues related to prescribing, dispensing, and monitoring medications have been identified by various authors.

According to Yang et al. (2021), This study found that prescribing errors were common in New Zealand general practice, with 2.3% of all prescriptions having at least one error. The authors noted that the use of electronic prescribing systems could reduce the incidence of errors. The review of Goodyear-Smith et al. (2019), identified several medication safety issues in New Zealand primary care, including prescribing errors, medication-related adverse events, and medication non-adherence. According to the Manias,Kinney,Cranswick, and Williams (2014) research, in New Zealand, most common errors were found in medication, with 16.7% of all medication orders having at least one error. Studies of Robb et al. (2017) stated that the most common adverse events in New Zealand were medication errors. The survey of Halcomb et al. (2015), found that medication safety was a concern, with many respondents reporting that they had experienced medication errors or near misses.

According to Halcomb et al. (2015), prescribing errors were common in a New Zealand tertiary hospital, with 18.7% of all medication orders having at least one error. Jamie (2019), discussed and analyzed reports of medication safety incidents in New Zealand primary care and found that prescribing errors were the most common type of incident. Haua et al. (2019), states that prescribing errors were common in New Zealand hospitals, with medication omissions and incorrect dosages being the most frequent types of errors. In New Zealand, per year, 1.2% errors occurred in general practice, as the above studies prove. It also brought attention to significant problems of prescription and medication errors. The prevalent types of harm were adverse drug reactions, medication non-adherence, and prescribing errors. Most older patients with chronic conditions were at higher risk of experiencing harm. Factors contributing to medication-related harm included difficulties with prescribing, dispensing, and monitoring medications.

2.5.5.3 Unequal Access to PMS

For various reasons, a group of people or underserved communities may become disengaged from the healthcare system. One reason is the belief that the healthcare system mistreats patients or does not provide equal access to services, which affects patients' perceptions and trust towards the system, leading to disengagement. Other reasons for disengagement may include the inability to afford the cost of treatment and prescriptions, difficulties and high costs of transport to hospitals or clinics for patients in rural areas, inability to take leave from work or personal beliefs that conflict with established medical practices. This study focuses on the prescription management system and issues related to perceptions of inequality in relation to the fulfillment of prescriptions by patients.

Advancements in technology have resulted in a rapid increase in digital devices and technologies aimed at improving healthcare information systems (HIS) (Stephen, 2000). However, Goslee et al. (1998) highlighted certain groups of people, such as underserved Maori and Pasifika communities, who have limited access to digital infrastructure due to factors like long-term medical or disability issues, cultural or language barriers, and slow internet speeds in rural areas. These inequalities in access to digital platforms can lead to disparities in healthcare delivery, as pointed out by (Engelhardt, 2017).

The social impact of these disparities is significant, as they result in unequal levels of access to healthcare. The inequalities between Maori and non-Maori in New Zealand have received significant scholarly attention, as evidenced by a substantial body of literature (Lawson, 2019). Studies have found that Maori individuals experience poorer lifestyles and health outcomes than non-Maori counterparts, with a life expectancy gap exceeding eight years. Furthermore, Maori have higher smoking rates than non-Maori. Despite the government's commitments over the last decade to reduce these disparities, the problem has only worsened. According to Goodyear-Smith et al. (2019), the system has yet to effectively address the disparity between Maori and non-Maori populations.

Recent developments and reforms in the healthcare industry have been made, but the problem persists in the system. According to Dawson et al. (2019), factors contributing to inequity in healthcare, specifically in PMS, include prescription cost, physical access to the system, timely care provision, acceptability, and cultural factors. The study by Lawson (2019) found that mental illness among Maori and Pasifika has increased due to ethnic disparities. The study included 15,822 respondents who responded to a questionnaire to assess the risk of depression and anxiety. The study's outcome showed that underserved people are underdiagnosed with mental illness due to inequality (Harris et al., 2018). However, Lane et al. (2019) argue that inequalities among Maori and Pasifika exist outside the healthcare system. Tupai (2018) also examined the inequality problem in New Zealand and found that healthcare services cost twice as much for Maori compared to non-Maori people. It is hypothesised that limited and unequal access to HIS for Maori is due to an inadequate healthcare system, affecting Maori health and disengaging them from the healthcare system. The study of Sheridan et al. (2011) revealed that Māori and Pacific's people experience significant disparities in access to primary healthcare services compared to non-Māori and non-Pacific populations, which results in worse health outcomes for these groups.

The study also identified various factors contributing to these inequities, including socioeconomic status, racism and discrimination, cultural barriers, and limited access to appropriate health services. As per Neville et al. (2022), there are several barriers to participation, including language and communication, cultural differences in health beliefs and practices, and a lack of understanding of the healthcare system. Furthermore, the paper mentions that many older Pacific people face socioeconomic challenges, such as poverty and limited access to transportation, which can limit their ability to access healthcare services. Figure 2.3 on page 39 depicts the issues identified during the literature review process.

2.5.5.4 Other Factors Associated With Unequal Access

Inadequate access and inequality in the prescription management system can significantly negatively impact the Maori population. These impacts can include:

- Decrease trust: When the healthcare system is perceived as unfair or biassed, trust in healthcare providers may decrease. Patients may require additional time to seek medical care and adhere to treatment plans, which results in improved health outcomes. (Lawson, 2019) .Maori and Pasifika individuals in New Zealand lack confidence in the healthcare system due to the inequalities and disparities they have encountered as a result of systematic racism and discrimination (Ellison-Loschmann et al., 2006). As a result, these communities have experienced substantial health disparities and believe that their healthcare needs are not being met adequately. Inequalities in the healthcare system that affect Maori and Pasifika include unequal access to healthcare services, a lack of culturally competent healthcare providers, and an absence of culturally appropriate services (Harris et al., 2018). These factors have contributed to health disparities between these communities and non-Maori/Pasifika populations citeeriksson2017inequities.

- Loss of status: Maori's may feel that their cultural identity and values are not respected by the healthcare system, resulting in a loss of status and cultural pride. This can lead to a lack of representation, disrespect, and discrimination against Maori culture and heritage in healthcare (Harris et al., 2018; Eriksson et al., 2017).

- Racial bias: Inequality and lack of access in the prescription management system could be considered racial bias. This may increase Maori discrimination and marginalisation within the healthcare system (Al-Fageh et al., 2018; Eriksson et al., 2017). It can also contribute to the need for greater understanding and awareness of the unique health needs of the Maori population.

- Loss of value: When healthcare services are not accessible or equitable, the Maori community's health may be undervalued, resulting in poorer health outcomes. Socioeconomic factors and a lack of healthcare access may worsen this. (Puaar et al., 2018; Eriksson et al., 2017).

- Class difference: Inequalities in the prescription management system can contribute to developing of different classes in the Maori community. Those who can afford private healthcare may receive better care, whereas those who cannot face barriers to care access. This can prolong health disparities among Maori's (Almutairi et al., 2018; Eriksson et al., 2017).
- Cultural differences: This may also contribute to cultural differences between communities. The healthcare system's lack of representation and respect for Maori culture and heritage of representation and respect for Maori culture and heritage within the healthcare system can perpetuate cultural stereotypes and misunderstandings. This can contribute to a lack of comprehension and awareness of the unique health needs of the Maori population (Neuspiel et al., 2013; Eriksson et al., 2017).

2.5.5.5 Example Cases in PMS

A prescription error is an avoidable situation that leads to unnecessary medication use or harm to the patient (Hatch et al., 2011). Recent studies have shown that many prescription errors occur due to inadequate use of HIS. This leads to wrong dosages, medication errors, and unequal access to HIS for Maori (Tran et al., 2019). These systems were intended to reduce medication dosage errors but instead contribute to prescription errors (Health & Commissioner, 2018). Studies have found that errors can include the omission of life-saving medications and potentially cause moderate to severe harm (Puaar et al., 2018; Almutairi et al., 2018; Aldridge, 2016). Research shows that more than 770,000 injuries and deaths occur annually due to adverse drug events (ADEs), often resulting from errors in prescription lists (Al-Fageh et al., 2018). In addition, when a patient's prescription history is incomplete at admission, it can lead to complications such as prolonged hospital stays or deaths. Problems with Prescription

Management Systems (PMS) are standard worldwide and can result in deaths (Kohn et al., 2000). In New Zealand, studies have shown that prescription errors have increased from 7.8% to 30% among Maori in the last decade. Research suggests that these errors, such as wrong dosages, wrong medications, and prescription cloning, are caused by inequalities in PMS. People in under-served communities may be unable to afford prescriptions, leading them to resort to illegal means, which can further contribute to the problems (Tavva et al., 2011; Phalke et al., 2011; Karna et al., 2012).

According to Cavell et al. (2019) report, healthcare professionals, such as doctors, clinicians, and nurses, write and control prescriptions for patients. Wittich et al. (2014) state that prescription errors are responsible for one death out of 854 Maori inpatients and 1 out of 131 outpatients. Children are particularly vulnerable to these errors, as their physiology, size, and disability make them more susceptible (Neuspiel et al., 2013).

2.5.5.5.1 Report Cases: Martin (2018) reports that a midwife obtained cloned prescriptions by using other people's names to acquire medication. The medications included 100 x 50mg Tramadol tablets with two repeats, Ibuprofen, Paracetamol and 20 x 60mg Codeine phosphate tablets. Wall (2019) noted that the midwife was addicted to Tramadol, and the doctor would always give her electronic prescriptions. She would then change the dates on the prescription and print them out before visiting different pharmacies to obtain the medication. This incident occurred to avoid doctor's fees and highlights that the high cost of healthcare can lead to patients disengaging from the system. Robb et al. (2017) report that 28% of patients in six district health hospitals in New Zealand have experienced some form of prescription problems. Approximately 30% of these patients are primary care patients treated by general practitioners, dentists, and community pharmacies. However, it is unknown what percentage of this harm is directly caused by prescription problems. A study by the Safety Commission NewZealand (2017) found that 12% of adverse events in New Zealand's public healthcare centers are related to medication taken without prescriptions or in wrong doses, which can lead to severe damage such as death or disability. Furthermore, a survey by Robb et al. (2017) found that 8% of adverse events were caused by wrong dosages and wrong types of prescriptions taken by patients without consulting doctors. Research on the causes and types of medications involved in these events is published (Walls et al., 2004).

Patients may disengage from PMS due to perceptions of inequality and a lack of trust in the system, often resulting from negative experiences. According to a report by Health and Commissioner (2018), 310 complaints were registered from 2009 to 2016, with examples such as: a woman who has prescribed the wrong medication (Salazopyrin instead of Pentasa), which led to hospitalisation with diagnosed liver dysfunction, a child with cerebral palsy who has prescribed an incorrect dosage of a muscle relaxant (Baclofen) resulting in three hospital visits with increased seizures and shortness of breath, a woman with breast cancer who has prescribed the wrong dosage of a five-year course of Tamoxifen and a three-month prescription of Tenoxicam, a medication used for treating joint pain and a resident of a community residential mental health service who was given a high dose of a medication called Antipsychotic Clozapine, despite having never taken it before (Health & Commissioner, 2018).

Additionally, the study gathered data from a source Health and Commissioner (2018) and analysed it using descriptive analyses. The results are presented in Figure 2.4 on the following page, 2.5 on page 49, and Figure 2.6 on page 50. These figures demonstrate that prescription problems exist within PMS. Figure 2.7 on page 51 shows that inappropriate medication and wrong dosage are the primary contributors to patient prescription problems. The data and figures indicate that prescription problems are a major cause of inequality and patient disengagement from the system.

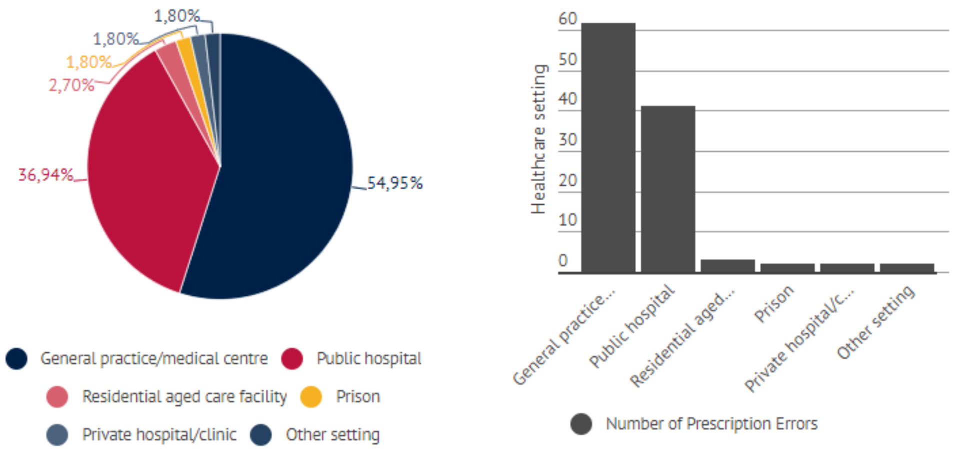


Figure 2.4: Setting of Prescribing Errors
(Health & Commissioner, 2018)

Healthcare setting	Number of prescription errors	Proportion of prescription errors
General practice/medical Centre	**61**	**55%**
Public hospital	**41**	**37%**
Private hospital	**2**	**2%**
Prison	**2**	**2%**
Residential ages care facility	**3**	**3%**
Other settings	**2**	**2%**
Total	111	

Table 2.2: Setting of Prescribing Errors
(Health & Commissioner, 2018)

2.6 Research Question(s) and Hypotheses

This section presents research questions arising from the literature review and hypotheses generated for a theoretical model. The literature reviewed by using the PRISMA method in section 2.2 identified issues in HIS (Gagnon et al., 2015). The study focuses

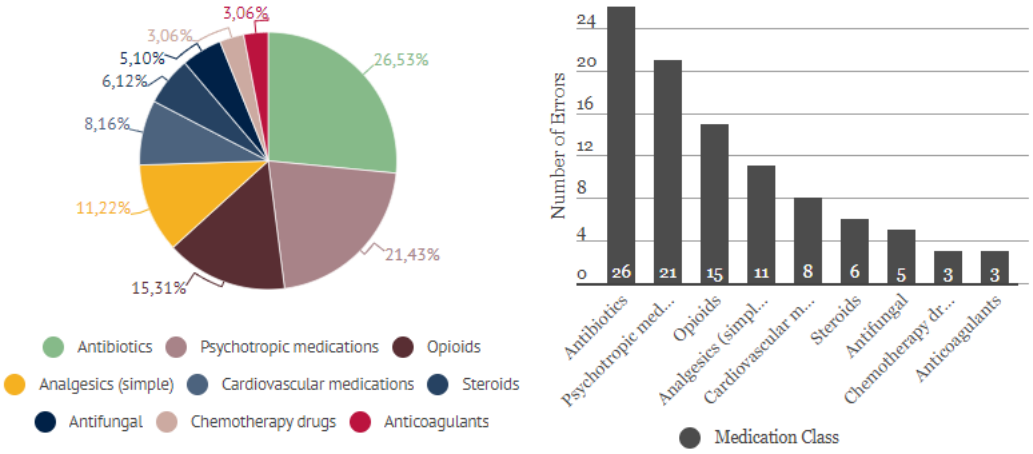


Figure 2.5: Classes of Medications
(Health & Commissioner, 2018)

Medication class	**Number of prescription errors**	**Proportion of prescription errors**
Antibiotics	**26**	**23%**
Psychotropic medications	**21**	**19%**
Opioids	**15**	**14%**
Analgesics	**11**	**10%**
Cardiovascular medications	**8**	**7%**
Steroids	**6**	**5%**
Antifungal	**5**	**5%**
Chemotherapy drugs	**3**	**3%**
Anticoagulants	**3**	**3%**
Total	111	

Table 2.3: Classes of Medications
(Health & Commissioner, 2018)

on unequal access to PMS and associated problems for Māori and Pasifika. The following are the research questions formulated according to the challenges.

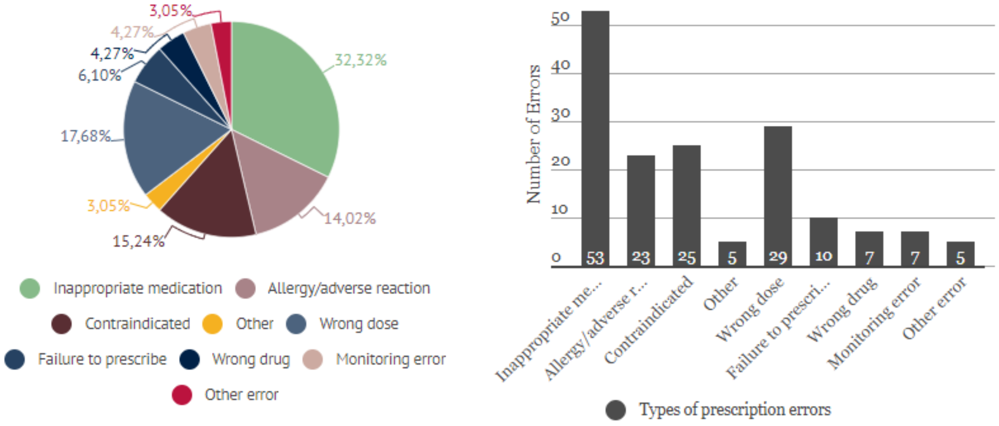


Figure 2.6: Types of prescription errors
(Health & Commissioner, 2018)

Types of error	Number of errors	Proportion of errors
Inappropriate medication	**61**	**55%**
Wrong dose	**23**	**21%**
Failure to prescribe	**10**	**9%**
Wrong drug	**7**	**6%**
Monitoring errors	**7**	**6%**
Other errors	**5**	**5%**
Total	111	

Table 2.4: Types of prescription errors
(Health & Commissioner, 2018)

RQ1 What issues exist within current prescription practices?

(a) How do prescription issues manifest?

(b) What are the current practices to counter these issues?

(c) Are current practices effective in HIS?

RQ2 What are the reasons for unequal access to Maori in PMS?

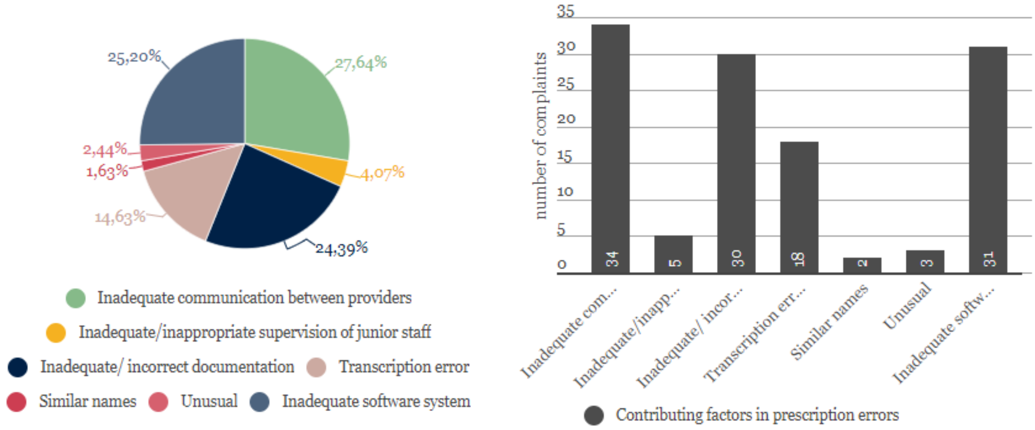


Figure 2.7: Contributing factors in Prescription Errors
(Health & Commissioner, 2018)

(a) Are current PMS accessible and engageable to Maori and Pasifika?

(b) Are Maori and Pasifika trusting the current PMS?

2.6.1 Hypothesis

At this stage, six hypotheses are constructed to address the questions. The hypotheses are not final, as Design Science Research allows us to refine the hypotheses during the evaluation phase of the research later on.

H1 The current prescription practices in HIS are ineffective and error-prone.

H2 The impact of unequal access to PMS affects the health outcomes of Maori and Pasifika, as it also contributes to their disengagement from healthcare services.

H3 The unequal access to PMS among Maori and Pasifika undermines the system's trustworthiness.

H4 The prescription system's inadequacy contributes to both prescription errors and the disengagement of Maori and Pasifika.

2.7 Conclusion

The PRISMA method is used in this research to systematically review the literature and identify the challenges in HIS. To guide the research, first specific questions were identified which are used throughout the thesis. This chapter highlights that the main challenges in the healthcare system are: security and privacy concerns, lack of data transparency, data heterogeneity, counterfeit and substandard drugs, and unequal access to PMS.

- How do cultural differences and other factors affect Māori health in the New Zealand healthcare system?
- What are the issues and problems associated with HIS?
- What solutions does blockchain technology provide to HIS?
- Does the paper present a blockchain solution or propose a proof of concept?

This Chapter 2 focuses on two main questions: How do cultural differences and other factors affect Maori health in the New Zealand healthcare system? What are the issues and problems associated with HIS? The study specifically focuses on the issue of unequal access or inequality in the PMS. Additionally, it includes references to papers and reports and government-controlled department articles in section 2.5.5 on page 38 that raise questions about strong cases of unequal access in the healthcare system. Systematic literature analysis found that most studies are linked to unequal access and inequality in PMS. This chapter identifies key points that contribute to the thesis' overall direction:

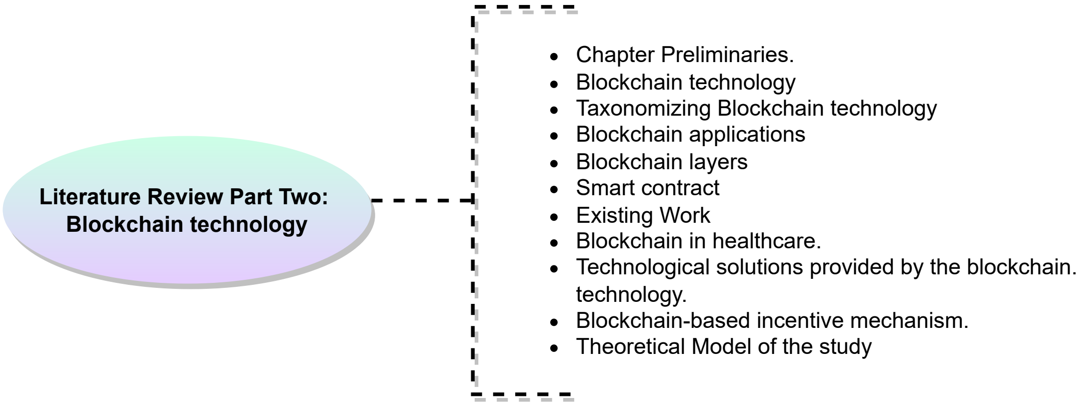
- Systematic Literature review.
- Cultural analysis of Maori and Non-Maori health status in New Zealand healthcare system and factors contributing to Maori health.

- HIS issues and their relevance with New Zealand healthcare system.
- PMS and its challenges.
- Research Questions and Hypothesis.

The Chapter 2 aims to review the current literature and identify gaps in HIS. Therefore, Chapter 3 specifically addresses the question, "What solutions does blockchain technology provide for HIS?" and examines whether the literature presents a blockchain solution or proposes a proof of concept. Additionally, it identifies the numerous information issues in the healthcare information system. It focuses on the problems Maori and Pasifika face regarding medication and prescriptions in the prescription management system. These problems include the distance from the healthcare system due to inequality or unequal access and disengagement due to a lack of trust. Therefore, this chapter concludes that the Prescription management system needs a robust technological solution to overcome these issues. The following chapter will discuss blockchain technology architecture and potential solutions for addressing these issues.

Chapter 3

Literature Review Part 2: Blockchain Technology



- Chapter Preliminaries.
- Blockchain technology
- Taxonomizing Blockchain technology
- Blockchain applications
- Blockchain layers
- Smart contract
- Existing Work
- Blockchain in healthcare.
- Technological solutions provided by the blockchain. technology.
- Blockchain-based incentive mechanism.
- Theoretical Model of the study

3.1 Introduction

Chapter 2 employed the PRISMA method to conduct a systematic literature review (SLR) for this research project. The literature review is divided into two phases. Phase 1 examined the literature on the healthcare information system and PMS, focusing on issues such as inequality and unequal access to PMS, engagement, and trust of an under-served community. Based on the findings from Phase 1, research questions were formulated in Section 4.3. Chapter 3 presents Phase 2 of the literature review, which focuses on blockchain technology. It provides background information on blockchain technology and its consensus algorithms. It also discusses the purpose and potential uses of blockchain technology in the field of HIS. Additionally, it critically analyses studies that have adopted blockchain technology in healthcare and the proposed frameworks, as well as incentive mechanisms proposed in these studies to overcome the challenges identified in Phase 1 of the literature review.

The organisation of the chapter is as follows: Section 3.2 presents an overview of blockchain technology and discusses the core component of the technology, applications, layers, and smart contract. Section 3.3 on page 65 discusses existing work in the area of HIS. Section 3.4 on page 72 presents technological solutions given by the Decentralised ledger technology in different fields of study, including healthcare. In the context of this study, blockchain-based incentivisation studies are discussed in section 3.5 on page 75. The theoretical model is presented in section 3.1 on page 78, and the chapter concludes with a literature review summary.

3.2 Chapter Preliminaries

This section presents a brief introduction to blockchain technology foundation, and cryptographic methods.

3.2.1 Blockchain Technology

Blockchain technology is a distributed, decentralised ledger system that enables secure and visible transactions, and it is the fundamental technology behind digital currencies like Bitcoin and other virtual assets (Nakamoto, 2008; Buterin, 2015). A digital ledger containing transaction records is replicated and distributed throughout the network of computer systems that constitute the blockchain (Patel, 2018). Each block within the chain has multiple transactions. Whenever a new transaction occurs, it is recorded on each participant's ledger (Brodersen et al., 2016a), and the distributed ledger is maintained by multiple participants in the decentralised database. Blockchain technology possesses several distinguishing characteristics, including its ability to facilitate secure and traceable transactions. Transactions are grouped into blocks and added to the chain sequentially, in a time-stamped manner (Rabah, 2017). The chain of blocks is highly resistant to tampering and revision because of its cryptographic security. Transactions are also transparent, allowing all users to view the blockchain's transaction history. Furthermore, the immutability of the blockchain guarantees that once a block is appended to the chain, it cannot be modified, thereby preserving the transactions' integrity on the blockchain (Christidis et al., 2016). However, Transactions on public blockchains like Bitcoin or Ethereum can be stuck in a queue for an extended period due to factors such as network congestion, limited block space, low transaction fees, network upgrades, fee estimation errors, rapid price fluctuations, complex smart contracts, and external events. Miners prioritize transactions with higher fees, and during times of high demand or network activity, lower-fee transactions can experience delays in confirmation.

There are different cryptographic techniques used by blockchain technology, but those relevant to BlockPres are discussed below. Hashing is a fundamental component in blockchains (Christidis et al., 2016; Patel, 2018; James, 2018). A hash function is a cryptographic technique that converts input into a deterministic fixed-length value. Azaria et al. (2016) state that there are several hashing algorithms to protect data, such as MD4, MD5, MD6, SHA256, and so on. Moreover, a hash function may be irreversible (one way), meaning a person cannot discern from the output what the input was (Gokalp, 2018). Trying to decrypt a hash using a brute force method, requires trying every possible input (Brodersen et al., 2016a). This would be too costly in most circumstances.

Another core component of the blockchain architecture, the Merkle tree, provides the internal block data structure and hashing process. The tree nodes are collected together to form disjoint clusters, where two leaf nodes are hashed, then two branch nodes that each have hashed leaf nodes are hashed, and so on up through the tree until the tree's root is reached. Data is not tampered with in the process because the Merkle tree can reach any node downwards through the hash pointers (Cartwright-Smith et al., 2016). The process strength is that the tree's hashing algorithm can be rerun at any point to produce the same result, verifying that the contents in the leaf nodes have not changed.

The third essential component that is addressed in this paper is digital signatures which are the methods that ensure the integrity and security of information stored in the blockchain network. These apply public/private key signatures to ensure the integrity and security of, in this instance, patient records in the BlockPres. Digital signature serves as identity and to detect modification in transit. However, Once the origin of a record is secured using a digital signature it is impossible to alter or modify the record and this provides non-repudiation (Sharma et al., 2018). Protocols and algorithm blockchains are used to make the network trustworthy and reliable. One of them is Proof of work and Proof of stake.

Proof of Work (PoW) is a method many blockchain networks use to verify transactions and maintain network integrity. Using computational power, miners compete to solve complex mathematical puzzles, and the first miner to do so is rewarded with newly created cryptocurrency. This puzzle, known as a "hash," involves nonce that combine with other block data and generate a block hash. While PoW prevents fraudulent transactions and secures the network, it is resource and energy-intensive due to the high computational power required by miners (Gupta et al., 2020). On the other side, POS is also used to validate transactions and create new blocks in the blockchain network. The validators in POS are the ones who hold a certain amount of cryptocurrency and stake in the network. Moreover, They must put up a certain amount of cryptocurrency as a stake, which they will lose if they attempt to validate fraudulent transactions. Validators are then randomly selected to validate new blocks and are rewarded with transaction fees and newly minted cryptocurrency. PoS is less resource-intensive and energy-intensive than PoW and is used in many blockchain networks such as Ethereum 2.0 and Cardano. (Saad et al., 2020).

3.2.2 Taxonomising Blockchain Technology: Characteristics and Applications

This section presents the taxonomy of blockchain technology and its characteristics and features of are discussed. Blockchains can be broadly classified into two categories based on network permissions: public and private blockchains. Public blockchains, also known as permissionless blockchains, allow anyone to join the network, access its content, submit new transactions, write new blocks to the ledger, or verify the correctness of existing blocks (Wüst & Gervais, 2018). Moreover, allowing anyone to join the network may increase untrusted participants in the network is possible at the cost of blockchain performance. This type of blockchain uses POS and POW to validate transactions and is relatively computationally expensive to deter malicious activity. Some examples of public blockchains are Ethereum, Bitcoin, and Zcash (Bano et al., 2019).

On the other hand, Private blockchains only allow approved users can connect to the network, submit transactions, or update the ledger. Private blockchains are maintained and operated by the organisation, and permissions are granted on a need-to-know basis. This type of blockchain uses a Byzantine fault tolerance consensus algorithm in which most users are trustworthy. Hyperledger fabric and R3 Corda are excellent examples of private blockchains. Several consensus protocols are proposed for Permissioned and permissionless blockchains, such as POW and POS, Byzantine fault tolerance, Proof of service, and extended versions of the consensus protocols. Proof of work is the most common consensus protocol used in public blockchains.

Smart contracts are computer programmes that execute on a blockchain network to facilitate and enforce participants' agreements without the need for third-party. The Internet of Things (IoT) is one of the applications where smart contracts can be utilised. Ethereum is the most prevalent permissionless platform for smart contracts, whereas Hyperledger is the most common permissioned platform for smart contracts. (Alharby et al., 2019, 2018). However, Most blockchain networks use Public addresses to send a transaction instead of actual identities to identify the user in the network. According to (Kuo et al., 2019), this process does not ensure the authenticity of transactions as it is possible to track and trace the transactions made by the user by examining the address. Platforms like Dash, Zcash, and Monero are designed in a way that is difficult to track and trace. In this study, IPFS is used to store patients information. In addition, Every platform has different features. For example, some support smart contracts, and some are not (Kuo et al., 2019; Alharby et al., 2018, 2019; Zhang et al., 2016c).

Blockchain technology aims to secure data while making it accessible to authorised users. This is performed via various characteristics, such as keeping a ledger of all transactions and nodes in the network can not make changes in data. Data is also encrypted to prevent unauthorised access. Access to the data requires a specific identification key, adding an extra layer of security (Abouelmehdi et al., 2018).

EMR systems typically allow clinicians to control patient medical data and access it through medical staff without the patient's authorisation. Incorporating blockchain features in medical data management gives patients control over who has access to their information using a key signature. Additionally, blockchain systems track all data access actions, making it easy to identify any unauthorised changes. Data integrity and trustworthiness are crucial in healthcare systems, and blockchain technology can ensure that data is accurate, updated, and secure. It also allows for sharing of credible information among patients, insurance companies, and healthcare institutions. Furthermore, the blockchain system is space-efficient and requires minimal computational resources, as the verification process is done through record nodes.

Decentralization, transparency, and immutability are key blockchain features that enable effective measures to ensure payments are tied to service value and deter illegal transactions. Decentralization ensures that no single entity has control, transparency provides visibility into transactions, and immutability prevents alteration of recorded data. These features collectively enhance accountability and security in payment processes. .For example, a patient may key in reimbursement for a health practitioner to be processed only when the set conditions are reached on the blockchain features. This will ensure or build trust between a patient and the healthcare provider. Attaching a financial penalty into the system would reduce medical errors among healthcare providers, as most would be more careful to avoid a penalty charge. Blockchain would ensure that all the previous medical history and tests of patients are available in the system and can be accessed upon request. This would prevent redundancy of repeating the same tests during treatment (Ahmed et al., 2018; Ananth et al., 2018)

Blockchain technology can provide adequate measures to ensure payments are made based on service value and prevent illegal transactions. For instance, a healthcare provider can set conditions on the blockchain to pay patients reimbursement. This can help build trust between patients and healthcare providers. Additionally, attaching a financial penalty to the system can reduce medical errors among providers, as they will be more cautious to avoid penalty charges. Blockchain also allows easy access to a patient's medical history and previous test results, preventing an unnecessary repetition of tests during treatment (Ahmed et al., 2018; Ananth et al., 2018).

3.2.3 Blockchains Applications

This section briefly overviews blockchain technology and its various uses, including the cryptocurrencies Bitcoin, Ethereum and the open-source blockchain platform Hyperledger.

3.2.3.1 Bitcoin

The first and most well-known permissionless blockchain platform is Bitcoin. It functions as a distributed cryptocurrency system with no centralised authority. Bitcoin proposes PoW as its consensus protocol to achieve a global blockchain state in a non-trusted environment. However, to maintain the blockchain state, PoW requires more computations power, making it an inefficient protocol. Numerous alternative cryptocurrencies have emerged since Bitcoin's success, some of which use different consensus protocols. (Alharby et al., 2018; Agbo et al., 2019).

3.2.3.2 Ethereum

Ethereum is a computerised and user-friendly interface that allows the coding of decentralised systems without interference from external parties. It employs the "Proof of Work" protocol, but there are plans to switch to the "Proof of State mechanism." This means that in the future, individuals can participate in the mining process and will only be limited by the stake cost. Compared to Proof of Work, Proof of State is more energy-efficient and transparent, as only those with the set stake can participate in mining. However, there exists the potential for those with a larger stake to manipulate transactions dishonestly. Ethereum Virtual Machines are used to generate and execute smart contracts, and they operate publicly without third-party influence or fraud. Serpent, Solidity, and other accessible languages are used to code in Ethereum, and development is done using the truffle framework. Lastly, Ethereum can maintain a stable state despite network conditions.

3.2.3.3 Hyperledger

Hyperledger is a collaborative open-source project that aims to improve permissioned blockchains. It provides numerous modules and tools for developing blockchain platforms. As variants of Hyperledger, various permissioned blockchain systems, such as Fabric, Iroha, Sawtooth, and Indy, have been developed, each with its own architecture and consensus protocol. Fabric, the first blockchain platform capable of executing smart contracts, employs Kafka as its consensus protocol (Androulaki et al., 2018).

3.2.4 Blockchain Layers

Blockchain technology comprises several layers, each with its specific function. The main layers of a blockchain are described in the following sub-sections.

3.2.4.1 The Application Layer:

This layer is the topmost layer of a blockchain and is responsible for interacting with users. It is the interface through which users interact with the blockchain network. Applications built on a blockchain, such as decentralised exchanges, wallets, and smart contracts, are part of the application layer (Wang et al., 2019; Alharby et al., 2018, 2019).

3.2.4.2 The Smart Contract Layer:

The smart contract layer is responsible for executing the logic of a blockchain application. Smart contracts are self-executing contracts with the terms of the agreement written into code. They are used to automate processes and enforce the rules and penalties around an agreement. They are executed by the network nodes and stored on the blockchain (Badr et al., 2018).

3.2.4.3 The Consensus Layer:

The consensus layer ensures the validity of all transactions and the security of the blockchain. The consensus layer ensures that the blockchain's integrity is not compromised and that all nodes concur on the network's state. The consensus algorithm a blockchain uses can vary and include proof-of-work, proof-of-stake, and others (Wang et al., 2019; Alharby et al., 2018, 2019).

3.2.4.4 The Network Layer:

This layer must maintain the communication between the nodes on the blockchain network. By broadcasting transactions and blocks to the nodes, it ensures that the nodes have a consistent view of the blockchain (Gervais et al., 2016).

3.2.4.5 The Storage Layer:

This layer is responsible for the blockchain's data storage. This includes transactions, blocks, and other data. The storage layer can be implemented using various technologies such as a distributed file system or a distributed database (Bocek et al., 2017).

3.2.4.6 Incentive layer :

The incentive layer establishes an incentive structure and distributes rewards to miners who maintain the blockchain ledger using the blockchain's cryptocurrency. This framework is necessary to preserve the permissionless nature of the blockchain. The incentives should compensate the miners fairly for the work they do and motivate them to behave ethically. In addition, they protect the system from common Ethereum attacks such as

DDoS (Alharby et al., 2018, 2019). In many blockchain systems, rewards are linked to the generation of blocks and the completion of transactions, referred to as reward and transaction fees, respectively. There can be significant variations in rewards based on the particular blockchain; for example, in Ethereum, a reward in the form of stale blocks is offered even if they do not enter the blockchain when conflicts get resolved. When a miner is rewarded, their balance increases.

The application layer is the interface between the user and the blockchain. The smart contract layer is responsible for executing the logic of the application. The consensus layer ensures the integrity of the blockchain. The network layer provides communication between the nodes on the blockchain network. It is important to note that all the layers of blockchain technology are not necessarily different and separate. The distinction between layers is primarily conceptual and can help understand a blockchain's different functions.

3.2.5 Smart Contract

Smart contracts are small programmes installed on the blockchain that execute specific business logic in response to changes in the blockchain or network topology (Kumar et al., 2018). The author of Sadouskaya (2017) suggests employing smart contract-enabled blockchain to establish trust and regulate access to IoT devices. MedRec, a blockchain and smart contract-based prototype, was proposed by Ekblaw et al. (2016) to address security issues and ensure the integrity and authenticity of electronic health records. In Agbo et al. (2019), a smart contract was developed to store metadata about record ownership, permissions, and data integrity, execute policies, and permit legitimate transactions to modify data. The original intent of smart contracts was to represent traditional written contracts in a way that eliminates the need for trusted third parties, such as lawyers, to ensure that contract criteria are met (Dagher et al., 2018).

Nevertheless, smart contracts can be any programme that executes business logic that is suitable for installation on a blockchain.

A smart contract is a program that outlines a set of rules that must be met for it to execute. These rules, or constraints, are set in stone once the contract is installed on an immutable blockchain, eliminating the need for an intermediary to ensure compliance(Zhou et al., 2018). However, However, the immutability feature of blockchain technology can make it difficult to fix errors in the contract. Ethereum is a widely-used blockchain platform known for implementing smart contracts written in a language called Solidity(Kumar et al., 2018). Ethereum's developers develop Solidity, which is also used by other blockchain platforms. Moreover, Other programming languages like Java and Python can also be used to write smart contracts on specific blockchain platforms.

3.3 Existing Work

This section discusses research and proposed solutions to improve the effectiveness and performance of HIS through the use of blockchain technology.

3.3.1 Blockchain in Healthcare

In the HIMS environment, sensitive private data are the norm and are distributed between healthcare providers as a matter of course (Cartwright-Smith et al., 2016). Of concern to providers is limited data accessibility, incomplete data where patients may suffer actual harm (Meng et al., 2018; Han et al., 2018; Liu et al., 2017), data provision is timely, and of a form that is compatible with the receiver (Raghupathi et al., 2014). For example, timely access to patient data is important to ensure continuous and correct treatment (Gokalp, 2018), and the presentation of patient data transfers between healthcare providers or treatment facilities (Yang et al., 2015). This raises two issues: what data providers require to be shared, and whether systems are in place to seamlessly share the data (Peterson et al., 2016). To define relationships between providers, MedRec applies smart contracts where relevant data are preserved on the ledger. In addition, MedRec empowers the patient such that the patient may choose to reject or accept the patient-provider relationship (Azaria et al., 2016; Ekblaw et al., 2016). Shared management of patient records ought to lead to greater control of personal records by the patient themselves (Sujansky et al., 2010; Wu et al., 2017; Sadiku et al., 2018).

The security of data held by providers is important where measures are required to detect and prevent intrusion (Omar et al., 2017). Often, it is inadequate standards that are applied to authentication methods that result in breaches, for example through poor access control policies (Dias et al., 2018), credential sharing, or weak passwords. To address these issues, Zhang et al. (2016b) propose two protocols for DLTs, one to improve IEEE 8.02.15.6 and establish secure links for mobile devices with unbalanced computational requirements, the other to distribute healthcare data among Pervasive Social Network (PSN) devices. Alternatively, making it more difficult to discern access control privileges with smart contracts Dagher et al. (2018) or with cryptographic signatures Xia et al. (2017b) may provide the same level of security but with less overhead. DLTs can also provide a decentralised and consensus-based approach to privacy, security measures, and patient data tracking (Dorri et al., 2017; Brodersen et al., 2016a; Han et al., 2018). Abouelmehdi et al. (2018) suggest data integrity is maintained when a decentralised architecture employed by DLTs, with no single point of failure and very high levels of redundancy, is deployed.

The blockchain's implied immutability means that once records are appended to the chain, they cannot be altered easily (Vimercati et al., 2007). While this presents advantages like the prevention of unauthorised changes, it also means that errors may be more difficult to correct in subsequent additions. In such a scenario, an error in data requires a new record to be appended and any interface that reads and reports on the DLT must be able to retrieve the latest entry. In this way, the usability of a HIMS plays a critical role in patient safety to minimise error rates. Factors to consider when improving HIMS include naturalness, consistency, error prevention, minimisation of cognitive load, interaction efficiencies, feedback mechanisms, effective use of language, and customisability or flexibility (Howe et al., 2018), thus giving caregivers, healthcare providers, clinicians, and technicians more time for individual patients (Alshamari, 2016). Additionally, instances exist where the quality or veracity of data may only be assured if there is third party notarisation on a smart contract, for example, when a biomedical database is queried, the enquirer may need assurance that the data are valid (Kleinaki et al., 2018).

The volume of data in HIMS across the range of health services is enormous, complex, and heterogeneous. Furthermore, the number of dependent and independent HIMS that are poorly integrated, the constant updates to existing data, inconsistent data representation and data structures, missing and incomplete data, and the difficulty in finding the required answers in large data sets returned from queries make knowledge discovery difficult and expensive (Hosseinkhah et al., 2009). DLT solutions are presented, for example, to provide an enterprise bus or as a searchable index (Gokalp, 2018; Zhang et al., 2017b; Jiang et al., 2018). In addition, applications around supply management and provenance tracking are mooted for DLTs and a special case for this is the tracking of drugs by using a chain of custody to trace where drugs have been (Sylim et al., 2018), and provenance tracking to trace counterfeit drugs that may have found their way into the supply chain (Bell et al., 2018). Another example of how accurate returns on queries facilitate knowledge acquisition from data is pandemic or epidemic identification by isolating, discovering, and driving change for environmental conditions that impact public health (Rabah, 2017).

Where patients pay directly for healthcare services and where insurance may be used to reimburse costs, the insurer needs assurance that costs are accurate and not inflated (Nardi et al., 2016). Incorrect billing is also a result of inconsistencies in recorded data, inaccuracies in patient medical histories, and patient information not shared with healthcare providers and stakeholders (Gokalp, 2018). DLT public ledger provides transparency and ensures accuracy in billing (Patel, 2018). Furthermore, if the patient can take ownership of their health record, then the patient should be able to exercise greater control over expenses and make decisions based on the financial impact of healthcare costs (Kaur et al., 2018). For example,Rabah (2017) argues that smart contracts can be applied to a patient's healthcare record as a means of alerting providers of treatments or tests that have already been undertaken or additional tests and treatments they may not be necessary. The table 3.1 on the following page shows that there is no such study propose for prescription issues and access management considering Maori and Non Maori people who are facing inequity problem in healthcare system . Most studies focused on security and privacy, access control of patients data, and authentication.

Table 3.1: Article summary (Blockchain based Projects)

Name of Project	**Author, Year**	**Purpose**	**Limitations**
MediBChain	Omar et al., 2019	Authentication based on activity, Other party data is inaccessible, Pseudonymity, Registration is required for participation	Interoperability concerns, Cryptofuel require for Smart Contract, Data recovery problems
Blockchain-based Architecture Framework for Secure Sharing of Personal Health Data	Amofa et al., 2018	punishment for violation, Data privacy, Policy improvement	Scalability concerns
Blockchain based monitoring for clinical trails	Zhuang et al., 2018	Real time monitoring, Encryption, Access control	Required permission to retrieve data, Data sharing problem between providers, Database required
Multi tier blockchain framework for IoT-EHRs systems	Badr et al., 2018	Pseudonymity, No key required for Iot devices	Vulnerable to attach, Privacy regulation, Integration concerns
Blockchain based Identity and Access Management	Mikula et al., 2018	Identity and access control , Patients approved records, Required registration	Problems with scalability

Continued over page/..

Name of Project	**Author, year**	**Purpose**	**Limitations**
Smart Contract for Secure Automated Remote patient Monitoring	Griggs et al., 2018	Access Control, Cloud storage for data, Blocks validating using signatures	Time limit for data transmission, Open channel communication, Nodes must be online for validation of blocks
MedicalChain	Abdullah, 2019	Unable communication among healthcare providers, Patients centred protocols, Two factor Authentication More privacy and security using double encryption	No control over tokens, Require currency
MedRec 2.0	Abdullah, 2018	Address of data link to Smart Contract, HIPPA satisfaction, Attack free, Vulnerabilities address using smart contract	Privacy and security concerns , Patients supposition, Scalability issues
Trusted Sharing Model for Patient Records based on Permissioned blockchain	Kim et al., 2017	Double encryption of data and server, Access control , Interoperability	Privacy preservation concerns and Regulation issues
Blockchain for Pharma Supply chain	Bocek et al., 2017	Improves Data Integrity Offline access of data, IoT devices use for data collection and tracking	Scalability concerns, Interoperability, Daniel of service, Forking
Peer-to-Peer EMR Storage	McFarlane et al., 2017	Control on Data Access, Real time Management, Security of storage	Tokens used, Purchase Storage, Incentives on Validation
Secure and trustable electronic medical records	Dubovitskaya et al., 2017b	Availability of Service, Double encryption, Patient control over data, Cloud storage	Data sharing problem with other providers, Uncategorised data

Continued over page/..

Name of Project	**Author, year**	**Purpose**	**Limitations**
Novel Privacy Risk Control healthcare system	Yue et al., 2016	Data Anonymization	Different type of data stored, During computation the data must be private and offline
MedRec 1.0	Azaria et al., 2016	The only implemented project in HIS, Fragmentation of data, Interoperability, Audit trails and Encryption	Scalability issues with project, Required mining, Security concerns

3.4 Technological Solutions Provided By DLTs

The first approach to the use of DLTs involves some variation of a financial or value-based transactional system (Peters et al., 2015), for example in order to secure transaction integrity, Noyes (2016a) described how to build a peer-to-peer financial multiparty computation market. Whether DLTs influence will be significant is open to discussion, and it is questionable whether the hype will outlast the energy required to make the promise a reality. However, Microsoft and IBM have committed significant investment into the development of platforms for designing and building apps on DLTs (Cengiz, 2018; Microsoft, 2019). Investment trading platforms provide opportunities for fraud but, the public ledger provides opportunities to develop apps to resolve risk management issues and reduce the cost of auditing where blockchain provides a basis for speedier verifiable data retrieval, improving decision making in areas such as share trading (Pilkington, 2016; Morini, 2016).

Apart from financial systems, Internet-based applications are moving towards decentralisation and the deployment of microservices. Areas such as e-health, the maritime industry, logistics management, Radio Frequency Identification integration, smart grids, smart homes, and many more developments have emerged (Atzori et al., 2010; Miorandi et al., 2012). These approaches provide an avenue for the adoption of new business models, such as Distributed Autonomous Corporations (DACs) with decentralised transaction processing in which participants are motivated to interact with sensors and from the sharing of data, earn income from cryptocurrency coin distribution (Zhang et al., 2015). However, the decentralised environment creates a complex set of security and privacy problems and to address this (Hardjono et al., 2016) propose a method of proof of manufacturer as a means of providing privacy on IoT devices. Further privacy measures can be designed with DLT in identity services, and supply chain and device management Jaag et al. (2017).

DLTs are also being used for rewards-based loyalty schemes where customers earn cryptocurrency coins for performing specific tasks. For example,Gogerty et al. (2011) describe a cryptocurrency, Solarcoin, from which households earn by contributing electricity to a grid by producing electricity using solar panels. In another example, cryptocurrency coins are suggested as a reward system for students that complete learning tasks (Devine, 2015), however, such a system opposes accepted pedagogical practice and as such, is unlikely to be adopted on any scale.

Cryptocurrencies have their genesis in the domain of libertarians and so issues that relate to the inhibition of personal expression and activity have found solutions in DLTs. For example, Namecoin provides a platform for censorship resistance, decentralisation of Transport Layer Security TLS (HyperText Transfer Protocol Secure HTTPS) certificate validation, and seeks to provide applications for voting, and notary verification (Kraft et al., 2019), the use of DLTs in other social functions such as marriage registration, income taxation systems, and patent management have been proposed and some effort has been made toward achieving these goals (Akins et al., 2014), albeit with limited success. In addition, reputation is important for organisations and individuals and is easily lost, thus the proliferation of social media-based feedback systems, from Google and Facebook to Trip Advisor has become important to grow and reinforce reputation. However, such systems present weaknesses such as the motivation of the poster, false/misleading postings, or troll activity. To provide motivation, a rewards-based approach may encourage greater participation (Carboni, 2015). Such an approach provides a transparent record that is difficult to alter or falsify, and incorporates an identity verification system. As we are all too aware, academic integrity is tied to reputation and Sharples et al. (2016) propose an educational record and reputation system that rewards researchers and provides a means for verifying the authenticity and the sources of research data.

The use of DLTs in the verification of identity is extended to the actualisation of property rights without recourse to legal means (Ishmaev, 2017). The principle is that data are stored on the blockchain and records are verified as part of the mining process. However, such a system relies on trust that the data are correct and that errors or omissions are rectified before they are committed to the chain. Presently, most attempts at developing this type of solution have been met with failure, from the implementation of the system to acceptance by the parties involved. Personal privacy is also a concern, not just for those that are libertarian. In the US, a lasses fair approach to the collection and ownership of personal data has led to a proliferation of large repositories from which personal information is traded. Other jurisdictions have seen this spread as a problem and sought to limit the scope of the collection, for example, Europe's GDPR. Zyskind et al. (2015) suggest a technological solution through a decentralised personal data management system that provides authentication of data ownership.

In another instance in which data are proposed to be stored on a blockchain for security, Noyes (2016a) stores various signatures to enhance fault tolerance and the reliability and trustworthiness of security infrastructures. Given the processing overhead required to update and search virus databases, a rapid and community-based method for finding matched signatures may be useful but the added processing power required to validate the entry of data onto a blockchain may negate any advantages. DLT solutions designed to verify authenticity and provenance appear to present more successful outcomes than most. Supply chain management is an area that is complex and verifying product sources, stock movement, and package destinations are difficult and provide opportunities for DLTs.

Lu et al. (2017) gives an example of product traceability in China. However, such systems must integrate with existing current and legacy systems, where the system must be transparent and tamper-proof, be updatable, and decisions need to be made about what will be stored on the blockchain. Food products provide a special case for the use of this type of system, ensuring products are fresh, have been properly handled, meet local import standards to reduce issues of food-borne illness, and reduction of fraud and falsified data (Ahmed et al., 2017).

3.5 Blockchain Based Incentivisation

This section presents studies that propose incentive mechanisms and schemes for different applications. In a reputation-based system, each user is assigned a score that reflects their likelihood of behaving honestly. This score can identify misbehaving users by others in the network (Mousa et al., 2015; Pouryazdan et al., 2017; Kantarci et al., 2015; He, Wu & Khosla, 2006). For example, a user may use a "watchdog" to monitor their peers' behavior. If any misbehavior is detected, the user can broadcast the uncooperative reputation of that peer to others in the network (He et al., 2006). Some reputation systems also use a combination of centralised evaluations and collaborative reputation values based on votes (Zhong et al., 2003). However, reputation systems can also have drawbacks such as lack of formal specification and analysis of incentives, potential for selfish users to collude, and vulnerability to Sybil and whitewashing attacks (Feldman et al., 2006).

By exchanging services based on their prior contributions, barter-based schemes like Tit-for-Tat (Buttyan et al., 2007; Rahimzadeh et al., 2017; Lee et al., 2015) encourage mobile users to collaborate. These incentives have been suggested as a mechanism for DTNs and to prevent free-riding in video streaming applications in studies like (Buttyan et al., 2007) and (Rahimzadeh et al., 2017) . These schemes are constrained, though, in that they can only be used in applications with lengthy sessions and might not be able to satisfy the various service requirements of users (Ning et al., 2011).

In Credit-based systems, such as those proposed by(Zhong et al., 2003; Zhang et al., 2016a; B. B. Chen & Chan, 2010; Wang et al., 2016), a central authority assigns virtual money to each user. When a user needs help from others, they must pay a certain amount of virtual money to the helper. However, as the payments are based on user reports, selfish users may attempt to cheat the system to maximise their benefits. Efforts have been made to counteract such cheating behaviors, such as the cheat-proof credit-based system proposed by (Zhong et al., 2003) and the use of pricing strategies in game theory frameworks by (Felegyhazi et al., 2006) and (Zhang et al., 2016a). These schemes, however, assume that the routing path is determined prior to data transmission, making it difficult to predict who will be rewarded and how much will be paid. Other credit-based schemes of interest include those proposed by (Zhu et al., 2008) and (B. B. Chen & Chan, 2010). A layered incentive scheme for dynamic routing in DTNs was proposed by (Zhu et al., 2008) . To generate new layers, the sender generates a base-layer message containing the payment policy, and intermediate nodes append a non-forged digital signature. According to the payment policy, these messages are sent to a trusted center for validation and payment assignment.

The proposed mechanism in this study focuses on generating and verifying secure layered messages but needs to include a detailed pricing strategy. Other credit-based incentive schemes, such as those proposed by (B. B. Chen & Chan, 2010) and (Bogliolo et al., 2012), have emphasized pricing strategies to prevent selfish actions from resulting in more significant rewards. However, these schemes rely on central trusted authorities that do not exist in P2P applications and have yet to propose a secure virtual digital currency system. This study aims to propose a blockchain-based incentive mechanism/protocol to encourage underserved communities to participate in and use the healthcare system and be rewarded for their services. However, the study already formulated research questions related problems identified in Chapter 2 on page 11, section 3.5. In reference to chapter 3, this Chapter formulated questions and hypotheses in context of technological solution to the problems identified in Chapter 2.

RQ3 How can unequal access and inequality be solved through Blockchain technology?

(a) How can Blockchain technology be applied to engage patients with PMS?

(b) How can Blockchain technology be applied to build patients' trust?

(c) How can Blockchain technology be applied to mitigate inequalities and ensure the participation of patients in PMS?

RQ4 How specifically to build a Blockchain-Based incentive mechanism to mitigate unequal access and inequalities in PMS?

RQ5 How the proposed system will be evaluated.

H5 The proposed Blockchain based framework reduces prescription errors and inequality in the healthcare system.

H6 The Proposed incentive mechanism increases engagement and participation in PMS, improving healthcare outcomes and better patient experiences.

H7 By providing equal access to Maori and Pasifika, the proposed PMS system enhances the level of trust in the system

3.6 Theoretical Model of the Study

According to Maxwell (2005), a theoretical model is used in research to specify the relationship between concepts and theories from the literature review. It also helps to guide the research direction by defining the research problem and allowing the researcher to generalise and interpret the research idea in order to approach a feasible solution. The theoretical model also highlights key variables and examines their relationship by formulating research questions and hypotheses (Trochim, 2006). In this research, the model's focus in Figure 3.1 on the next page is on the inequality in access to PMS and the associated problems. It examines the disengagement of patients from the system due to trust and the cost of healthcare services, and how patients' perceptions of inequality in the healthcare system contribute to health disparities among Maori and non-Maori in PMS.

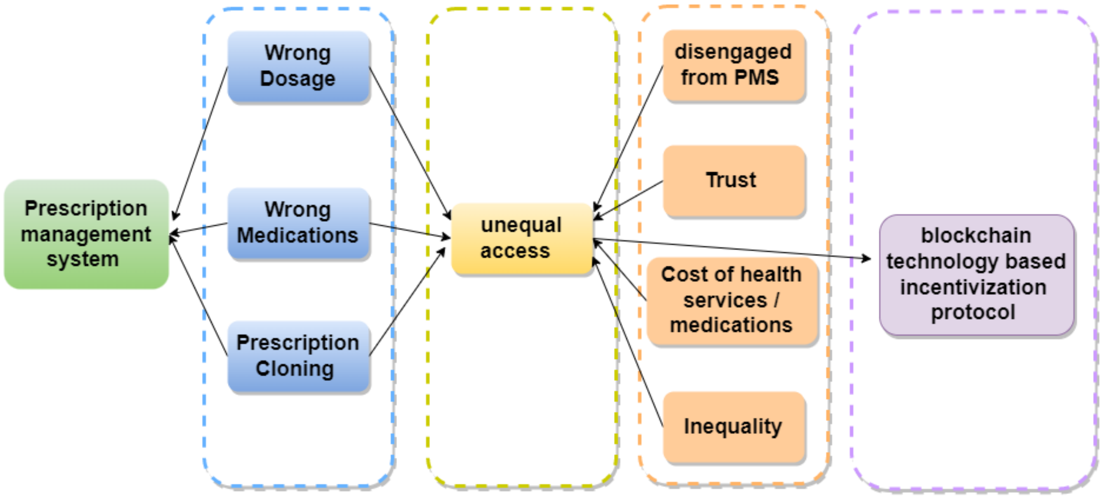


Figure 3.1: Theoretical Model

3.7 Conclusion

In conclusion, Chapter 3 examines literature related to blockchain technology and its potential to address unequal access and inequality issues in Prescription Management Systems (PMS). The studies reviewed discuss various protocols, schemes, frameworks, and security models, primarily focusing on security and privacy. However, few studies specifically address the issue of unequal access and inequality in healthcare and PMS. The study aims to propose an incentive mechanism to encourage participation, sharing, and trust in the PMS using blockchain technology. The literature suggests that blockchain technology can minimise problems related to unequal access and inequality in healthcare and PMS. Research questions have been formulated in the context of blockchain technology and the proposed incentive mechanism for the thesis.

- Chapter Preliminaries.

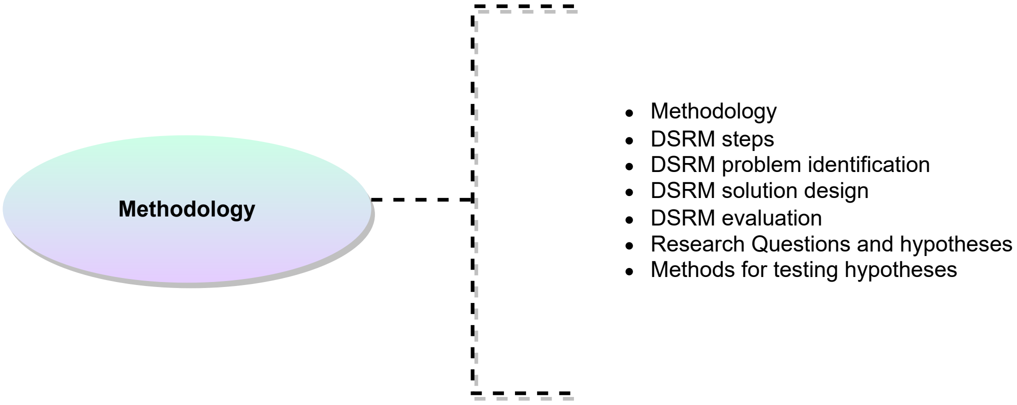
- Blockchain Layers.
- Blockchain in healthcare.
- Technological solution provided by the blockchain. Technology.
- Blockchain-based incentive mechanism.
- Research Question in the Context of BC.
- Theoretical model of the study.

Chapter 3 provides a background on the potential of blockchain technology in healthcare. In chapter 4, methods will be developed based on the research questions formulated in chapter 3.

Chapter 4

Research Methodology

4.1 Introduction



In Chapter 2, an SLR is presented and explains the significance of the theoretical framework for a HIS by focusing on the prescription management system and its related issues. It further defines different challenges in PMS, namely unequal access, inequalities, and engagement of the under-served communities. Chapter 3 presented blockchain technology architecture and its uses for the HIS solutions. Further, it also reviewed blockchain based studies and prevalent incentive mechanisms. Thus, the research questions were formulated for blockchain technology solutions for ways through which unequal access, inequalities and disengagement of under-served communities can be investigated. Chapter 4 provides an overview of the design of the study, including the research framework, and methodology adopted to guide the process steps. It reiterates the research questions and hypotheses derived in Chapters 2 and 3, and elaborates the decisions made to make the research functional, and achievable. The Design Science Research Methodology (DSRM) is adopted and customised for high-level process guidance and a consistent reference framework. In this way the research is systematic and follows the learning from many other researchers on how to build and make innovations through technology applications. Specific methods used to test the hypotheses are defined, including the mapping of methods to specific hypotheses where some hypotheses require more than one method for testing. Evaluation methods are also elaborated to fill specific operational gaps in the high-level DSRM.

The organisation of this chapter includes a presentation of the chosen methodology and research process in Section 4.2 the question and hypotheses in Section 4.3.3, and the correlation between questions, hypotheses, and methods in Section 4.4.

4.2 Methodology

The research methodology used in this study is called DSR, which stands for "Design Science Research." DSR is a methodology that provides a structured approach to identifying a research problem and then designing an artifact or solution to that problem. This process is effective and it has been used in many research studies in the past. The DSRM also involves evaluating the design and presenting the results. DSRM is considered as a solution-oriented methodology, which means it focuses on creating solutions to problems. Additionally, it contains a rational decision cycle which is a process used to answer knowledge questions. This methodology is supported by many research studies and is widely accepted and followed in the research community. Examples of research studies that have used DSR include those by (Furda et al., 2019; Wieringa et al., 2012; Walls et al., 2004; Markus et al., 2002), DSR is widely acknowledged and utilised as a research methodology in various prominent research domains. The authors highlight numerous communities of practice that are dedicated to DSR, which include the Association for Information Systems (AIS),Design Research Society, Design Special Interest Group (SIGSAND), AIS Systems Analysis and Information Science Institute (ISI). Additionally, they also mention several research centers and laboratories that focuses on DSR, such as the Center for Design Research at Stanford University, UT Institute of Design at Illinois Institute of Technology, and ISEing-Information Systems Evaluation and Integration Group at Brunel University. The study plans to design and develop a framework using DSR (as depicted in Figure 4.1) to address a research problem. DSR helps to expand human and organisational capabilities through the creation of new and innovative Artifacts (Dresch et al., 2015). The DSR process is divided into three phases: problem identification, solution design, and evaluation. The research process starts by identifying a problem and then designing and proposing a blockchain-based solution. Once the solution is proposed, then the proposed solution is evaluated. Every action taken is followed by an evaluation to determine its effectiveness, and the results of this evaluation can lead to progress in the next stage or a return to the previous stage for improvement (Peffers et al., 2007; Hevner et al., 2010; Venable et al., 2012).

In this research, the following mechanisms are used to evaluate the design processes:

- In section 4.2.1.2.2, the researcher employed formal methods to assess the incentive mechanism of the BlockPres Artifact. Formal methods employ cryptographic techniques to ensure the protection of information and communication between patients and healthcare providers, as well as the patient wallet where tokens are stored. Additionally, consensus approaches utilising blockchain technology are employed to guarantee transparency, immutability, and trust.

- Model-based testing is used to assess both the functional and non-functional behavior of the system. This approach ensures the reliability and robustness of the system.
- In Chapter 7, the study developed the BlockPres Prototype, which employed the Ethereum blockchain and rosbsten network to implement the framework. The prototype is presented in Section A.
- Quantitative approaches were utilised to evaluate the data collected from the BlockPres prototype. In BlockPres, the researcher created several accounts for patients, hospitals, GPs, and pharmacies to test the artifact's usability. Statistical methods such as standard error, straight line fit, and R-square were utilised to calculate different variations. However, the study still needs to evaluate BlockPres' usability by gathering feedback from experts, which will be included in future work.

In scientific research projects, methods are tailored to the specific project requirements. One potential starting point for creating a set of procedures for design science in information systems is the method used in design research. The issue addressed in Section 2.3 on page 39 is the lack of equal access, inequality in prescription management systems, and disengagement of under-served communities. The proposed solution is a blockchain-based prescription management system framework and incentive mechanism to address these issues and promote engagement and participation of under-served communities. Furthermore, Hevner et al. (2010) discusses the following guidelines in table 4.1 on page 85. In this research, these steps are used to propose a blockchain based solution to mitigate inequality and improve engagement and participation in the HIS.

- Chapter 2 presents the problem identification process, which identifies specific problems within the context of DSRM.

- The second phase of the DSR methodology is to produce an artifact, and in Chapter 5, the study proposes the BlockPres artifact.
- The proposed artifact is designed to address the inequality problem in the PMS and improve engagement and participation among Maori and Pasifika communities. For this reason, the study proposes an incentive mechanism.
- The proposed artifact is evaluated against the research questions and hypotheses formulated in Chapter 2. The testing results of the developed prototype demonstrate its effectiveness and usefulness in record management and building patient trust.
- The study contributes to the body of knowledge by publishing journal and conference papers.

  The study followed the DSRM guidelines of (Hevner et al., 2010) and customised it to the context of this research as discussed above.

Problem identification	A specific problem must be identified in order to provide a solution through the creation of an artifact.
Artifact Design	The research must produce a functional artifact.
The significance of the artifact in relation to the issue to the Problem	The goal of the research is to create an artifact that can effectively solve the problem at hand
Evaluation of the Artifact.	The proposed artifact must be evaluated, proven through testing, and justified in its effectiveness. The artifact should demonstrate usefulness.
Research Contributions	The research must make a distinct and meaningful addition to existing knowledge in the field.
Research Rigour	The solution artifact should be developed and evaluated using thorough and systematic methods.
Communicating the Research Results	The design science research should be communicated clearly and effectively to both technical and business-focused audiences.

Table 4.1: DSRM Guidelines
Hevner et al. (2010)

Chapter 4 introduces a methodology for designing a research study in the field of Health Information Systems (HIS) utilising a chosen method of information systems. The methodology includes a series of steps that can be followed for a successful outcome.

4.2.1 DSRM Steps

The initial phase of the research methodology for designing a HIS (Health Information System) is to identify a problem area and establish the objectives of the study. This phase includes several steps such as problem identification, literature review, and pre-evaluation of relevance. The literature review is conducted using the PRISMA method, as detailed in Section 2.1 on page 15, which reveals various issues highlighted in Section 2.5.5 on page 38. The study focused on the problems faced by the prescription Management System (PMS), and these problems are identified through a Systematic literature review. This study's main focus is to address unequal access in PMS to

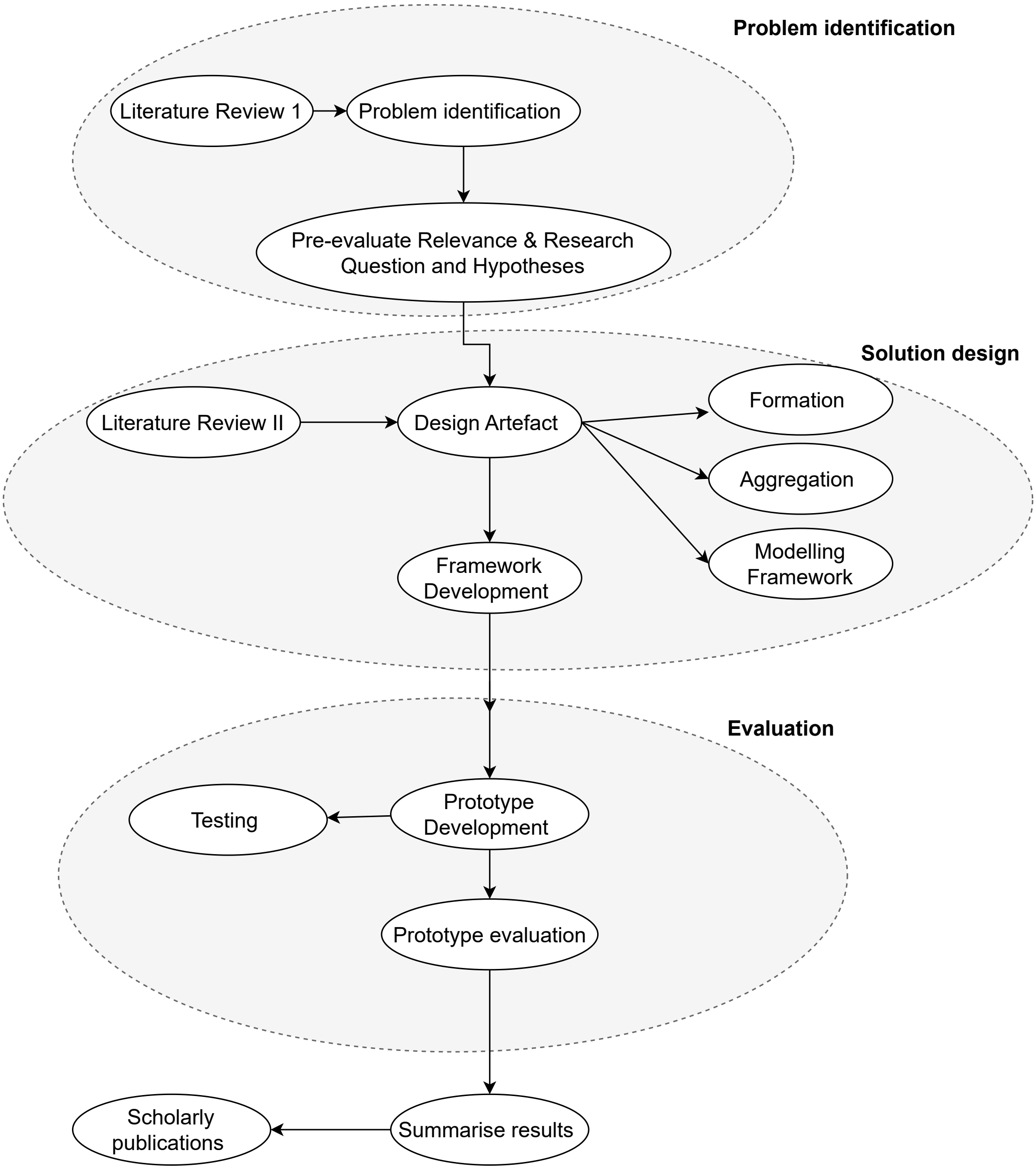


Figure 4.1: Design Science Research Methodology

underserved communities. These communities have a distrustful perception of the healthcare system due to existing inequalities, leading to their disengagement. The key points of the problem statement are:

- According to research by Graham et al. (2020); Gilmour et al. (2016) , underserved communities perceive the healthcare system as mistreating them or providing unequal access to healthcare services, which leads to a decrease in trust towards Patient Management Systems (PMS). These communities often experience inequalities in the treatment they receive from healthcare professionals, such as differences in body language, facial expressions, and mispronounced names. Additionally, during the COVID-19 outbreak in New Zealand, underserved communities, particularly Maori and Pasifika, had poorer access to the healthcare system in terms of vaccination policies, and were among the highest unvaccinated communities (Steyn et al., 2021). These types of inequalities lead to disengagement from the healthcare system and negatively impact their health and well-being. Key points are:
- The underserved community may become disengaged due to their low income, which makes it difficult for them to pay for most prescriptions.
- Most District Health Boards (DHBs) have different systems in place and patient records are not centralised, creating problems for the underserved community as they have to repeat treatments and feel disengaged.

Currently, the New Zealand Patient Management System (PMS) is centralised across all DHBs, but each DHB operates its own information system, which leads to incomplete information sharing and further disengagement among the underserved communities.

A technological solution is required to address the aforementioned problems. The following sections discuss blockchain technology as a solution to these problems. The RQs and hypotheses are formulated in chapters 2 and 3 of the literature review and presented in Section 4.3. The research gap mapping also identifies the limitations and the proposed solution.

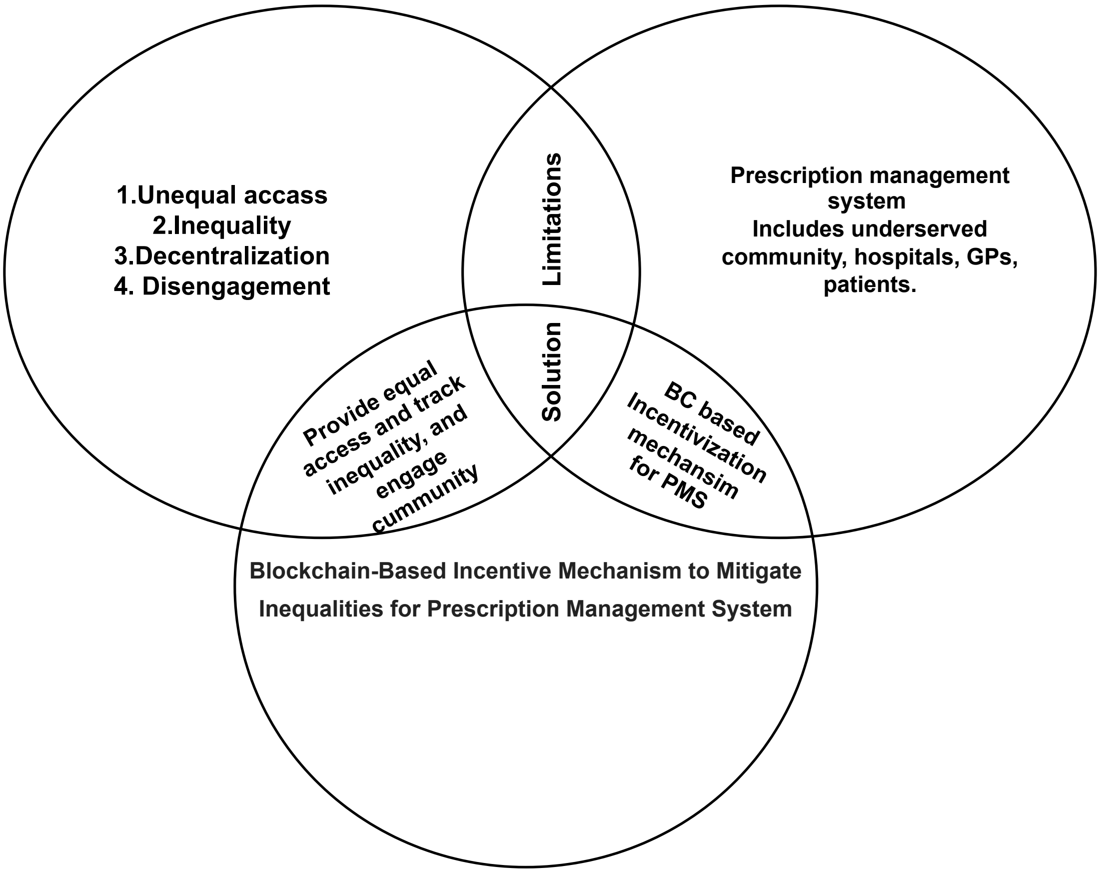


Figure 4.2: Research Gap Mapping

4.2.1.1 DSRM-Solution Design

The second phase of the DSR process deals with solution design, which is divided into two steps: Artifact design and relevant literature review. The literature review step in this phase is different from the one conducted during the problem identification phase of the research process. In phase 2, the focus is on relevant scientific articles to understand the proposed solution for the problem identified in the literature review and the work that has been done related to the proposed solution. This entry point aims to support the design of the Artifact, which is documented in the literature review and implemented in the methodology section to ensure that the design solution achieves the research objective. The resultant Artifact is a novel blockchain-based Incentive mechanism to mitigate unequal access or inequality in the Patient Management System (PMS). To design and build a solution, the study first designs a framework, secondly proposes the concept of an incentive mechanism, and then develops a blockchain-based decentralised application. The blockchain development process follows the DSR methodology and consists of the following sub-sub-section steps:

4.2.1.1.1 Blockchain Ideation: The primary objective of this step is to design a high-level framework for blockchain-based systems and how all the stakeholders and components interact within the framework. Figure 4.3 illustrates a comprehensive view of the proposed framework. This section describes the process of making the framework. Firstly, when a new patient visits a hospital or GP for treatment, the healthcare provider registers the patient's information in the healthcare system. The patient is then assigned to a specific doctor for a check-up. At the same time, the patient receives instant incentives in the form of tokens in their wallet for registration, which improves patient engagement and can be used to acquire things. Secondly, if patients experience any unfair behavior from healthcare providers such as lack of attention, delayed treatment, or neglect, they can use blockchain to sign a smart contract called a Fair Contract with healthcare providers before receiving health treatment and prescriptions. The purpose of this contract is to prevent inequality, unethical treatment, or discrimination. Additionally, the contract will be signed using an API when accessing a patient's profile or entering a patient's details immediately after assigning a doctor or nurse to the patient. The rules for this contract are discussed under the Fair Contract section

In the second scenario, if patients experience mistreatment or misbehavior, they can use an API to report the situation to the blockchain network through a Smart Contract. A verification layer will verify the patient's identity. The complaint will be broadcaste to all members, such as the hospital, GPs, District Health Boards (DHBs), and the Ministry of Health in the blockchain network through the Smart Contract. Then, the Ministry of Health can analyse the complaint using a verification layer and the smart

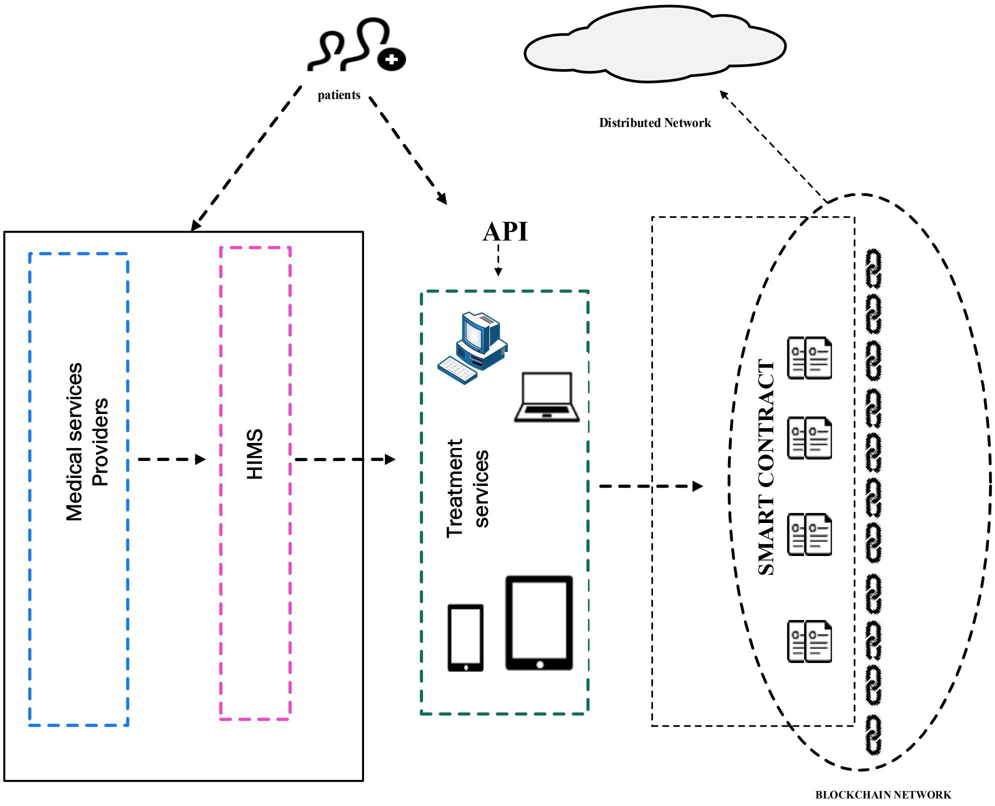


Figure 4.3: Holistic view of Proposed Framework

contract on blockchain technology to examine the patient and healthcare provider's history. The history will be examined to check if the patient or healthcare provider faces any abnormalities or issues or if any past incident between both parties led to this complaint. In addition, patients can trace and track their appointment time and duration of treatment and later provide a review regarding the experience or treatment they received. Patients will have full access to the system and can access records. The third scenario is that the healthcare system is disengaged, and multiple systems run in different DHBs, which causes problems. Blockchain technology makes the record decentralised and available to all healthcare providers under one system.

4.2.1.1.2 Technical Proof of Concept: Framework Evaluation: This step aims to design an incentive mechanism, create a laboratory prototype based on the Framework designed in the solution design section of the DSR process, and conduct a pilot test using dummy healthcare data. Additionally, the study included stakeholders and experts to gather feedback on the prototype design and its potential usefulness in the healthcare system.

4.2.1.2 DSRM-Evaluation

The DSRM framework proposed by Pries-Heje et al. (2008) is utilised to evaluate the proposed research. An ex-post evaluation approach is adopted for this study, which involves testing the artifact in an artificial simulation environment. Several researchers validate this approach in their studies, including (Pries-Heje et al., 2008; Venable, 2006; Venable et al., 2012) and (Walls et al., 2004). As this approach is employed after the design and development of the artifact, the evaluation is conducted in chapter 7. Dummy accounts are created in order to test the artifact. The logical simulation of the model and the use of formal methods for framework validation in the form of an incentive mechanism presented in Chapter 4, assure consistency in the approach. According to March et al. (1995); Hevner et al. (2010) and Hevner et al. (2010), the Framework and methods proposed during research are classified as artifacts. In the field of Design Science Research (DSR), both models and methods are recognized as types of artifacts, as established by (Aken, 2004) and (Kotzé et al., 2015). In Design Science Research, artifacts refer to the tangible outputs of the research process designed and created to address a particular problem or challenge. Different types of artifacts can be created in Design Science Research, including the examples in the following sub-sub-sections:

4.2.1.2.1 Types of Artifacts : According to Kotzé et al. (2015), the outcome of DSR is the Proposed artifact. However, Kotzé et al. (2015) have identified various categories of artifacts.

- Prototype: The development of the prototype is based on the Framework designed for the study.
- Methods: Artifacts related to developing algorithms and practices to solve the problem.
- Models: These artifacts consist of statements or propositions employed to clarify a group of constructs to address the research problem.
- Constructs: The construction of symbols, concepts, and syntax are presented in a specified way to produce an artifact and incorporate the problem.
- Framework : A framework is an interconnected set of models and methods that are used to develop and evaluate solutions for a particular problem. The framework provides a design that directs the development of the artifact and ensures that the solution is effective and meets the desired requirements. A framework can be used to develop various Artifacts, including software systems, algorithms, and practices.

4.2.1.2.2 Formal Modelling : The formal methods are used to evaluate the proposed Framework within the context of Design science research methodology. Formal methods are utilised as a validation tool to ensure the correctness and reliability of a system. The formal methods are used to analyse system behavior by applying mathematical techniques. This process allows for finding potential errors and flaws in the design. By using formal methods to validate the system, the researcher needs to evaluate the system against the evidence and check whether the system behaves as intended and is free of errors that can lead to failures.

Easterbrook et al. (1998) adopted formal methods to design spacecraft fault protection systems. This approach is beneficial in safety-critical applications, such as aerospace and healthcare, where the consequences of system failure can be severe (Clarke et al., 1981; Queille et al., 1982) (Kripke, 2007). In this study, different types of formal methods are used to evaluate the Framework.

4.2.1.2.2.1 Cryptographic Techniques: Cryptographic techniques are the core of blockchain technology and have four objectives: confidentiality, integrity, authentication and authorisation, and non-repudiation. As per Omar et al. (2017), encryption techniques protect information and communication from unauthorised access. Additionally, a digital signature prevents user data and information from being spoofed or forged. According to Benkaouz et al. (2015), user data and information integrity is guaranteed through a cryptographic technique known as hash functions. The techniques are an integral part of blockchain technology and are discussed in the next section.

4.2.1.2.2.2 Consensus Approaches: This section of the study discusses the use of blockchain technology as a decentralised network of nodes that provides transparency, security, trust, privacy, and immutability. According to Ali et al. (2017), no central authority controls or validates transactions. Alharby et al. (2018) states that consensus protocols validate and verify all transactions and decentralise the technology. In blockchain technology, a consensus algorithm is a mechanism that allows nodes in a distributed network to agree on the state of the ledger even in the presence of faulty or malicious nodes. A consensus algorithm's primary goal is to ensure that all network nodes have a consistent view of the ledger and that any new transactions added to the ledger are valid and agreed upon by the network. (Ali et al., 2017; Noyes, 2016b).

Proof of work is a popular consensus algorithm in blockchain technology, and it is used by the Bitcoin blockchain. Nodes in a PoW system compete to solve a complex mathematical puzzle. The first node to solve the puzzle receives newly minted cryptocurrency as well as the ability to add a new block of transactions to the blockchain.

Once the block has been added to the network, other nodes must validate it to ensure that it follows the system rules and that the transactions contained in the block are valid. (Mingxiao et al., 2017; Bhardwaj et al., 2020).

Proof-of-Stake (PoS) is a consensus algorithm used by Ethereum and other blockchain networks. In a Proof of Stake consensus algorithm, nodes holding a certain amount of cryptocurrency are selected to validate transactions and generate new blocks based on their network stake. This technique is frequently regarded as more energy-efficient than PoW because it does not require the same amount of computational power to solve mathematical puzzles (Lepore et al., 2020). Additionally, the study proposes a BlockPres incentive mechanism to build equality, and trust, provide incentives, and ensure engagement and participation. The BlockPres incentive mechanism is discussed to overcome inequality, unequal access, and disengagement of an Underserved Community.

4.2.1.2.3 Model Based Testing : Model-Based Testing (MBT) is a system testing methodology that involves generating and executing test cases based on models of the system being tested. The main idea behind MBT is that you can test the system's behavior more systematically and comprehensively by creating system models. MBT tests different systems' functional and nonfunctional behavior and evaluates their performance. It also ensures that the system works as per requirements and is reliable and robust. (Krichen et al., 2004, 2006a, 2006b).

4.2.1.2.4 Quantitative Approach : The quantitative approach uses statistical methods to analyse participant data using structured tools like questionnaires. This approach aims to find correlations between variables and establish relationships between them in a population. Numeric data is gathered and employed to comprehend the social significance. However, proposed research in the information system field does not involve participants and instead focuses on developing a framework and mechanism as Artifacts, and evaluating the validity of these artifacts. The research uses statistical methods to evaluate the results, such as Standard Error, straight line fit, and R-square, to calculate transaction variation (Creswell et al., 2017; Dixon-Woods et al., 2005).

4.3 Research Question(s)

This section presents research questions formulated based on the literature review in Chapter 2 and Chapter 3, along with hypotheses based on a theoretical model. The literature review uses the PRISMA method in Section 2.1 to identify issues in HIS (Gagnon et al., 2015). The study identified challenges such as inequality, lack of access to PMS, and disengagement of an underserved community. The following are the research questions formulated based on these challenges.

RQ1 What issues exist within current prescription practices?

  (a) How do prescription issues manifest?
  (b) What are the current practices to counter these issues?
  (c) Are current practices effective in HIS?

RQ2 What are the reasons for unequal access to Maori in PMS?

  (a) Are current PMS accessible and engageable to Māori and Pasifika?
  (b) Are Maori and Pasifika trusting the current PMS?

RQ3 How can unequal access, distrust, and disengagement be solved through blockchain technology?

  (a) How can blockchain technology be applied to engage patients with PMS?
  (b) How can blockchain technology be applied to build patients' trust?

  (c) How can blockchain technology be applied to mitigate inequalities in PMS?

RQ4 How specifically to build a blockchain-based incentive mechanism to mitigate unequal access and inequalities in PMS?

  (a) How the proposed system will be evaluated?

4.3.1 Hypotheses

At this stage, six hypotheses are constructed to address the questions.

H1 The current practices of prescriptions in HIS are not effective and efficient for the Underserved Community compared to other communities.

H2 Unequal access to PMS contributes to a higher incidence of prescription problems.

H3 Inequalities in PMS with the Underserved Community make the system untrustful and lead to disengagement from the system.

H4 The cost of healthcare services and prescriptions leads to disengagement from the healthcare system.

H5 The proposed system for PMS provides equal access to an Underserved Community and increases the trust factor in the system.

H6 Using the proposed incentive mechanism, the participation, and engagement of the Underserved Community can be increased, enhancing the trust level in the prescription system.

H7 The proposed Framework is usable in the prescription system and can be used in practice.

H8 The prototype is more productive and user-friendly for patients and healthcare providers.

The hypotheses presented above will be tested using various methods discussed in the next section 4.3.2. The questions and hypotheses are all related to the main problem identified in the literature review. Studies and evidence suggest that unequal access, inequality, and disengagement caused by trust levels make the prescription system vulnerable for the under-served community. The development and testing of the proposed blockchain-based incentive framework, according to the formulated hypotheses, can help assess the redress of these issues.

4.3.2 Methods for Testing Hypotheses

This section presents methods for testing the hypotheses which fit the research methodology's context. The methods listed below are designed as approaches for testing the hypotheses. The following methods are proposed for testing the hypotheses in the context of the research methodology:

- **M1 :** Explore the current prescription practices in HIS using SLR.
- **M2:** Developing a framework to improve PMS using the DSR approach principles, including formal methods.
- **M3:** Explore consensus algorithms to suit the scenario best and perform better in healthcare.
- **M4:** Explore different incentive mechanisms and propose an incentive mechanism to minimise PMS issues within the DSR principles.
- **M5:** Explore approaches to develop Proof of Concept in the form of Decentralised Application within the support of M2, M3, M4, and within the context of DSR.
- **M6:** Explores different standard quantitative approaches to evaluate the prototype and get feedback from the relevant and industry people.

4.3.2.1 Method 1

Method 1 (M1) involves conducting secondary research in the form of a literature review using the SLR and PRISMA methodologies. This involves referring to external sources, particularly peer-reviewed journals and conference papers that discuss Blockchain in Healthcare, as well as related issues such as inequality, unequal access, trust, and disengagement within the PMS system. Recent articles are also considered to stay updated on current inequality and unequal access issues. This study aims to comprehend the essence of the existing problem, establish the problem domain, and create a classification system. The literature review is conducted from a concept oriented perspective rather than an author-centric one, as suggested by (Webster et al., 2002). This method examines current prescription practices and the challenges faced by the underserved communities in the prescription system. Additionally, this method tests hypotheses H1, H2, H3, and H4 within the principles of SLR and DSR.

4.3.2.2 Method 2

M2 is a method for defining the conceptual structure and specifications of a blockchain based prescription management framework. As a result, a conceptual overview of the framework is validated at a high level, which is subsequently verified utilising the formal techniques of POW and POS. Other cryptographic techniques like Zeroknowledge Proof and digital signature are also used to evaluate the framework's security and efficiency in terms of cost and speed. The framework is then compared to an incentive mechanism approach.

4.3.2.3 Method 3

The proposed incentive mechanism is developed in this method. M3 addresses the processing details of the blockchain-based prescription management framework and how the incentive mechanism functions within the framework. It also examines how the incentive mechanism can benefit under-served communities by promoting patient participation and engagement. Algorithms are developed to demonstrate the framework and incentive mechanism's processing approaches, and the steps are illustrated using a flowchart.

4.3.2.4 Method 4

Method 4 builds on the approaches presented in Method 3 but specifically focuses on how a blockchain-based incentive mechanism can develop a decentralised application (DApp) that provides access and equality in secure communication and storage of information using IPFS (InterPlanetary File System) through blockchain. IPFS offers a secure environment for storing patient data and providing access.

4.3.2.5 Method 5

M5 is focused on creating a proof of concept (PoC) for the blockchain-based prescription management system (PMS). This method incorporates a sample application and algorithms into the PMS architecture. Subsequently, the system's computational feasibility is evaluated by utilising formal methods. A logical simulation of the framework is also included in this approach. Additionally, a prototype will be developed as part of the evaluation and PoC.

4.3.2.6 Method 6

This method involves evaluating the framework and incentive mechanism through expert feedback. A standard quantitative model is used to gather information from experts, either through a questionnaire or interview.

4.3.3 Relationship Between Research Questions, Hypotheses, and Methods: Mapping

Methods are developed in section 4.3.2 on page 97 for testing hypotheses that are formulated to address research questions. These three elements are interrelated, and their relationships and dependencies are mapped and presented in Figure 4.3.3. The map shows how four hypotheses are used to investigate three research questions and how five methods are used to test the hypotheses. It also depicts the connections between the hypotheses and research questions, as well as the methods used to test each hypothesis. The research process includes two methodological approaches: DSR (Design Science Research) and Formal Methods.

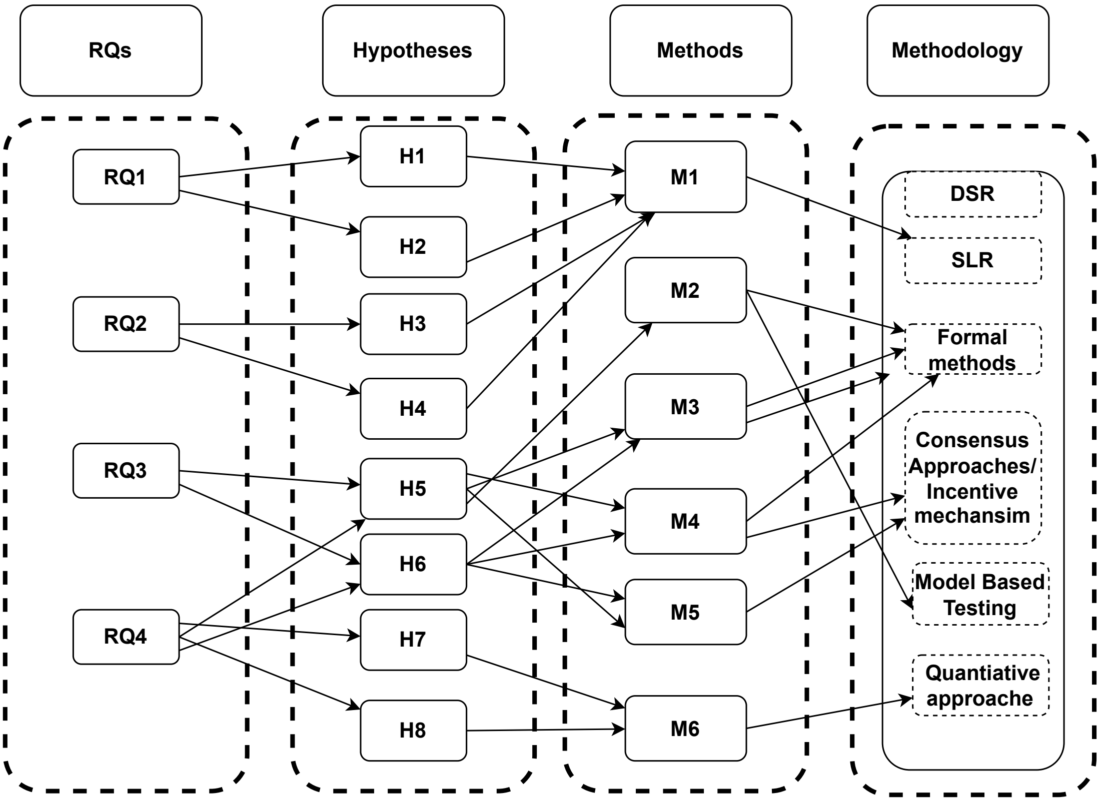


Figure 4.4: Relationship Between Research Questions, hypotheses, and Methods

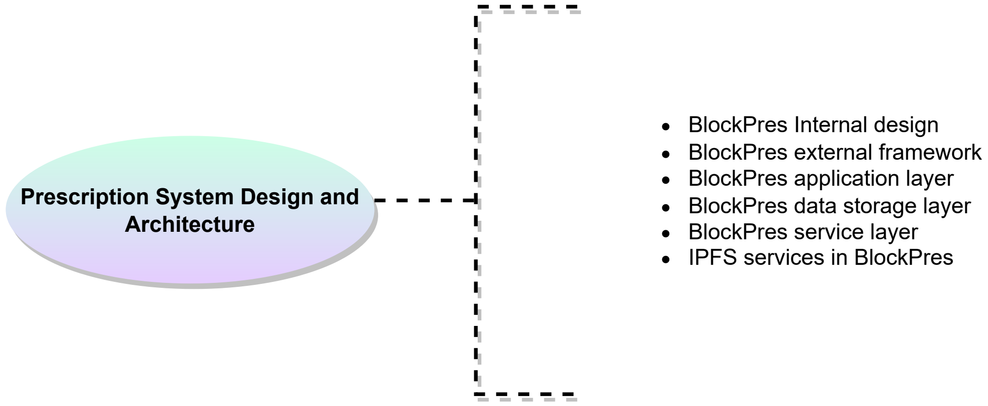
4.4 Conclusion

The research process is adaptable, and changes may be made to the initially established criteria as the research progresses. For example, the research questions may be reviewed and revised. It is anticipated that earlier stages of the research process may require adjustments, and therefore it is expected. Developing research questions, hypotheses, testing methods, selecting research methodology, and determining the research process all contribute to a structured and planned approach to initiating research. This chapter overviewed the various steps involved in Design Science Research (DSR). Research questions and hypotheses have been constructed to contribute to this research. Additionally, research methods have been proposed to answer the research questions and test the hypotheses in the context of DSR. At each research stage, the research design serves as a guide for the next step. Therefore, the research problem must be defined at this p oint, and the high-level specifications and requirements of the proposed PMS framework must be established. Chapter 5 presents the design and architecture of BlockPres Artifact using Archimate Modeling language.

Chapter 5

Prescription System Design and Architecture

5.1 Introduction



Chapter 2 defined the problem of unequal access and inequality in the PMS in Section 2.5 and Section 2.5.5. Moreover, Chapter 2 presented a systematic literature review of HIS and established Research Questions and Hypotheses to mitigate the problems, and Chapter 3 discussed blockchain technology as a technological solution in Section 3.3.1 and 3.4 as an effective solution. Therefore, In Chapter 4, the DSR methodology was presented for conducting the research, designing, and evaluating the solution. The methods are designed to address the formulated research questions are also outlined in Chapter 4. Thus, Chapter 5 presents the design solution in the context of DSRM for the problem described in Chapter 2. This Chapter presents the design and architecture of the proposed solution in the form of BlockPres, a blockchain-based PMS. First, some of the concepts used in the development of BlockPres are discussed in Section 5.2 followed by a design of the Blockpres in Section 5.2.1, the system is broken down into the business, application, and technology layers, with a diagram using ArchiMate and an explanation of the key components of each layer. Section 5.3 presents the Blockpres framework. It describes the physical entities and their relationship in the context of the PMS.

5.2 BlockPres Internal Design

This section presents BlockPres architecture that is designed and developed to mitigate the problems of PMS discussed in section 2.5.5 on page 38. The Incentive mechanism is designed in the BlockPres Artifact to answer the questions formulated in Chapter 2in the context of problems and challenges. Moreover, blockchain technology is adapted to design a BlockPres Artifact. The researcher discussed blockchain applications and characteristics in section 3.2.2 on page 58 to better understand the technology in the context of PMS problems. In addition, the researcher presents several other research studies in section 3.3.1 on page 65 and 3.5 on page 75 to design a blockchain-based solution for equal access in PMS. Therefore, this section discusses the internal architecture, consisting of software and information technology components and the different layers. The architecture is designed using ArchiMate, and it is used to create diagrammatic and visual representations of the system. The ArchiMate tool provides a holistic view of all the system components and how the components work together. Moreover, the internal design and architecture follow the process, design, and construction of (Gutiérrez et al., 2020) to develop the BlockPres internal design and architecture.

5.2.1 Design of the System

This section describes the BlockPres design, including its components and layers. Layered views are created in ArchiMate 3.1 to show the connections between the components and layers, as shown in FigurevrefBlockPresSystemDesign. BlockPres is intended to increase patient engagement and participation by offering incentives through blockchain technology. The architecture of BlockPres is composed of the following layers: application components, technology services, technology, application services, process services, processes, and presentation. The characteristics of these layers are covered in the subsequent sections.

5.2.1.1 Technology Layer

The technology layer of the system includes the hardware components used to support the system's functionality. These include communication equipment and servers used for medical record storage and management. The medical records are saved on the blockchain, which makes them accessible to all participants on the network. TThe proposed design includes several types of servers, which are listed in the following sub-sub-sections.

5.2.1.1.1 Microservices Servers: A specialised server that runs one or more microservices.Microservices are a software development technique in which a large application is constructed as a collection of small, independent, and loosely coupled services that communicate over a network. A microservices server in a prescription management system would host one or more microservices responsible for specific functions within the system. These microservices could include:

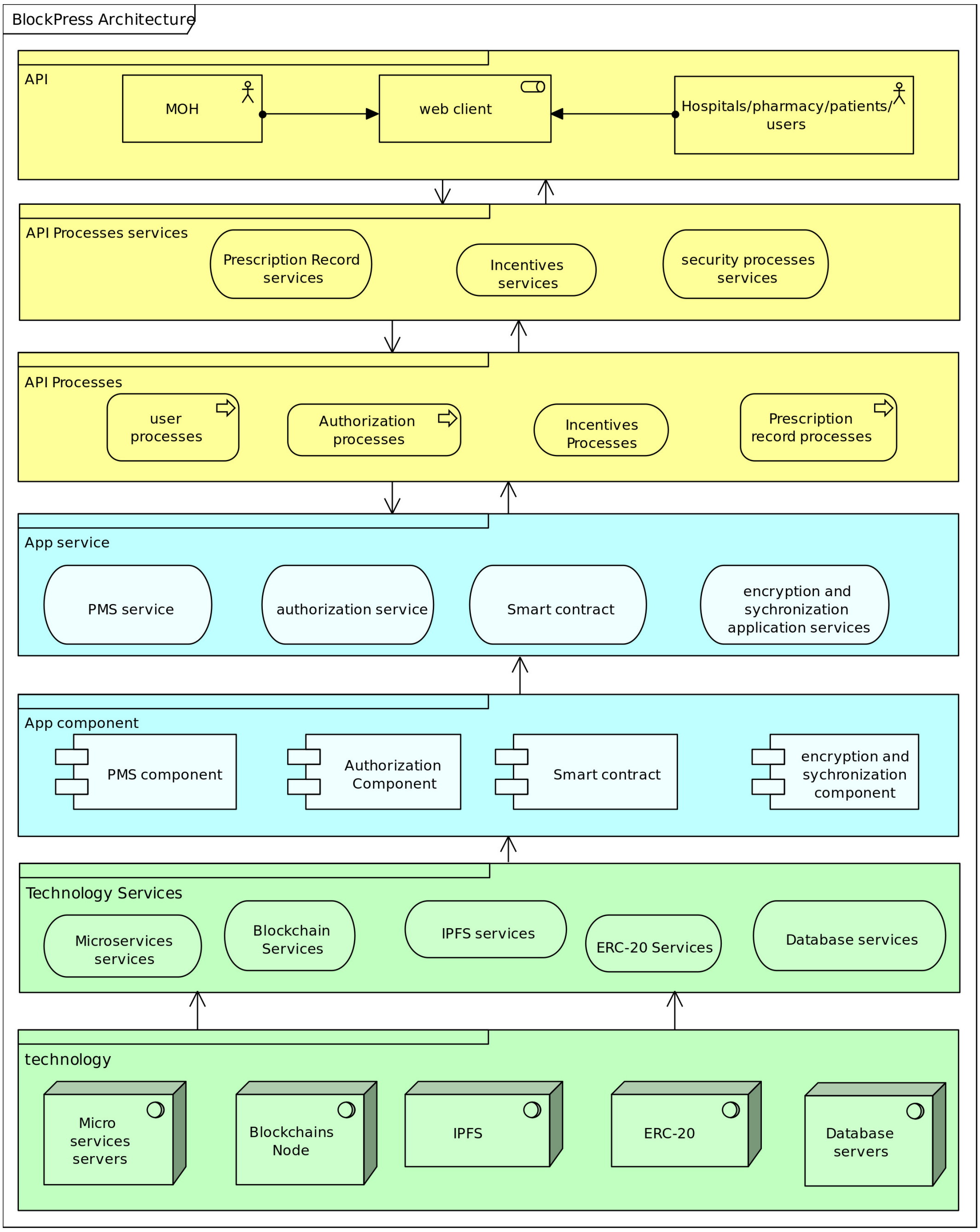


Figure 5.1: BlockPres System Design

- A microservice for patient registration and management
- A microservice for prescription management
- A microservice for incentivisation

- A microservice for communication with the blockchain network

Each microservice is responsible for a specific task that can be developed, deployed, and scaled independently. The independent nature of the microservices allows more flexibility by enabling other microservices to be updated with out affecting the rest of the system. Moreover, The microservices server in a BlockPres artifact can play an important role in the functionality of the proposed system by allowing other microservices to communicate with each other in blockchain network. It would also enable the system to be more resilient, scalable, and flexible, as each microservice can be developed and deployed independently without affecting the overall system.

5.2.1.1.2 Database Servers: Database Servers are utilised to store patients' medical records on the network. While healthcare facilities may have their systems, they must be able to exchange information with BlockPres bidirectionally. This would enable the transfer of locally stored patient data to the network and grant access to participating nodes.

5.2.1.1.3 Blockchain Servers: The blockchain network comprises smart contracts that act as an interface for configuring network entities and regulating their connections with one another to establish a dependable blockchain network. The consensus mechanism is critical to the operation of a blockchain network. The proposed design recommends using either Proof of Authority or Proof of Work as the consensus protocol, depending on their strengths and features.

5.2.1.1.4 IPFS Server: IPFS servers involve healthcare providers uploading patient records to the local database, as described in the Database Servers section. Subsequently, the blockchain network receives the records' location. Prescription files and other data files are loaded onto IPFS. Some of IPFS's benefits include its lower upload costs compared to the blockchain network and shorter transaction times. Additionally, it enables healthcare providers to access patients' records offline.

5.2.1.2 Technology Services Layer

The technology layer offers various services, including blockchain, IPFS, and database services. It says how information is transmitted within the technology sub-layer and its application elements.

5.2.1.2.1 Blockchain Services: Blockchain service functions include:

- Backend tasks such as web hosting are executed.
- Establishing a blockchain connection serves dual purposes. Firstly, it acts as a wallet that assigns unique identities to system nodes for smart contract interactions. Secondly, it connects architectural layers to the blockchain layer (e.g., Ethereum), enabling actions and information retrieval from local databases.
- The blockchain is utilised as an information storage for healthcare data, including medical prescriptions and patient records (treatments, medicines administered, etc.) from hospitals, pharmacies, and other medical facilities.

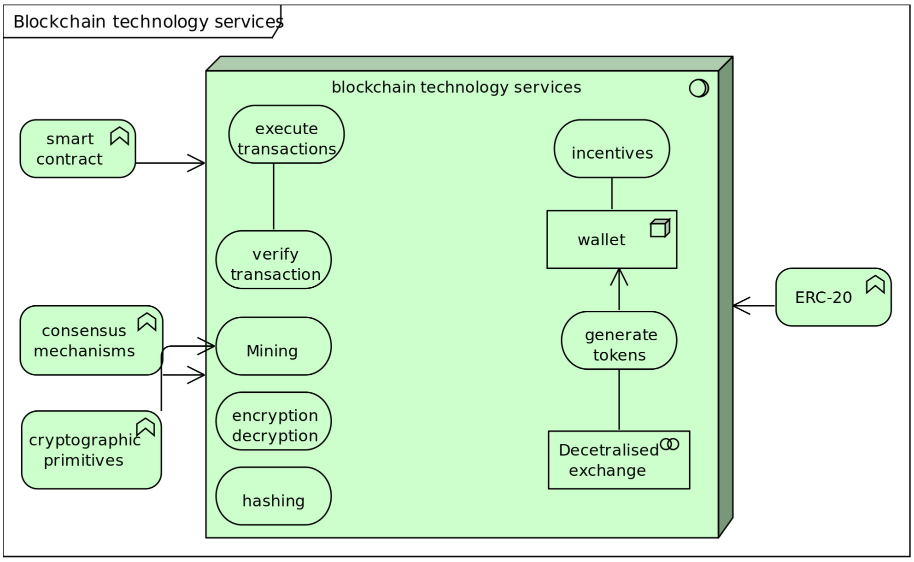


Figure 5.2: Blockchain technology services

5.2.1.2.2 Microservices Services: The web service acts as an intermediary between different layers of an architecture and the server. It is responsible for several key tasks to ensure the smooth functioning of the architecture. Firstly, it establishes connections between the layers, which can either be unidirectional or bidirectional and synchronous or asynchronous, depending on the requirements (Li et al., 2021).

Secondly, the web service implements a web communication and delivery protocol to access the functionalities offered by the suggested architecture. This protocol ensures the seamless exchange of data and information between the different layers (de Almeida et al., 2022).

Thirdly, the web service encrypts prescription records to ensure the confidentiality and security of sensitive patient information. This is necessary to protect patients' personal health information and ensure their privacy. (de Almeida et al., 2022).

Finally, the web service synchronises the prescription records from local hospital databases that store the prescription records within the blockchain. This allows for easy access and retrieval of the prescription records and ensures that they are updated in real-time (Li et al., 2021).

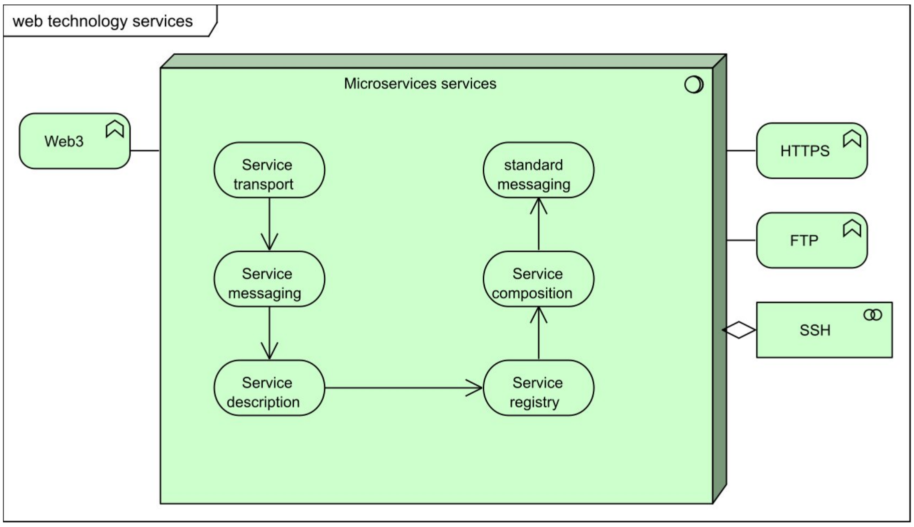


Figure 5.3: Web Technologies Services

5.2.1.2.3 IPFS Services: The IPFS (InterPlanetary File System) protocol is a critical tool that helps the upper layer of architecture in storing large files. Large files can be challenging to store and retrieve efficiently in a blockchain network. The IPFS protocol provides a solution by distributing the storage burden to address this. Blockchain stores only the keywords and file hashes instead of storing the patient's file on the blockchain network. This process reduces the time and costs of retrieving and storing the data. Moreover, IPFS provides offline access to the patient's files even if one entity is not connected to the network. IPFS controls and manages all types of records in a decentralised manner, and no entity in the network controls the data. IPFS removes multiple copies of the same record, reducing congestion in the network and improving efficiency (Zareen et al., 2021; Doan et al., 2022).

5.2.1.2.4 ERC20 services: The ERC-20 token is used as an incentive in the proposed system to encourage patients to use the prescription management system and share healthcare records honestly with healthcare providers.

The ERC-20 token is a digital asset developed by an organisation specialising in technology. The tokens can be used for various purposes, such as rewarding patients for engaging and participating in the Healthcare system and using healthcare services, completing specific tasks, or giving users the right to vote on decisions. In the beginning, the ERC-20 tokens are sold to investors through an initial coin offering (ICO) to raise funds for the newly launched tokens. The Ethereum community approved the ERC-20 as a standard to ensure the interaction of tokens (Morales et al., 2020).

The ERC-20 smart contract has six functions and two events, as shown in figure 5.4. The Total-Supply function indicates the total number of tokens in the smart contract, and the second function shows the number of tokens owned by an account. The Transfer function enables an address to send tokens to another address. The Transfer-From and Approve functions work together to allow an address to send tokens on behalf of another address. The Approve function permits a token owner to approve an address and allow the receiving account to spend the tokens. The Transfer-From function permits the receiving account to send the tokens. The Allowance function allows the token owner to see the number of tokens the receiver still has and can withdraw from the account. The execution of functions such as Transfer-From, Approve, and Transfer triggers the event phase. Sending ERC-20 tokens to an address using the Transfer operation, where the address does not have smart contract code to interact with the address, leads to the loss of tokens. The EOA event can make the operation secure (Chen et al., 2020).

5.2.1.2.5 Database server Services: The database services mentioned in the figure 5.5 refer to computer systems that manage and store healthcare providers' medical information and patient health records. These services control and regulate access to the databases where every healthcare provider must store patient records locally. In other words, these database services act as gatekeepers for accessing patient information and ensure that the information is securely stored, organised, and protected. The database services listed in the figure are examples of such systems used in the healthcare industry (Schmidt et al., 2019).

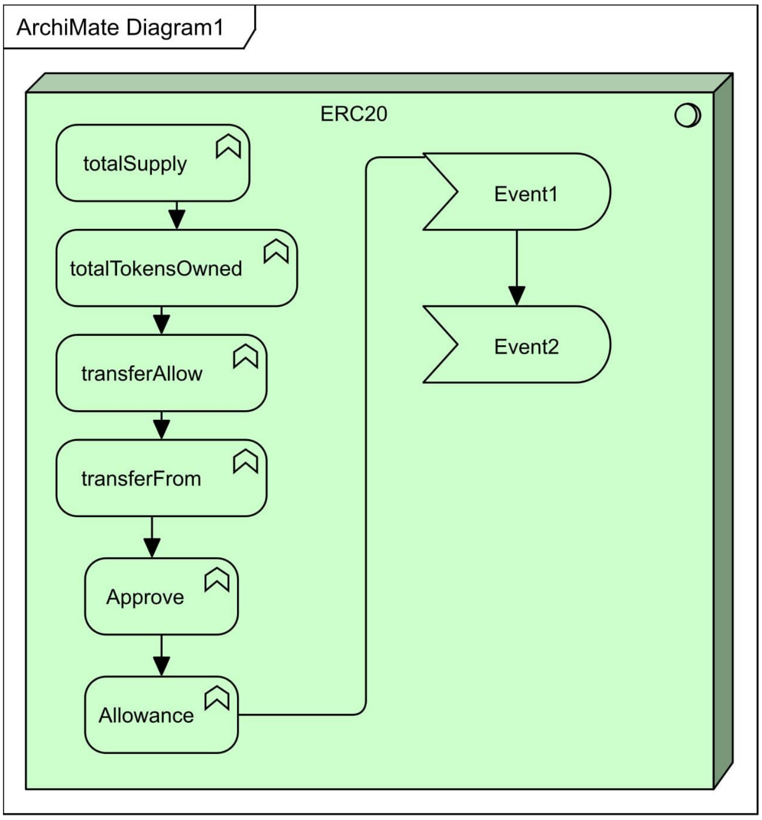


Figure 5.4: ERC20 Services

5.2.1.3 Application Component Layer

This comprises four components: PMS component, smart contracts, security, synchronisation, and encryption. These components provide the platform for users and promote the privacy and security of the platform. These functions are highlighted as follows:

5.2.1.3.1 PMS components: The PMS component is composed of a healthcare provider, an HL7 component, healthcare data standards, data acquisition, data repositories, and a zero-knowledge proof (ZKF) Component.

- Healthcare Provider:

  The healthcare provider manages the structure of data for records, such as the various sections and fields that may be contained in the records. They are only responsible for the records stored in the healthcare provider's database.

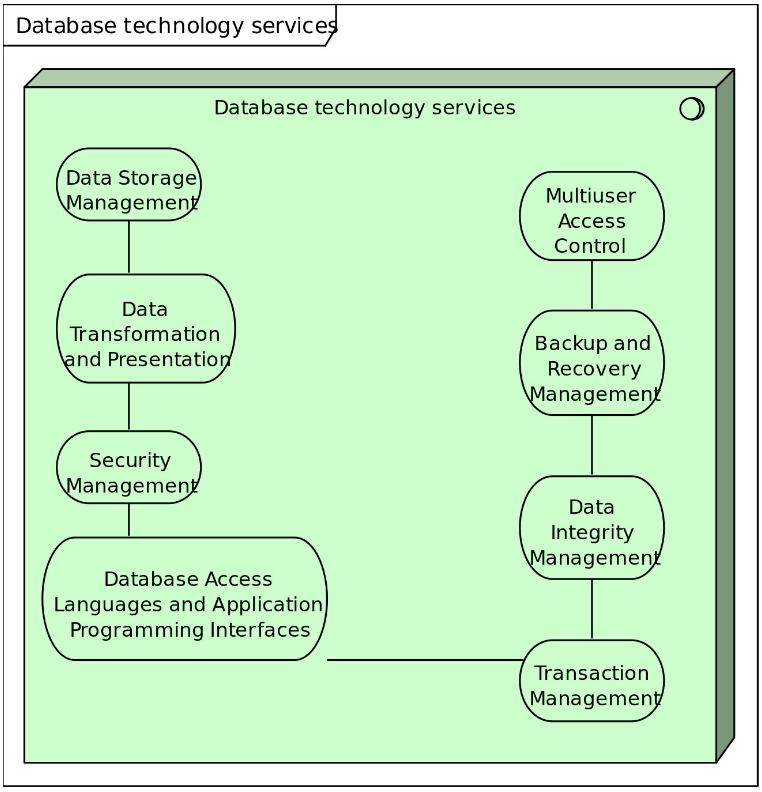


Figure 5.5: Database technology services

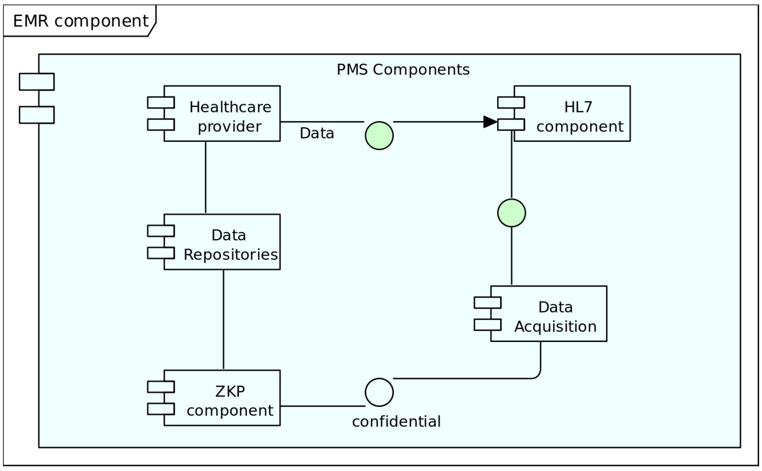


Figure 5.6: PMS component

- Health Level Seven (HL7):

  This is a group of global standards that provide guidance on the transfer and sharing of data among healthcare service providers. The standards are used in the exchange, sharing, integration, and retrieval of health information in electronic format. Adopting these standards supports healthcare management and practices, evaluation, and delivery of services.

- Data Acquisition:

  Data is made available to accountability or learning systems through various means, such as abstracting from paper records, entering directly into a computer system, and reusing data that was collected through different systems. Information capture takes various forms, such as free text and clinical imaging, such as x-rays, motion video, and binary e-data representations, such as laboratory values, operational status, and device settings. Other forms include waveforms, graphical codes, and clinical encoding (Salem et al., 2019).

- Data Repositories:

  A data repository is a database for collecting and storing patient health information from various sources. It is optimised for storing and retrieving patient information and is used to support healthcare delivery, clinical decision-making, and surveillance support.

- Zero Knowledge Proof (ZKF):

  Zero-knowledge proof (ZKF) is a cryptographic method used to verify the information without revealing any additional information beyond the fact that the information is true. In this study, the patient's privacy is also a key concern in the BlockPres artifact. Using ZKF, healthcare providers can view patients' information in compliance with specific criteria, e.g., being older than 18 or having some medical problems. Without revealing any other information, the provider can access patients' information. This process ensures the patient's privacy (Banerjee et al., 2022).

5.2.1.3.2 Authorisation Component: This Component is responsible for assigning roles to entities, providing access to system users, issuing keys to users, and registering and verifying the user accessing the records from the healthcare provider database and blockchain.

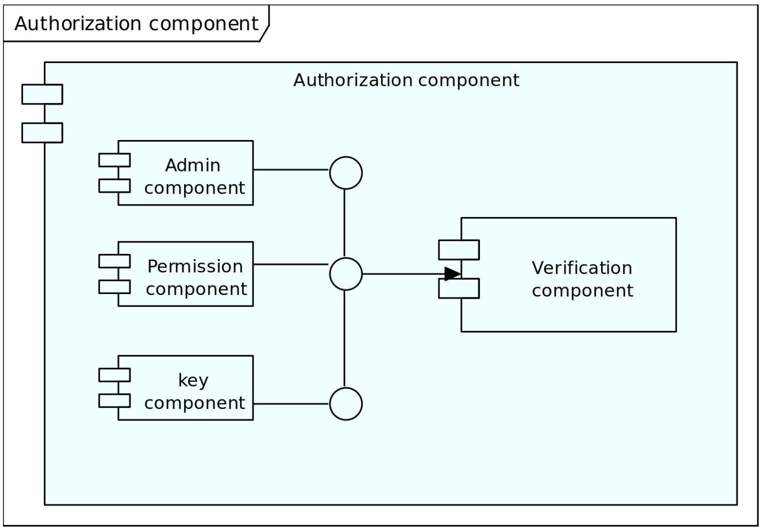


Figure 5.7: Authorization component

- Admin Component :

  This Component manages role assignments for system participants. Every registered participant in the system is assigned a specific function, such as doctor, patient, administrative, or other roles, which entails different levels of access that correspond to the assignment of predetermined permissions to achieve simplicity by establishing user access to clinical data for patients.

- Permission Component:

  The permission component manages access requests for patient clinical information. Requests may be issued by doctors or other entities, but only if the approval is given by the patients or the family doctor. When approved, it establishes a relationship between the record of the patient and the participant whose request was approved.

- Key Component :

  The core component manages and creates user accounts, allowing them to participate in transactions and communicate within the blockchain network. Unlike traditional systems, which use a password/user combination for authentication, the blockchain utilises accounts with cryptographic pairs of private and public keys as access credentials. As a result, every user must have an associated account in the blockchain with their private and public keys as their access information. The core component also generates the private and public keys used by the encryption component for encryption purposes. The accurate creation, administration, and verification of these keys are critical for the successful implementation of EMR encryption (Gutiérrez et al., 2020; Mamun et al., 2022).

- Verification Component:

  The authentication component is in charge of registering and validating various system actors, such as doctors and hospitals. During the registration process, a user is assigned a name, password, and access level, with default limited access. This Component also generates private and public keys for use in interacting with the blockchain, which are saved in the user's system account for future use. The keys are later used as encryption keys, with the public Key stored in the blockchain for information sharing between system users and the private Key kept secure with the user. The user will use the assigned password, username, and private key to gain access to the system (Gutiérrez et al., 2020; Mamun et al., 2022).

5.2.1.3.3 Smart Contract Component: The Ethereum smart contracts are used to create digital versions of medical records stored on the network by various entities. The contracts contain information about record ownership, authorised entities, permissions, and patient prescriptions. The blockchain transactions include cryptographically signed instructions for managing properties, and the smart contract functions enforce policies through legitimate transactions that modify the data. The rules can be structured to enforce any regulations related to medical records as long as they can be expressed computationally. For example, a policy may require separate consent transactions from the patient and healthcare professionals before granting viewing access to a third party (Khatoon, 2020; Gutiérrez et al., 2020).

The smart contract system can instruct workflows and incentivisation processes, with functions for authorising entities and verifying patient tokens. Smart contracts stored on the blockchain can be designed with various conditions, from managing access permissions to offering incentives. Data authorisation rules are defined in the smart contracts and help track actions from origin to completion with unique IDs. The processes are well-defined and embedded within the smart contracts, eliminating the need for centralised entities to manage and approve operations, and reducing administration costs. The medical records are stored in a local database for performance and economic reasons, and the data's hash is committed to the blockchain as part of the block's data aspect (Pham et al., 2018).

5.2.1.3.4 Encryption and Synchronisation Component This section discuses to ensure that PMS record is encrypted and synchronised on the Blockchain network.

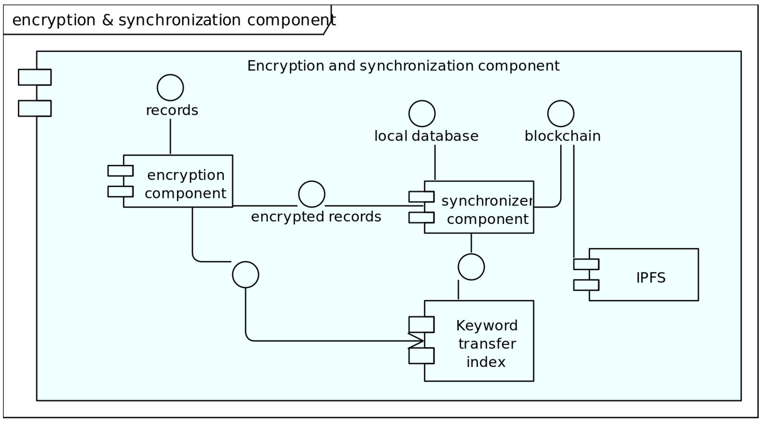


Figure 5.8: Encryption and Synchronisation Component

- Encryption Component: Cryptography is the process of encoding information to keep it confidential for authorised individuals only. There are two types of encryptions in cryptography. Secret key encryption uses one key for encrypting and decrypting the data, known as symmetric encryption. On the other side, public key encryption uses two different keys. The public key is shared with the concerned parties, and the private key is secret.. The BlockPres system employs public key cryptography as it offers higher security and extra caution must be taken while sharing the private key with users.
- Keyword Transfer Index: Once the registration is completed, the patient's information is saved in a local database. The keyword transfer index then sends keywords of the patient's prescription to the blockchain. When a healthcare provider views the patient's records, they only see the keywords, which retrieve the actual records from the provider's local database, reducing the cost and time of storing large files on the blockchain and retrieving the records.

5.2.1.3.5 Synchroniser Component: The synchroniser component acts as an intermediary between the healthcare facilities' internal databases and the blockchain network. It works by temporarily storing the blocks and transactions that need to be sent to the blockchain, before finally transmitting them. Additionally, it ensures that the tokens generated for patients are properly synchronised with their wallets, enabling them to keep track of their medical records and information on the blockchain.

5.2.1.4 Application Services Layer

The application layer makes the services provided by its component parts accessible. These services consist of authorisation, execution of smart contracts, PMS services, security encryption, and synchronisation. These services are used by the BlockPres process layer and are supported by the PMS, encryption, security, and synchronisation

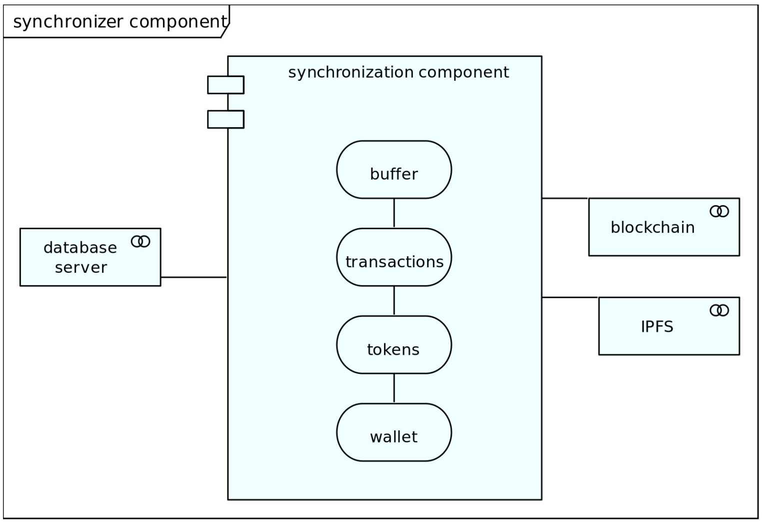


Figure 5.9: Synchroniser Component

components. The application's security service comprises key management, authentication, and permission services.

5.2.1.5 Application Processes Layer

The layer implements three processes to make BlockPres architecture functional: authorisation, user and incentives, and prescription record. The processes are described as follows.

5.2.1.5.1 User Processes: The healthcare provider begins by registering the user and then verifying their identity. The system utilises the verification services from key, authentication, and administration components. If the request is for "creation," the patient is rewarded and the user's data is registered and supported by the data registration service provided by the authentication component. The patient receives the private key for storage after the system generates the public and private keys for the blockchain. Access is determined based on the user's type and role and granted by the administrative component. The transaction is completed through the application services of the synchronisation and encryption component, which obtain, encrypt, and save transaction information on the blockchain. For requests other than creation, such as updates or reads, the user's data is verified using the data registration service from the authentication component and the request is processed. The transaction is completed through the application services of the synchronisation and encryption component, which encrypt and save the transaction information on the blockchain and local database.

5.2.1.5.2 Authorisation Processes: Healthcare service providers, such as doctors or hospitals, initiate the process by requesting access to the patient's prescription record. The patient or authorised guardian authenticates themselves using the authentication service from the key, authentication, and role component. The patient then uses the CRU (Create, Read, Update) functionality to grant access to new users and modify or update access to his or her medical data based on the access service provided by the role component. The transaction is finalised by the application services of the synchronisation and encryption component, which obtain the transaction data, encrypt it, and store it in both the blockchain and local database.

5.2.1.5.3 Incentives Processes: Incentive processes in the application processes layer of anachronistic model in prescription management systems involve rewarding patients or users for participating in the process. This layer is responsible for managing the application processes that are performed within the BlockPres system, and incentivising patients is one way to encourage their engagement.

5.2.1.5.4 Prescription Record Processes: A patient visits a provider of medical services to start the process. Then, using the authentication service provided by the key, role, and authentication components, the provider authenticates themselves. The system determines whether the provider is authorised to view, create, or modify the patient's medical records. The provider can perform CRU (Create, Read, Update) operations on the patient's ER through the Electronic Medical Record (EMR) application service, which is supported by the obfuscator, HL7, and the synchronisation and encryption application services from the synchronisation and encryption components, if the provider is authorised to access the EMR. The role component's system access service typically makes it possible for medical service providers to request access to the EMR if they are unable to access the patient's records. The synchronisation and encryption application services obtain the transaction data, encrypt it, and save it in both the blockchain and local database. This completes the transaction in either case.

5.2.1.5.5 Processes Services Layer: The layer exposes the services provided by the process layer. The presentation layer uses these services to advance the processes. There are two classes of these services: process security services and EMR services. These services are available to users, who can then rely on the processes offered in the process layer for functionality.

5.2.1.6 Presentation Layer

The presentation layer is the output layer of the system. It contains the browser-supported web client through which users can access the system. In addition, interfaces for patients, clinical use, and administrative use are included. These interfaces make it possible to manage and consult EMR, local and administrative entities, and administrative functions. Local administrative staff in healthcare facilities use the interface for tasks such as assigning a physician to a patient. The administrative entities interface is used to create or update system users.

5.3 BlockPres External Framework

In this section, the BlockPres external framework is presented. The researcher defines the internal architecture of the BlockPres in Section 5.2. The internal and external framework and architecture are based on the proposed studies in section 3.3.1 and 3.5. Since the overall BlockPres framework is extensive, this will only address those related to hospital and GP generated prescriptions are defined.

5.3.1 System Components

This section provides descriptions of the entities or system participants involved in BlockPres. In order to enhance the efficiency of patient treatment and to build trust in the system, healthcare providers want to share patient healthcare records with peers. The framework consists of system components that include the New Zealand Ministry of Health (MOH), healthNZ and healthcare providers such as doctors, nurses, hospitals and pharmacies (*Key health sector organisations and people*, 2021).

5.3.1.1 Ministry of Health (MOH)

Controls the healthcare system running in New Zealand. All healthcare providers and pharmacies are registered with MOH. In BlockPres, MOH generates parameters for healthcare providers and provides a unique public key.

5.3.1.2 HealthNZ

Exists in each district to control and manage healthcare providers and pharmacies. HealthNZ is responsible for the integration of services provided to healthcare providers and patients.

5.3.1.3 Healthcare providers

Medical service providers who provide medical services to patients. The healthcare providers consist of medical staff such as doctors and nurses. Medical staff have access to local computer systems and HIS. In BlockPres, the doctor enters patient data and the data are copied to a hospital server. The local database maintains a private blockchain that verifies incoming blocks. The doctor broadcasts unique keywords generated from individual patient records to a public blockchain. Patient registration and prescription records are stored locally. When a healthcare provider receives a request from another healthcare provider to a access patient record, the public blockchain provides authentication of the entity.

5.3.1.4 User

Users are patients in the system and are the primary entities in BlockPres. Patients can either register online to see the doctor or visit in person to obtain an appointment. Each user obtains a public key called a National Health Index (NHI) to interact with the healthcare provider or doctor. The specific NHI number is evidence that the patient receives the treatment and the doctor then generates the record.

5.3.2 System Design and Workflow

The BlockPres framework and its workflow Figure 5.10 is divided into the following three sections: the application layer, data storage layer and service layer. The figure describes the patient's registration and prescription process from a healthcare provider to a pharmacy and how patients obtain incentives, and registration provides permission to their records. The capability to store data on blockchain and IPFS is also included.

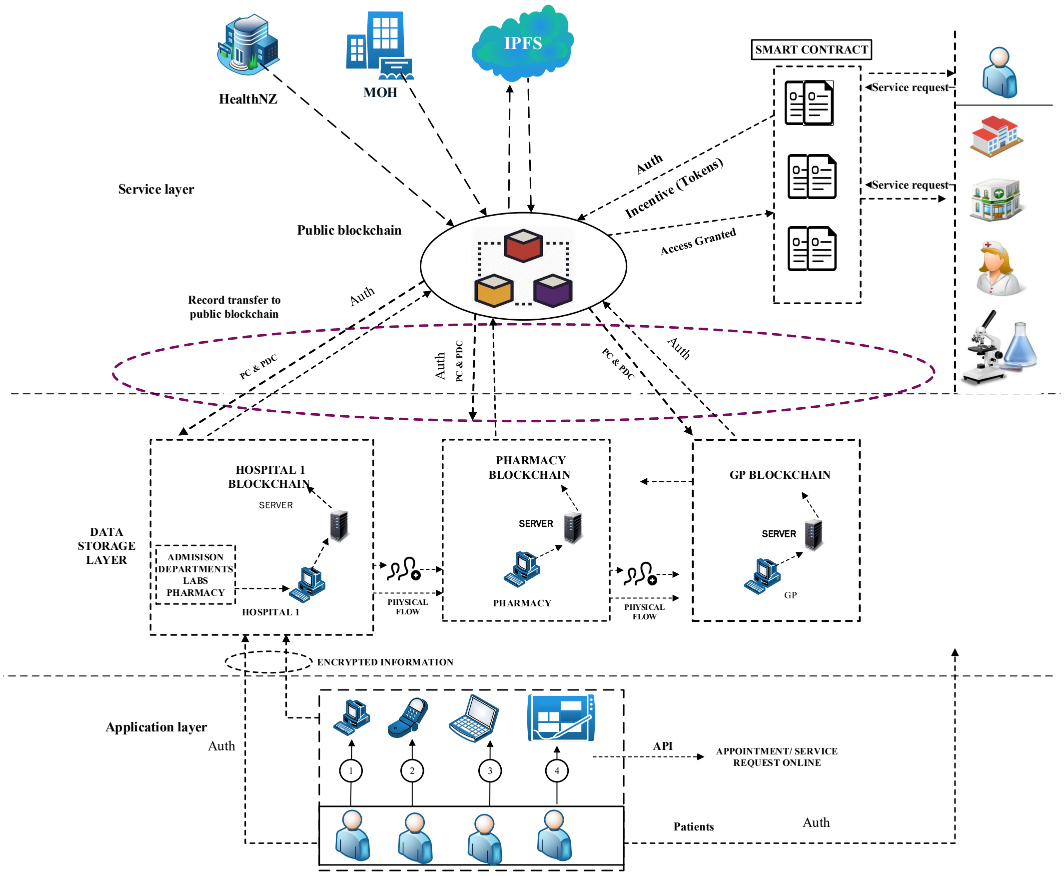


Figure 5.10: BlockPres Framework.

5.3.3 BlockPres Application Layers

The application layer provides an Application Programming Interface (API) for the system participants. The system participants are denoted by the following.

Patients	$PT_K(PT_1, PT_2, PT_3, \ldots PT_m)$
Doctors	$DT_K(DT_1, DT_2, DT_3, \ldots DT_m)$
Nurses	$N_K(N_1, N_2, N_3, \ldots N_m)$
Hospitals	$H_K(H_1, H_2, H_3, \ldots H_m)$
Pharmacies	$PH_K(PH_1, PH_2, PH_3, \ldots PH_m)$

Figure 5.11 illustrates the booking and registration process. When the patient, PT_K, is registered with BlockPres, they are provided with public and private identifiers (IDs). The IDs allow for further interactions on the system and the authorisation of events as

they occur. The patient, PT_K, obtains an appointment online by using the API or he can travel straight to the hospital. Figure 5.12 illustrates the consultation process and Figure 5.13 presents the prescription process of patients traveling from the healthcare provider to the pharmacy.

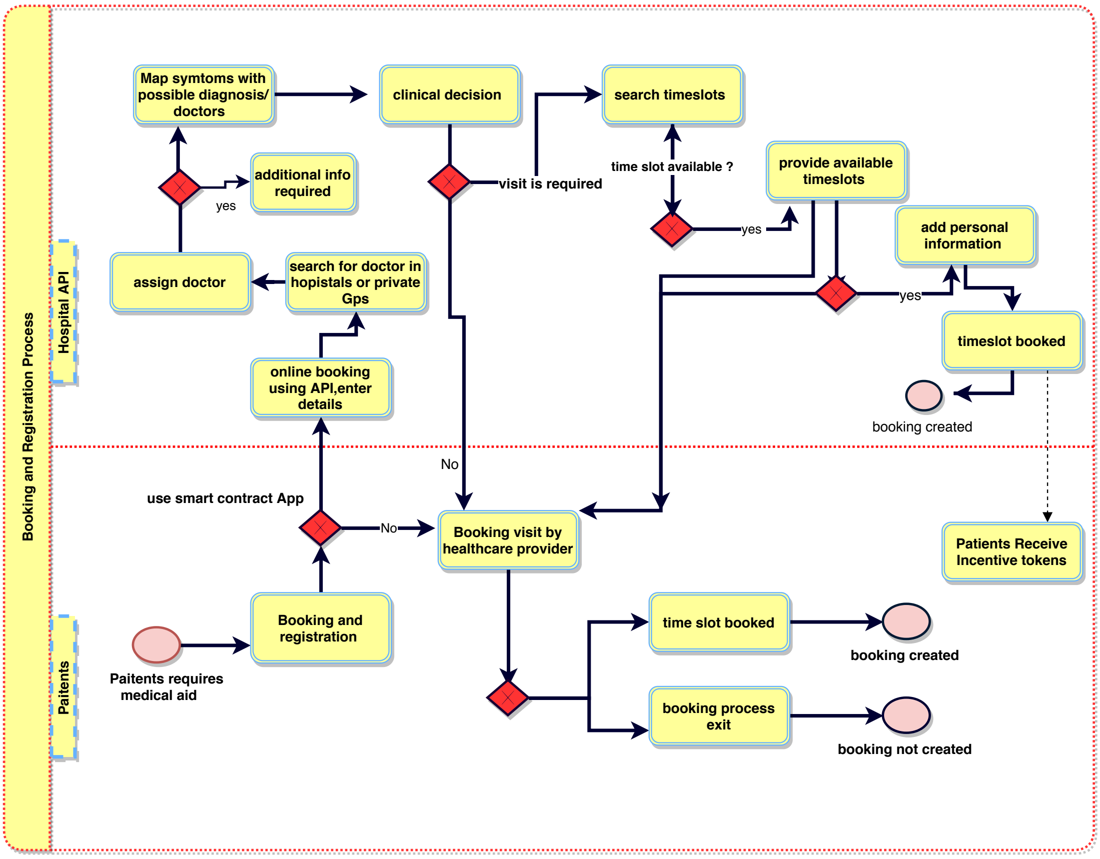


Figure 5.11: BlockPres booking and registration process.

5.3.4 BlockPres Data Storage Layer

Participant records are stored at the data storage layer. When a patient, PT_K, visits a hospital H_K or general practitioner GPS_K for service, the H_K administrator registers the patient's presentation information; otherwise, the patient PT_K registers %online with a device and using the API Figure 5.11.

Algorithm 1 presents the patient registration to the diagnostic service process.

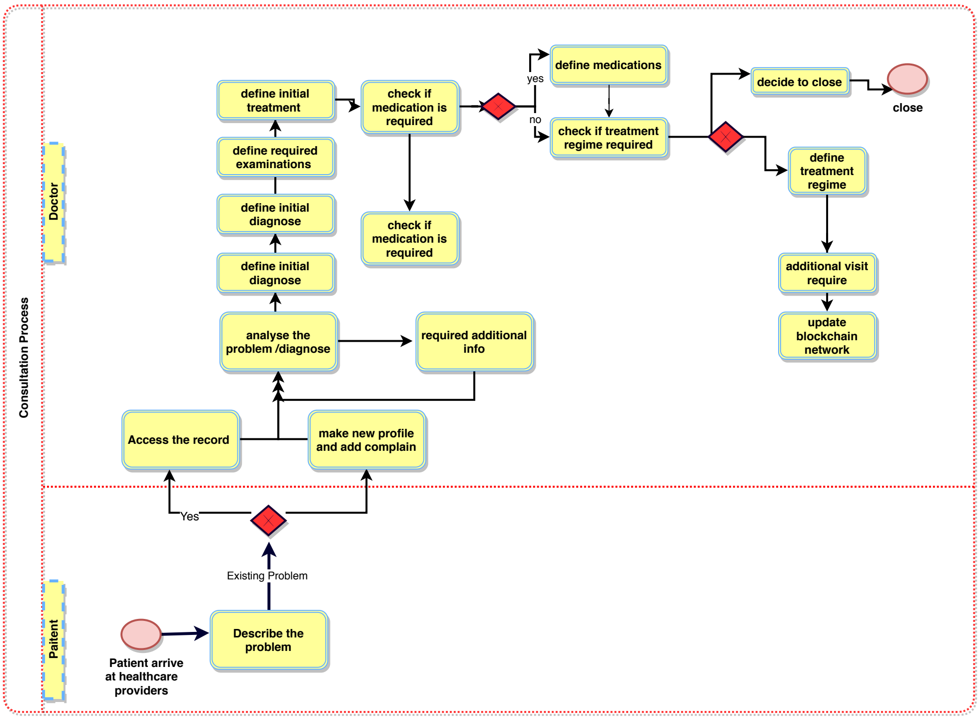


Figure 5.12: BlockPres consultation process.

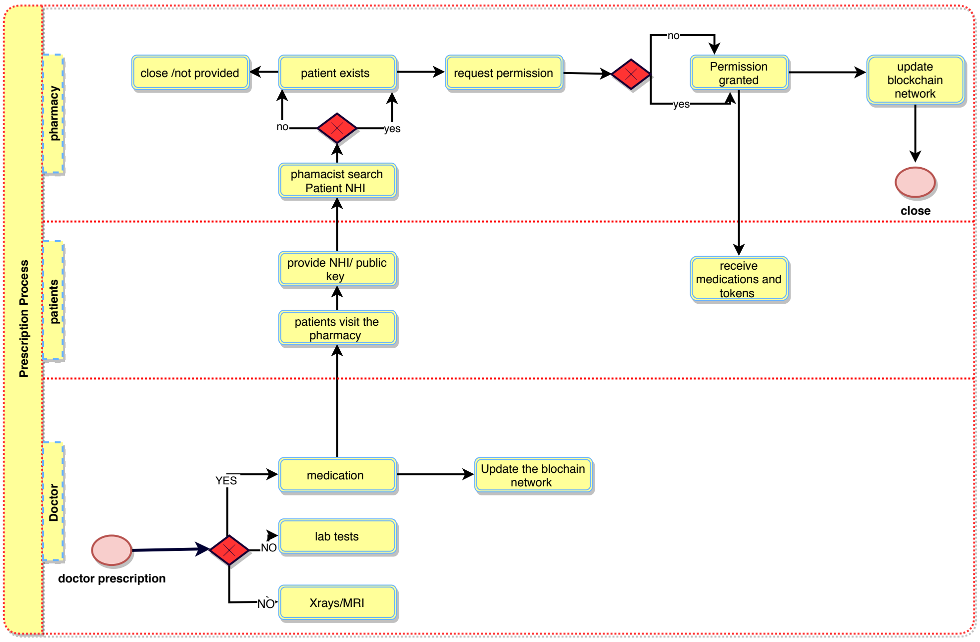


Figure 5.13: BlockPres prescription process.

For any case, a Registry Contract, RC (part of the Smart Contract, SC), is required to be signed. The patient, PT_K, provides personal information and presentation information in the RC. During the consult, the doctor, DT_K, assesses the patient, PT_K, and, where it is required, prescribes treatment or makes a request for further testing (Figure 5.12). When a doctor, DT_K, prescribes medication or makes a request for tests (Figure 5.13), a transaction will result and consists of the IDs for the doctor (DT_K), patient (PT_K), details of medications or tests, dosage instructions and a timestamp.

Algorithm 1: Patient visits the Hospital/GP for a specific problem

```
$PT_k$Registration → online or visit hospital //patients register to hospital
while (register==true) do
    $PT_K \rightarrow PK_P||SK_P||RC$
    $H(PT_{Ko})$ → medical_record
end
$DT_K$ check $PT_K$ : decrypt record → auth
if $PT_K$ == serious then
    Admitted $(PT_K)$ == hospital
    Update_record $(DB(H_1) \rightarrow PU_{bc}$(keyword)$)$
else
    Prescribe (medication) → $PT_K$
    Update_record $(DB(H_1) \rightarrow PU_{bc}$(keyword)$)$
end
$PT_K$visits → $PH_1$(get Record)$(PT_K)$ : auth$(PT_K)||PK_P||SK_P$
if $(PT_K$ == true) then
    Deliver → medication : Update_record$(DB(PH_1) \rightarrow PU_{bc}$(keyword)$)$
else
    $(PT_K$ == false) then
    Discard: process_medication
    Deliver→ medication: Update_record $DB(H_1) \rightarrow PU_{bc}$(keyword)
end
```

When the transaction is assembled, the record is stored in a transaction pool to be added to a block in a DB for the hospital H_K. When the pooled transactions have been validated, they are added to a public ledger. Note that no patient data are added at this point. The public ledger can only contain a record of the smart contract's existence.

A patient, PT_K, may then visit a pharmacy or other healthcare providers Algorithms 2 and 3 and provide the public key to grant access to the prescription transaction Figure 5.14. The pharmacy will use the patient's (PT_K) private key to decrypt the transaction. The service agent cannot have access to the key itself because this is an automated process. A record of the completed prescription is created, which is encrypted using the patient's (PT_K) private key and stored on a single chain and then submitted to the public chain.

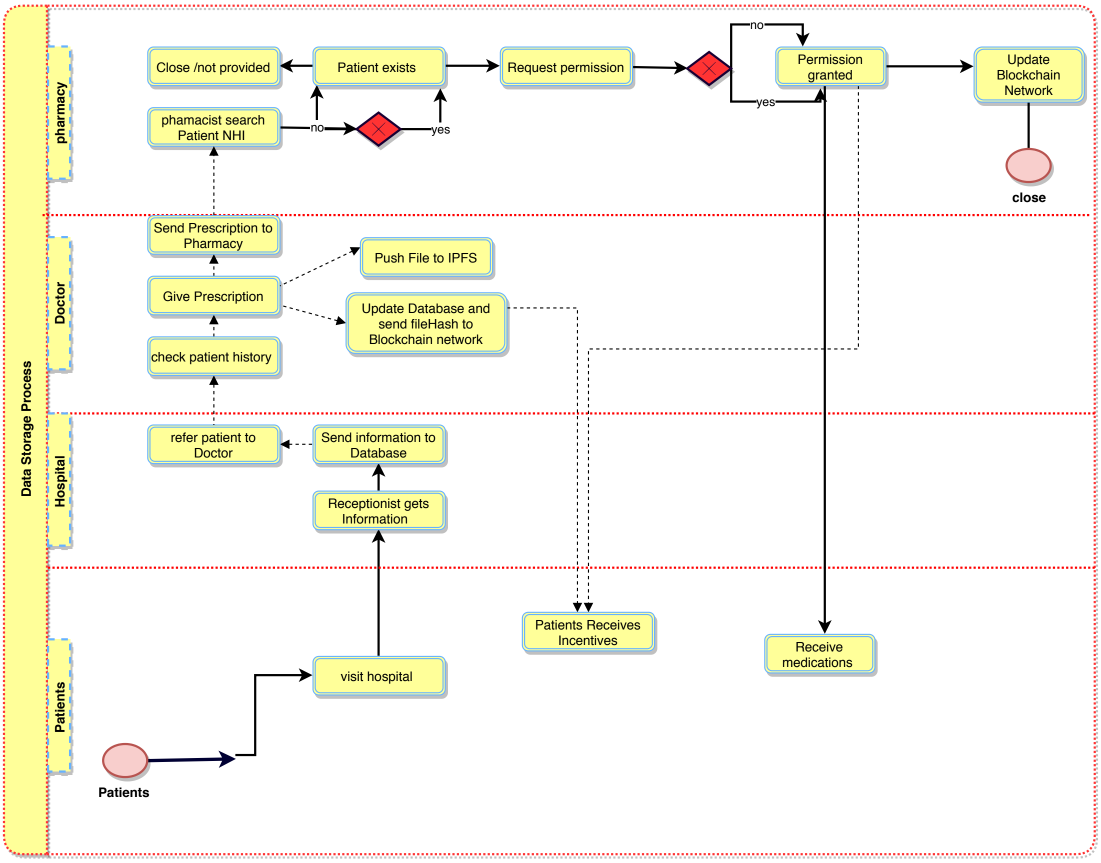


Figure 5.14: BlockPres data storage process.

5.3.5 BlockPres Service Layer

In this layer, data are stored in a second layer by healthcare providers and uploaded to a public blockchain, $PUbc$, to provide services to the healthcare provider (Figure 5.15).

Algorithm 2: Accessing patient's record from a different healthcare provider

```
Input: $PT_K, NHI, H_2, ID, PT_{key}$, keyword Index
Output: patients record
$H_2 \rightarrow PU_{bc} \rightarrow PT_K\, NHI \rightarrow Kw$
while (search $KW$ ==true) do
    if $H_2 \rightarrow$ grant_Access $||PT\, NHI$ ==(true) then
        $KW \rightarrow PT\, NHI \rightarrow KEY$ == (authorize);
        Verify_ $H_2 \rightarrow PT\, NHI$ == true;
    else
        f
    end
    alse;
    return;
end
```

The lower layer, H_1, holds encrypted data from patients and information is stored in a healthcare provider database, DB, and then the data are broadcasted to the decentralised and distributed network. The selected systems are responsible for verifying the blocks of data before forwarding them to the public blockchain, $PUbc$. In this phase, the patient's (PT_K) record is stored in a public blockchain ($PUbc$), for example, the InterPlanetary File System (IPFS) (Ismail et al., 2020; Fan et al., 2018; Brodersen et al., 2016b). IPFS is a Distributed File System (DFS) that operates as an alternative to the Domain Name System (DNS) that currently dominates the Internet. IPFS promises to distribute the World Wide Web and render it more efficient. IPFS is appropriate for this solution because it can store large files and the data can be retrieved using keywords or a hash of the related content (Christidis et al., 2016; James, 2018; Bell et al., 2018).

Figure 5.16 illustrates communication and transaction processes between entities in the healthcare system and Algorithm 3 describes the process of obtaining patient records from various hospitals. When a third-party provider such as a pharmacy needs to access a patient record, permission is obtained from the patient (PT_K). The healthcare provider sends a service request to the public blockchain, $PUbc$, and then to a healthcare provider, Hp. The process of accessing the data is secured by public encryption with

Algorithm 3: Patient's visits to a different hospital

```
//Patients visit to a different hospital $PT_k$Registration → online or visit hospital
while (register==true) do
    $PT_K(H_2) \rightarrow PK_P||SK_P||RC$
    $H(PT_K) \rightarrow$ medical_record
end
$DT_K$ check $PT_K$ : decrypt record → auth
if $PT_K$ == new(true) then
    treatment $(H_2)||PT_K$
    Update_record $(DB(H_2) \rightarrow PU_{bc}$(keyword)$)$
else
    $PT_K$ == new(false) then
    Request (get_record) $(PT_K) \rightarrow PU_{bc}$(keyword) $\rightarrow DB(H_2)$ :
      $DT_K(H_2)||(PT_K) \rightarrow PK_P||SK_P$
    Request_accepted (get_record)||encrypt($PT_K$_record)
    treatment → medication/test: Update_record $DB(H_2) \rightarrow PU_{bc}$ (keyword)
end
```

search keywords (James, 2018; Linnet, 2018). The healthcare provider must sign the patient's PT_K RC on the SC and then sign a Permission Contract to access the patient's PT_K data. In order to access the patient's (PT_K) data, a Permission Contract (PC) is used to sign an agreement between healthcare providers and to obtain confirmation from the patient (PT_K) before sharing their data with other providers. Moreover, this phase includes an incentive mechanism (Algorithm 4) to encourage patients to use the healthcare system and to behave honestly when sharing medical records with healthcare providers. In return, patients will obtain incentives as Ethereum tokens by using the ERC-20 protocol (Gervais et al., 2016; Buterin, 2015). Patients can use the tokens earned wherever they may be redeemed to obtain discounts on healthcare charges, to purchase coffee in a coffee shop, to purchase apparel from clothing stores and so on.

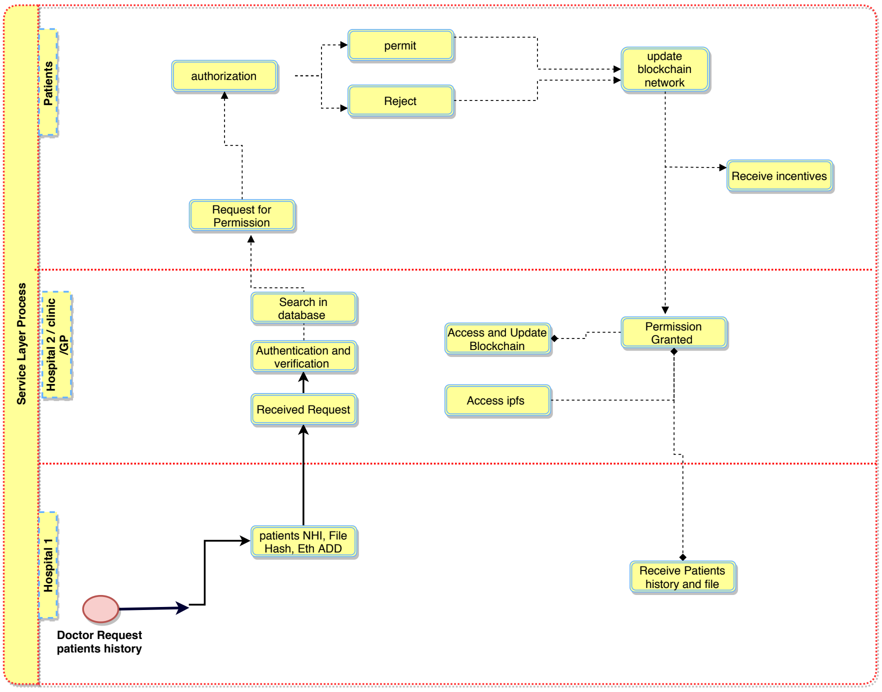


Figure 5.15: BlockPres service layer processes.

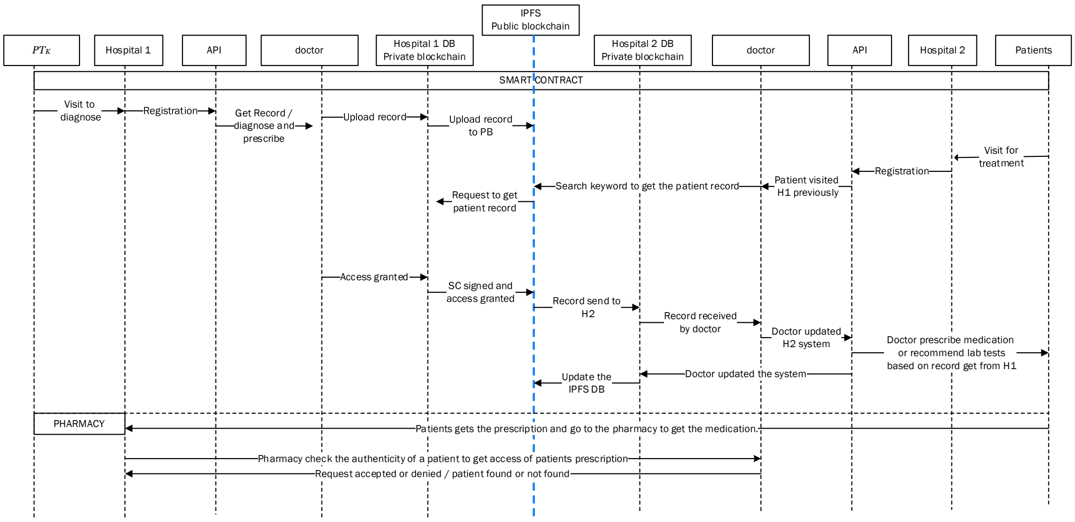


Figure 5.16: BlockPres transaction processes.

The BlockPres framework provides critical functions. The first function is to enhance equality across the PMS. Secondly, the network is decentralised and thus records are distributed since the blockchain is highly redundant (Vasin, 2014; Hussein et al., 2018). Every network node receives an updated copy of all records (Zhou et al., 2018; Zhang et al., 2017b). Thirdly, the system provides integration, which enhances integrity and trust. The fourth function is to provide an incentive mechanism to encourage patients to participate and use the healthcare system and to behave honestly to obtain rewards in tokens.

Algorithm 4: Patient Obtaining Incentives

```
Input: Grant_access, $PT, DT, H_2, KW$
Output: tokens transferred
$H_2 \rightarrow PU_{bc} \rightarrow H_1 \rightarrow KW$
while (register==true) do
    if Authorize_PT → Grant_access == (true) then
        $H_2$ → Get_access ||key|| $PT$;
        $PT$ → Token → MyEtherWallet == (confirmed);
    else
        ;
    end
    return
end
```

5.3.6 IPFS Services in BlockPres

This section presents Interplanetary File System (IPFS) services in the proposed BlockPres Artifact. The purpose of IPFS is to store, share and access the record in a secure and encrypted manner.

5.3.6.1 Storing Data on IPFS

The registration is the first step to start storing data on IPFS, and it is already discussed in Section 5.3.3. This is the beginning of the Process of storing prescription records for patients. This Process comprises several components, including a local database, authentication, synchroniser, data encryption, and IPFS upload. The synchroniser is responsible for uploading data from the local database to the blockchain network, including unique search keywords, strings, and file hash. If the user is not logged into the blockchain network, the file hash will remain in a queue until the user logs in. Once logged in, the file hash will be uploaded to the blockchain network, and both the file hash and file will also be uploaded to the IPFS.

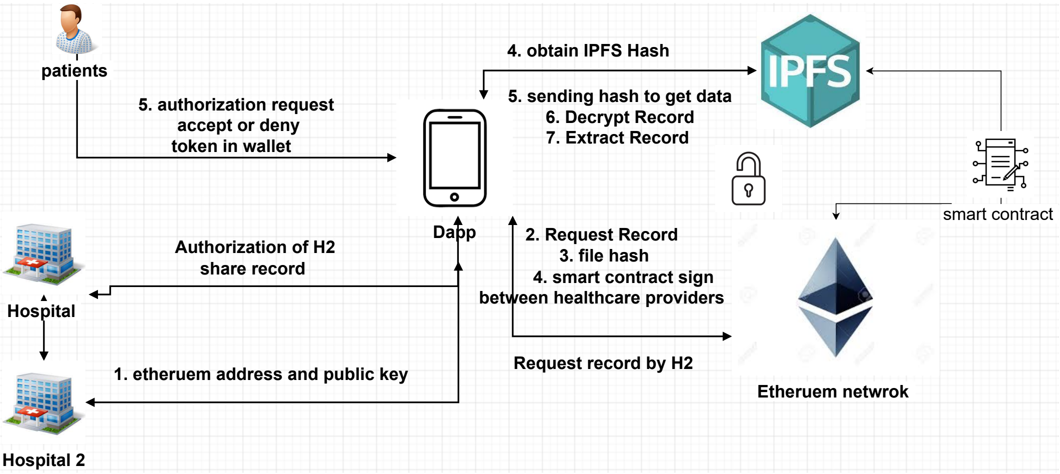


Figure 5.17: Storing Process using IPFS

5.3.7 Accessing Data on IPFS

To access patient prescription records stored on both the blockchain and IPFS, healthcare providers require the patient's Ethereum address, private key, and file hash. When a request is made to IPFS for a patient's prescription record, the patient receives authorisation notifications on the decentralised application. Patients are given the option to either provide authorisation or deny the request. If authorisation is granted, patients receive incentives through tokens, which can be used to obtain discounts on prescriptions or purchase items from shops. Furthermore, in this scenario, the Record Access Contract is revoked, and POW validates the request to ensure that the transaction requested is legitimate once the patient grants authorisation. Healthcare providers access the records using the file hash and the patient's private keys from IPFS.

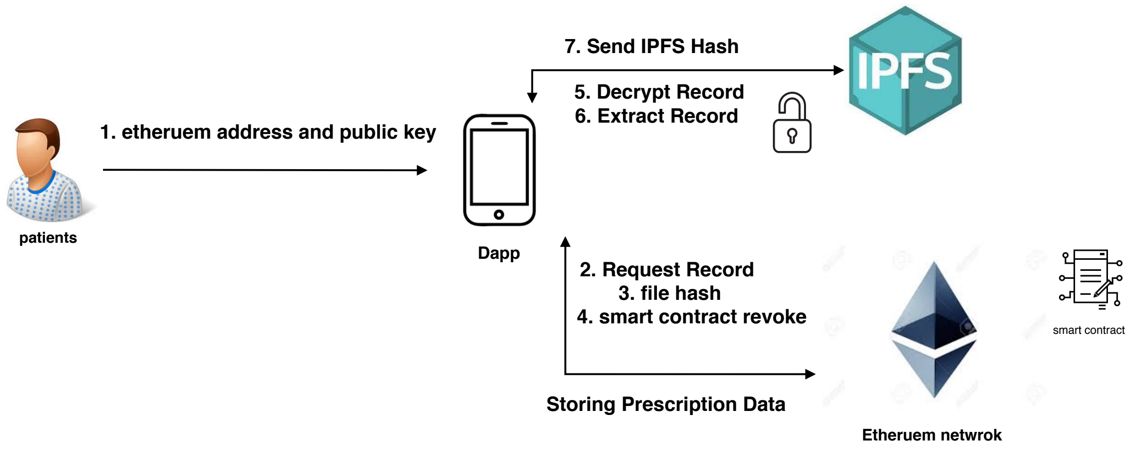


Figure 5.18: Accessing Process using IPFS

5.3.8 Sharing Data using IPFS

Healthcare providers hp_1 share patients' records based on requests received by the other healthcare provider hp_2.

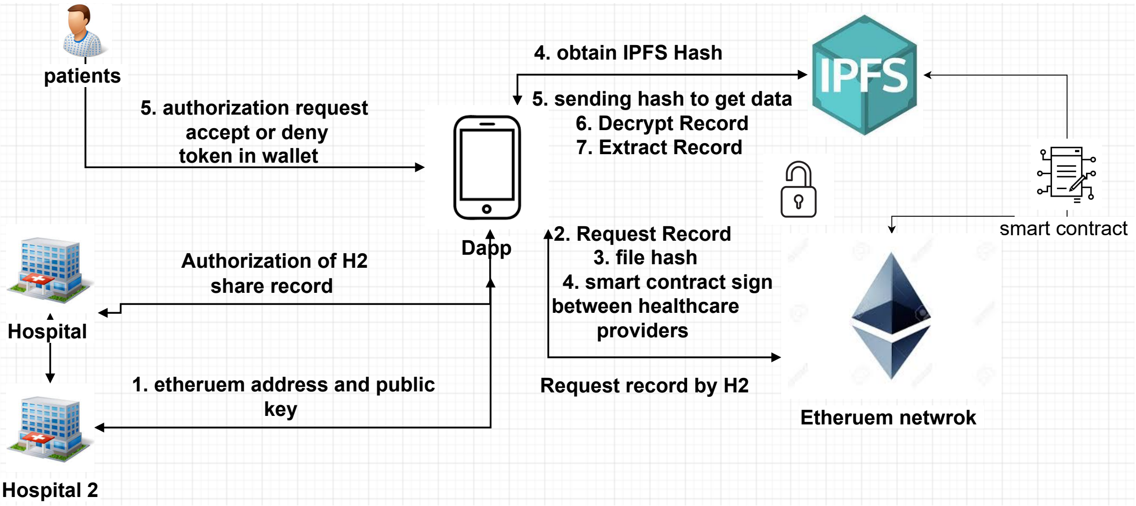


Figure 5.19: Sharing Process using IPFS

Consider a scenario where a patient visits a healthcare provider hp_2 in another city for treatment. During the visit, healthcare provider hp_2 requests access to the patient's previous medical history and records. To do so, healthcare provider hp_2 contacts healthcare provider hp_1, who had previously treated the patient, and requests the patient's records. However, to access the records, the patient's consent and authorisation must be obtained to share their records with healthcare provider hp_2. Once the patient grants consent and authorisation, they receive incentive tokens, and healthcare provider hp_2 receives the patient's private key to access the records.

Healthcare provider hp_2 then updates the patient's new treatment or prescription report to the blockchain network and IPFS. To ensure the privacy of patients' data, the system uses Zero-Knowledge Proof to safeguard patients' privacy while sharing and accessing prescription records among healthcare providers and pharmacies.

5.3.9 Algorithms' Description

In this section, the algorithms used for storing, accessing and sharing data on IPFS are described one by one. Algorithm 5 discusses how data stored in the IPFS and hashes are generated and stored in the blockchain. Once the data is stored in IPFS, it checks the authentication and the permission level assigned to every new medical entity M_{ent}. If the medical entity is authorised, a patient-medical pair is formed. Data is accessed and shared according to the permission levels (Algorithm 6, ranging from 0 to 2. 0 means no data sharing, while 2 means maximum data sharing.

Algorithm 5: Algorithm of Storing Data on IPFS

```
Initialisation
Inputs: Patient data $P_{data}$, Patient ID $P_{ID}$, Medical entity $M_{ent}$, Medical
  entity's ID $M_{entID}$
Output: Send data to the $M_ent$
for (Each $P_{ID}$ = 1, ..., n) do
    Check for the authorization of the patient
    if Patient is authorised then
        Ask for the data to be saved
    else
        Discard the patient
    end
end
for (Each $M_{entID}$ = 1, ..., m) do
    Check for the authorisation of the medical entity
    if Entity is authorised then
        Entertain the data request
    else
        Discard the medical entity
    end
end
for Data uploaded by authorised patient do
    Store the information in IPFS
    Assign hash to each file stored in IPFS
    Send the hash value to the blockchain
end
for Each new incoming file retrieval request do
    Check for the authorisation of the $M_{ent}$. Check for the permission level of
      $M_{ent}$
    if $M_{ent}$ is verified and Permission level = 0 then
        Do not create a $P_{ID}$ and $M_{entID}$ pair for data sharing
    end
    if $M_{ent}$ is verified and Permission level = 1 then
        Create a $P_{ID}$ and $M_{entID}$ pair and share basic information
    end
    if $M_{ent}$ is verified and Permission level = 2 then
        Create a $P_{ID}$ and $M_{entID}$ pair and share all information
    end
end
End
```

Algorithm 6: Algorithm of Access and Share Patients Record on IPFS

```
Initialisation
Inputs: Patients, Medical entities (Hospitals, Clinics, GPs) $M_1, M_2, ..., M_n$
Output: Medical Entity Access Patients Record
for $M_1$ Request $M_2$ for $P_1$ record do
    $M_2$ check authentication of $M_1$
    $M_2$ Check $P_1$ record in system
    if $P_1$ record found then
        Proceed further
    else
        Not found
    end
end
for $M_2$ Request $P_1$ for authorisation using Zero Knowledge Proof and Public
  Key Encryption Schemes do
    if $P_1$ Granted Access then
        Proceed further
        $M_2$ Granted Access to $M_1$
        $Update\ DB$ and IPFS
        $P_1$ Gets Incentives (Token) in Wallet
    else
        $P_1$ denied Access
    end
end
```

5.4 Conclusion

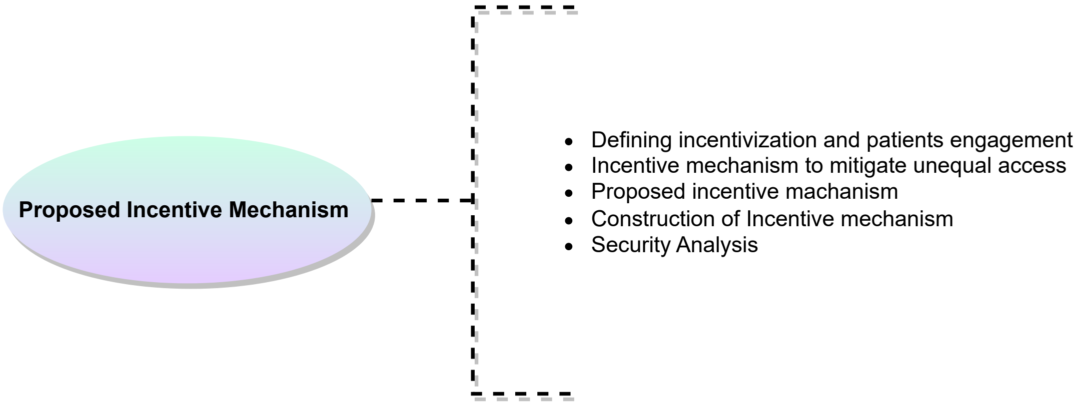
In conclusion, system design and architecture are crucial aspects of software engineering and information technology that aim to provide specific functionality by creating standalone units or components that work together. Using a modeling language such as ArchiMate allows for creating visual representations of systems and their components, facilitating better organisation and management. Layered architecture is a widely used method for designing and implementing IT systems. The design of BlockPres is presented using archimate, which aims to improve patient engagement and participation by providing incentives using blockchain technology.

The BlockPres framework is a comprehensive system for mitigating inequality and patient engagement using incentives. Moreover, sharing patient healthcare records with healthcare providers, consisting of various system components, such as the New Zealand Ministry of Health (MOH), HealthNZ, healthcare providers, and users. The framework's design and workflow involve three sections: the application layer, data storage layer, and service layer. The system allows doctors to enter patient data and broadcast unique keywords generated from individual patient records to a public blockchain. Patients are given a National Health Index (NHI) public key to interact with the healthcare provider or doctor. The system stores participant records at the data storage layer. The lower layer, H1, holds encrypted data from patients, which are stored in a healthcare provider database and then broadcasted to the decentralised and distributed network. Moreover, IPFS is used to store PMS and patient records securely. Altogether, patients will be incentivised throughout the process using the proposed framework. The BlockPres framework can improve the patient engagement process using incentivisation and the efficiency of patient treatment and build trust in the healthcare system. The next chapter discusses and presents the construction of the proposed incentive mechanism within the BlockPres Artifact.

Chapter 6

Proposed Incentive Mechanism

6.1 Introduction



The theoretical aspect of the technological solution in the form of blockchain technology is established in Chapter 3. Blockchain solutions are discussed in the sections 3.2.2, 3.3.1 and 3.5. However, instead of inequality, engagement, and participation in PMS, studies focused on other issues. As a result, this study proposes an incentive mechanism to reduce inequality while increasing engagement and participation. Chapter 5 describes the design and architecture of the BlockPres Artifact. This chapter describes the Artifact's internal architecture using Archimate language modeling, providing insight into how the Artifact works. This chapter also presents BlockPres's external design, as well as the functionality of its components and the incentives for engaging with HIS.

The proposed solution as an incentivisation mechanism for the PMS is presented in this chapter 6. The concept of incentivisation and its potential impact on patient engagement in healthcare is explored in Section 6.2. The incentive mechanism to address unequal access is discussed in section 6.3 on page 144. The proposed incentivisation mechanism is discussed in Section 6.3.1 on page 146, and a concrete construction of the mechanism using formal modeling is presented in Section 6.3.2 on page 147. Finally, a security analysis is completed to ensure a secure incentive process from patient to provider as well as secure data transmission.

6.2 Defining Incentivisation and Patients Engagement

The BlockPres Artifact is used to explain how patients can be incentivised to engage and participate. Section 3.5 discusses various studies proposing different incentivisation systems, including a reputation-based system discussed by (Mousa et al., 2015; Pouryazdan et al., 2017; Kantarci et al., 2015), in which users are assigned a score reflecting their behavior, and those with lower scores are considered dishonest. Other incentivisation systems, such as barter-based schemes and credit-based systems, are also discussed in Section 3.5. All of these systems are designed to improve users' behavior and participation. This section follows the existing studies to design an incentive mechanism in Section 6.3 that can encourage patients to engage and participate.

In this section, the concept of patient engagement through incentivisation is defined. While the incentivization process is briefly discussed in chapter 4, this section elaborates on how incentivisation is implemented within the BlockPres Artifact.

Incentivisation and patient engagement processes can be effective strategies to address these inequalities and improve access to healthcare services for the Maori, as presented in Figure 6.1 on the following page. Incentivising health providers to increase the accessibility and quality of care for Maori individuals can help reduce disparities¯ in health outcomes. Additionally, engaging Maori patients in healthcare can help¯ build trust and increase their participation in preventive care and health services. This can include education, awareness campaigns, and culturally-sensitive approaches to healthcare delivery. Improving access to technology, such as electronic prescriptions, can also help reduce barriers to care and increase access to healthcare services for Maori.

Incentives can be an effective method for improving patient behavior, attitude, and identity in prescription management. By providing rewards or positive reinforcement for desired actions or outcomes related to medication adherence, incentives can increase trust and value in the prescription management system among patients and healthcare providers.

One way incentives can improve patient behavior is by encouraging adherence to medication regimens. Lack of consistency is another tricky situation in the healthcare system as it may lead to adverse effects such as inadequate health outcomes and surged costs. However, providing incentives for following the medication prescriptions can help improve the patient's health. This may include tokens, gift cards, and discounts.

Incentives help improve patients' attitudes and have a feeling of self-assurance arising from an appreciation of one's abilities or qualities. For example, suppose a patient regularly monitors their health conditions and strictly follows the prescribed medications. In that case, they should be rewarded with financial incentives to care for themselves. This may lead to healthy and positive change. Such kind of rewards in the form of incentives will make them think they are not being left out or victimised. They will take better care of their health to achieve those incentives. By encouraging collaboration and cooperation between patients, providers, and payers, incentives can help boost trust and value in the prescription management system. For instance, providing rewards to healthcare professionals that collaborate to coordinate patient care can help to increase the continuity and standard of care. Similarly, rewarding patients who actively engage in their care and participate in decision-making can encourage shared accountability for health outcomes.

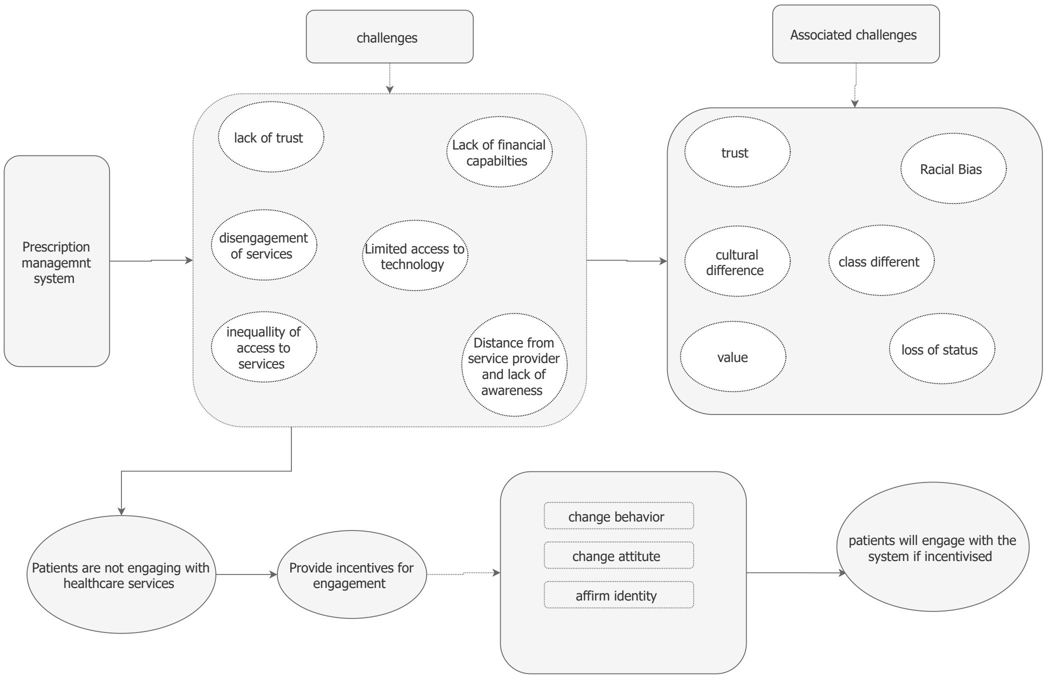


Figure 6.1: Conceptual Model

Additionally, Loss of status and class differences may lead to how incentives can be used in the Prescription management system. For example, Loss of status can lead to specific changes in patients' behaviors, and they may change their patterns of medication and may not take good care of their health. People who may feel disconnected from or feel that they may lose status might hesitate to participate. For example, a patient offered incentives or rewards to take medication for a chronic condition may be hesitant to participate if they feel that having the condition is an accepted part of their cultural or social identity.

Eliminating class differences leads people to consider taking part in the incentives in PMS. For example, if a patient is given protocol, is taken care of in an exceptional manner, and is treated well towards the special incentives offered, they may likely want to participate. While on the other hand, patients with a lower economic background can be convinced by providing them with highly valued gifts and opportunities like traveling.

Healthcare providers must consider and understand these biases when designing incentive programs for patients, especially for Maori and Pasifika, in the context of this study. Moreover, If cultural and social sensitives are kept in mind, it can increase trust and value in the prescription management system. Providing incentives can also empower Maori and Pasifika and help towards better healthcare outcomes. For example, Instead of providing them with materialistic incentives, it could be oriented around education and self-care. Considering these types of incentives may result in better outcomes than material ones. Additionally, Racial bias can affect how incentives are perceived and used in underserved communities, particularly communities divided by color. Moreover, Studies show that underserved communities are less likely to participate in clinical trials, even when offered financial incentives, due to a lack of trust in the healthcare system and concerns about exploitation.

While designing incentive programs, another thing to be kept in mind is health literacy. Patients with poor health literacy can require assistance comprehending and participating in incentive programs. Healthcare providers should consider providing education on using incentives and understanding the patients at all levels. Staff should be well trained to provide the patients and people with appropriate information with low health literacy. The staff can use different techniques such as diagrams, demos, and pictures, break down complex information into smaller and understandable blocks, and, most importantly, use plain language. They may use other tools to help understand patients.

Moreover, Providers of such incentive programs must and should be able to adjust the program's needs according to the patients, what they want, and what kind of incentives they require. Also, involving patients in designing the incentive program can be a good way to ensure that the program is tailored to their specific needs and accessible reasonable, and appropriate to them. Trust, values, class contrasts, loss of status, and racial bias can be generally exacerbated by unequal access to patient prescription management systems. Inequal access to prescription management systems can have several negative consequences for patients. For example, Underserved communities with lower socioeconomic backgrounds need equal access as they are getting a different treatment level than others.

6.3 Incentive Mechanism to Mitigate Unequal Access

This section describes an incentivisation mechanism to mitigate the negative effects of unequal access to healthcare services. Perceptions that prevent engagement in fulfilling prescriptions may be overcome if patients are encouraged to participate through incentivisation. In this study, a system that incorporates cryptocurrencies might show positive benefits if an incentivisation scheme was introduced to the prescription fulfillment process. The incentive is to earn tokens as a reward for successfully filling prescriptions. The the tokens may be redeemed for health services, products, etc. It is also possible that the patient can send their earned tokens to others to help them obtain additional services.

The incentive platform is built on a cryptocurrency blockchain with a specifically designed incentivisation protocol. Algorithm 4 incentivises or rewards patients accessing their records. When a patient signs up for the service using the API (Figure 6.2), the patient's account creates a unique address for authorisation and identification. A patient crypto wallet is installed, which enables the patient to receive rewards from the system. It is also necessary to link the system to appointment bookings and prescription repeats. The cases below show how the incentive is accounted for with respect to the

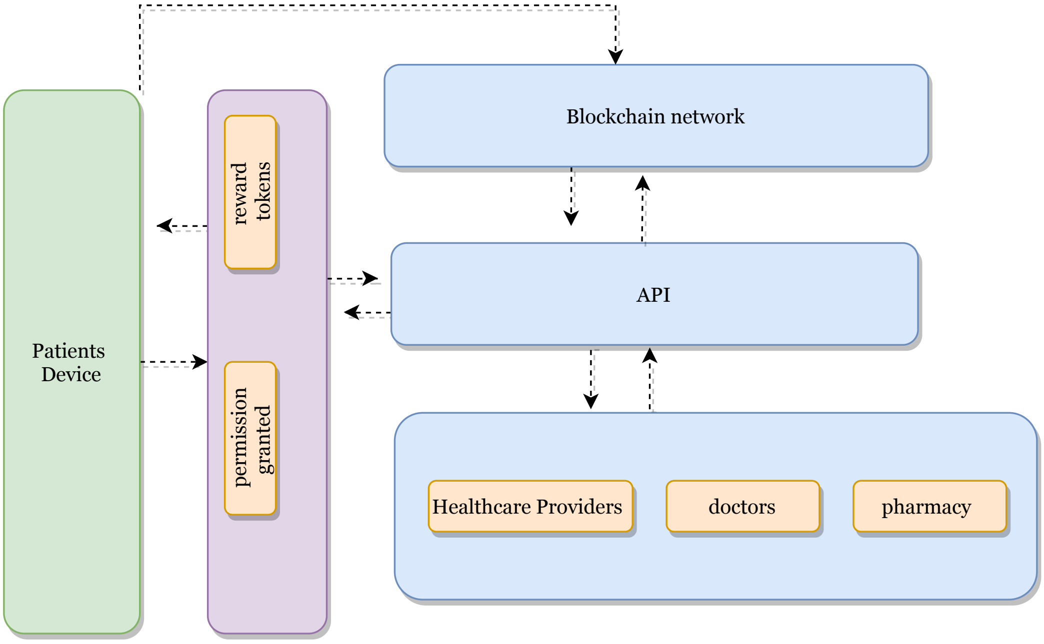


Figure 6.2: BlockPres incentive mechanism.

patient's wallet.

Case 1 Whenever patients visit a healthcare provider or doctor for treatment and register with healthcare providers, the patient receives a reward (token). The workflow of the incentivisation process is illustrated in Figure 5.15.

Case 2 When a patient is issued a prescription from the doctor and then visits a pharmacy to obtain the medication, the pharmacy enters the patient's NHI to obtain the prescription. The access request alerts the doctor for authorisation and, at the same time, the patient receives an authorisation request. The patient receives a reward for authorising access with respect to obtaining a prescription from the pharmacy.

Case 3 Whenever the patient visits other healthcare providers or doctors, for example, in cases of emergency, the doctor accesses the patient's previous record or history of treatments and prescriptions. The doctor requests the patient's healthcare provider to grant access to the patient's record. In this case, the patient will receive permission requests from their healthcare provider doctor:“the provider, ABC, needs to access your record. Do you give permission?” Once the patient’s permission is obtained, the patient will receive a reward.

Case 4 When the healthcare provider shares a patient record for any purpose with any other healthcare provider, doctor, and organisation, the patient will receive incentives (tokens) for permission to access the record.

6.3.1 Proposed Incentive mechanism

This process ensures the patients’ engagement using incentivisation. Also ensure the secure engagement of users and data transmission in a blockchain, an encryption technique is used, where four entities are connected with their private blockchain, and these blockchains are further connected with the public blockchain. The communication (Message) is encrypted using the public key, and the decryption will be performed using the private key. The whole process from start to end guarantees the secure incentivisation process to engage patients and data transmission as the private key has not to be disclosed. The following are the steps for blockchain encryption:

- Entity A sends a message M to entity B using its own public key, $C_A = E_A(M)$
- Entity B starts sending the request to A, entity A then generates one time key $PK_{A\leftrightarrow B}$
- Entity A sends C_A and $PK_{A\leftrightarrow B}$ to the agent.
- The agent transforms the ciphertext C_A to C_B using the already generated key $PK_{A\leftrightarrow B}$, here, C_B is referred to as a ciphertext generated from message M using public key of entity B. agent is transferring the message and cannot get the plaintext.

- The ciphertext C_B is delivered to entity B
- The entity B decrypts the ciphertext C_B using its own private key to get the plaintext M.

6.3.2 Construction of Incentive Mechanism

This proposed incentive mechanism is based on proxy encryption technique to secure incentive mechanism and sharing the prescritiop data on the block chain of the hospital. It also provides data privacy with zero knowledge proof.There are system manager SYS_m, hospital H_i, patients P_i are the participants in the network. Health management department is acting as a trusted third-party system manager SYS_m who is responsible in generating the master key and system parameters. Initially hospital H_i registers with the system manager SYS_m and generates its private and public keys, patients P_i also need to register and generate their public and private keys with the system manager if they want to see the doctors in the hospital. After the patient visit doctor complete the diagnosis and publish the result in the blockchain. Server verify them, if they have passed the verification process, the medical diagnosis/results of the P_i will be stored in the block chain of the hospital H_i if any doctor needs to check the history of particular patient P_i, the doctor and the patient need to apply to the system manager SYS_m at the same time. SYS_m then generates the master key and convert the medical history record re-encrypted by the doctor's public key, into ciphertext. The SYSm sends this ciphertext to the doctor. This incentive mechanism includes enrolment phase, hospital join phase (for doctors and patients both), authentication and authorisation phase, data storage phase, data synchronisation phase, incentivisation phase.

6.3.2.1 Enrolment Phase

- $SYSm$ initialise a security parameter $1^k (k \in N)$, here we need to select two multiplicative groups $\mathbb{G}_1$ and $\mathbb{G}_2$ along with bilinear map e, both groups have the same prime p and g is generated from $\mathbb{G}_1$.
- Three secure hash functions are generated by system manager.

(a) $\mathrm{Hash}_1 : \{0,1\}* \rightarrow \mathbb{G}_1,$

(b) $\mathrm{Hash}_2 : \mathbb{G}_2 \rightarrow \{0,1\}^k$

(c) $\mathrm{Hash}_3 : \mathbb{G}_1 * \{0,1\}^k * \{0,1\}^{sp} \rightarrow \mathbb{Z}_p^*$

- A random function

a. $F : \mathbb{G}_2 * \mathbb{G}_1 * \{0,1\}^k \rightarrow \{0,1\}^{sp-sp1} \| \{0,1\}^{sp1}$, where sp and sp1 are the security parameters

- Now, as the system master key, system manager SYS_m selects $x \in \mathbb{Z}_p^*$ randomly.
- Set public key $Y = g^x$.
- Select random numbers $g_1, g_2, x, y, z \in \mathbb{G}_1$.
- Publish $\left\{ \begin{array}{c} p, g, g_1, g_2, u, v, d, Y, \text{ Hash }_1 \text{ Hash }_2 \\ H_{ash}, F, sp, sp_1 \mathbb{G}_1 \mathbb{G}_2 \end{array} \right\}.$
- Patient P_i, randomly select $x_j \in \mathbb{Z}_p^*$ as a private key.
- Compute the public key $PK_{\iota j} = g^j$ - The hospital H_ι randomly select $x_\iota \in \mathbb{Z}_p^*$ as the private key and its public key is set as $PK_\iota = g^\iota$.
- The doctor D_ι randomly selects $x_D \in \mathbb{Z}_p^*$, as private key and compute its public key $PK_D = g^D$.

6.3.2.2 Patient Joining Phase

Following are the steps that are required to be followed, if any patient P_ι wants to see a doctor in the hospital H_l.

- P_ι sends the identity ID_ι to the hospital server H_ι.
- Server assign a doctor D to check the patient P_t.
- Server randomly select $\partial \in \mathbb{Z}_p^*$ as an evidence for patient he is going to see.
- Sends ∂ to P_l and store it for doctor D.
- During the visit patient P_ι see the doctor D and present ∂ as a consent to make a diagnosis. This information will be used to access the patient history records. D generates the result R and grant token $t_t \in T$.
- Patient randomly selects $X_\iota \in \mathbb{Z}_p^*$.
- Computes patient's pseudo identity $P_\iota^{ID} = E_D\left(ID_\iota \oplus \partial_\iota \| \partial_l\right)$.
- D inputs PK_l, Y, m, t_l randomly.
- Select $r \in \mathbb{Z}_p^*$.
- Computes.

a. $C_1 = p_1^r$

b. $C_2 = PK_l^r$

c. $U = \varrho\left(p, p_2^{t_1}\right)^r$

d. $C_3 = \mathrm{Hash}_2(U)$,

e. $K = \varrho(g, g)^r$

f. $C_4 = \left([F(K, C_1, C_3)]_{sp-sp_1} \| [F(K, C_1, C_3)]_{sp1} \oplus R\right)$

g. $h = \mathrm{Hash}_3\left(C_1, C_3, C_4\right)$

h. $C_5 = (x^h yz)^r$

i. Hence, the ciphertext of R is $C_l = C_1, C_2, C_3, C_4, C_5$

j. D sends $P_\iota^{ID}, P_{\iota j}^{ID}, t_l$ to P_ι securely

k. D computes $X_{\iota j} = E_l\left(\beta \,\|ID_\iota\|\, P_\iota^{ID}\|ID_D\right)$ using H_l public key and send it to the server of the hospital.

6.3.2.3 Authentication and Authorisation Phase (Data Storage Phase)

The doctors join the system from different department and have different professional knowledge. Therefore, a light weight and robust consensus mechanism is used. It will provide a necessary agreement on a single data value. It also provides agreement on a single state network among distributed process. In data storage process, doctors act as a delegate to broadcast and record data that is generated by them in the blockchain network. The hospital server works as a verifier to provide reliability. One credit score scheme is also set up for hospital and doctors. $SYSS_m$ and hospital server are allowed to check the effectiveness of every doctor record, if doctor enters a wrong record, one credit score will be subtracted. Any doctor with lowest credit score will be terminated from the hospital. Hospital is also supervised by SYS_m and allowed to punish the hospital over wrong behaviour. Doctors have a right to report any wrong behaviour of the hospital to the SYS_m. - Doctor D generates patients P_ι medical record $C_\iota = (C_1, C_2, C_3, C_4, C_5)$

- Data is broadcasted in a private blockchain of the H_ι.
- Hospital server H_ι is verifier because SYS_m supervised it.
- The server decrypts the ciphertext $X_{\iota j}$ using hospital H_ι private key to check the identity of the doctor and patient.

If the verification is successful, data is transferred to the blockchain and all the other nodes connected to the blockchain, update the records. Following is the figure represents the general structure of the blockchain. Following are the important steps to follow:

- Medical data is broadcasted in a private blockchain of a hospital by the doctor D.
- Data is verified by the hospital server after every minutes.
- After this verification, 10 correct records are added in a new block of a blockchain.
- All the connected nodes of the blockchain will update the record and store data.

6.3.2.3.1 Utilisation of Cryptographic Keys in BlockPres: In this section, the utilisation of cryptographic keys is described. Cryptographic keys play a significant role to ensure data privacy (Guo et al., 2018; Zheng et al., 2018). Public/private key pairs are used to provide P_i transaction confidentiality when the record traverses untrusted channels (Rohr et al., 2018; King et al., 2012). In BlockPres, there are multiple entities P_i, D_i, N_K, AD, PH_K and NS_K and thus the system creates keys for each entity using a cryptographic method called El Gamal (Omar et al., 2019; Wood, 2014; Victor et al., 2019). The key pair of an entity is symbolised by PK_k and SK_k, where PK_k is a public key of an entity and SK_k is a private or secret key of an entity. Moreover, the SK_k must be kept secret by the entity, while PK_k can be distributed among healthcare providers and other entities in the system. Therefore, the public key set is $PK_k = (PK_1, PK_2, PK_3, PK_4, \dots PK_k)$. The secret or private key relation is established between entity A and B by using a secure algorithm (for example, AES) (Victor et al., 2019). A Diffie–Hellman key exchange mechanism is responsible for establishing keys before communication occurs between A and B and it is only known to the entities communicating with one another (Dyson et al., 2020; *Ropsten Testnet Explorer*, 2021; Zheng et al., 2017). The keys are required to ensure the integrity, security and authenticity of the transactions when both entities generate transactions (Ismail et al., 2020; Zheng et al., 2018).

6.3.2.3.1.1 Transactions Patterns: In BlockPres, a set of attributes is defined as a transaction related to the P_i prescription record and information inside the record is encrypted with SK between the sender and receiver. In this case, the sender and receiver can be P_i, D_i, healthcare providers and vice versa. There are three types of the transactions described in the following sections: Genesis transaction (Tx_{Gen}), DB transaction (TX_{DB}) and PU_{bc} transaction ($TX_{PU_{bc}}$).

6.3.2.3.1.2 Genesis Transaction: Genesis transaction (Tx_{Gen}) (Equations (6.1) and (6.2)) creates the first hash in a new blockchain. Initially, the transaction is created when the P_i registers and is stored in a hospital database. The DB stores data from the connected department in a hospital, for example, a surgical dept where the following is the case:

Tx_{Gen}	is a genesis transaction created by any user in the system;
$txid$	is a transaction ID;
Pid	is a patient ID;
SKP	is a secret key;
PKP	is a public key;
SC	is a smart contract;
DB	is a private database;
$Signs1, s2, s3, s4, \ldots sn$	is a message signed by the patient/doctor using a private key which contains attributes related patients medical record.

$$Tx_{Gen} = Reg([Fname, Lname, Add,], SKP, PKP, SC, Sign) \tag{6.1}$$

$$Tx_{Gen} = \epsilon nc([txid, PTid, Sign(s_1, s_2, s_3, s_4, \ldots s_n, PKP)], SKP, DB) \tag{6.2}$$

Equation (6.2) is the encrypted transaction created by the users in using a private key.

6.3.2.3.1.3 Local Database Transaction: In order to store the prescription record, P_i, in the hospital DB and for validation, this transaction (Equation (6.3)) is created by the healthcare provider: D_i, N_K and administration. The transaction can be represented as a tuple where, in addition to the previous variables, the following are included:

Tx_{DB}	is a DB transaction created by any user in the system;
D_i	is a Doctor ID;
SKd	is a doctor secret key;
PKd	is a doctor public key.

$$\begin{aligned} TxDB = &\epsilon nc([txid, PTid, Sign(s1, s2, s3, s4, \ldots sn, PKP)], SKP, [D_i, SKd, PKd, \\ &Sign(s1, s2, s3, s4, \ldots sn, DB) \end{aligned} \tag{6.3}$$

Equation (6.3) is the encrypted transaction created by the healthcare providers to store the patient record using the private key.

6.3.2.3.1.4 Public Blockchain Transaction: Healthcare providers generate this transaction (Equation (6.4)) to upload patient records as keywords to IPFS, which works as a $PUbc$ in the system. The transaction accesses the record at a healthcare provider if and only if the patient has a prescription record. This transaction is represented as a tuple below.

$TxPUbc$	is a public blockchain transaction;
Kw	is a keywords search by healthcare providers in a $PUbc$;
PRd	is a patient record.

$$TxPUbc = \epsilon nc([txid, PTid, PKP], [D_2ID, PKd, Sign, kw, SC, DB], PUbc) \tag{6.4}$$

In the transaction above, H_2 sends a request to H_1 DB from $PUbc$ to access a specific patient record. By signing SC using a public and private key, the transaction in (6.5) represents the reply from H_1, providing the patient record and allowing H_2 access to the patient record. Please confirm if the brackets are correctly added. If not, please revise.

$$TxPUbc = \epsilon nc([txid, Pid, PKP], [D_2ID, PKd, Sign, kw, SC, DB, PRd], PUbc) \tag{6.5}$$

6.3.2.4 Data sharing & Synchronisation Phase

Patient P_l visits the hospital H_ι to see the doctor D. Doctor D needs to access patient history in the hospital H_k to identify the diagnosis. Data synchronization phase includes the following steps are required to be executed using the input:

- $PK_\iota = g^j$ and $PK_D = g^D$
- If the doctor gets the permission of P_ι
- D and P_l sends private keys and identities to the SYS_m
- SYS_m computes the re-encryption key $rk_{j\to D} = x_D/x_j \bmod p$
- SYs_m sends extraction instruction about patient P_ι medical records to the hospital H_k

- The server of H_k sends encrypted history records to the SYS_m
- SYS S_m initially computes $h = \mathrm{Hash}_3(C_1, C_3, C_4)$ if $\varrho(C_1, PK_l, jx^h yz) = \varrho(g_1, C_2 C_5)$ includes
- SYs_m computes $C_2 = C_2^{rkj \mapsto D} = PK_D^r$ sends the ciphertext $C_D = (C_1, C_2, C_3, C_4, C_5)$ to D using the server of H_l
- P_l computes $P_1 = g^r$

a. $P_2 = \left(g_2^{t\iota j}\right)^{1/xj} \mathrm{Hash}_1\left(PK_l^r\right)$ and sends

b. $P_\beta = (P_1, P_2)$ to the server of H_ι where $r \in \mathbb{Z}_p^*$ as a random number

- The server of H_ι make sure $\varrho(C_1, PK_{\iota j} x^h yz) = \varrho(g_1, C_2, C_5)$ include the server computes $P = P_2 / \mathrm{Hash}_1\left(U_1^{tl}\right)$ to ensure $C_3 = \mathrm{Hash}_2(C_2, P)$ is true, if not, the session is terminated
- D computes $K = \varrho(C_2, g)^{1/xD}$ if $[F(k, C_1, C_3)]_{sp-sp_1} = [C_4]_{sp-sp_1}$ then D recovers $m = [C_4]_{sp1} \oplus [F(k, C_1, C_3)]_{sp1}$, otherwise the session will be terminated.

6.3.2.5 Incentivisation Phase

The incentivisation program will be offered to patient P_l and P_{l+1} to encourage them to use the hospital services. Following are the key steps that are required to be followed:

- P_ι sends P_ι^{ID} and $P_{\iota j}^{ID}$ to $P_{l+1,j+1}$ and then
- $P_{l+1,j+1}$ send P_{l+1}^{ID} and P_{j+1}^{ID} to P_{lj}
- $P_{\iota j}$ select a secret integer $\eta_{\iota j} \in \mathbb{Z}_p^*$ and a prime number $z \in \mathbb{Z}_p^*$ randomly
- Compute $\alpha = z^{-1} \bmod p$
- $S_{\iota j} = g^{z\eta_{\iota j}}$ and $T_{\iota j} = g^{\alpha\eta_{\iota j}}$

- $P_{\imath j}$ send $(z, S_{\imath j}, T_{lj})$ to $S_{l+1,j+1} \cdot S_{l+1j+1}$ randomly

- Select $\eta_{t+1j+1} \in \mathbb{Z}_p^*$

- Compute $\alpha = z^{-1} \bmod p$

- $S_{l+1j+1} = g^{z\eta l+1j+1}$ and

- Sends message (S_{l+1j+1}, T_{l+1j+1}) to $P_{\imath j}$

- $P_{\imath j}$ computes $k_{\iota j} = T_{\iota+1j+1}^{\eta\iota j}$

a. $MAC_{lj} = MAC_{k\iota j}\left(T_{lj}, \alpha, S_{l+1j+1}, P_{l+1}^{ID}{}_{j+1}, I_{lj}\right)$

b. Sends MAC_{lj} to P_{l+1j+1}

c. Then P_{l+1j+1}

d. Computes $k_{l+1j+1} = T_{lj}^{\eta\iota+1j+1}$

e. $MAC_{l+1j+1} = MAC_{kl+1j+1}\left(P_{l+1j+1}^{ID}, S_{l+1j+1}, T_{lj}, \alpha, I_{lj}\right)$

f. If $MAC_{l+1j+1} = MAC_{\iota j}$ contains $P_{\iota+1j+1}$

g. Compute $MAC_{l+1j+1}^{I} = MAC_{kl+1j+1}\begin{pmatrix} P_{lj}^{ID}, S_{lj}, T_{l+1j+1}, k_{l+1j+1}, \\ I_{l+1j+1} \end{pmatrix}$

h. Send it to $P_{\imath j}$, otherwise session will be terminated

- P_{lj} computes $MAC_{lj}^{I} = MAC_{k\iota j}\left(P_{lj}^{ID}, S_{lj}, T_{l+1j+1}, k_l, I_{lj}\right)$

a. If $MAC_{lj}^{I} = MAC_{l+1j+1}^{I}$ is True

b. The P_{lj} computes the session key $K = S_{l+1}^{\eta\iota j}$

c. The ciphertext $K = E_{k\iota j}(k)$

d. Sends $\mathbb{K} = E_{k\iota j}(K)$

e. Sends $\mathbb{K}$ to $P_{l+1}j + 1$

f. If not, then session will be terminated.

- $P_{\iota+1j+1}$ decrypt ciphertext $\mathbb{K}$ to get the session key K, if incentivisation tokens $I_{\iota j}$ and $I_{\iota+1j+1}$ are same, the correct incentive will be given to the patient P_ι using the following protocol

a. $k_{\iota+1j+1} = T_{\iota j}^{\eta_{\iota+1j+1}} = g^{\alpha\eta_{\iota+j+1}\eta_{\iota j}} = T_{l+1j+1}^{\eta_{\iota j}} = k_{\iota j}$

6.4 Security Analysis

In this section the security analysis is completed as part of the the incentive mechanism which secures the incentivisation process, resists attacks. and proves robustness.

6.4.1 Mutual authentication

This security analysis is based on mutual authentication process where only authenticated patient P_ι can exchange the information with SYS_m.SYS_m then verifies that the patients is legitimate using the following protocol.

$$P_\iota = a_\iota \frac{1}{S_{\eta\iota j}} b_\iota \left(P_\imath^{ID} + T_{\imath j}\right)$$

$$=a_\iota b_\iota \left(K_\iota\right)$$

Therefore, it is not possible for a malicious user to know the value of a_ι, b_ι because of strong authentication, hence SYS_m achieves the authentication of patient P_l

6.4.2 User Anonymity

It is not possible for an attacker to know and produce this unique identity for each user as this identity will be stored on the blockchain. This identity is same as storing the public key in a public blockchain. In every authentication step, P_ι pseudo-identity $P_\iota^{ID} = E_D\left(ID_\iota \oplus \partial_\iota \| \partial_l\right)$ is accepted instead of actual identity. Additionally, during data sharing and synchronisation phase, H_l stores pseudo-identity P_l^{ID} in the blockchain which does not disclose patient ID, therefore, the identity of patient is hidden, and this scheme prove anonymity.

6.4.3 Non-Repudiation

To achieve the non-repudiation in the system, patient credential is stored in the blockchain with some unique characteristics, such as uniqueness, unforgeability and difficult to replicate. Furthermore, this scheme provides a strong feature of revocation and update of patient credential. Therefore, if any patient losses his/her app, the system immediately performs revocation and block all the access and revoke credentials. This functionality also added in the blockchain ledger. Hence, this scheme supports nonrepudiation in blockchain.

6.4.4 Impersonation Attack

This scheme provide security if any attacker tries to impersonate, if any attacker A_ι impersonate patient P_ι and tries to create a valid request with the key $K_{\iota j}$, where $K_{\iota j}$ represents shred key between patient P_ι and system manager SYS_m. Therefore, the authentication will be achieved using Auth $h_{\iota j}$ = $\mathrm{Hash}_\iota\left(P_\iota \| K_l \| T_\imath \| S_l\right)$. Computing the key a_l, b_l, P_l is difficult in $\mathbb{Z}_p^*$.

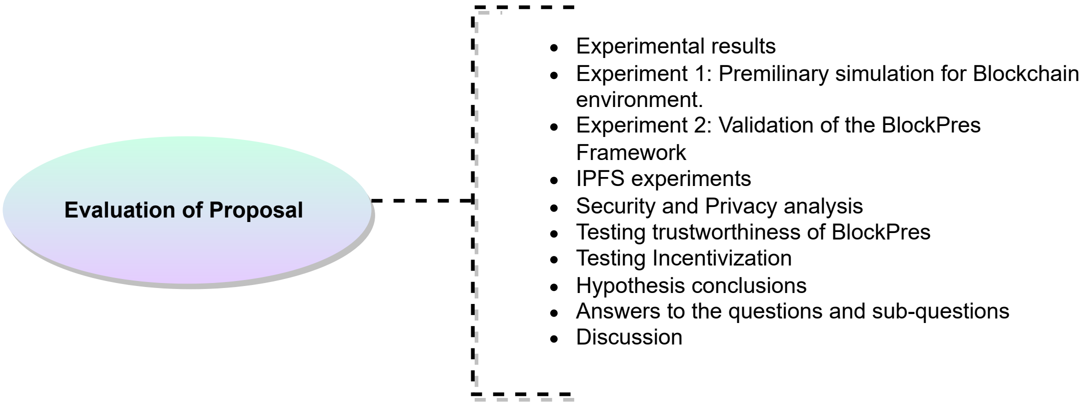
6.5 Conclusion

This chapter specifies the proposed incentivisation mechanism for the prescription system to address inequality. The contributing factors to the inequality, such as trust and value, loss of status, class differences, and racial bias, are explained and show that the factors play an important role in leading to inequality in the prescription system. Incentivisation and patient engagement are proposed as effective solutions to address the inequalities and improve access to healthcare services for Maori people. Therefore, Incentives can improve patient behavior, attitude, and identity, increase trust and value in the prescription system, and promote collaboration between patients, providers, and payers. The proposed incentivisation mechanism and its concrete implementation are presented using formal methods to prove the solution mathematically. Additionally, security parameters are analysed to ensure the secure and trustworthy provision of the incentivisation process and patient data to healthcare providers.

Chapter 7

Evaluation of Proposal

7.1 Introduction



In Chapter 2, questions and hypotheses were formulated, which served as the basis for designing the BlockPres system architecture and framework in Chapter 5. The previous Chapter 6 presents the construction of an incentive mechanism in the context of BlockPres Artifact using cryptographic techniques. Chapter 7 evaluates the Artifact and incentive mechanism proposed.

A prototype for a blockchain-based prescription management system is developed and tested to evaluate the artifact and incentive mechanism using simulated data. The

BlockPres framework and prototype are evaluated using experimental results on the Ethereum network, which is implemented using the Solidity language in the Remix integrated development environment. Initially, a preliminary blockchain simulation is conducted to test the blockchain technology's performance, followed by the experimental results for the BlockPres system. Hypotheses are evaluated to determine their acceptability in relation to the literature review and the study's findings. Moreover, research questions and sub-questions are answered accordingly. Finally, a discussion is presented to reconcile the study's contributions.

Chapter 7 is structured as follows. Section 7.2.1 presents the system specification and simulation environment, while Section 7.2.2 presents the preliminary results of the Ethereum blockchain's performance. The evaluation of the BlockPres framework is presented in Section 7.2.3, and the experimental results for IPFS are presented in Section 7.2.4. Section 7.3 discusses the security and privacy analysis of the proposed system, while Section 7.13 evaluates the trust level of the BlockPres system. Hypotheses conclusions are presented in Section 7.5 on page 198, and Section 7.6 on page 207 evaluates the hypotheses from the literature by answering the research questions and sub-questions. Finally, a discussion section reconciles the findings with the literature review chapters.

7.2 Experimental Results

This section presents an evaluation of the BlockPres framework and model. Section 7.2.1 details the simulation preparation, the environment and system specifications. Section 7.2.2 presents the preliminary simulation to validate the effectiveness of an instantiation of the model. When satisfied with the performance of the blockchain, an instantiation of BlockPres is presented in Section 7.2.3 and the effectiveness of the model is assessed.

7.2.1 System Specification and Simulation Environment

The evaluation uses the Ethereum network to perform a simulation of BlockPres. The Ethereum network provides more features than the bitcoin network (*Ropsten Testnet Explorer*, 2021; Zheng et al., 2017), for example, the application of smart contracts and scripting through Solidity (Kamel Boulos et al., 2018; Ismail et al., 2020), that Ethereum consumes less computational power to validate transactions (Rahman et al., 2019; Gordon et al., 2018), Ethereum is able to validate more transactions per second than bitcoin (Gordon et al., 2018) and the capability to build Decentralised Applications (DApps).

This simulation makes use of the Remix Integrated Development Environment (IDE), which uses the Solidity language to simulate the creation and use of Smart contracts (Kamel Boulos et al., 2018). In addition, Ganache is also used, which is a blockchain-based environment that provides virtual accounts that are linked to the Remix IDE and enables the execution of smart contracts. The ability for Ganache to produce unique IDs, the provision of mining processes to validate transactions and the ability to write the transactions to the blockchain provides the core functions in the simulation. Moreover, every virtual account has predefined amounts in the form of ether stored. Virtual accounts use these predefined ether amounts as a cryptocurrency (Ismail et al., 2020). The third important component is MetaMask, which is a browser extension that provides connectivity with Ganache and the Remix IDE (Dong et al., 2019). The initial simulation is run on a local machine with the following specifications: Macbook Pro, HDD volume of 500 GB, 16 GB of RAM, CPU is a X64-based Intel processor running at 1.61 GHz and a 64-bit operating system.

7.2.2 Experiment 1: Preliminary Simulation for Blockchain Environment

To verify that a blockchain can process a sufficient number of service requests, two months of Ethereum transactions have been analysed (Rahman et al., 2019). The evaluation assesses the performance metrics block size, number of transactions per block, transactions per second, total number of transactions, median confirmation time and average block size.

The data shown in below figures illustrates Ethereum blockchain performance during the simulation. The blockchain grew at a more or less constant rate, at 2.686 GB per day Figure 7.1, but during that period the median confirmation time was less constant in Figure 7.2, although the overall median confirmation time is 10.2 min per block. The number of unique transactions per block is 2200 Figure 7.3 and the average block size is 1.2 MB Figure 7.4. In terms of average speed, the Ethereum blockchain network executed six transactions per second Figure 7.5 with a total number of transactions processed per day of 360,000 Figure 7.6.

Consideration of the raw data allows a summary conclusion that Ethereum is sufficient to cope with the needs of BlockPres. This solution meets the basic requirements of BlockPres and satisfies the needs of storage and retrieval of patient records in a secure and trusted environment.

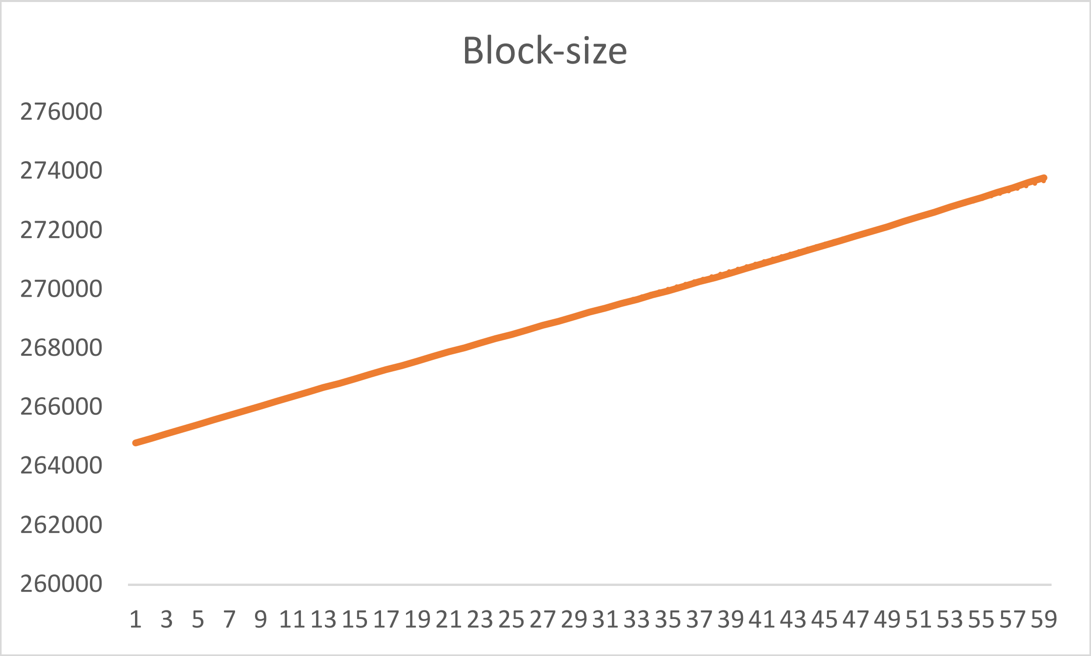


Figure 7.1: Ethereum block size growth

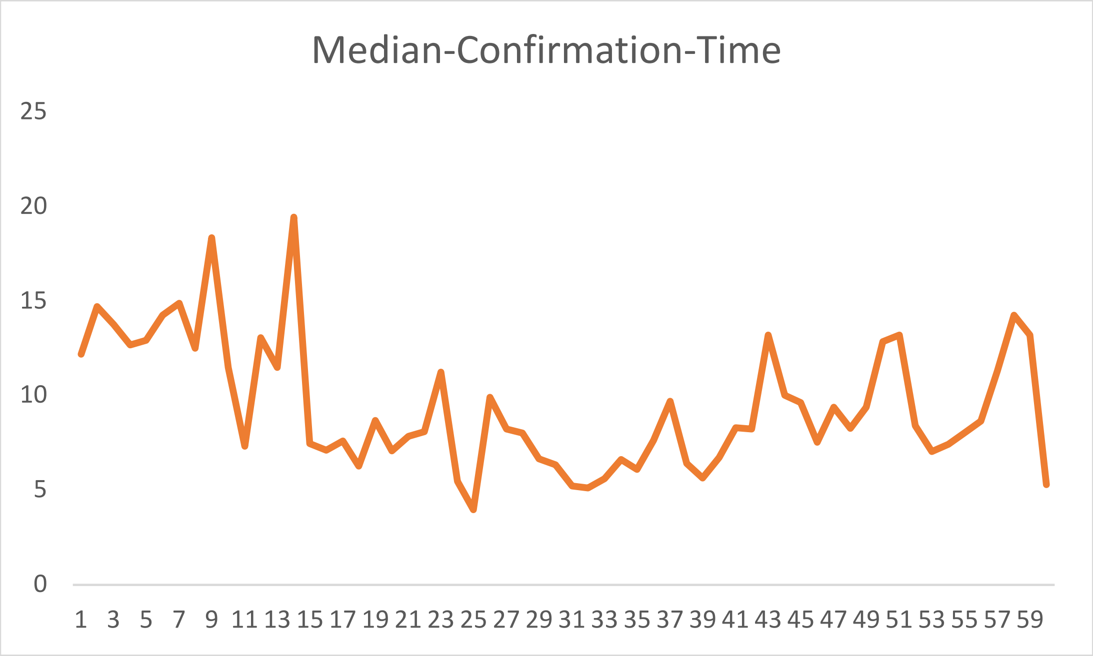


Figure 7.2: Transaction confirmation time

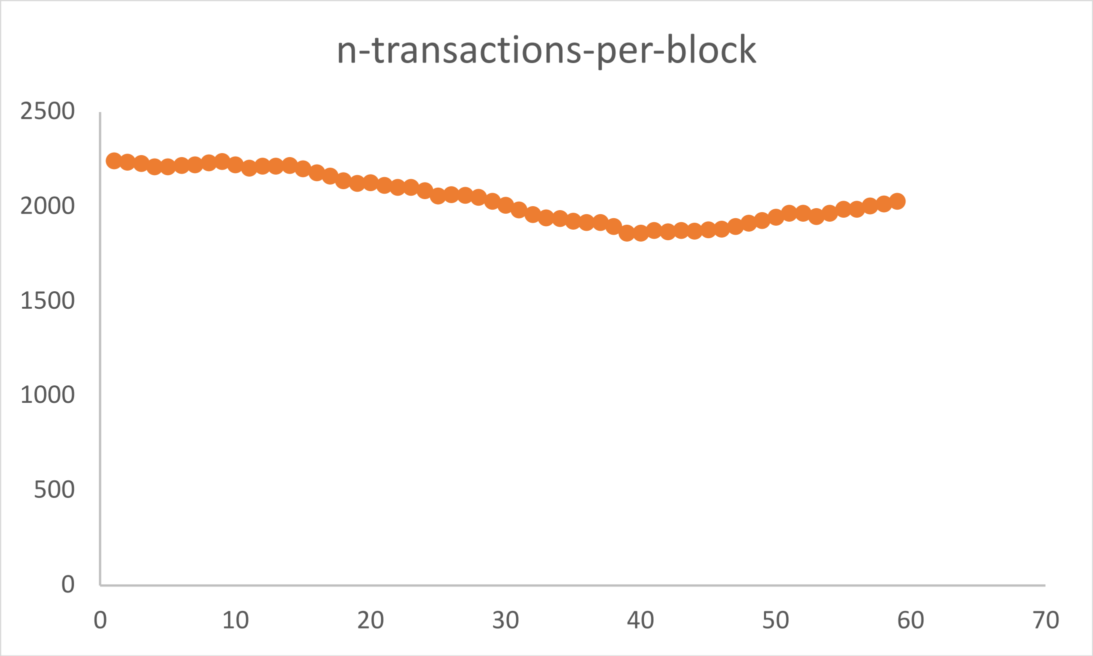


Figure 7.3: Number of transactions per block

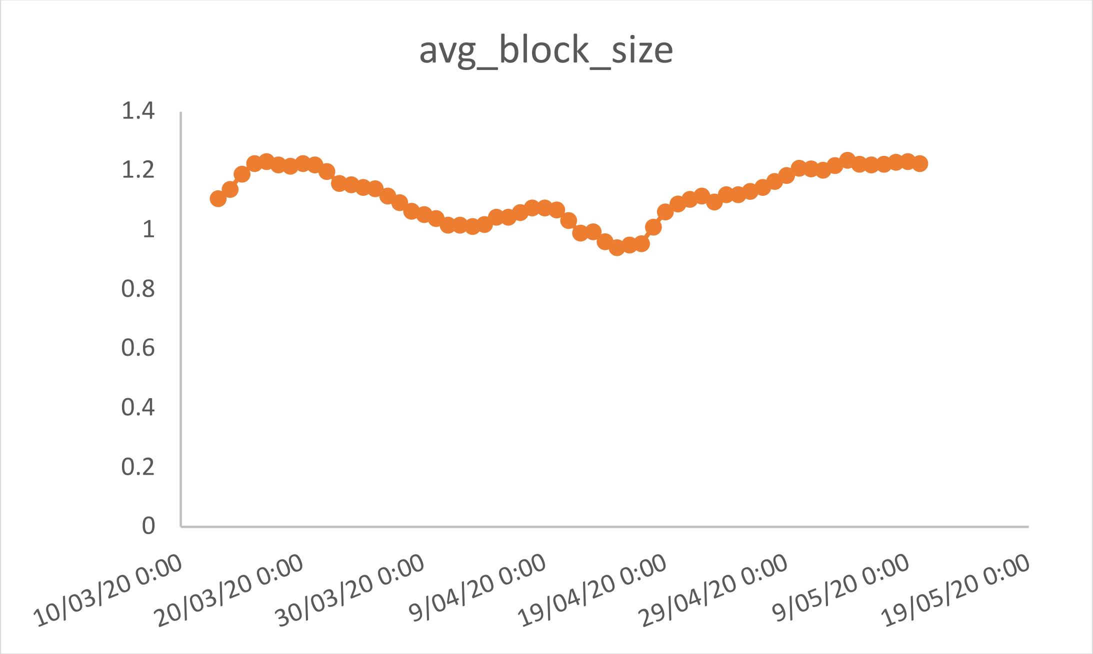


Figure 7.4: Transaction confirmation time

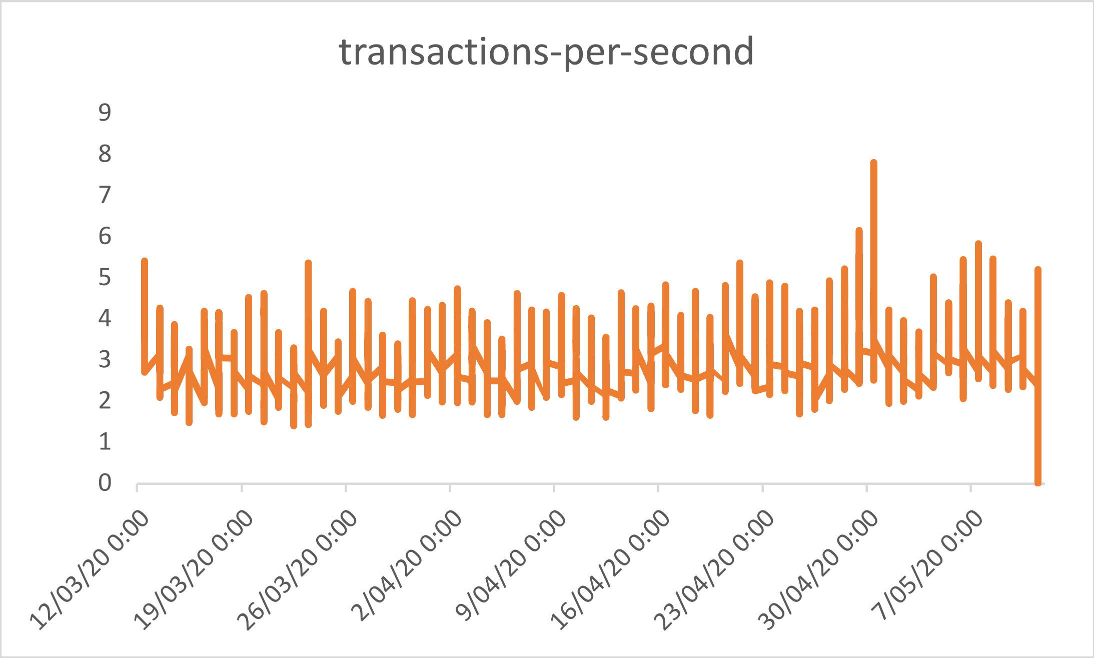


Figure 7.5: Number of transactions per second

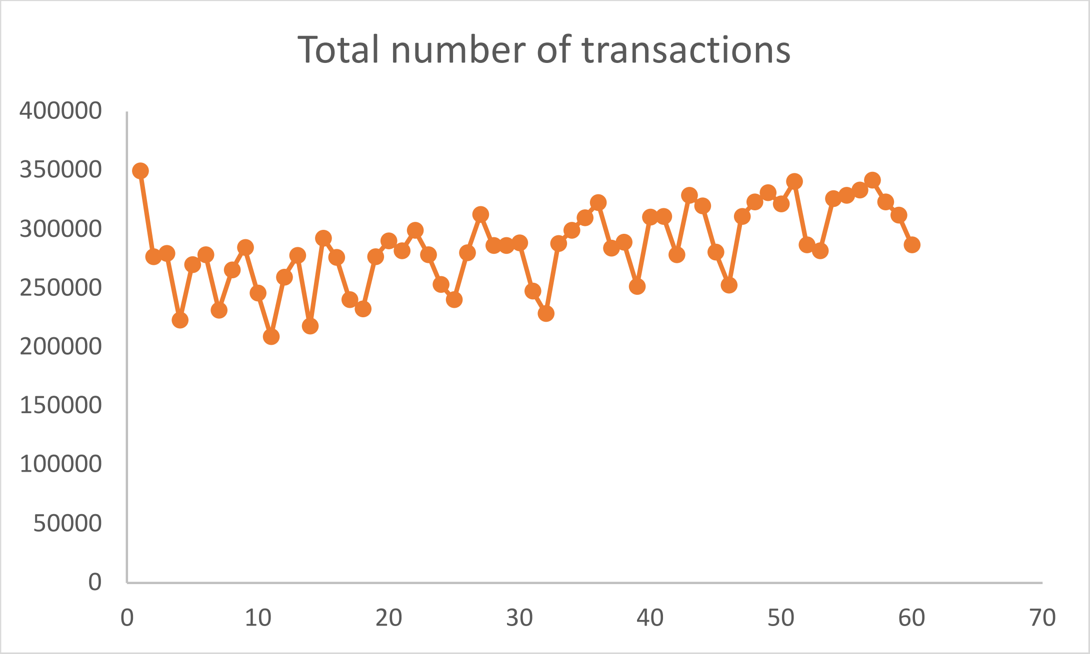


Figure 7.6: Total number of transactions

7.2.3 Experiment 2: Validation of the BlockPres Framework

Gas is a fundamental component of the Ethereum blockchain and its use impacts transaction speed and computational power (Rahman et al., 2019; Dong et al., 2019). There is an assumed difference in cost if Proof of Work (PoW) or Proof of Stake (PoS) are used. On the Ethereum network, each time a transaction is completed, a smart contract is executed and a cost is incurred measured as gas. The amount of gas consumed is the cost of mining blocks and sending them to the blockchain network. The unit of gas depends on the size of the block or smart contract complexity. For example, a simple transfer may use as much as 21,000 gas whereas a more complex transaction such as that seen in a complicated financial transaction could use more than 1,000,000 gas (Yanwei et al., 2019). These issues have largely been resolved on the Ethereum ecosystem but the potential remains for excessive transaction costs.

Each unit of gas has a price referred to as the “gas price”. Gas prices are denoted in Gwei (Daniel & Roth, 2021), where 1 ETH = 10^18 Gwei. Given a Gwei price of five, a 21,000 gas transaction would cost 21,000 × 5 = 105,000 Gwei. The transaction cost can be calculated by using Equation (7.1) (Yanwei et al., 2019).

$$\text{Total Cost Gwei} = \text{Gas Used} \times \text{Gas Cost} \tag{7.1}$$

A comparison of PoW and PoS is carried out on the simulation and shown in Table 7.1 and Figure 7.7. PoW is shown as the blue bars and PoS as the orange bars in the figure.

Table 7.1: Comparison of Transactions per second, PoW vs. PoS.

Transaction Per Second	PoS (Transaction)	PoW (Transaction)
0.5	2.5	0.5
1	3.6	0.8
1.5	4.2	1.8
2	5.1	3.1
2.5	5.4	3.5
3	6.2	4.3

Table 7.1 shows a comparison of PoS versus PoW transactions per second. Overall, the present data show that PoS takes less time to validate a transaction, such that, in 0.5 s, PoS validates 2.5 transactions compared with PoW which validates 0.5 transaction or that it takes around twice as long to process the first transaction. The gap closes over longer periods but, on the face of it, the appearance is that PoS is somewhat more time efficient.

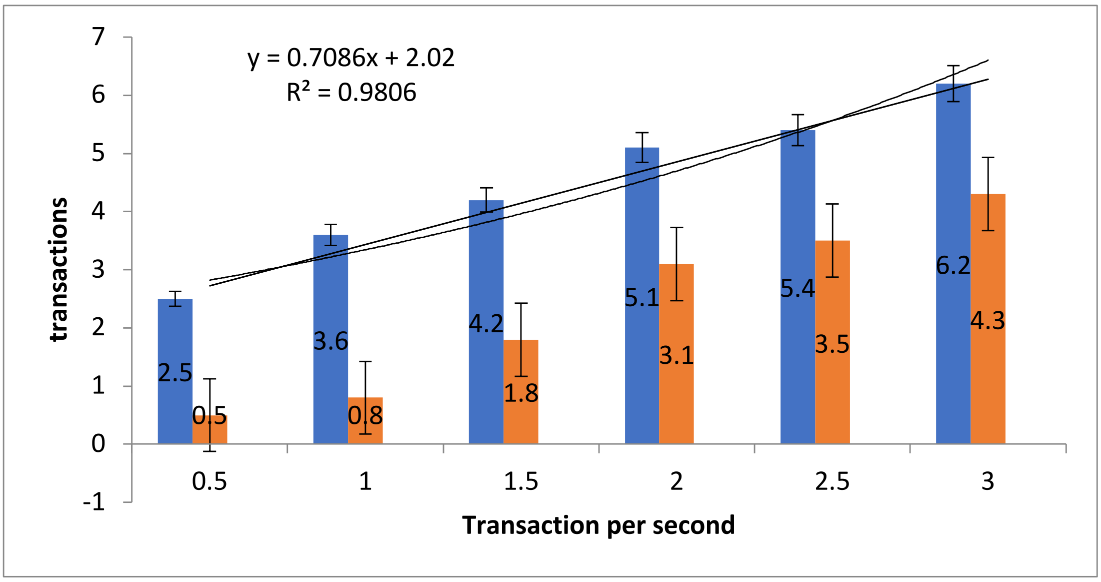


Figure 7.7: Comparison of transaction speed between PoW and PoS.

$$SE = \frac{\sigma}{\sqrt{n}} \tag{7.2}$$

A Standard Error (SE) is calculated (Equation (7.2)) where SE represents the standard deviation of the transactions and total number n of transactions per second. The standard deviation shows the variability and dispersion of the transactions. The SE of PoW is ± 0.86 and PoS is ± 1.54, indicating that the mean value of transactions is close to the actual mean value and that, relatively, the error rate of PoW is less than PoS.

The Straight-line fit and R^2 are applied to calculate the variation in transactions. The value $y = 0.7086x$ shows the difference in time when transactions increase and 2.02 represents the $y - intercept$. The value of R^2 at 0.9806 implies a correlation between transaction and time.

The smart contract deployment cost is set as a default gas price of ten (10) gwei. Various applications of smart contracts consume different amounts of gas. Table 7.2 and Figure 7.8 illustrate the gas consumption of the two consensus mechanisms simulated in the system. To calculate the transaction cost and execution cost of PoS and PoW, two algorithms are deployed on the smart contract. The minimum transaction and execution gas of PoS is 3,000,000 with a file size of 75 kb. The minimum transaction gas for PoW is 28,000,000. The experimental analysis shows that PoS is more efficient than PoW in terms of gas consumption on both the transaction and execution of blocks and processing of smart contracts. The PoW requires a lot of computational power to verify blocks and needs significant execution time.

Table 7.2: Comparison of Smart Contract deployment cost of PoS vs. PoW.

2*File Size (kb)	PoS	PoW
	Gas (mill.)	Gas (mill.)
12,098	2.0	51.0
6098	1.5	45.0
3043	1.2	40.0
2034	1.0	35.0
456	6.0	31.0
75	3.0	28.0

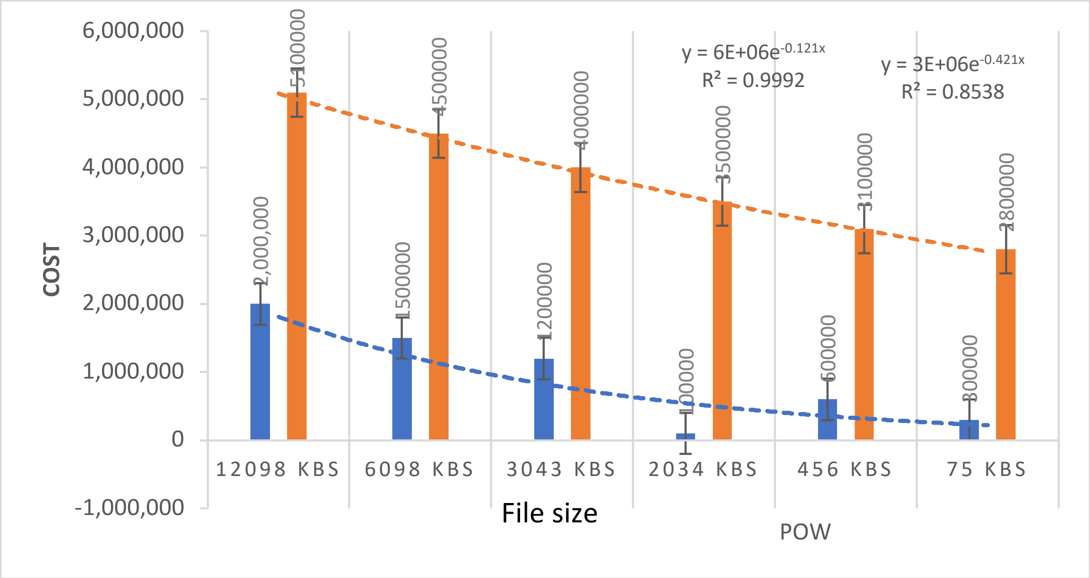


Figure 7.8: Comparison of smart contract deployment cost of PoW and PoS.

In Figure 7.8 SE , the straight-line fit and R^2 are calculated. The SE shows the variability and dispersion of the smart contract deployment cost for PoW and PoS. The SE of PoW is $\pm 46 \times 10^6$ for file size 12,098 kb; $\pm 41 \times 10^6$ for 6086 kb; $\pm 35 \times 10^6$ for 3043 kb; $\pm 32 \times 10^6$ for 2034 kb; $\pm 27 \times 10^6$ for 456 kb; and $\pm 23 \times 10^6$ for 75 kb. The SE of PoS is $\pm 16 \times 10^6$ for file size 12,098 kb; $\pm 12 \times 10^6$ is for 6098 kb; $\pm 9 \times 10^6$ for

3043 kb; ±7 × 10^6 for 2034 kb; ±4.5 × 10^6 for 456 kb; and ±2 × 10^6 for 75 kb. The SE implies that the mean value of deployment cost is close to the actual mean value and that the deployment cost of PoW is relatively high compared with PoS. The straight-line fit (y) and R^2 are calculated to determine the change in deployment cost. The y value shows the difference in cost when the file size increases in both PoS and PoW. The R^2 value shows the correlation between cost and file size.

The smart contract includes the functions to add, delete, access and retrieve files (Figure 7.9 and Table 7.3). The gas is consumed whenever a healthcare provider adds a file to the Blockchain network, deletes an existing file from the network with the permission of the record owner, access a file when a patient visits another healthcare provider and retrieves it. Here, the files are prescriptions generated by the healthcare provider and uploaded to the smart contract. Figure 7.9 and Table 7.3 present the minimum transaction and execution cost of functions deployed on smart contracts.

Table 7.3: Gas consumption cost to add, delete, access and retrieve files.

2***File Size (kb)**	**Functions (as Gas Consumed)**			
	Add File	**Delete File**	**Access File**	**Retrieve File**
6098	56,334	29,110	79,900	79,110
3043	51,023	27,990	58,009	16,012
2034	46,800	25,120	37,100	14,540
456	36,610	22,231	9210	12,203
75	24,022	20,021	7001	10,012

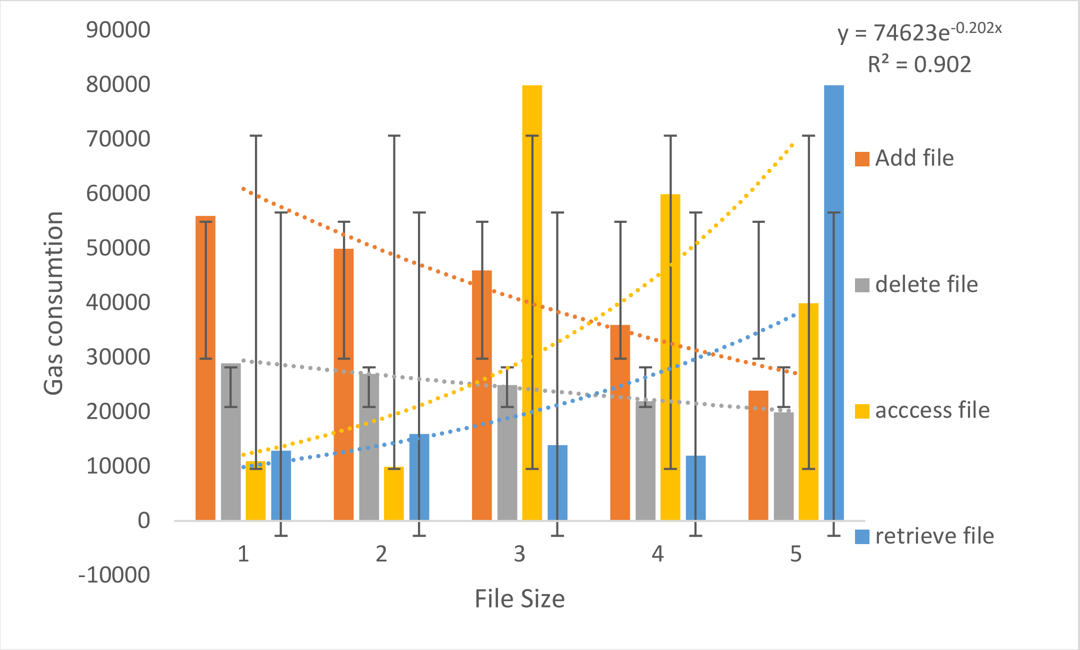


Figure 7.9: Gas consumption cost to add, delete, access and retrieve files.

The SE calculated for the gas consumption cost of the add function is ±43,432 for 6098 kb; ±38,993 for 3043 kb; ±35,003 for 2034 kb; ±26,321 for 456 kb; and ±15,022 for 75 kb. SE for the delete function is ±24,011 for 6098 kb; ±19,012 for 3043 kb; ±15,001 for 2034 kb; ±14,210 for 456 kb; and ±13,211 for 75 kb. The SE for access functions is ±65,900 for 6098 kb; ±49,324 for 3043 kb; ±33,021 for 2034 kb; ±6003 for 456 kb; and ±5541 for 75 kb. SE for the retrieve function is ±71,122 for 6098 kb; ±12,431 for 3043 kb; ±12,001 for 2034 kb; ±9229 for 456 kb; and ±7671 for 75 kb. SE implies that the mean value of gas consumption cost of functions is close to the actual mean. The straight-line fit is 74,623e and R^2 is 0.902 calculated as the change in Gas consumption and correlation between Gas and file size.

Figure 7.12 and Table 7.4 show a comparison of transaction latency and throughput. Transaction latency (Figure 7.12a) is how much time it takes for a miner to validate a transaction. The latency is calculated as an average of transactions (Equation (7.3)) run on the simulated system and measured in milliseconds (ms). The average time to validate transactions is 2343 ms and miners validate five transactions in 9234 ms. The SE calculated for Figure 7.12a are 0.5 transactions in ±932 ms, 1 in ± 1912, 2 in ± 2401, 3 in ± 3405 , 4 in ± 4532 and 5 in ± 7098. The straight fit line is 878.26, which shows the change in latency, and R^2 is 0.9357, which shows a correlation between latency and transactions.

$$\text{Latency} = \frac{\text{Total time}}{\text{Total Tx}} \tag{7.3}$$

Table 7.4: Transaction latency and throughput.

Latency		**Throughput**	
Transactions	**Latency (ms)**	**Patients**	**Throughput (ms)**
0.5	1123	5	300
1	2343	10	500
2	3000	20	1300
3	4590	25	1600
4	6712	30	2400
5	9234	40	3000

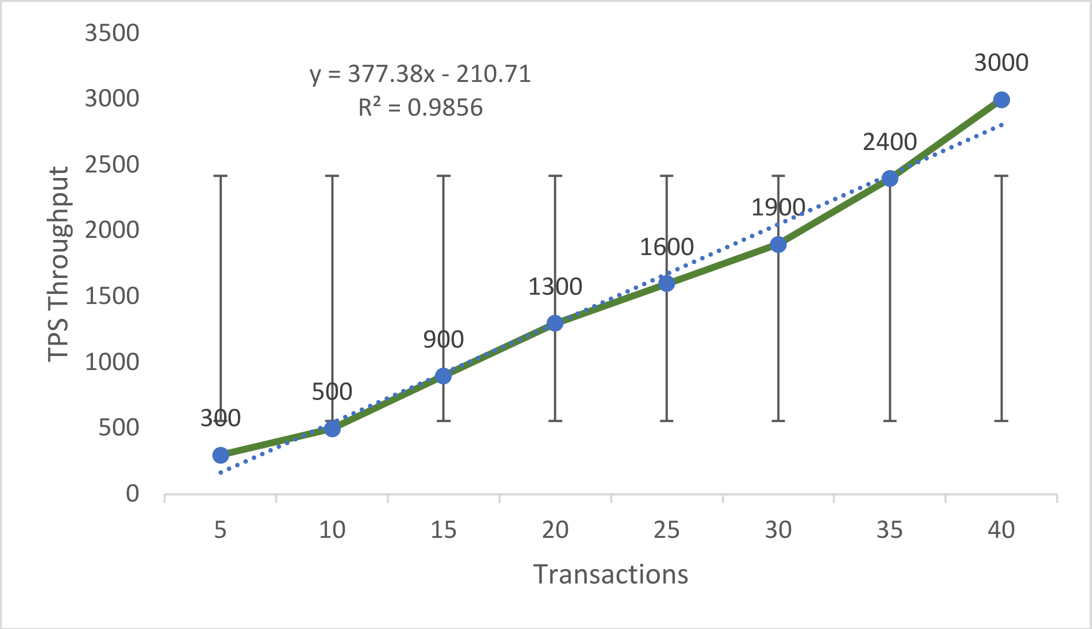


Figure 7.11: Transaction throughput

Figure 7.12: Comparison of transaction latency and throughput.

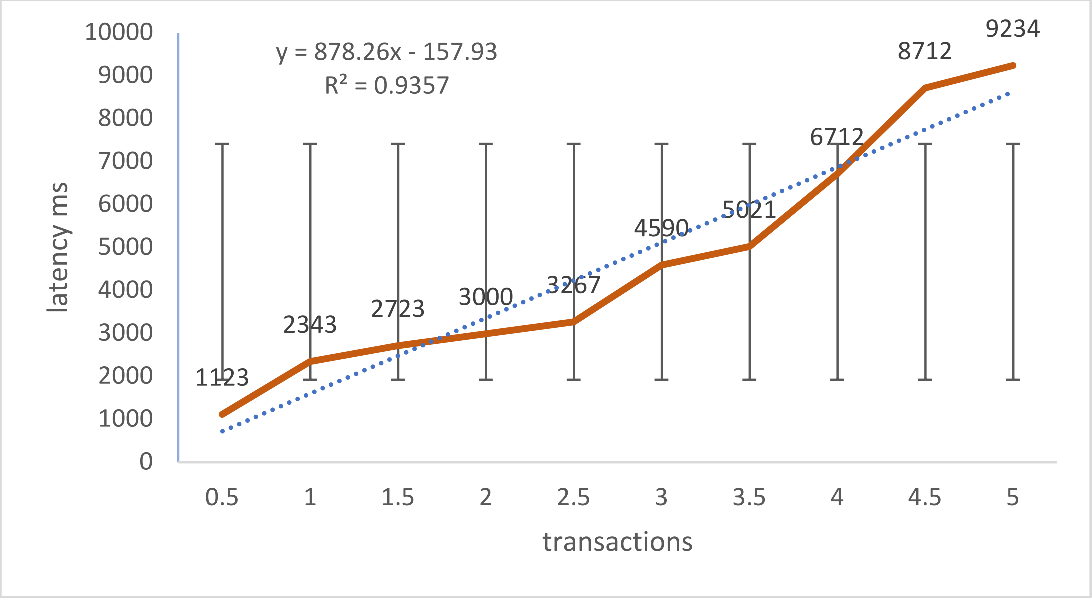


Figure 7.10: Transaction latency

Throughput (Figure 7.12b) is how much time it takes for a transaction be validated and is the average of the total time it takes to process transactions over the overall total of time (Equation (7.4)).

$$\text{Throughput} = \frac{\text{Total Time tx}}{\text{Total Time}} \tag{7.4}$$

The simulation data in Section 7.2.2 shows that as the number of users increase, the throughput also increases in a linear fashion. This provides some evidence of the efficiency of the BlockPres system. The SE of transactions over throughput are five transactions in ±300 ms, 15 in ±900 ms, 25 in ±600 ms, 30 in ±1900 ms, 35 in ±2400 ms and 40 in ±3000 ms. The straight fit line is 377.38, which shows the change in throughput, and R^2 is 0.9856, implying a correlation between throughput and transactions.

The transaction and execution cost of adding entities to the smart contract Table 7.5 and Figure 7.13 are calculated as Gwei. The entities are hospitals, doctors, pharmacies and associated functions such as the adding of prescriptions, modification of prescriptions and so on. The cost varies depending on what consensus algorithm is used to perform the smart contract functions. The transaction and execution cost of adding an entity is 260,000, verifying an entity is 125,000, adding and modifying costs are 105,000 and 85,000, respectively, and the costs of adding a pharmacy are 95,000 and 86,000. The SE for the transaction and execution costs of adding a hospital are ±250,000 and ±210,000; costs for adding a doctor are ±280,000 and ±230,000; costs for verifying a doctor are ±100,000 and ±90,000; costs for adding prescription are ±7000 and ±6530; costs for modifying prescription are ±9500 and ±6430; and costs for adding a pharmacy are ±6400 and ±6210. By highlighting the difference between transaction and execution cost, the straight-fit lines for transaction and execution costs are 38.2411 and 32.1808. R^2 is 0.7621 for the transaction cost and 0.7904 for execution cost, which indicates a correlation between execution cost and transaction cost.

Table 7.5: Function cost comparison for transactions and execution.

Function	Transaction Cost	Execution Cost
Add hospital	290,000	240,000
Add doctor	330,000	270,000
Verify doctor	130,000	120,000
Add prescription	100,000	90,000
Modify Prescription	110,000	80,000
Add pharmacy	95,000	86,000

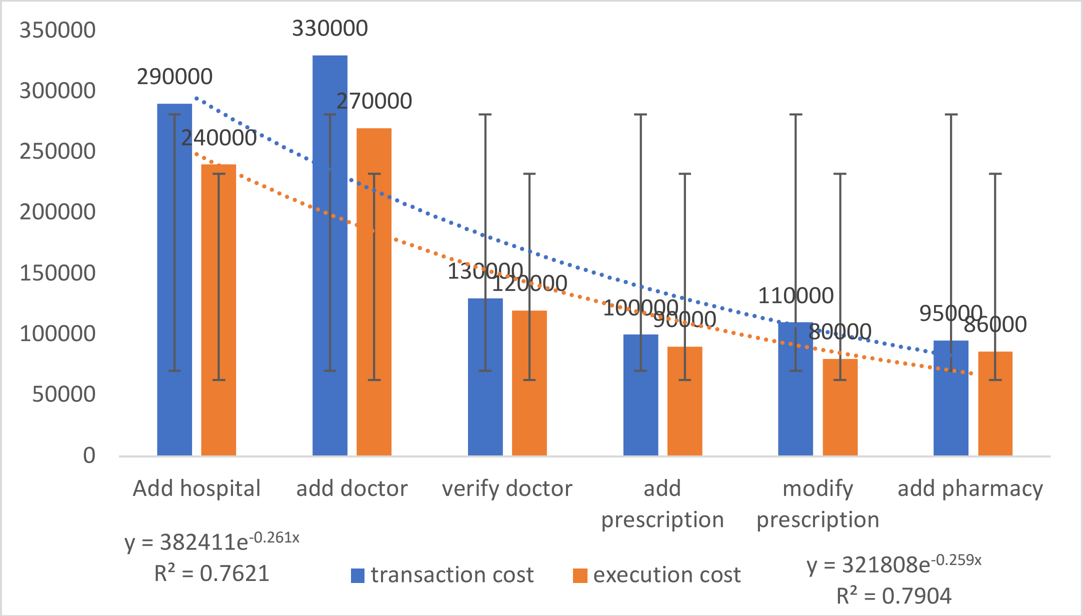


Figure 7.13: Function cost comparison for transactions and execution.

7.2.4 IPFS Experiments

In this section, the experiments of IPFS services in "BlockPres" prototype are performed, and the results are discussed.

7.2.4.1 Experiment 1: Records Uploading Speed

This section presents the experiments conducted on IPFS services in the "BlockPres" prototype and the resulting discussion.

The first experiment, "Experiment 1: Records Uploading Speed," focused on the upload speed of patients' records and the size of the files on IPFS. In this experiment, 51 patient records were uploaded to IPFS after being first uploaded to the blockchain network using Smart Contract and then sent them to IPFS using synchroniser. To determine the upload speed, the study selected 11 patients with different record numbers, namely 1, 5, 10, 15, 20, 25, 30, 35, 40, 45, and 51. Figure 7.14 and Table 7.6 present the results, showing that the upload speed for patient records of the 1atients is 1221ms, 1837ms for 5th, 1734ms for 10th, 1234ms for 15th, 1704ms for 20th, 1765ms for 25th, 1234ms for 30th, 1356ms for 35th, 1523ms for 40th, 2109ms for 45th, 2476ms for 51th. To assess accuracy and efficiency, the study calculated the standard error using Equation 1, measuring the difference between the actual mean value and the experimental values.

$$SE = \frac{\sigma}{\sqrt{n}}. \quad (1)$$

The SE of patients uploading speed for 1atient is ±1012ms, ±1534ms for 5th, ±1401ms for 10th, ±907ms for 15th, ±1509ms for 20th, ±1402ms for 25th, ±901ms for 30th, ±1123ms for 35th, ±1278ms for 40th, ±1845ms for 45th, ±2106ms for 51th. The straight fit line is y = 13.3x+1320.3, which shows the change and effect in patients and uploading speed in Equation 2. The R^2 is 0.2217, which shows the correlation between patients and uploading speed in Equation 3.

Similarly, Figure 7.15 and Table 7.6 show the calculated uploading speed of different file sizes. The uploading speed of file size 75kb is 1321ms, 456kb is 2423ms, 2034kb is 3145ms, 3043 is 3397ms, 6098kb is 3865ms, 12098kb 4796ms is measured. It is proved that the proposed "BlockPress" prototype efficiently uploads patient records on IPFS. Further, the SE of filesize 75kb is ±1045ms, ±2509ms for 456kb, ±3156ms for 2034kb, ±3334ms for 3043kb, ±3790ms for 6098kb, ±5012ms for 12098kb. The SE implies that the mean value of patients uploading speed and filesize speed on IPFS is close to the actual value. The straight fit line (regression analysis) using Equation 2 is y

= 62.227x + 1813.4 to show the change and effect when values increase, R^2 is 0.9559, implying a correlation between values in patients and uploading speed Equation 3.

$$Y_i = f(X_i, \beta) + e_i \ (2)$$

$$Correl(X, Y) = \frac{\sum(\bar{x} - \bar{x})(\bar{y} - \bar{y})}{\sum(\bar{x} - \bar{x})^2 \sum(\bar{y} - \bar{y})^2}$$

(3)

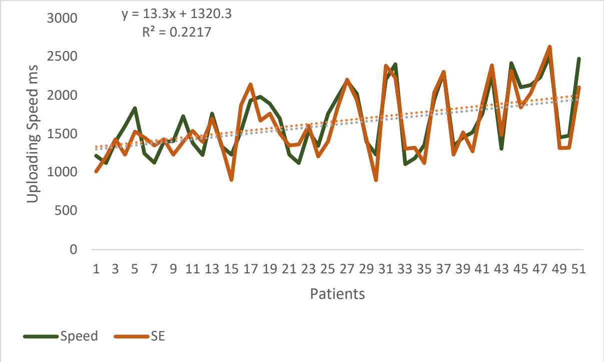


Figure 7.14: Patients Records Uploading Speed in IPFS

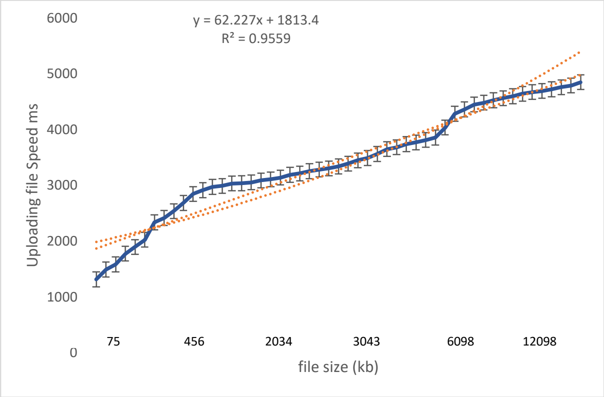


Figure 7.15: Patients file size (Uploading) Speed in IPFS

7.2.4.2 Experiment 2: Records Accessing Speed

The records accessing speed of patients and file sizes are measured in this section. This experiment analyses the accessing speed whenever a healthcare provider wants to

Patients Record Uploading Speed on IPFS					File Size Uploading Speed				
Patients	Uploading Speed (ms)	SE	(y)	R^2	File Size	Uploading speed (ms)	SE	(y)	R^2
1	1221	1012	51*13.3x+1320.3	51*0.2217	75kb	1321	1045	51*62.227x + 1813.4	51*0.9559
2	1123	1204			90kb	1498	1502		
3	1402	1432			110kb	1590	1634		
4	1602	1234			150kb	1783	1823		
5	1837	1534			190kb	1903	1934		
6	1245	1456			250kb	2032	2098		
7	1129	1354			356kb	2345	2465		
8	1398	1434			456kb	2423	2509		
9	1409	1232			510kb	2545	2534		
10	1734	1401			656kb	2690	2696		
11	1387	1543			1012kb	2852	2812		
12	1229	1398			1256kb	2920	2856		
13	1767	1698			1540kb	2980	2985		
14	1343	1357			1623kb	2996	2990		
15	1234	907			1756kb	3040	3050		
16	1538	1876			1812kb	3045	3050		
17	1934	2143			1856kb	3060	3045		
18	1984	1675			1915kb	3095	3056		
19	1893	1765			1956kb	3115	3098		
20	1704	1509			2034kb	3145	3156		
21	1234	1354			2256kb	3195	3165		
22	1123	1365			2343kb	3220	3190		
23	1543	1609			2596kb	3260	3190		
24	1345	1209			2612kb	3290	3245		
25	1765	1402			2796kb	3312	3320		
26	1980	1843			2856kb	3345	3312		
27	2190	2209			3043kb	3397	3334		
28	2020	1934			3496kb	3456	3387		
29	1398	1432			4056kb	3498	3420		
30	1234	901			4512kb	3538	3490		
31	2209	2390			4896kb	3656	3690		
32	2409	2233			5024kb	3690	3620		
33	1109	1309			5456kb	3745	3823		
34	1187	1321			5696kb	3776	3720		
35	1356	1123			5812kb	3820	3813		
36	1943	2034			6098kb	3865	3790		
37	2309	2309			7056kb	4043	4101		
38	1340	1232			7956kb	4290	4020		
39	1456	1521			8896kb	4368	4490		
40	1523	1278			9345kb	4456	4390		
41	1765	1903			9856kb	4489	4409		
42	2276	2392			10366kb	4533	4501		
43	1309	1490			10669kb	4570	4521		
44	2423	2321			10996kb	4604	4612		
45	2109	1845			11256kb	4648	4534		
46	2134	2032			11490kb	4678	4686		
47	2234	2320			11634kb	4699	4646		
48	2523	2634			11856kb	4730	4690		
49	1456	1320			11912kb	4765	4770		
50	1478	1322			12098kb	4796	5012		
51	2476	2106			12156kb	4856	4830		

Table 7.6: Patients Records Uploading Speed On IPFS And File Size Uploading Speed On IPFS

access patient records from other healthcare providers. The fluctuation of speed Fig 7.16 depends on the number of patients and file size of patients' records. Also, it depends on the blockchain network and system specification. In Figure 7.16 and table 7.7, 1434ms speed is measured for 1atient, 1674ms for 5th, 1589ms for 10th, 1490ms for 15th, 1233ms for 20th, 1789ms for 25th, 1434ms for 30th, 1578ms for 35th, 2389ms for 40th, 2234ms for 45th, 2498ms for 51. The SE for 1atients is ±1254ms speed, ±1309ms for 5th, ±1324ms for 10th, ±1298ms for 15th, ±1089ms for 20th, ±1634ms for 25th, ±1265ms for 30th, ±1354ms for 35th, ±2165ms for 40th, ±1978ms for 45th, ±2245ms for 51. The SE indicates that the speed is close to the mean speed. The straight fit line is y=10.787x +1310 to show that patient increase can change and affect speed. The R^2 0.2154 implies the correlation between patients and speed.

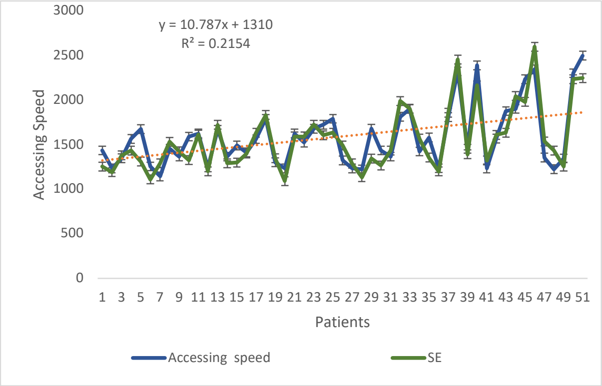


Figure 7.16: Patients Records Accessing Speed in IPFS

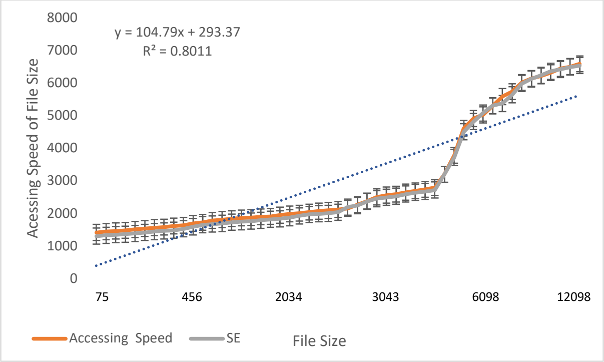


Figure 7.17: Patients filesize Accessing Speed in IPFS

Patients Record Accessing Speed On IPFS					File Size Accessing Speed on IPFS				
Patients	Accessing Speed (ms)	SE	(y)	R^2	File Size	Accessing speed (ms)	SE	(y)	R^2
1	1434	1254	51*10.787x + 1310	51*0.2154	75kb	1421	1309	51*104.79x + 293.37	51*0.8011
2	1232	1190			90kb	1445	1335		
3	1345	1378			110kb	1466	1353		
4	1564	1434			150kb	1487	1367		
5	1674	1309			190kb	1512	1390		
6	1254	1109			250kb	1543	1422		
7	1143	1290			356kb	1567	1445		
8	1453	1532			456kb	1589	1467		
9	1365	1423			510kb	1622	1489		
10	1589	1324			656kb	1643	1531		
11	1623	1612			1012kb	1698	1597		
12	1243	1201			1256kb	1734	1654		
13	1667	1721			1540kb	1787	1680		
14	1365	1289			1623kb	1815	1698		
15	1490	1298			1756kb	1845	1734		
16	1411	1398			1812kb	1868	1754		
17	1561	1631			1856kb	1875	1768		
18	1789	1831			1915kb	1899	1798		
19	1300	1345			1956kb	1912	1822		
20	1233	1089			2034kb	1953	1843		
21	1623	1591			2256kb	1989	1877		
22	1523	1590			2343kb	2012	1932		
23	1678	1723			2596kb	2045	1976		
24	1723	1604			2612kb	2076	1995		
25	1789	1634			2796kb	2098	2009		
26	1323	1490			2856kb	2123	2045		
27	1233	1287			3043kb	2156	2198		
28	1222	1132			3496kb	2273	2245		
29	1678	1343			4056kb	2387	2376		
30	1434	1265			4512kb	2512	2456		
31	1365	1432			4896kb	2567	2498		
32	1811	1989			5024kb	2599	2534		
33	1900	1903			5456kb	2657	2598		
34	1422	1565			5696kb	2699	2645		
35	1578	1354			5812kb	2742	2679		
36	1234	1198			6098kb	2799	2724		
37	1809	1856			7056kb	3203	3198		
38	2321	2454			7956kb	3789	3723		
39	1453	1390			8896kb	4621	4509		
40	2389	2165			9345kb	4919	4824		
41	1233	1321			9856kb	5032	5087		
42	1567	1609			10366kb	5306	5313		
43	1876	1634			10669kb	5592	5378		
44	1900	2043			10996kb	5745	5643		
45	2234	1978			11256kb	6023	5993		
46	2344	2598			11490kb	6145	6132		
47	1354	1534			11634kb	6226	6245		
48	1223	1434			11856kb	6328	6367		
49	1344	1254			11912kb	6454	6423		
50	2300	2234			12098kb	6512	6499		
51	2498	2245			12156kb	6597	6545		

Table 7.7: Patients Accessing Speed On IPFS And File Sizes Accessing Speed On IPFS

The speed of filesizes is measured in Figure 7.17 and table 7.7, the speed of 75kb file size is 1421ms, 456kb is 1589ms, 2034kb is 1953ms, 3043kb is 2156ms, 6098kb is 2799ms, 12098kb is 6512ms. The SE of 75kb is ±1309ms, ±1467ms for 456kb, ±1843ms for 2034kb, ±2198ms for 3043kb, ±2724ms for 6098kb, ±6499ms for 12098kb. The SE shows that the actual file size and speed values are close to the simulated values. The straight fit line is y= 104.79x + 293.37, implying that an increase in file size can change and affect the speed. The R^2 0.8011 shows the correlation between file size and speed.

7.2.4.3 Experiment 3: Records Sharing Speed

Figure 7.18 and Table 7.8 show the speed of patient records shares among healthcare providers. The calculated speed of 1.atient record is 5021ms, 5267 for 5th, 5467ms for 10th, 5682ms for 15th, 3109ms for 20th, 3609ms for 25th, 5489ms for 30th, 4598ms for 35th, 5809ms for 40th, 5289ms for 45th, 4209ms for 51. The SE of 1.atients is ±4812ms, ±4909ms for 5th, ±5112 for 10th, ±5345ms for 15th, ±2809ms for 20th, ±3223ms for 25th, ±5200ms for 30th, ±3901ms for 35th, ±5601ms for 40th, ±4810 msfor 45th, ±4019ms for 51. There is a close margin between experimental values and SE values. The values in Figure 7.18 and table 7.8 show that the SE is somehow close to the actual values. The straight fit line is y=3.7618x + 4277.1, indicating the effect and change of speed over increasing patients. The R^2 is 0.0032, indicating the correlation between sharing speed and patients.

The sharing speed of file size on IPFS in Figure 7.19 and Table 7.8 shows that the minimum sharing speed for filesize is 1801 for 75kb and the maximum is 9567 for 12156kb. The minimum SE of sharing speed for filesize 75kb is 1502, and the maximum is 9018 for 12156kb. The cause and effect of patients' over-sharing speed are y= 172.73 + 455.63, and R^2 is 0.9404, which indicates the correlation between sharing speed of filesize and patients.

Patients Record Sharing Speed On IPFS					File Size Sharing Speed On IPFS				
Patients	Sharing Speed (ms)	SE	(y)	R^2	File Size	Sharing speed (ms)	SE	(y)	R^2
1	5021	4812	51*3.7618x + 4277.1	51*0.0032	75kb	1801	1502	51*172.73x + 455.63	51*0.9404
2	4521	4209			90kb	1823	1534		
3	3423	3245			110kb	1842	1555		
4	5234	5145			150kb	1888	1599		
5	5267	4909			190kb	1945	1643		
6	3234	2909			250kb	2065	1734		
7	5356	5167			356kb	2189	1854		
8	4534	4267			456kb	2267	1923		
9	2312	2134			510kb	2276	1965		
10	5467	5112			656kb	2373	2054		
11	5478	4909			1012kb	2434	2110		
12	5490	5298			1256kb	2554	2189		
13	3411	3265			1540kb	2698	2298		
14	2721	2456			1623kb	2787	2388		
15	5682	5345			1756kb	2893	2487		
16	5603	5376			1812kb	2967	2576		
17	5530	5176			1856kb	2998	2598		
18	3300	3211			1915kb	3045	2654		
19	3220	3144			1956kb	3076	2689		
20	3109	2809			2034kb	3243	2734		
21	5634	5433			2256kb	3389	2865		
22	5609	5366			2343kb	3449	2898		
23	5430	5243			2596kb	3634	3043		
24	5390	5117			2612kb	3712	3076		
25	3609	3223			2796kb	3812	3290		
26	3909	3676			2856kb	3933	3323		
27	4390	4187			3043kb	4163	3576		
28	4709	4400			3496kb	4409	3843		
29	5609	5211			4056kb	4829	4109		
30	5489	5200			4512kb	5189	4412		
31	3245	3022			4896kb	5218	4632		
32	5709	5234			5024kb	5406	4843		
33	5823	5434			5456kb	5794	5189		
34	5890	5643			5696kb	5945	5375		
35	4598	3901			5812kb	6034	5495		
36	4857	4567			6098kb	6185	5578		
37	4739	4587			7056kb	6545	6104		
38	3498	3245			7956kb	6945	6536		
39	3098	2867			8896kb	7629	7384		
40	5809	5601			9345kb	7841	7598		
41	5845	5612			9856kb	8108	7862		
42	5698	5323			10366kb	8472	8094		
43	5487	5345			10669kb	8634	8248		
44	5376	5134			10996kb	8839	8413		
45	5289	4810			11256kb	9023	8598		
46	3687	3345			11490kb	9134	8697		
47	3845	3612			11634kb	9245	8756		
48	3598	3245			11856kb	9334	8876		
49	4598	4210			11912kb	9461	8963		
50	4573	4409			12098kb	9534	8999		
51	4209	4019			12156kb	9567	9018		

Table 7.8: Patients Sharing Speed On IPFS And File Sizes Sharing Speed On IPFS

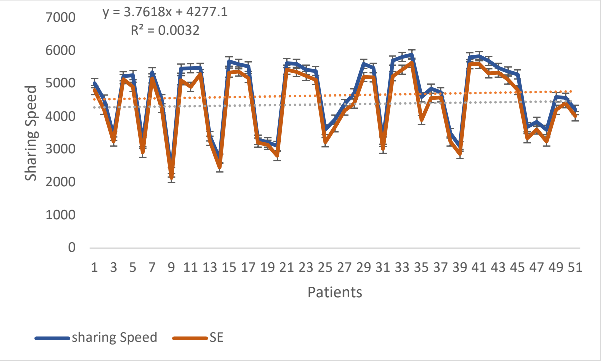


Figure 7.18: Patients Records sharing speed on IPFS

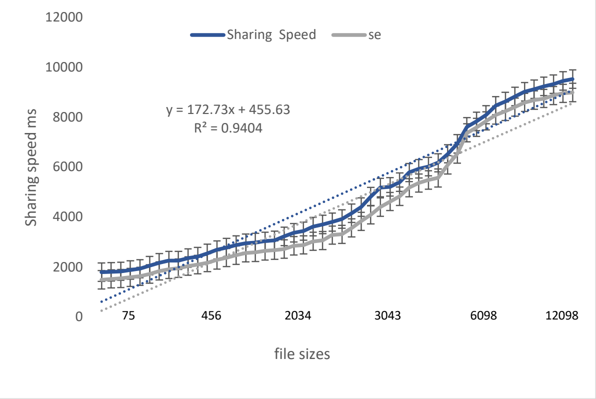


Figure 7.19: Patients filesize sharing speed on IPFS

7.2.4.4 Experiment 4:Smart Contract Gas Consumption Using IPFS

This section presents experimental results of smart contract Gas consumption of uploading records, gas consumption of accessing records, and Gas consumption of sharing records using IPFS. The unit of Gas consumption is gwei, and used in the rest of the section.

Figure 7.20 and table 7.9 shows the smart contract Gas consumption of uploading patients' records on IPFS. The minimum Gas consumption is 21,000$gwei$ for one patient, and the maximum Gas is 40,023$gwei$. Gas consumption increases linearly when more patient records are uploaded. The fluctuation in figure 7.20 indicates that different sizes of records are uploaded to IPFS. The SE of minimum Gas consumption is 19,000$gwei$, and the maximum is 34,890$gwei$. The values of SE are slightly lower than the experimental values. The straight fit line is y=172.14x+23080 to show the linear change and effect of patients' Gas consumption. The R^2 is 0.255, indicating the correlation between Gas consumption and patients.

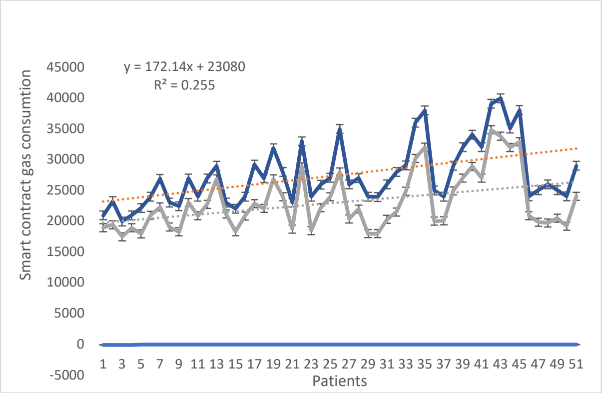


Figure 7.20: Smart Contract Gas consumption of uploading patients record on IPFS

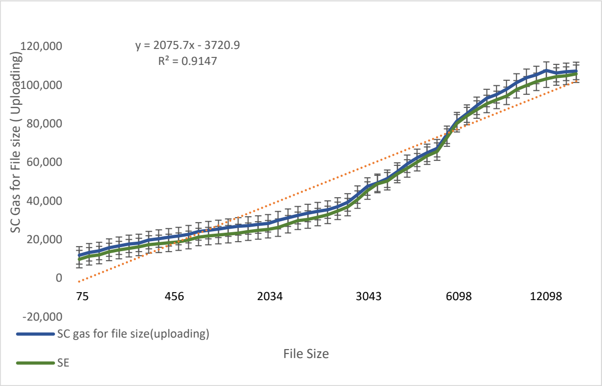


Figure 7.21: Smart Contract Gas Consumption of patients file size (uploading) on IPFS

The Gas consumption of different file sizes of patients is calculated in Figure 7.21 and Table 7.9. The Gas of the minimum file size is 12,021$gwei$, and the maximum is 54,012$gwei$. The SE of the minimum file size is 10,023$gwei$, and the maximum is 51,023$gwei$. The straight fit line is y=7857x+4685.9, which indicates the change in Gas consumption when file sizes increase, and R^2 is 0.985, implying the correlation between Gas consumption and file sizes. Fig 7.21 shows that when file sizes increase while uploading, the Gas consumption increases linearly.

SC Gas for Uploading Patients Records On IPFS					SC Gas Consumption for File Sizes On IPFS				
Patients	Gas ($gwei$)	SE	(y)	R^2	File Size	Gas ($gwei$)	SE	(y)	R^2
1	21,000	19,000	51*172.14x + 23080	51*0.255	75kb	12,012	10,023	51*20.75x + 3720.9	51*0.9147
2	23,301	19,500			90kb	13,567	11,538		
3	20,012	17,543			110kb	14,303	12,156		
4	21,023	18,987			150kb	15,983	13,730		
5	22,212	18,002			190kb	16,947	14,765		
6	24,023	21,034			250kb	17,875	15,657		
7	26,943	22,342			356kb	18,345	16,342		
8	23,092	19,092			456kb	19,876	17,576		
9	22,503	18,321			510kb	20,654	17,980		
10	27,000	23,090			656kb	21,342	18,487		
11	24,034	20,923			1012kb	21,998	18,996		
12	26,981	22,782			1256kb	22,876	19,956		
13	29,034	26,902			1540kb	24,343	21,432		
14	23,054	21,220			1623kb	24,980	21,988		
15	22,093	18,345			1756kb	25,654	22,475		
16	24,054	20,890			1812kb	26,343	22,998		
17	29,234	22,902			1856kb	26,994	23,546		
18	27,023	22,123			1915kb	27,435	24,234		
19	31,923	26,909			1956kb	27,997	24,878		
20	28,034	24,023			2034kb	28,543	25,453		
21	23,094	18,789			2256kb	30,121	26,345		
22	33,043	28,892			2343kb	31,462	28,120		
23	24,045	18,543			2596kb	32,768	29,876		
24	26,000	22,234			2612kb	33,897	30,543		
25	27,092	24,012			2796kb	34,864	31,793		
26	35,023	28,034			2856kb	35,654	32,987		
27	26,023	20,432			3043kb	37,234	34,987		
28	27,045	22,043			3496kb	39,423	36,984		
29	24,043	18,034			4056kb	43,483	40,905		
30	23,980	18,034			4512kb	47,654	45,463		
31	26,043	20,345			4896kb	49,543	48,943		
32	28,032	21,546			5024kb	51,735	50,363		
33	29,123	24,934			5456kb	55,353	54,095		
34	36,032	30,242			5696kb	59,352	57,043		
35	38,034	32,043			5812kb	62,543	60,234		
36	25,054	20,043			6098kb	65,094	63,543		
37	24,023	20,123			7056kb	67,432	65,705		
38	29,043	24,987			7956kb	74,435	72,943		
39	32,043	27,045			8896kb	81,434	80,345		
40	34,098	28,954			9345kb	85,345	84,098		
41	32,093	27,045			9856kb	89,425	87,439		
42	39,093	34,890			10366kb	93,438	90,435		
43	40,023	33,834			10669kb	95,342	92,543		
44	35,094	32,034			10996kb	98,054	94,535		
45	38,093	32,943			11256kb	101,453	97,934		
46	24,098	20,923			11490kb	103,954	99,985		
47	25,098	19,903			11634kb	105,435	101,854		
48	26,035	19,789			11856kb	107,685	103,435		
49	25,093	20,543			11912kb	106,435	104,543		
50	24,093	19,234			12098kb	106,998	104,986		
51	29,032	24,098			12156kb	107,463	105,986		

Table 7.9: Smart Contract Gas Consumption Of Uploading Patients Records On IPFS and Smart Contract Gas Consumption Of File Sizes On IPFS

Figure 7.22 and table 7.10 show the Gas consumption of smart contracts while sharing patients' records using IPFS. The minimum Gas for one patient is 19,021$gwei$, and the maximum Gas for one patient is 46,023$gwei$. Some records cost gas because of the file size or complex computational calculations. The minimum SE of one patient is 17,023$gwei$, and the maximum is 45,934$gwei$. In fig 7.22 and table 7.10, some values are high from the experimental values, and some are low. The straight fit line is y=403.8x+16387, which shows the cause and effect of sharing patients' records over Gas consumption. The R^2 (0.4732) indicates the correlation between sharing patient records and Gas consumption.

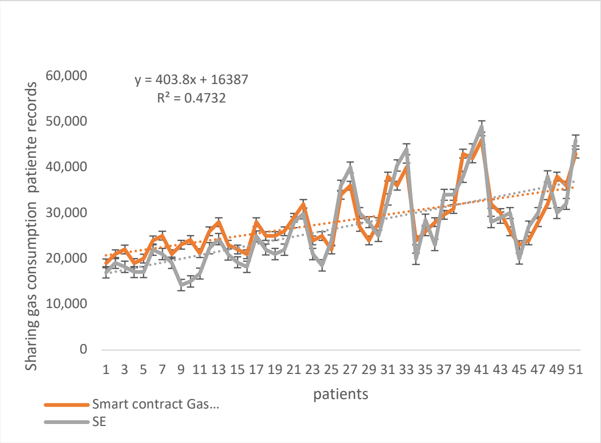


Figure 7.22: Smart Contract Gas consumption of sharing patients records on IPFS

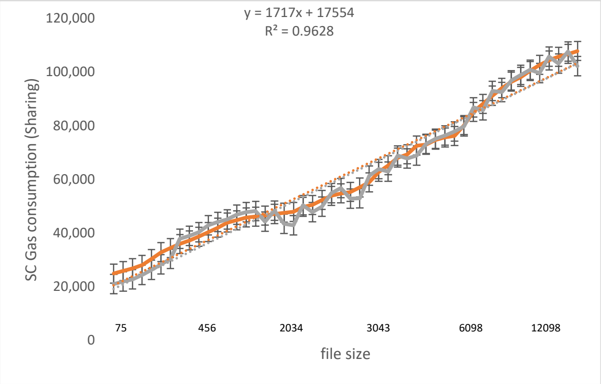


Figure 7.23: Smart contract gas consumption of patients filesize (sharing) on IPFS

Figure 7.23 and table 7.10 implies the Gas consumption of file size on IPFS. It

SC Gas for Sharing Records On IPFS					SC Gas Consumption for File Sizes On IPFS				
Patients	Gas ($gwei$)	SE	(y)	R^2	File Size	Gas ($gwei$)	SE	(y)	R^2
1	19,021	17,023	51*403.8x + 16387	51*0.4732	75kb	1321	1045	51*1717x + 17554	51*0.9628
2	21,034	19,098			90kb	25,987	21,978		
3	22,034	18,232			110kb	26,987	22,879		
4	19,043	17,098			150kb	28,232	24,432		
5	20,054	17,092			190kb	30,432	26,345		
6	24,024	22,023			250kb	32,987	28,453		
7	25,065	21,023			356kb	34,543	30,546		
8	21,032	19,103			456kb	36,022	38,032		
9	23,076	14,243			510kb	37,342	39,094		
10	24,123	15,035			656kb	38,783	40,435		
11	21,234	16,780			1012kb	40,432	42,984		
12	26,023	22,342			1256kb	42,104	44,232		
13	28,034	24,340			1540kb	43,987	45,234		
14	23,043	20,978			1623kb	44,893	46,934		
15	22,043	19,234			1756kb	45,879	47,904		
16	21,023	18,232			1812kb	46,234	48,354		
17	28,043	24,933			1856kb	46,654	44,345		
18	25,023	22,032			1915kb	47,234	48,395		
19	25,024	21,024			1956kb	47,684	43,543		
20	26,043	22,023			2034kb	48,022	43,054		
21	29,024	28,023			2256kb	49,876	50,453		
22	32,023	29,943			2343kb	50,584	47,934		
23	24,023	21,024			2596kb	52,453	49,943		
24	25,024	18,546			2612kb	53,987	54,935		
25	22,024	24,024			2796kb	54,904	56,943		
26	34,024	36,034			2856kb	55,453	52,945		
27	36,024	40,024			3043kb	57,110	53,043		
28	27,023	30,043			3496kb	59,034	61,543		
29	24,024	28,023			4056kb	62,903	63,945		
30	28,024	25,034			4512kb	65,345	63,043		
31	38,034	33,034			4896kb	68,264	69,043		
32	36,044	40,453			5024kb	69,456	67,943		
33	40,034	44,035			5456kb	72,754	69,043		
34	24,024	20,024			5696kb	73,102	73,342		
35	26,024	28,543			5812kb	74,935	75,234		
36	28,024	23,043			6098kb	75,765	76,456		
37	29,654	34,044			7056kb	76,345	77,945		
38	30,923	34,034			7956kb	80,342	79,954		
39	43,024	37,983			8896kb	85,345	86,934		
40	42,034	44,034			9345kb	88,341	85,834		
41	46,023	49,034			9856kb	91,345	93,095		
42	32,024	28,065			10366kb	94,205	92,654		
43	30,033	29,034			10669kb	96,546	97,095		
44	26,024	30,043			10996kb	98,345	99,054		
45	23,022	20,032			11256kb	100,543	100,987		
46	24,024	27,024			11490kb	102,843	99,843		
47	28,024	30,043			11634kb	104,546	105,934		
48	32,024	38,043			11856kb	105,876	103,342		
49	38,024	30,043			11912kb	106,875	107,843		
50	36,024	32,043			12098kb	108,000	102,342		
51	43,024	45,934			12156kb	110,453	109,435		

Table 7.10: Smart Contract Gas Consumption Of Sharing Patients Records On IPFS, Smart Contract Gas Consumption Of Sharing Records Of Different File Sizes On IPFS

shows that the minimum Gas is 25,000$gwei$ for file size 75kb, and the maximum Gas is 110,453$gwei$ for 12156kb. However, the SE is different from the experimental values. the minimum SE for 75kb file size is 21,032$gwei$, and the maximum is 109,435$gwei$ for 12156kb. The straight fit line is y = 1717x + 17554, and R^2 is 0.9628 showing a strong correlation between file size and Gas consumption.

Figure 7.24 and table 7.11 represent smart contract Gas consumption of accessing patients' records when interacting with IPFS. The hashes of patient records are stored on a blockchain network, and files transfer to IPFS to minimise the cost of storing files on the blockchain network. The smart contract deployed on the blockchain network interacts with IPFS whenever healthcare providers need to access patients' records, and it needs to be done by spending Gas. The minimum Gas consumption for accessing a patient's prescription record is 24,000$gwei$, and the maximum Gas consumption is 54,943$gwei$. The Gas consumption varies from patient to patient and their previous prescription history. If patients have long prescription history and healthcare providers want to access it, it will cost more Gas due to large files and high computational power. Moreover, it also depends on the protocol used to validate the transaction. If POW is used, then the Gas will be higher than POS. Further, the SE for Figure 7.24, shows that the minimum SE of the patient is 26,032$gwei$, and the maximum is 49,893$gwei$. The fluctuation of values shows that the SE is close to the experimental Gas values. The straight fit line is y = 340.82x + 25629, showing the change in Gas consumption when patient records increase, and R^2 is 0.3242 indicating the correlation between accessing Gas consumption and patient records.

Figure 7.25 and table 7.11 shows the gas consumption of different file sizes accessed by healthcare providers. As presented in above Figure 7.25, patient records size or file size matter in increasing gas consumption, and that can be seen in figure 7.25 and table 7.11. The minimum Gas is 28,000$gwei$ for a file size 75kb, and the maximum is 124,435$gwei$ for 12156kb. It is noted that Gas consumption increases linearly whenever

SC Gas for Accessing Records On IPFS					SC Gas Consumption for File Sizes On IPFS				
Patients	Gas ($gwei$)	SE	(y)	R^2	File Size	Gas ($gwei$)	SE	(y)	R^2
1	1221	1012	51*340.82x + 25629	51*0.3242	75kb	1321	1045	51*2132.6x + 11828	51*0.9441
2	23,032	20,342			90kb	28,453	27,435		
3	24,023	25,034			110kb	28,994	29,943		
4	25,023	23,023			150kb	29,543	30,436		
5	24,023	19,893			190kb	30,102	29,432		
6	23,023	22,032			250kb	30,654	29,894		
7	25,054	21,032			356kb	31,324	31,984		
8	26,234	28,903			456kb	31,987	30,874		
9	26,912	22,323			510kb	32,543	33,432		
10	23,032	25,202			656kb	33,974	32,232		
11	27,023	20,212			1012kb	36,754	37,673		
12	28,024	30,323			1256kb	38,432	36,743		
13	32,043	35,564			1540kb	40,342	41,987		
14	26,025	24,543			1623kb	41,987	40,324		
15	25,043	23,943			1756kb	43,123	42,984		
16	36,024	38,903			1812kb	44,342	41,874		
17	38,024	34,923			1856kb	44,987	41,987		
18	32,024	29,043			1915kb	46,192	45,343		
19	33,943	30,423			1956kb	46,765	44,324		
20	42,032	44,932			2034kb	47,453	48,543		
21	38,043	39,943			2256kb	49,324	47,109		
22	32,022	28,943			2343kb	50,213	51,329		
23	44,032	42,932			2596kb	52,654	49,324		
24	39,032	38,943			2612kb	54,231	50,094		
25	47,023	48,943			2796kb	55,543	54,987		
26	43,024	39,943			2856kb	56,509	54,876		
27	44,029	39,943			3043kb	58,435	55,354		
28	49,342	53,943			3496kb	61,432	62,987		
29	35,043	32,543			4056kb	64,824	61,320		
30	24,043	21,943			4512kb	67,453	63,234		
31	26,043	22,943			4896kb	69,654	67,106		
32	27,043	22,676			5024kb	71,805	72,043		
33	29,043	32,984			5456kb	74,345	73,094		
34	30,033	29,943			5696kb	76,543	75,345		
35	34,035	39,943			5812kb	78,985	79,434		
36	38,043	32,943			6098kb	80,032	79,434		
37	45,025	39,345			7056kb	82,095	83,032		
38	42,043	43,234			7956kb	88,875	87,343		
39	52,043	49,893			8896kb	98,435	94,943		
40	54,035	47,432			9345kb	103,987	101,843		
41	34,035	36,432			9856kb	107,094	104,984		
42	38,053	36,654			10366kb	108,453	107,874		
43	39,043	38,345			10669kb	112,094	111,893		
44	34,024	35,954			10996kb	115,345	114,873		
45	43,034	44,234			11256kb	119,343	120,343		
46	44,024	47,434			11490kb	120,984	119,303		
47	51,032	53,543			11634kb	121,843	118,980		
48	49,043	46,234			11856kb	122,893	119,893		
49	28,043	27,094			11912kb	123,323	120,890		
50	29,043	28,943			12098kb	123,987	121,938		
51	32,043	34,894			12156kb	124,435	122,465		

Table 7.11: Smart Contract Gas Consumption Of Accessing Patients Records On IPFS, Smart Contract Gas Consumption Of Accessing Records Of Different File Sizes On IPFS

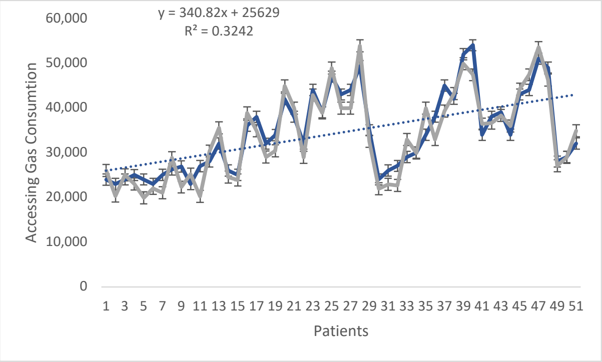


Figure 7.24: Smart Contract Gas consumption of patients accessing records on IPFS

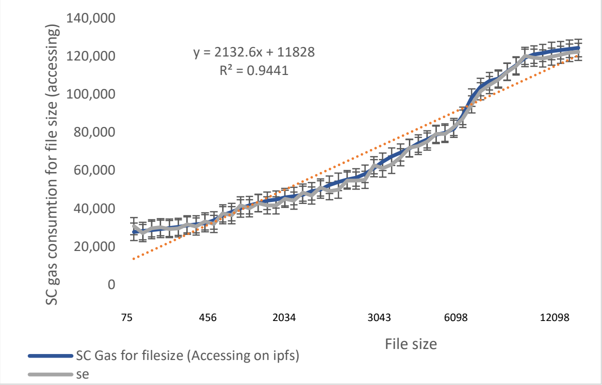


Figure 7.25: Smart contract Gas consumption of patients file size (accessing)on IPFS

file sizes increase. The minimum SE is 27,435$gwei$ for filesize 75kb, and the maximum SE is 122,465$gwei$ for filesize 12156kb. The straight fit line is y=2132.6x + 11828, showing the change in Gas, and R^2 is 0.9441, representing the correlation between Gas and file size.

To sum up, smart contract Gas consumption experiments of uploading, sharing, and accessing patient's records and Gas consumption of different file sizes. It is noted that uploading patients' records and files is the lowest Gas consumption as healthcare providers do not need to interact with other healthcare providers or patients while uploading patient records. On the other hand, Gas consumption for sharing patient records is slightly higher due to patient and healthcare provider authorisation. It took longer to share the patient's records. However, accessing patient records and file size

Gas consumption is relatively higher than sharing records as it involves more processes, i.e., patients authorisation, revoking permission, and incentivisation. The incentivisation process takes more computational time, power, and Gas to attract patients to participate in the proposed BlockPres system.

7.2.4.5 Experiment 5:Resource Utilisation

Figure 7.26 and table 7.12 represent the system's resource utilisation during experimentation of the BlockPres prototype. The parameters used to test the system are memory(RAM), CPU usage, Disk usage, and Traffic in and out. The minimum memory usage is 4MB for 75kb, and the maximum is 23Mb for 12098kb. The minimum CPU usage is 5MB for 75kb, and the maximum is 87MB for 12098kb, the disk throughput is 6MB for 75kb and 190MB for 12098kb. The traffic-in is 8MB for 75kb and 346MB for 12098kb. The traffic-out is 9MB for 75kb and 660MB for 12098kb. The resource utilisation experiments instigate that the system remains controllable during performed experiments. Whenever smart contracts interact with IPFS, the CPU and memory usage go high, and the Traffic out is high while accessing large files.

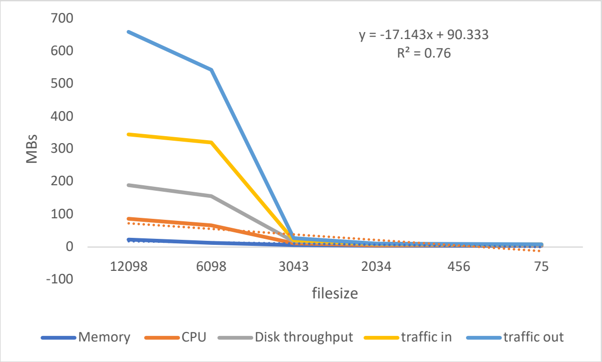


Figure 7.26: Resource Utilisation of Proposed system

Filesize	Memory	CPU	Disk Throughput	Traffic-in	Traffic-out
12098	23	87	190	346	660
6098	13	67	156	321	543
3043	6	12	17	21	27
2034	4	5	8	10	10.4
456	4.5	6	7	9	10
75	4	5	6	8	9

Table 7.12: Resource Utilisation Of Blockpres Using Smart Contract And IPFS

7.2.4.6 Experiment 6:Computational Speed of Encryption Schemes

The Figure 7.27 experiment shows the computational speed of different encryption-decryption schemes used during an interaction between smart contract and IPFS. The comparison is carried out between AES (128), AES (256), and SSS. The computation speed of AES(128) is 5.2, and AES (256) is 9.3. on the other hand, SSS computational speed is 2.4, the lowest among other schemes. These schemes are differentiated based on computational speed as AES (128) perform 2^{128} different combination of keys to decrypt a file. Similarly, AES (256) performs 2^{256} combinations of keys to decrypt a file. However, the computational speed is less as there are no key combinations. The BlockPres uses SSS for records and file encryption-decryption on IPFS as the computational speed of SSS is better than other schemes.

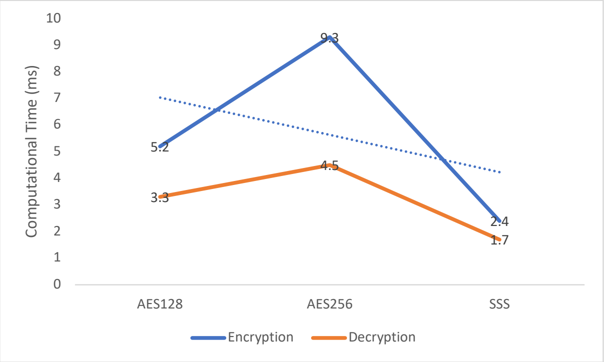


Figure 7.27: Computational Speed of AES(128), AES(256) and SSS

7.3 Security and Privacy Analysis

Security and privacy are essential to every system, especially in healthcare. The data should be handled with considerable privacy and protected from access by medical entities deemed malicious. This section considers the blockchain-based secure storage of patients' prescription records using IPFS. However, simultaneously, the security and privacy of the blockchain-based system using IPFS are important to be considered and proved using various threat scenarios.

$Theorem\ 1$: It is assumed that entities may access the PMS within IPFS with no consent of the medical entity. That attacker may not be capable of reading the medical information.

$Proof$: In the proposed blockchain-based solution for the prescription management system, all prescription records are secured in IPFS through a unique symmetric key for every medical entity. Symmetric encryption based on a 256-bit system, such as public-key encryption and zero-knowledge Proof, is used to ensure that it is difficult for an attacker to make guesses of such keys and maintain the privacy of medical entities. Although the adversaries may guess medical entities' symmetric keys, decrypting all files is difficult. The keys matching the medical entities are protected and stored within the secure public key encryption on IPFS. Because the keys are secured via medical entities' public key, to obtain the keys, the medical entity or adversaries will first access them through public key encryption. With the adoption of zero-knowledge Proof, medical entities will ensure not to disclose entity information.

$Theorem\ 2$: Assuming that an adversary gets patients' NHI or Ethereum address to access or misuse prescription records. No adversary can misuse a patient's NHI or Ethereum address, claim a prescription, or misuse the information.

$Proof$: The adversary must fulfill the requirements sets implementing zero-knowledge Proof to use the patients' information at a health services provider. Cross-check permission from the patients will also take place to get authorisation. The digital signature will also ensure the patient's identity. The current implementation of the smart contract enables the contract owner, such as HealthNz or MOH, to trace and track patients' accounts when the patient's record is accessed without authorisation.

7.4 Testing Trustworthiness of BlockPres

This section presents the evaluation of BlockPres using a trust scoring system proposed by (John et al., 2018), which defines trust as a function of Persistence (P), Competence (Cp), Reputation (Re), Credibility (Cr), and Integrity (Ig). The proposed trust score can be calculated using Equation 7.5, where K is the Trust Equating Factor or Trust Normalisation Constant. Each parameter is normalised to a unit value, and the Trust Normalisation Constant is 0.2 since all parameters have equal weights. Persistence is measured through the stability and consistency of the platform, where stability refers to the platform's ability to provide appropriate resources or data for a user's request, and consistency refers to the platform's ability to respond whenever it receives a request from the patients with the possible resource. The average turnaround time required by the system to process requests and the average response time is used to measure competence. Information accessibility (I) and compatibility (C) are the two criteria for evaluating reputation. (C). The accuracy and potency of the system's findings for users are measured by credibility. The availability (A) and confidentiality (C) of the system are the two parameters used to determine the integrity of the system. (Cf).

$$TrustScoreT = F(P, C_P, R_E, C_R, I_G) = K.(P + R_E + C_R + I_G + C_P) \tag{7.5}$$

7.4.1 Trustability co-efficient of variation

The trust score is determined by utilising the trustworthiness coefficient of variation as introduced in (John et al., 2018). To assess the reliability of data and transactions, the section used a trustworthy coefficient of variation from (John et al., 2018). This includes evaluating transaction latency and throughput across various file sizes. The normalised values in Table 7.13 on the next page elevate the trust score level because dummy data and simulations can influence the results. The trust score, response time, throughput, and latency will likely be higher in actual real-time scenarios.

7.4.2 Incentivisaion

The patients in Blockpres are provided with tokens that can be used for registration and completing various processes, such as accessing records, prescriptions, and medication. The number of tokens a patient receives depends on the healthcare provider. It varies for different tasks, such as 1 token for registration, 2 for authorisation, 2 for completing prescribed medication, etc. The healthcare provider can determine the value of each token. Patients can redeem these tokens for discounts or purchase anything they desire. The distribution of tokens is presented in Table 7.14 on page 198. This system incentivises patient participation and engagement and helps reduce healthcare costs by allowing patients to earn or receive tokens.

Table 7.13: Trust Score calculation

Patient.id	**File Size**	**Trust Score**
1	75kb	0.8100
2	90kb	0.8112
3	150kb	0.8156
4	250kb	0.8212
5	510kb	0.8290
6	1012kb	0.8342
7	1540kb	0.8398
8	1812kb	0.8423
9	1915k	0.8534
10	2343kb	0.8599
11	2856k	0.8634
12	4056kb	0.7034
13	5024kb	0.6500
14	7056kb	0.2341
15	8896kb	0.7013
16	9496kb	0.3021
17	9856kb	0.8945
18	10996k	0.2
19	10596k	0.2322
20	11856kb	0.8870

Table 7.14: Incentive distribution

Event	**Tokens Distribution (On Ave.)**
Registration	1 token
Authorisation	2 tokens
Completed Prescribed medication	2 tokens
Share files	2 tokens
Engagement and participation	1 token

7.5 Hypothesis Conclusions

The present thesis study uses and evaluates Design Science Research Methodology. The methodology involves four main steps: problem identification, solution design, evaluation, and summarising results. Chapter 2 formulates a set of hypotheses to test the researcher's artifact, which is developed based on the literature review presented in Chapter 2. This section evaluates the rationale between the questions, hypotheses, and findings from Chapter 2 and experimental results from Chapter 8.3. The results obtained from evaluating theory, prototype experimental results, and formal modeling of the incentive mechanism are also discussed. The methodology adopted in this part is based on the Quasi-judicial (Cardozo et al., 2010) approach, which employs rational argumentation to support or refute the hypothesis. The weight of judgment is considered while arguing against the hypothesis. Table 7. 15 summarises the hypothesis 1 evaluation for this research.

Table 7.15: Hypothesis 1 Conclusion

H1: The current prescription practices in HIS are ineffective and error-prone.	
For	Against
Chapter two of the study utilised a Systematic Literature Review (SLR) to investigate the research hypothesis. To address the hypothesis, various methods are used, and method **M1**, described in section 4.3.2.1 on page 98, is utilised to find the solution. The study also examined several related studies on current prescription practices in Section 2.5.5.2 on page 39. These studies indicated that medication errors or harm resulting from medication are a significant issue in New Zealand. Furthermore, the evidence presented in sections 2.5.5.5 on page 45 and 2.5.5.3 on page 41 supports the claim that current practices are prone to errors.	After conducting a Systematic Literature Review, the thesis developed a hypothesis that some studies suggest the current prescription system may address prescription issues, but there is uncertainty surrounding this claim. However, the majority of studies supported the H1.
Verdict: There is insufficient evidence to reject the hypothesis. The study adopted the PRISMA method in Section 2.2 on page 13 and Figure 2.1 on page 15 to conduct a systematic literature review, which supported Hypothesis 1 and assist it in being accepted.	

Table 7.16: Hypothesis 2 Conclusion

H2: The impact of unequal access to PMS affects the health outcomes of Maori and Pasifika, as it also contributes to their disengagement from healthcare services.	
For	Against
Chapter 2 supports H3 in section 2.5.5.3 on page 41, citing research articles and reports from health and disability commissioners. Additionally, other factors contributing to unequal access and disengagement of Maori and Pasifika are identified in section 2.5.5.4 on page 43. The challenges Maori and Pasifika face are illustrated with real-life cases in section 2.5.5.5 on page 45. In Chapter 3, M1 is developed to validate the hypothesis.	After conducting research and reviewing the relevant literature, information has yet to be found that refutes the hypothesis.
Verdict: There is insufficient evidence to reject the hypothesis. The validation of H2 is based on a thorough review of the relevant literature, and the facts and figures presented in the section 2.5.5.3 on page 41 provide support for H2 and contribute to its acceptance.	

Table 7.17: Hypothesis 3 Conclusion

H3: The unequal access to PMS among Maori and Pasifika undermines the system's trustworthiness.	
For	Against
Chapter 2 on page 11 validates the correlation between trust and disengagement with unequal access and other contributing factors, as discussed in Section 2.5.5.4 on page 43. Multiple sources have verified this correlation	After conducting research and reviewing the relevant literature, no information has been found that refutes the hypothesis.
Verdict: There is insufficient evidence to reject the hypothesis. The validation of H3 is based on a thorough review of the relevant literature. The facts and figures presented in section 2.5.5.5 on page 45 support H3 and contribute to its acceptance.	

Table 7.18: Hypothesis 4 Conclusion

H4: The prescription system's inadequacy contributes to both prescription errors and the disengagement of Maori and Pasifika.	
For	Against

Table 7.18: Hypothesis 4 Conclusion

H4: The prescription system's inadequacy contributes to both prescription errors and the disengagement of Maori and Pasifika.	
In Chapter 2, Section 2.5 on page 35, various issues present in healthcare information systems, including security and privacy concerns, data transparency, data heterogeneity, counterfeit and substandard drugs, and prescription management system issues. These issues highlight the inadequacy of the healthcare system. Furthermore, Section 2.3.2 on page 29 validates that Maori health status has declined due to disparities in the system. In Chapter 3, The validation of H4 is supported by the M1 method.	After conducting a Systematic Literature Review, the thesis developed a hypothesis that some studies suggest the current prescription system may address prescription issues, but there is uncertainty surrounding this claim. However, the majority of studies supported the H1.
Verdict: There is insufficient evidence to reject the hypothesis. The validation of H4 is based on a thorough review of the relevant literature, and the facts and figures presented in the section 2.5.5 on page 38 provide support for H4 and contribute to its acceptance.	

Table 7.19: Hypothesis 5 Conclusion

H5: The proposed framework reduces prescription errors and inequality in the healthcare system.	
For	Against
In Chapter 4 on page 80 ,Section 4.2.1.1 on page 88 and figure 4.3 on page 90 presented solution design where the solution is proposed to satisfy H1,H2,H3,H4. In chapter 5 on page 102, BlockPres framework is proposed in Section 5.3 on page 121. The results show in Section 7.2.3 on page 167 that the proposed system can reduce prescription errors by providing patient authority, and smart contracts can bring equality in the form of records. In Chapter 4, M2 is used to validate the H5.	After developing the proposed BlockPres framework, the results are generated on dummy data, and the result can be different if the framework is implemented in a real environment.
Verdict: There is insufficient evidence to reject the hypothesis. The validation of H4 is based on a thorough review of the relevant literature related to blockchain technology, and the framework and results presented in the section 7.2.3 on page 167 provide support for H4 and contribute to its acceptance.	

Table 7.20: Hypothesis 6 Conclusion

H6: The Proposed incentive mechanism increases engagement and participation in PMS, leading to improved healthcare outcomes and better patient experiences.	
For	Against
The literature review in Chapter 3 on page 54 suggests that various incentive mechanisms have been proposed in different fields to enhance user engagement and increase participation, as discussed in Section 3.5 on page 75. In chapter 6 on page 139, developed an Incentive mechanism and explained the incentivisation and engagement process. Moreover, the formal method is adopted to construct the incentive mechanism. In Chapter 7 on page 160, the effectiveness of the Blockpres system is evaluated by creating a prototype and conducting experiments. The results of the experiments are presented in Section 7.2 on page 161, which demonstrate that the proposed system can indeed improve engagement.	After developing the proposed BlockPres framework, the study constructed an incentive mechanism, and Chapter 7 results are generated on dummy data. The result can differ if the framework is implemented in a real environment.

Table 7.20: Hypothesis 6 Conclusion

H6: The Proposed incentive mechanism increases engagement and participation in PMS, leading to improved healthcare outcomes and better patient experiences.	
Verdict: There is insufficient evidence to reject the hypothesis. The validation of H6 is based on the experimental results and the prototype development, which support H6 and contribute to its acceptance.	

Table 7.21: Hypothesis 7 Conclusion

H7: By providing equal access to Maori and Pasifika, the proposed PMS system enhances the system's trust level.	
For	Against

Table 7.21: Hypothesis 7 Conclusion

H7: By providing equal access to Maori and Pasifika, the proposed PMS system enhances the system's trust level.	
Chapter 5 on page 102 presents the Blockpres framework, which addresses the issues identified in Chapter 2 on page 11. In Chapter 6 on page 139, an incentive mechanism is proposed, and Chapter 7 on page 160 includes experimental results. The system's trust is evaluated using the trust score system proposed by John et al. (2018), and the results are promising, indicating a high level of trust based on the trust score. However, it should be noted that the trust score has not been tested in real-time scenarios and requires actual patient data to validate its effectiveness.	However, to establish the system's trustworthiness, it needs to be tested in real-time settings, and external opinions are necessary.
Verdict: Not Accepted To validate H7, the Trust score system is utilised. However, it requires expert feedback and real-time usage to calculate the trust level accurately. H7 has not been fully achieved or accepted. Further testing and validation are necessary	

7.6 Answers to the Questions and Sub-Questions

This section answers the questions and sub-questions formulated in chapter 2 on page 11 , section 4.3 on page 95. There are four questions and seven sub-questions.

RQ1 *What issues exist within current prescription practices?*

  (a) *How do prescription issues manifest?*

  (b) *What are the current practices to counter these Prescription issues?*

  (c) *Are current practices effective in HIS?*

To address the first question and its sub-questions, the study utilised an SLR and PRISMA methodology outlined in Chapter 2. Section 2.2 on page 13 aided in finding relevant articles and narrowing down the research problem. For sub-question 1, the study examined various reports from government entities and other studies to gather facts and figures to find prescription issues discussed in section 2.5.5 on page 38. The effects of prescription issues on Maori and Pasifika communities were explored in section 2.5.5.2 on page 39. The sub-questions were validated by citing a number of studies in chapter 2 on page 11. Sub-question 2 was addressed by discussing several practices used to counter prescription issues, such as the Prescription Monitoring Program, Pharmacovigilance, and Electronic Prescription Service, in section 2.5.5.5 on page 45. However, the current practices were insufficient, as validated by H1 and H2 in section 7.5 on page 198. For sub-question 3, the study examined current practices in section 4.3 on page 95 and identified issues in the healthcare system in section 2.5 on page 35 using various studies and health and disability reports. Overall, the three sub-questions revealed the existence of issues in the healthcare system related to prescription services.

RQ2 *What are the reasons for unequal access to Maori in PMS ?*

(a) *Are current PMS accessible and engageable to Māori and Pasifika?*

(b) *Are Maori and Pasifika trust the current PMS ?*

Chapter 2 on page 11 validates sub-question 4 by presenting evidence that highlights the lack of proper access to PMS for Maori and Pasifika communities due to various reasons such as cultural differences, inequality, cost, racial bias, and values. The relevant evidence is discussed in the section 2.5.5.4 on page 43, and H1 is formulated to address this sub-question.

Additionally, sub-question five is identified in Chapter 2, and a hypothesis is formulated to answer the question. The literature review evaluates and validates this sub-question. The section 2.5.5.4 on page 43 further discusses that trust is an important issue in the current PMS, and it is associated with the unequal access experienced by Maori and Pasifika communities.

RQ3 *How can unequal access, distrust, and disengagement be solved through blockchain technology?*

(a) *How can blockchain technology be applied to engage patients with PMS?*

(b) *How can blockchain technology be applied to build patients' trust ?*

(c) *How can blockchain technology be applied to mitigate inequalities in PMS ?*

Chapter 3 on page 54 analysed the characteristics and potential applications of blockchain technology in section 3.2.2 on page 58, specifically it has potential to address healthcare issues. To address sub-question 3, a blockchainbased solution is proposed in Section 4.2.1.1 on page 88, in the context of DSRM to address unequal access, distrust, and disengagement in the prescription management system. To answer sub-question 6, the study proposes an incentive-based mechanism to engage Maori and Pasifika populations, which is outlined in chapter 6 on page 139. Various incentivisation methods are proposed and validated in section 3.5 on page 75. Noting that the studies were conducted in different fields and areas. Regarding sub-question 7, the incentive mechanism proposed in Chapter 6 on page 139 is implemented through the development of a DApp (Decentralised Application) prototype, and experimental testing is conducted in section 7.2 on page 161 . Trust levels are calculated using the trust scoring system proposed by (John et al., 2018) without user feedback. However, the trust level is high based on the values. Additionally, sub-question 8 aims to provide equality to Maori and Pasifika by granting patients the authority to provide access to their healthcare records to healthcare providers. blockchain technology's Decentralised and inter-operable nature ensures that inequality is not possible, as everyone can see and follow updates.

RQ4 *How specifically to build a blockchain-based incentive mechanism to mitigate unequal access and inequalities in PMS?*

(a) *How the proposed system will be evaluated?*

In response to question 4 and sub-question 8, a blockchain-based incentive mechanism is constructed in chapter 6 on page 139, and a DApp prototype is developed to evaluate the mechanism. The prototype is evaluated through experimental results in section 7.2 on page 161 of the same chapter 7 on page 160. Based on the results, the prototype performs well, and the smart contract and decentralisation features minimise inequality. While patient and expert feedback would be helpful for further system evaluation, due to time constraints, the study will conduct this aspect of the evaluation in future work.

7.7 Discussion

This section presents the findings and contribution of the research. The literature review has been conducted focusing on the context of New Zealand using a Systematic Literature review. SLR allows the researcher to break down the problem into sub-problems in section 2.1 on page 11. The study uses PRISMA methods to make the article selection manageable. In Chapter 2, the study contributed the following points. The study identified various issues within the New Zealand healthcare system, highlighting problems that need to be addressed to improve inequality and prescription issues. The study conducted a cultural analysis of Maori and Non-Maori populations in New Zealand, focusing on disparities in health outcomes. The World Health Organisation (WHO) has recognised these disparities as a significant concern. The study also examined factors contributing to poorer health outcomes for Maori, as detailed in Section 2.3.2 on page 29. Chapter 2 on page 11 of the study focused on issues related to the prescription management system, including unequal access. Chapter 2 provided the foundation for the formulation of research questions and hypotheses. It also established a connection between Chapter 2 on page 11 and Chapter 3 on page 54, which explored different blockchain technologies. Chapter 3 on page 54 provided a comprehensive overview of blockchain and its applications in finance, supply chain management, voting, and digital identity verification. The study drew on existing research to develop a blockchain-based incentive mechanism to address these issues, using formal methods to construct the incentive mechanism in Chapter 6 on page 139. The study also utilised cryptographic techniques to share patient information securely. The prototype is built using the Ethereum platform with Rosten and Metamask.

The findings of the study are presented in Chapter 7 on page 160 and are backed by the literature reviewed in Chapter 3 on page 54. Chapter 3 on page 54 also identified various methods and tools for developing the prototype and evaluated different performance parameters such as throughput, latency, cost, and access time. Furthermore, the trust scoring system is identified to test the level of trust in the proposed system. This is a crucial part of the system's testing, as there was no other way to measure the trust level except by obtaining feedback from experts and patients. Chapter 3 proposes methods for incentivisation, and this study explicitly selects a token system for patients as a recommended approach. Chapter 3 on page 54 also outlined the security and privacy frameworks that supported the study in designing a secure system for patient data. These findings served as the basis for the development of the architecture and helped to reconcile the study's results with the original problem statement.

7.8 Conclusion

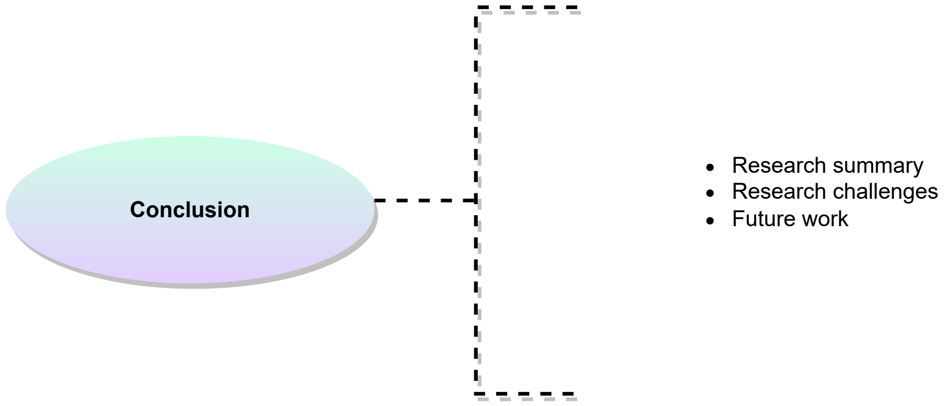
In chapter 7, the findings of chapter 2 and 3, and the proposed incentive mechanism is evaluated and tested to answer the research questions and hypothesis which were presented in chapter 4 on page 80. Chapter 7 is crucial for the thesis as research questions and hypotheses are reconciled with the experimental and theoretical data to get answers. In section 7.2.2 on page 163, a simulation of blockchain technology is performed to assess the performance using the Ethereum network. It is clear from the test that blockchain technology can answer the questions formulated in section 4.3 on page 95. Moreover, experiments have been conducted to evaluate the BlockPres system and use different metrics to test the system in the context of questions and hypotheses. The experimental results show the efficiency and effectiveness of the proposed system. It is also a cost-effective solution for the current healthcare system. Moreover, an incentive mechanism is also calculated, and the tokens will be given to each patient who participates in and use the healthcare system. Trust is also tested and calculated using a trust score system which shows the system can be trustworthy according to the score calculation. However, experts must test it for a real trust data. The hypothesis conclusion is also presented in section 7.5 on page 198 to report whether the hypothesis is accepted or rejected against the evidence. The questions and sub-questions are answered in the context of DSR methodology. The discussion section reconciled the findings with the literature review.

Chapter 7 evaluated and tests the proposed incentive mechanism and the findings of Chapter 2 and 3 in relation to the research questions and hypothesis presented in Chapter 4 on page 80. The chapter is of utmost importance as it involves experiments to test the research questions and hypotheses. Section 7.2.2 on page 163 performs a simulation of blockchain technology using the Ethereum network to evaluate its performance in answering the questions formulated in Section 4.3 on page 95. The experiments conducted to evaluate the efficiency and effectiveness of the proposed BlockPres system, used different metrics to test it in the context of the research questions and hypothesis. The results show that the proposed system is cost-effective and trustworthy, as indicated by the score system, although further expert testing needs to be done. Additionally, the incentive mechanism is calculated, and tokens will be awarded to each patient who participates in and uses the healthcare system. The hypothesis conclusion is presented in Section 7.5 on page 198 to report whether the evidence supports or refutes the hypothesis. The questions and sub-questions are addressed within the context of the DSR methodology. Finally, the discussion section reconciles the findings with the literature review.

Chapter 8

Conclusion

8.1 Inroduction



In Chapter 7, the proposed BlockPres Artifact is evaluated. The research questions and hypotheses are evaluated using experimental and theoretical results. Moreover, the trust level of the system is evaluated using a trust scoring system. The research questions and hypothesis are verified and reconciled with the findings in chapter 2 and 3 on page 54 using Quasi judical methods in section 7.5 on page 198. However, to conclude the thesis, the researcher summarises the research by identifying the key points, challenges, and areas for further research. Therefore, chapter 8 is structured as follows: Section 8.2 presents a thesis summary from chapter 2 to chapter 8. The challenges faced by the researcher throughout the study are discussed in section 8.3 on page 217. Section 8.4 on page 218 is concluded by discussing the future work of the study.

Chapter 7 presents the evaluation of the BlockPres Artifact , and experimental results are used to evaluate the research questions and hypotheses. Additionally, the trust level of the system is evaluated using a trust scoring system. The findings in chapter 2 and 3 on page 54 are verified and reconciled with the help of Quasi-judicial methods in section 7.5 on page 198. The researcher concluded the thesis by summarising the study, challenges, and future research areas. Chapter 8 is structured as follows: Section 8.2 summarises the thesis from chapter 2 to Chapter 7. The challenges faced by the researcher throughout the study are discussed in section 8.3 on page 217. The future work of the study is discussed in section 8.4 on page 218.

8.2 Research Summary

This section summarises the literature, problem identification, proposed BlockPres framework, and incentive mechanism. Moreover, the research methodology in the form of DSRM is evaluated. The main objective of Chapter 2 is to identify the gaps and problems in the New Zealand healthcare system. Therefore, the study adopted the DSR methodology to conduct different phases of the research. The main goal is to mitigate inequality and improve the disengagement and participation rates of Maori and Pasifika in the healthcare system using a Blockchain-based incentive mechanism.

In Chapter 2, the research used the PRISMA method to systematically review the literature and identify challenges in HIS. The study has focused on the healthcare system in New Zealand. It has identified several issues, including security and privacy concerns, data heterogeneity, counterfeit and substandard drugs, and unequal access to PMS in section 2.5 on page 35. Moreover, the study has examined how cultural differences and other factors affect Maori health in the New Zealand healthcare system and the issues and problems associated with HIS. The study focused on unequal access or inequality in the healthcare prescription system and identified reports and studies supporting the above issues in section 2.5.5.2 on page 39. The study formulated questions and a hypothesis in section 3.5 on page 76, and based on the RQs and Hypothesis, the researcher mapped a theoretical framework. Therefore, The study highlighted the need for a robust technological solution to address the issues Maori and Pasifika face regarding medication and prescriptions in the prescription management system. Chapter 3, explores Blockchain technology's potential to address unequal access and inequality issues in the Prescription Management Systems (PMS) and healthcare. The literature suggests that Blockchain technology can offer solutions to minimise these problems by providing a secure and open platform for data sharing, incentivising participation, and enhancing trust. Chapter 3 overviews Blockchain technology, its characteristics, applications, layers, and use in healthcare. Moreover, it also explored the incentive mechanism proposed by authors in different research areas. It helped the researcher to design a Blockchain-based incentive mechanism to encourage participation and sharing in the PMS. Therefore, the research questions formulated in the context of Blockchain technology and the proposed incentive mechanism were the main focus of the thesis.

Chapter 4 highlights the importance of adapting the research process as it progresses and making necessary adjustments to research questions, hypotheses, and testing methods. The Design Science Research (DSR) approach provides a structured and planned methodology for conducting research. The chapter provides an overview of the various steps involved in the DSR methodology, including problem identification, solution design and development, and solution evaluation. It also emphasises the importance of selecting appropriate research methods to answer the research questions and test the hypotheses. Chapter 6 defines the proposed incentivisation mechanism for the prescription system to mitigate inequality in the healthcare system for Maori and Pasifika. Moreover, the factors contributing to inequality, such as trust, value, loss of status, class differences, and racial bias, are explained by unequal access. The proposed incentivisation mechanism and its implementation are presented, along with formal methods to prove the solution mathematically. The Chapter 6 also analyses security parameters to ensure the secure and trustworthy provision of incentivisation processes and patient data to healthcare providers. In Chapter 5 the BlockPres framework is presented as a solution to mitigate inequality and improve patient engagement in the healthcare system using incentives and Block-chain technology. The system architecture is communicated using ArchiMate, which allows for better organisation and management of the various system components. The system workflow involves three layers: application, data storage, and service. The framework aims to incentivise patients throughout the process and increase the efficiency of patient treatment. It has the potential to improve patient engagement and build trust in the healthcare system. Hence, the BlockPres framework is promoted as a comprehensive and promising solution to address the challenges faced by the healthcare system. Chapter 7 of the thesis evaluates the proposed artifact and incentive mechanism. The experiments to test the research questions and hypothesis are presented in Chapter 4.

The chapter provides a comprehensive analysis of the efficiency and effectiveness of the BlockPres artifact, along with the incentive mechanism and trust score system. The results show that the proposed artifact is cost-effective, efficient, and trustworthy, potentially improving patient engagement and participation in the healthcare system. Moreover, the hypothesis tests and conclusions presented in Section 7.5 on page 198, indicate that the evidence supports the hypothesis, and the research questions and sub-questions are addressed within the context of the DSR methodology. Finally, the discussion section reconciles the findings with the literature review, highlighting the significance of the research and its contribution to the field of healthcare IT.

8.3 Research Challenges

The primary challenge faced by the researcher in this novel study is the need for more relevant literature and research papers available in digital libraries that highlight the issue of unequal access or inequality in the healthcare prescription system. Despite conducting a thorough search, the researcher found it difficult to locate published articles focused on the New Zealand healthcare system and highlighted the issue of unequal access or inequality. Additionally, the researcher encountered a challenge related to the emerging field of Blockchain technology, as only a few studies had implemented Blockchain technology in healthcare. Most of the research available was theoretical. Furthermore, no published studies explored the adoption of Blockchain technology as a potential solution to address the issue of unequal access or inequality.

Secondly, the researcher faced challenges when designing and developing the BlockPres framework and incentive mechanism. The researcher encountered difficulties during the prototype development and implementation phase, as there needed to be more studies that implemented Blockchain technology for reference. Consequently, it took time to select the right platform for implementation and tools for the Artifact . Thirdly, this research is supported by Orion Health, and it was challenging to convince them to continue supporting financially and provide support on time. Lastly, the university's financial recovery plan resulted in the redundancy of most of the supervisors, which significantly impacted the researcher's progress and the ability to continue research on the project.

8.4 Future Work

This section presents several potential areas of research that could be pursued to enhance and expand upon the findings outlined in this thesis. The following opportunities are worth considering.

8.4.1 Enhancement of BlockPres Framework

In Chapter 4, the researcher proposed the BlockPres framework as a solution to mitigate the issue of inequality or unequal access in the healthcare system using blockchain technology. The current framework requires improvements to keep up with the ongoing changes in the New Zealand healthcare system. The framework is initially designed based on the proposed infrastructure of healthcare, where all the District Health Boards (DHBs) merged to form one NZ Health entity, with all the hospitals and healthcare providers operating under it, as described in section 5.3 on page 121. However, with the possibility of future changes, the framework will need to adapt accordingly.

8.4.2 Expert Evaluation of BlockPres

In Chapter 4, the researcher proposed the BlockPres artifact, and in Chapter 6, proposed an incentive mechanism using blockchain technology. The researcher developed the BlockPres artifact using the Ethereum platform, created dummy patient accounts, and generated data to test the system, as described in Section 7.2 on page 161. However, the artifact needs expert feedback to improve its effectiveness. Additionally, it is essential to test the artifact on actual patients and real-time data to identify areas for improvement. As per the DSR methodology described in Section 4.2 on page 81, the artifact iteration process can be a part of the evaluation process. Due to time constraints, the artifact iteration process will be considered in future work.

8.4.3 Platform Concerns

The researcher used the Ethereum platform to implement the BlockPres artifact. Ethereum was chosen as the platform for BlockPres due to its secure and reliable infrastructure, smart contract feature, open-source nature, and compatibility with existing blockchain standards, making integrating with other healthcare systems easier. This allows for the automation, transparency, and security factors which are crucial in the healthcare industry. However, Ethereum has potential drawbacks that may affect the working of the BlockPres Artifact, such as scalability issues, costly gas fees, complexity, and energy consumption. However, these drawbacks can be addressed with context focused planning, design, and implementation, such as using development frameworks or experienced developers to address complexity or implementing layer two solutions or other blockchain platforms to address scalability issues. Moreover, other platforms can be explored to migrate the platform such as hyperledger fabric and IBM blockchain.

8.4.4 Consensus Mechanism

This study uses Proof of stake as a consensus mechanism in the Ethereum platform to achieve distributed consensus and to achieve distributed consensus and validate transactions on the network. In PoS, network participants, also known as validators, are chosen to create a new block based on the amount of cryptocurrency they hold and are willing to "stake" or lock up for some time. However, some POS issues exist, such as security vulnerabilities, slashing, and fairness concerns. These can be minimised by using the delegated Proof of stake or Proof of authority mechanisms.

8.4.5 Enhancement of Proposed Incentive mechanism

In Chapter 6, the researcher proposes an incentive mechanism to mitigate the disengagement of Maori and Pasifika who face barriers accessing the healthcare system, particularly the prescription management system, as discussed in Chapter 2. The proposed mechanism would provide financial benefits to those who struggle to afford healthcare expenses by distributing tokens that can be used for discounts or purchases, depending on the healthcare provider. However, this mechanism has not yet been tested in a real-world environment and may need to be refined based on feedback from healthcare providers. Additionally, there is a need for greater effectiveness in distributing and using the tokens.

8.5 Conclusion

This research study proposed a blockchain-based incentivisation mechanism to address the inequality and unequal access faced by Maori and Pasifika in the New Zealand healthcare system. A Design Science Research Methodology (DSRM) and a systematic literature review were used in the study to identify gaps and problems in the New Zealand healthcare system, explore the potential of blockchain technology in healthcare, and design and evaluate a blockchain-based incentivisation mechanism for prescription management systems. The BlockPres framework was presented in the study as a comprehensive and promising solution to the healthcare system's challenges. The proposed Artifact and incentive mechanism were evaluated effectively indicating their potential to improve patient engagement and participation in the healthcare system. Despite the difficulties encountered during the research, the study has made an important contribution to the field of healthcare IT by proposing a novel solution to the problem of inequality and unequal access in the healthcare system.

References

Abdullah, D. (2018). *Medrec 2.0.* Retrieved 05 Nov 2019, from `https://medicalchain.com/Medicalchain-Whitepaper-EN.pdf`

Abdullah, D. (2019). *https://medicalchain.com/medicalchain-whitepaper-en.pdf.* Retrieved 01 Nov 2019, from `https://medicalchain.com/Medicalchain-Whitepaper-EN.pdf`

Abouelmehdi et al. (2018). Big healthcare data: preserving security and privacy. *Journal of Big Data*, *5*(1), 1.

Agbo et al. (2019). Blockchain technology in healthcare: a systematic review. In *Healthcare* (Vol. 7, p. 56).

Ahern et al. (2006). What is ehealth (6): perspectives on the evolution of ehealth research. *Journal of medical Internet research*, *8*(1).

Ahmed et al. (2017). Food supply: Blockchain could boost food security. *Nature*, *550*(7674), 43.

Ahmed et al. (2018). Blockchain technology a literature survey. *International Research Journal of Engineering and Technology*, *05*(10), 1490–1493.

Aken. (2004). Management research based on the paradigm of the design sciences: the quest for field-tested and grounded technological rules. *Journal of management studies*, *41*(2), 219–246.

Akins et al. (2014). A whole new world: Income tax considerations of the bitcoin economy. *Pitt. Tax Rev.*, *12*, 25.

Al-Busaidi et al. (2018). Māori indigenous health framework in action: addressing ethnic disparities in healthcare. *The New Zealand Medical Journal (Online)*, *131*(1470), 89-93.

Al-Dhafian et al. (2017). Improving the security in healthcare information system through elman neural network based classifier. *Journal of Medical Imaging and Health Informatics*, *7*(6), 1429–1435.

Aldridge. (2016). Hidden wholesale: The drug diffusing capacity of online drug cryptomarkets. *International Journal of Drug Policy*, *35*, 7-15.

Al-Fageh et al. (2018). Perceived causes of prescribing errors by physicians: A qualitative study. *Tropical Journal of Pharmaceutical Research*, *17*(7), 1415–1422.

Alharby et al. (2018). Blockchain-based smart contracts: A systematic mapping study of academic research (2018). In *2018 international conference on cloud computing, big data and blockchain (iccbb)* (pp. 1–6).

Alharby et al. (2019). Blocksim: a simulation framework for blockchain systems. *ACM SIGMETRICS Performance Evaluation Review*, *46*(3), 135–138.

Ali et al. (2017). Blockstack: A new internet for decentralized applications. *Technical Whitepaper Version*, *1*.

Almutairi et al. (2018). Physicians' perceptions of electronic prescribing with electronic medical records in kuwaiti primary healthcare centres. *Sultan Qaboos University Medical Journal*, *18*(4).

Alshamari. (2016). Usability factors assessment in health information system. *Intelligent Information Management*, *8*(06), 170.

Amofa et al. (2018). A blockchain-based architecture framework for secure sharing of personal health data. In *2018 ieee 20th international conference on e-health networking, applications and services (healthcom)* (pp. 1–6).

Ananth et al. (2018). A secured healthcare system using private blockchain technology. *Journal of Engineering Technology*, *6*(2), 42–54.

Anderson et al. (2006). *Indigenous health 1: Indigenous health in Australia, New Zealand, and the Pacific the lancet.* London.

Androulaki et al. (2018). Hyperledger fabric: a distributed operating system for permissioned blockchains. In *Proceedings of the thirteenth eurosys conference* (pp. 1–15).

Ash et al. (2007). The extent and importance of unintended consequences related to computerized provider order entry. *Journal of the American Medical Informatics Association*, *14*(4), 415–423.

Atanasovski. (2018). On defining a model driven architecture for an enterprise e-health system. *Enterprise Information Systems*, *12*(8-9), 915–941.

Atzori et al. (2010). The internet of things: A survey. *Computer networks*, *54*(15), 2787–2805.

Axelsson et al. (2016). The field of indigenous health and the role of colonisation and history. *Journal of Population Research*, *33*(1), 1–7.

Azaria et al. (2016). Medrec: Using blockchain for medical data access and permission management. In *Open and big data (OBD), international conference on* (pp. 25–30). Vienna, Austria.

Badr et al. (2018). Multi-tier blockchain framework for iot-ehrs systems. *Procedia Computer Science*, *141*, 159–166.

Banerjee et al. (2022). Blockchain in iot and beyond: Case studies on interoperability and privacy. In *Blockchain based internet of things* (pp. 113–138). Springer.

Bano et al. (2019). Sok: Consensus in the age of blockchains. In *Proceedings of the 1st acm conference on advances in financial technologies* (pp. 183–198).

Bell et al. (2018). Applications of blockchain within healthcare. *Blockchain in Healthcare Today*, *1*, 1-7. Retrieved from `https://doi.org/10.30953/bhty.v1.8`

Benkaouz et al. (2015). Towards a decentralized osn for a privacy-preserving e-health system. *Procedia Computer Science*, *63*, 284–291.

Beverley. (2014). Counterfeit drugs and medical devices in developing countries. *Research and Reports in Tropical Medicine*, *2014*, 11–22.

Bhardwaj et al. (2020). Consensus algorithm. *Decentralised Internet of Things: A Blockchain Perspective*, 91–107.

Bocek et al. (2017). Blockchains everywhere-a use-case of blockchains in the pharma supply-chain. In *2017 ifip/ieee symposium on integrated network and service management (im)* (pp. 772–777).

Bogliolo et al. (2012). Virtual currency and reputation-based cooperation incentives in user-centric networks. In *2012 8th international wireless communications and mobile computing conference (iwcmc)* (pp. 895–900).

Boonstra et al. (2014). Implementing electronic health records in hospitals: a systematic literature review. *BMC health services research*, *14*(1), 370.

Braun et al. (2013). Community health workers and mobile technology: a systematic review of the literature. *PloS one*, *8*(6), e65772.

Brodersen et al. (2016a). *Blockchain: Securing a new health interoperability experience.* Retrieved from `https://bit.ly/2Hj5BjO`

Brodersen et al. (2016b). *Blockchain: Securing a new health interoperability experience* (Tech. Rep.). Accenture LLC. Retrieved from `https://www.healthit.gov/sites/default/files/2-49-accenture_onc_blockchain_challenge_response_august8_final.pdf`

Bulleit et al. (2018). *US patent app. 15/684,173. blockchain-based mechanisms for secure health information resource exchange.* USA: US Patents Office.

Buterin, V. (2015). *On public and private blockchains.* ethereum.blog. Retrieved 25 Nov, 2018, from `https://bit.ly/2yK9mLd`

Buttyan et al. (2007). Barter-based cooperation in delay-tolerant personal wireless networks. In *2007 ieee international symposium on a world of wireless, mobile and multimedia networks* (pp. 1–6).

Came et al. (2017). Health activism against barriers to indigenous health in Aotearoa New zealand. *Critical Public Health*, *27*(4), 515-521.

Campbell et al. (2006). Types of unintended consequences related to computerized provider order entry. *Journal of the American Medical Informatics Association*, *13*(5), 547–556.

Campbell et al. (2009). Computerized provider order entry adoption: implications for clinical workflow. *Journal of general internal medicine*, *24*(1), 21–26.

Carboni. (2015). Feedback based reputation on top of the bitcoin blockchain. *arXiv preprint arXiv:1502.01504*.

Cardenas et al. (2013). Big data analytics for security. *IEEE Security & Privacy*, *11*(6), 74–76.

Cardozo et al. (2010). *The nature of the judicial process*. Quid Pro Books.

Cartwright-Smith et al. (2016). Health information ownership: legal theories and policy implications. *Vand. J. Ent. & Tech. L.*, *19*, 207.

Castaneda et al. (2015). Clinical decision support systems for improving diagnostic accuracy and achieving precision medicine. *Journal of clinical bioinformatics*, *5*(1), 4.

Cavell et al. (2019). Magnitude of error: a review of wrong dose medication incidents reported to a uk hospital voluntary incident reporting system. *European Journal* *of Hospital Pharmacy*.

Cengiz. (2018). *Blockchain as a service on microsoft azure* [Internet web Page]. Retrieved 08 june 2019, from `https://bit.ly/2EbPrX5`

Chapron. (2017). The environment needs cryptogovernance. *Nature News*, *545*(7655), 403.

Charters. (2019). The declaration on the rights of indigenous peoples in New Zealand courts: A case of cautious optimism. *Available at SSRN 3356127*.

Chen et al. (2016). Towards autonomic security management of healthcare information systems. In *2016 ieee first international conference on connected health: Applications, systems and engineering technologies (chase)* (pp. 113–118).

Chen et al. (2020). Traveling the token world: A graph analysis of ethereum erc20 token ecosystem. In *Proceedings of the web conference 2020* (pp. 1411–1421).

Chen, B. B. & Chan, M. C. (2010). Mobicent: a credit-based incentive system for disruption tolerant network. In *2010 proceedings ieee infocom* (pp. 1–9).

Chitu. (2015, November). A guide to conducting a standalone systematic literature review. *Communications of the Association for Information Systems*, *37*(43), 879–910.

Christidis et al. (2016). Blockchains and smart contracts for the internet of things. *Ieee Access*, *4*, 2292–2303.

Clarke et al. (1981). Design and synthesis of synchronization skeletons using branching time temporal logic. In *Workshop on logic of programs* (pp. 52–71).

Colijn et al. (2017). Toward precision healthcare: context and mathematical challenges. *Frontiers in physiology*, *8*, 136.

Collins et al. (2017). Kidney disease in Māori and Pasifika in New Zealand. In *Chronic kidney disease in disadvantaged populations* (pp. 157–166). Elsevier.

Creswell et al. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.

Cunningham et al. (2018). Enabling patient control of personal electronic health records through distributed ledger technology. In *Medinfo 2017: Precision healthcare through informatics: Proceedings of the 16th world congress on medical and health informatics* (Vol. 245, p. 45).

da Conceição et al. (2018). Eletronic health records using blockchain technology. *CoRR*. Retrieved from `https://arxiv.org/abs/1804.10078`

Dagher et al. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable Cities and Society*, *39*, 283–297.

Daniel, R. & Roth, B. (2021). *Gwei: Ethereum base units.* Retrieved 5 July, 2021, from `https://gwei.io`

Das et al. (2016). Quality and accountability in health care delivery: audit-study evidence from primary care in india. *American Economic Review*, *106*(12), 3765–99.

Datta et al. (2017). Improving tuberculosis diagnosis: Better tests or better healthcare? *PLoS medicine*, *14*(10), e1002406.

Dawson et al. (2019). Barriers to equitable maternal health in Aotearoa New Zealand: an integrative review. *International journal for equity in health*, *18*(1), 168.

de Almeida et al. (2022). Authentication and authorization in microservices architecture: A systematic literature review. *Applied Sciences*, *12*(6), 3023.

Dégardin et al. (2014). Understanding and fighting the medicine counterfeit market. *Journal of pharmaceutical and biomedical analysis*, *87*, 167–175.

Deng et al. (2020). Retrospective analysis of the 13-year trend in acute and elective surgery for patients aged 60 years and over at Auckland city hospital, New Zealand. *J Epidemiol Community Health*, *74*(1), 42–47.

Denison et al. (2018). Inequities in exposure to occupational risk factors between Māori and non-Māori workers in Aotearoa New Zealand. *J Epidemiol Community Health*, *72*(9), 809–816.

Devine. (2015). Blockchain learning: can crypto-currency methods be appropriated to enhance online learning? In *ALT online winter conference.* The Open University: The Open University.

Dias et al. (2018). Blockchain for access control in e-health scenarios. *CoRR ArXiv*. Retrieved from `https://arxiv.org/abs/1805.12267`

Dixon-Woods et al. (2005). Synthesising qualitative and quantitative evidence: a review of possible methods. *Journal of health services research & policy*, *10*(1), 45–53.

Doan et al. (2022). Towards decentralised cloud storage with ipfs: Opportunities, challenges, and future directions. *arXiv preprint arXiv:2202.06315*.

Dong et al. (2019). Combination model of heterogeneous data for security measurement. *Journal of Universal Computer Science*, *25*(3), 270–281. doi: 10.3217/jucs-025-03-0270

Dorri et al. (2017). Blockchain: A distributed solution to automotive security and privacy. *IEEE Communications Magazine*, *55*(12), 119–125.

dos Santos et al. (2019). Comparison between counterfeit and authentic medicines: A novel approach using differential scanning calorimetry and hierarchical cluster analysis. *Journal of pharmaceutical and biomedical analysis*, *166*, 304–309.

Dresch et al. (2015). Design science research. In *Design science research* (pp. 67–102). Springer.

Dubovitskaya et al. (2017a). How blockchain could empower ehealth: An application for radiation oncology. In *Workshop on data management and analytics for medicine and healthcare* (pp. 3–6). Nature Switzerland.

Dubovitskaya et al. (2017b). Secure and trustable electronic medical records sharing using blockchain. In *Amia annual symposium proceedings* (Vol. 2017, p. 650).

Dyson et al. (2020). Scenario-based creation and digital investigation of ethereum erc20 tokens. *Forensic Science International: Digital Investigation*, *32*, 200894.

Easterbrook et al. (1998). Experiences using lightweight formal methods for requirements modeling. *IEEE Transactions on Software Engineering*, *24*(1), 4–14.

Ekblaw et al. (2016). A case study for blockchain in healthcare: “medrec” prototype for electronic health records and medical research data. In *Proceedings of ieee open & big data conference* (Vol. 13, p. 13). china.

Ellison-Loschmann et al. (2006). Improving access to health care among new zealand's maori population. *American journal of public health*, *96*(4), 612–617.

Engelhardt. (2017). Hitching healthcare to the chain: An introduction to blockchain technology in the healthcare sector. *Technology Innovation Management Review*, *7*(10).

Eriksson et al. (2017). *Inequities in health care: lessons from new zealand: A qualitative interview study about the cultural safety theory.*

Fadlallah et al. (2016). Strategies and systems-level interventions to combat or prevent drug counterfeiting: a systematic review of evidence beyond effectiveness. *Pharmaceutical medicine*, *30*(5), 263–276.

Fan et al. (2018). Medblock: Efficient and secure medical data sharing via blockchain. *Journal of medical systems*, *42*(8), 136.

Fatima et al. (2018). Security aspects in healthcare information systems: A systematic mapping. *Procedia computer science*, *138*, 12–19.

Feldman et al. (2006). Free-riding and whitewashing in peer-to-peer systems. *IEEE Journal on selected areas in communications*, *24*(5), 1010–1019.

Felegyhazi et al. (2006). Nash equilibria of packet forwarding strategies in wireless ad hoc networks. *IEEE Transactions on Mobile computing*, *5*(5), 463–476.

Fenoff. (2009). *Africa's counterfeit pharmaceutical epidemic:the road ahead* [Internet web Page].

Friedman et al. (2009). Across the atlantic cooperation to address international challenges in ehealth and health it: Managing toward a common goal. *international journal of medical informatics*, *78*(11), 778–784.

Furda et al. (2019). Advanced information technologies and techniques for healthcare digital transformation and adoption. *Data-Centric Business and Applications: Evolvements in Business Information Processing and Management (I).*, *2*, 19.

Gagnon et al. (2015). m-health adoption by healthcare professionals: a systematic review. *Journal of the American Medical Informatics Association*, *23*(1), 212–220.

Geifman et al. (2015). Opening clinical trial data: are the voluntary data-sharing portals enough? *BMC medicine*, *13*(1), 280.

Gervais et al. (2016). On the security and performance of proof of work blockchains. In *Proceedings of the 2016 acm sigsac conference on computer and communications security* (pp. 3–16).

Gilmour et al. (2016). Oral health experiences of māori with dementia and whānau perspectives-oranga waha mō ngā iwi katoa. *Nursing Praxis in New Zealand*, *32*(1).

Gogerty et al. (2011). *Deko: An electricity-backed currency proposal* [Internet Web Page]. Retrieved 25,Nov,2018, from `https://bit.ly/34Z6xlN`

Gokalp. (2018). Analysing opportunities and challenges of integrated blockchain technologies in healthcare. In *Eurosymposium on systems analysis and design* (pp. 174–183).

Goodyear-Smith et al. (2019). New Zealand health system: universalism struggles with persisting inequities. *The Lancet*, *394*(10196), 432–442.

Gordon et al. (2018). Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability. *Computational and Structural Biotechnology Journal*, *16*(1), 224–230. doi: 10.1016/j.csbj.2018.06.003

Goslee et al. (1998). *Losing ground bit by bit: Low-income communities in the information age. what's going on series.* ERIC. Retrieved from `https://eric.ed.gov/?id=ED424333`

Graham et al. (2020). Experiences of māori of aotearoa new zealand's public health system: a systematic review of two decades of published qualitative research. *Australian and New Zealand journal of public health*, *44*(3), 193–200.

Grandia. (2017). Healthcare information systems: a look at the past, present, and future. *Health Catalyst*, 1–4.

Griggs et al. (2018). Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *Journal of medical systems*, *42*(7), 130.

Guo et al. (2018). Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems. *IEEE Access*, *776*(99), 1–12.

Gupta et al. (2020). Evaluation of proof-of-work consensus algorithm for blockchain networks. In *2020 11th international conference on computing, communication and networking technologies (icccnt)* (pp. 1–7).

Gurney et al. (2020). Addressing cancer inequities for indigenous populations: The New Zealand story. *Journal of Cancer Policy*, 100209.

Gursel et al. (2016). Determining the weak sides of healthcare information systems: an empirical e-health evaluation study. *AJIT-e: Online Academic Journal of Information Technology*, *7*(23), 17–29.

Gutiérrez et al. (2020). Healthyblock: blockchain-based it architecture for electronic medical records resilient to connectivity failures. *International Journal of Environmental Research and Public Health*, *17*(19), 7132.

Halcomb et al. (2015). Consumer satisfaction with practice nursing: a cross-sectional survey in new zealand general practice. *Australian Journal of Primary Health*, *21*(3), 347–353.

Hamlin et al. (2016). Long-term effectiveness of the New Zealand green prescription primary health care exercise initiative. *Public Health*, *140*, 102–108.

Han et al. (2018). An architecture of secure health information storage system based on blockchain technology. In *International conference on cloud computing and security* (pp. 578–588). Nature Switzerland.

Hardjono et al. (2016). Cloud-based commissioning of constrained devices using permissioned blockchains. In *Proceedings of the 2nd ACM international workshop on IoT privacy, trust, and security* (pp. 29–36). Xi'an, China.

Harris et al. (2015). Investigating the relationship between ethnic consciousness, racial discrimination and self-rated health in New Zealand. *PLoS One*, *10*(2).

Harris et al. (2018). Ethnic bias and clinical decision-making among New Zealand medical students: an observational study. *BMC medical education*, *18*(1), 18.

Hartung et al. (2014). Reporting discrepancies between the clinicaltrials. gov results database and peer-reviewed publications. *Annals of internal medicine*, *160*(7), 477–483.

Hatch et al. (2011). Difference between pharmacist-obtained and physician-obtained medication histories in the intensive care unit. *Hospital Pharmacy*, *46*(4), 262–268.

Haua et al. (2019). Pharmacist integration into general practice in new zealand. *Journal of Primary Health Care*, *11*(2), 159–169.

He, Q., Wu, D. & Khosla, P. (2006). A secure incentive architecture for ad hoc networks. *Wireless Communications and Mobile Computing*, *6*(3), 333–346.

Health, T. & Commissioner, D. (2018). *complaints closed by the health and disability commissioner about medication errors: Analysis and report 2009–2016* [Internet web Page]. Retrieved 28 June2019, from `https://bit.ly/2VUPFbB`

Hevner et al. (2010). Design science research in information systems. In *Design research in information systems* (pp. 9–22). Springer.

Hobbs et al. (2019). Reducing health inequity for Māori people in New Zealand. *The Lancet*, *394*(10209), 1613–1614.

Horsky et al. (2005). Comprehensive analysis of a medication dosing error related to cpoe. *Journal of the American Medical Informatics Association*, *12*(4), 377–382.

Hosseinkhah et al. (2009). Challenges in data mining on medical databases. In *Database technologies: Concepts, methodologies, tools, and applications* (pp. 1393–1404). IGI Global.

Howe et al. (2018). Electronic health record usability issues and potential contribution to patient harm. *Jama*, *319*(12), 1276–1278.

Hussein et al. (2018). A medical records managing and securing blockchain based system supported by a genetic algorithm and discrete wavelet transform. *Cognitive Systems Research*, *52*.

Ichikawa et al. (2017). Tamper-resistant mobile health using blockchain technology. *JMIR mHealth and uHealth*, *5*(7).

Ishmaev. (2017). Blockchain technology as an institution of property. *Metaphilosophy*, *48*(5), 666–686.

Ismail et al. (2020). Blockchain paradigm for healthcare: Performance evaluation. *Symmetry*, *12*(8), 1200. doi: 10.3390/sym12081200

Jaag et al. (2017). Blockchain technology and cryptocurrencies: Opportunities for postal financial services. In *The changing postal and delivery sector* (pp. 205–221). Springer.

Jacobs, A. (2009). The pathologies of big data. *Queue*, *7*(6), 10.

James. (2018). *Consortium chain development* [Internet]. Github. Retrieved 25 Nov, 2018, from `https://bit.ly/3eRAAjA`

Jamie. (2019). Prescribing in 2019: what are the safety concerns? *EXPERT OPINION ON DRUG SAFETY*, 69-74. Retrieved 08 may 2018, from `https://doi.org/10.1080/14740338.2019.1571038`

Jiang et al. (2018). Blochie: a blockchain-based platform for healthcare information exchange. In *2018 ieee international conference on smart computing (smartcomp)* (pp. 49–56). Taormina, Italy.

John et al. (2012). Measuring the prevalence of questionable research practices with incentives for truth telling. *Psychological science*, *23*(5), 524–532.

John et al. (2018). A novel trust-scoring system using trustability co-efficient of variation for identification of secure agent platforms. *PloS one*, *13*(8), e0201600.

Julian et al. (2009). *Combating the spread of fake drugs in poor countries* [Internet web Page]. International Policy Network. Retrieved 08 may 2018, from `https://bit.ly/34ZxrtA`

Juneja et al. (2018). Leveraging blockchain for retraining deep learning architecture in patient-specific arrhythmia classification. In *Biomedical & health informatics (bhi), 2018 IEEE EMBS international conference on* (pp. 393–397). Las Vegas,NV,USA.

Kamel Boulos et al. (2018). Geospatial blockchain: Promises, challenges, and scenarios in health and healthcare. *International Journal of Health Geographics*, *17*(25). doi: 10.1186/s12942-018-0144-x

Kantarci et al. (2015). Crowdsensing with social network-aided collaborative trust scores. In *2015 ieee global communications conference (globecom)* (pp. 1–6).

Karna et al. (2012). Study and evaluation of medication errors in a tertiary care teaching hospital-a baseline study. *Int J Pharm Pharm Sci*, *4*(5), 587–93.

Kaur et al. (2018). A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment. *Journal of medical systems*, *42*(8), 156.

Kaushal et al. (2003). Effects of computerized physician order entry and clinical decision support systems on medication safety: a systematic review. *Archives of internal medicine*, *163*(12), 1409–1416.

Keene et al. (2016). Funding New Zealand's public healthcare system: time for an honest appraisal and public debate. *More flexible approaches are needed to improve cardiac rehabilitation*, *129*(1435).

Kelman et al. (2002). Research use of linked health data—a best practice protocol. *Australian and New Zealand journal of public health*, *26*(3), 251–255.

Key health sector organisations and people. (2021). Manatū Hauora Ministry of Health. Retrieved 4 July, 2021, from `https://www.health.govt.nz/new-zealand-health-system/key-health-sector-organisations-and-people`

Khatoon. (2020). A blockchain-based smart contract system for healthcare management. *Electronics*, *9*(1), 94.

Kim et al. (2017). A trusted sharing model for patient records based on permissioned blockchain. *J. Int. Comput. Serv*, *18*, 75–84.

King et al. (2012). *Ppcoin: Peer-to-peer crypto-currency with proof-of-stake* [Internet Web Page]. Retrieved 04 Dec 2018, from `http://bitcoin.peryaudo.org/vendor/peercoin-paper.pdf`

Kleinaki et al. (2018). A blockchain-based notarization service for biomedical knowledge retrieval. *Computational and structural biotechnology journal*, *16*, 288–297.

Kohli et al. (2016). Electronic health records: how can is researchers contribute to transforming healthcare? *Mis Quarterly*, *40*(3), 553–573.

Kohn et al. (2000). *Institute of medicine. to err is human: building a safer health* *system.* Washington, DC: National Academy Press.

Kombe et al. (2018). A review on healthcare information systems and consensus protocols in blockchain technology. *International Journal of Advanced Technology and Engineering Exploration*, *5*(49), 473–483.

Kotzé et al. (2015). Design science research as research approach in doctoral studies.

Kraft et al. (2019). *Namecoin* [Internet web Page]. Retrieved 08 june 2019, from `https://namecoin.org`

Krichen et al. (2004). Black-box conformance testing for real-time systems. In *International spin workshop on model checking of software* (pp. 109–126).

Krichen et al. (2006a). Interesting properties of the real-time conformance relation tioco. In *International colloquium on theoretical aspects of computing* (pp. 317–331).

Krichen et al. (2006b). State-identification problems for finite-state transducers. In *Formal approaches to software testing and runtime verification* (pp. 148–162). Springer.

Kripke. (2007). Semantical considerations of the modal logic. *Studia Philosophica*, *1*.

Kumar et al. (2018). Blockchain utilization in healthcare: Key requirements and challenges. In *2018 ieee 20th international conference on e-health networking, applications and services (healthcom)* (pp. 1–7).

Kuo et al. (2018). Modelchain: Decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks. *CoRR ArXiv*, 13. Retrieved from `https://arxiv.org/abs/1802.01746`

Kuo et al. (2019). Comparison of blockchain platforms: a systematic review and healthcare examples. *Journal of the American Medical Informatics Association*, *26*(5), 462–478.

Lane et al. (2019). Healthcare decision making: Allied health and equity. In *Mental health policy, practice, and service accessibility in contemporary society* (pp. 41–56). IGI Global.

Lawson, e. a. (2019). A principles framework for taking action on Māori/indigenous homelessness in Aotearoa New Zealand. *SSM-population health*, *8*, 100450.

Lee et al. (2015). Comon+: A cooperative context monitoring system for multi-device personal sensing environments. *IEEE Transactions on Mobile Computing*, *15*(8), 1908–1924.

Leitch et al. (2021). Medication-related harm in new zealand general practice: a retrospective records review. *British Journal of General Practice*, *71*(709), e626–e633.

Lepore et al. (2020). A survey on blockchain consensus with a performance comparison of pow, pos and pure pos. *Mathematics*, *8*(10), 1782.

Li et al. (2021). Understanding and addressing quality attributes of microservices architecture: A systematic literature review. *Information and software technology*, *131*, 106449.

Liang et al. (2017). Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In *Personal, indoor, and mobile radio communications (pimrc), 2017 ieee 28th annual international symposium on* (pp. 1–5). Montreal, QC, Canada.

Linnet, M. E. (2018). *Maersk and ibm introduce tradelens blockchain shipping solution.* Retrieved 08 july 2019, from `https://newsroom.ibm.com/2018-08-09-Maersk-and-IBM-Introduce-TradeLens-Blockchain-Shipping-Solution`

Litchfield, A. & Khan, A. (2021). Blockpres: A novel blockchain-based incentive mechanism to mitigate inequalities for prescription management system. *Sensors*, *21*(15), 5035.

Liu et al. (2017). Advanced block-chain architecture for e-health systems. In *e-health networking, applications and services (healthcom), 2017 ieee 19th international conference on* (pp. 1–6). Dalian, China.

Lu et al. (2017). Adaptable blockchain-based systems: a case study for product traceability. *IEEE Software*, *34*(6), 21–27.

Mamun, A. et al. (2022). Blockchain-based electronic health records management: a comprehensive review and future research direction. *IEEE Access*, *10*, 5768–5789.

March et al. (1995). Design and natural science research on information technology. *Decision support systems*, *15*(4), 251–266.

Markus et al. (2002). A design theory for systems that support emergent knowledge processes. *MIS quarterly*, 179–212.

Marriott et al. (2015). Indicators of inequality for maori and pacific people. *Journal of New Zealand Studies*(20), 24.

Martin, H. (2018). *Auckland midwife prescribed herself pain pills in others people's name.* stuff.co.nz. Retrieved 01 Nov 2019, from `https://bit.ly/2zuZs0D`

Mashima et al. (2012). Enabling robust information accountability in e-healthcare systems. In *Healthsec.*

Massi, M. et al. (2018). *Using prov and blockchain to achieve health data provenance* [Working Paper]. Retrieved from `https://eprints.soton.ac.uk/421292/`

Maxwell. (2005). Conceptual framework: What do you think is going on. *Qualitative research design: An interactive approach*, *41*, 33–63.

McFarlane et al. (2017). Patientory: A healthcare peer-to-peer emr storage network v1. *Entrust Inc.: Addison, TX, USA*.

McGuire et al. (2008). Confidentiality, privacy, and security of genetic and genomic test information in electronic health records: points to consider. *Genetics in Medicine*, *10*(7), 495.

Meng et al. (2018). When intrusion detection meets blockchain technology: a review. *IEEE Access*, *6*, 10179–10188.

Microsoft. (2019). *Blockchain: Develop, test, and deploy secure blockchain apps* [Internet web Page]. Retrieved 08 june 2019, from `https://azure.microsoft.com/en-us/solutions/blockchain/`

Middleton et al. (2013). Enhancing patient safety and quality of care by improving the usability of electronic health record systems: recommendations from amia. *Journal of the American Medical Informatics Association*, *20*(e1), e2–e8.

Mikula et al. (2018). Identity and access management with blockchain in electronic healthcare records. In *2018 21st euromicro conference on digital system design (dsd)* (pp. 699–706).

Mingxiao et al. (2017). A review on consensus algorithm of blockchain. In *2017 ieee international conference on systems, man, and cybernetics (smc)* (pp. 2567–2572).

Miorandi et al. (2012). Internet of things: Vision, applications and research challenges. *Ad hoc networks*, *10*(7), 1497–1516.

Miriovsky et al. (2012). Importance of health information technology, electronic health records, and continuously aggregating data to comparative effectiveness research and learning health care. *Journal of Clinical Oncology*, *30*(34), 4243–4248.

Moher et al. (2009). Preferred reporting items for systematic reviews and meta-analyses: the prisma statement. *Annals of internal medicine*, *151*(4), 264–269.

Morales et al. (2020). User behavior and token adoption on erc20. *arXiv preprint arXiv:2005.12218*.

Morini. (2016). From 'blockchain hype' to a real business case for financial markets. *Social Science Research Network*. Retrieved from `AvailableatSSRN:https://ssrn.com/abstract=2760184` doi: http://dx.doi.org/10.2139/ssrn.2760184

Mousa et al. (2015). Trust management and reputation systems in mobile participatory sensing applications: A survey. *Computer Networks*, *90*, 49–73.

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system* [Internet Web Page]. Retrieved 4 Dec 2018, from `https://bitcoin.org/bitcoin.pdf`

Nardi et al. (2016). Emerging issues and opportunities in health information technology. *Journal of the National Comprehensive Cancer Network*, *14*(10), 1226–1233.

Nayyar. (2019). Falsified and substandard drugs: Stopping the pandemic. *The American journal of tropical medicine and hygiene*, 1-8.

Nelson et al. (2016). *Health informatics-e-book: An interprofessional approach*. Elsevier Health Sciences.

Neuspiel et al. (2013). Reducing the risk of harm from medication errors in children. *Health services insights*, *6*, HSI–S10454.

Neville et al. (2022). Barriers to older pacific peoples' participation in the health-care system in aotearoa new zealand. *Journal of Primary Health Care*, *14*(2), 124–129.

Ning et al. (2011). Incentive-aware data dissemination in delay-tolerant mobile networks. In *2011 8th annual ieee communications society conference on sensor, mesh and ad hoc communications and networks* (pp. 539–547).

Noyes, C. (2016a). Bitav: Fast anti-malware by distributed blockchain consensus and feedforward scanning. *CoRR*, *abs/1601.01405*. Retrieved from `http://arxiv.org/abs/1601.01405`

Noyes, C. (2016b). *Bitav: Fast anti-malware by distributed blockchain consensus and feedforward scanning* [Internet web site]. Retrieved from `https://arxiv.org/abs/1601.01405`

Omar, A. et al. (2017). Medibchain: A blockchain based privacy preserving platform for healthcare data. In *International conference on security, privacy and anonymity in computation, communication and storage* (pp. 534–543). Guangzhou, China.

Omar, A. et al. (2019). Privacy-friendly platform for healthcare data in cloud based on blockchain environment. *Future Generation Computer Systems*, *95*, 511–521.

Paine et al. (2016). Explaining ethnic inequities in sleep duration: a cross-sectional survey of māori and non-māori adults in New Zealand. *Sleep health*, *2*(2), 109–115.

Patel. (2018). A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. *Health informatics journal*, *24*(1), 1–14.

Patil et al. (2014). Big data security and privacy issues in healthcare. In *Big data (bigdata congress), 2014 ieee international congress on* (pp. 762–765).

Peffers et al. (2007). A design science research methodology for information systems research. *Journal of management information systems*, *24*(3), 45–77.

Peters et al. (2015). Trends in cryptocurrencies and blockchain technologies: a monetary theory and regulation perspective. *Journal of Financial Perspectives*, *3*(3).

Peterson et al. (2016). *A blockchain-based approach to health information exchange networks* [White paper]. Retrieved 04 dec 2018, from `https://bit.ly/3eQN9fl`

Phalke et al. (2011). Prescription writing practices in a rural tertiary care hospital in western maharashtra, india. *The Australasian medical journal*, *4*(1), 4.

Pham et al. (2018). A secure remote healthcare system for hospital using blockchain smart contract. In *2018 ieee globecom workshops (gc wkshps)* (pp. 1–6).

Pilkington. (2016). Does the fintech industry need a new risk management philosophy? a sequential blockchain-based typology for virtual currencies and e-money services in luxembourg. *SSRN Electronic Journal*. Retrieved from `http://dx.doi.org/10.2139/ssrn.2744899`

Pouryazdan et al. (2017). Quantifying user reputation scores, data trustworthiness, and user incentives in mobile crowd-sensing. *IEEE Access*, *5*, 1382–1397.

Pries-Heje et al. (2008). Strategies for design science research evaluation. In *Conference proceedings, 16th european conference on information systems.*

Puaar et al. (2018). Impact of an inpatient electronic prescribing system on prescribing error causation: a qualitative evaluation in an english hospital. *BMJ quality & safety*, *27*(7), 529–538.

Qi et al. (2017). Advanced internet of things for personalised healthcare systems: A survey. *Pervasive and Mobile Computing*, *41*, 132–149.

Queille et al. (1982). Specification and verification of concurrent systems in cesar. In *International symposium on programming* (pp. 337–351).

Rabah. (2017). Challenges & opportunities for blockchain powered healthcare systems: A review. *Mara Research Journal of Medicine & Health Sciences-ISSN 2523-5680*, *1*(1), 45–52.

Raghupathi et al. (2014). Big data analytics in healthcare: promise and potential. *Health information science and systems*, *2*(1), 3.

Rahimzadeh et al. (2017). Svc-tchain: Incentivizing good behavior in layered p2p video streaming. In *Ieee infocom 2017-ieee conference on computer communications* (pp. 1–9).

Rahiri et al. (2018). Systematic review of disparities in surgical care for māori in New Zealand. *ANZ journal of surgery*, *88*(7-8), 683–689.

Rahman et al. (2019, July). A novel architecture for tamper proof electronic health record management system using blockchain wrapper. In *Proceedings of the 2019 acm international symposium on blockchain and secure critical infrastructure* (pp. 97–105). ACM. doi: 10.1145/3327960.3332392

Rebiere et al. (2017). Fighting falsified medicines: The analytical approach. *Journal of pharmaceutical and biomedical analysis*, *142*, 286-306.

Reid et al. (2005). *Building a better delivery system: a new engineering/health care partnership* (Vol. 15). National Academies Press Washington, DC.

Rezaeibagha et al. (2015). A systematic literature review on security and privacy of electronic health record systems: technical perspectives. *Health Information Management Journal*, *44*(3), 23–38.

Richardson et al. (2016). Modifiable lifestyle factors that could reduce the incidence of colorectal cancer in New Zealand. *Ann Richardson*, *129*(1447).

Robb et al. (2017). Medication-related patient harm in new zealand hospitals. *The New Zealand Medical Journal (Online)*, *130*(1460), 21.

Roehrs et al. (2017). Omniphr: A distributed architecture model to integrate personal health records. *Journal of biomedical informatics*, *71*, 70–81.

Rohr et al. (2018). Blockchain-based token sales, initial coin offerings, and the democratization of public capital markets. *Hastings LJ*, *70*, 463.

Ropsten testnet explorer. (2021). Ethereum. Retrieved 4 July, 2021, from `https://ropsten.etherscan.io/`

Ryks et al. (2019). The health and wellbeing of urban Māori in Aotearoa New Zealand. *Handbook of Global Urban Health*, 283.

Saad et al. (2020). Comparative review of the blockchain consensus algorithm between proof of stake (pos) and delegated proof of stake (dpos). *International Journal of Innovative Computing*, *10*(2).

Sadiku et al. (2018). Blockchain technology in healthcare. *IJASRE*, *4*, 154–159.

Sadouskaya. (2017). Adoption of blockchain technologyin supply chain and logistics.

Safety Commission NewZealand, H. Q. (2017). *A window on the quality of New Zealand's health care 2017.* Wellington. Retrieved 04 Sep 2019, from `https://www.hqsc.govt.nz/contact-us/`

Saleem et al. (2005). Exploring barriers and facilitators to the use of computerized clinical reminders. *Journal of the American Medical Informatics Association*, *12*(4), 438–447.

Salem et al. (2019). Internet of things solution for non-invasive vital data acquisition: a step towards smart healthcare system. In *Sustainable design and manufacturing 2019: Proceedings of the 6th international conference on sustainable design and manufacturing (kes-sdm 19)* (pp. 387–397).

Sands. (2004). *Help for physicians contemplating use of e-mail with patients.* BMJ Group BMA House, Tavistock Square, London, WC1H 9JR.

Schatz et al. (2017). Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law*, *12*(2), 8.

Schiff et al. (2009). Diagnostic error in medicine: analysis of 583 physician-reported errors. *Archives of internal medicine*, *169*(20), 1881–1887.

Schmidt et al. (2019). The danish health care system and epidemiological research: from health care contacts to database records. *Clinical epidemiology*, 563–591.

Shae et al. (2017). On the design of a blockchain platform for clinical trial and precision medicine. In *2017 ieee 37th international conference on distributed computing systems (icdcs)* (pp. 1972–1980). Atlanta, Georgia, USA.

Sharma et al. (2006). Electronic healthcare: issues and challenges. *International journal of electronic healthcare*, *2*(1), 50–65.

Sharma et al. (2018). Blockchain based hybrid network architecture for the smart city. *Future Generation Computer Systems*, *86*, 650–655.

Sharples et al. (2016). The blockchain and kudos: A distributed system for educational record, reputation and reward. In *European conference on technology enhanced learning* (pp. 490–496). Lyon, France.

Sheridan et al. (2011). Health equity in the new zealand health care system: a national survey. *International Journal for Equity in Health*, *10*(1), 1–14.

Shortliffe et al. (2000). Networking health: Prescriptions for the internet. *Computer Science and Telecommunications Board, The National Academies. Washington, DC: The National Academies Press.*

Singh et al. (2013). Types and origins of diagnostic errors in primary care settings. *JAMA internal medicine*, *173*(6), 418–425.

Sinha et al. (2009). Large datasets in biomedicine: a discussion of salient analytic issues. *Journal of the American Medical Informatics Association*, *16*(6), 759–767.

Stephen. (2000). *Disability and the digital divide. disability statistics abstract number 22.* ERIC.

Steyn et al. (2021). Māori and pacific people in new zealand have higher risk of hospitalisation for covid-19. *medRxiv*, 2020–12.

Sujansky et al. (2010). A method to implement fine-grained access control for personal health records through standard relational database queries. *Journal of biomedical informatics*, *43*(5), S46–S50.

Sylim et al. (2018). Blockchain technology for detecting falsified and substandard drugs in distribution: Pharmaceutical supply chain intervention. *JMIR research protocols*, *7*(9).

Taichman et al. (2016). *Sharing clinical trial data—a proposal from the international committee of medical journal editors.* Mass Medical Soc.

Tavva et al. (2011). Medication errors: A prospective study conducted and reported through prescription monitoring in tertiary care teaching hospital. *Archives of Pharmacy Practice*, *2*(1), 33.

Terry et al. (2000). Structural and legal implications of e-health. *Journal of health law*, *33*(4), 605–614.

Theodore et al. (2019). How a lifecourse approach can promote long-term health and wellbeing outcomes for Māori. *Journal of Indigenous Wellbeing*, *4*(1), 15-25.

Theunissen, E. (2011). The nurse's role in improving health disparities experienced by the indigenous Māori of New Zealand. *Contemporary nurse*, *39*(2), 281–286.

Tim et al. (2013). *Improving global health governance to combat counterfeit medicines: a proposal for a unodc-who-interpol trilateral mechanism* [Internet web Page]. BMC medicine. Retrieved 08 may 2018, from `https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4225602/pdf/1741-7015-11-233.pdf`

Tompkins. (2017). Social capital and its application to Māori social policy. *Aotearoa New Zealand Social Work*, *27*(4), 16–24.

Tran et al. (2019). Pharmacist-assisted electronic prescribing at the time of admission to an inpatient orthopaedic unit and its impact on medication errors: a pre-and postintervention study. *Therapeutic Advances in Drug Safety*, *10*.

Trochim. (2006). Philosophy of research. *Research Methods Knowledge Base*.

Tsai et al. (2016). Metaheuristic algorithms for healthcare: open issues and challenges. *Computers & Electrical Engineering*, *53*, 421–434.

Tseng et al. (2018). Governance on the drug supply chain via gcoin blockchain. *International journal of environmental research and public health*, *15*(6), 1055.

Tupai, F. e. a. (2018). Pasifika youth empowerment programme: a potential public health approach in tackling obesity-health related issues. *AlterNative: An International Journal of Indigenous Peoples*, *14*(1), 63–72.

UN. (2014). *Outcome document of the high-level plenary meeting of the general assembly known as the world conference on indigenous peoples.* https://digitallibrary.un.org/record/780897?ln=en.

Vasin. (2014). *Blackcoin's proof-of-stake protocol v2* [Internet Web Page]. Blockchain.co. Retrieved 04 dec 2018, from `https://blackcoin.co/blackcoin-pos-protocolv2-whitepaper.pdf`

Venable. (2006). A framework for design science research activities. In *Emerging trends and challenges in information technology management: Proceedings of the 2006 information resource management association conference* (pp. 184–187).

Venable et al. (2012). A comprehensive framework for evaluation in design science research. In *International conference on design science research in information systems* (pp. 423–438).

Viceconti et al. (2015). Big data, big knowledge: big data for personalized healthcare. *IEEE J. Biomedical and Health Informatics*, *19*(4), 1209–1215.

Victor et al. (2019). Measuring ethereum-based erc20 token networks. In *Financial cryptography and data security: 23rd international conference, fc 2019, frigate bay, st. kitts and nevis, february 18–22, 2019, revised selected papers 23* (pp. 113–129).

Vimercati, D. et al. (2007). Access control policies and languages in open environments. In *Secure data management in decentralized systems* (pp. 21–58). Springer.

Wall, T. (2019, March). *The addict at the centre of a fraudulent prescription scandal says pharmacists were incredibly lax.* stuff.co.nz. Retrieved 01 Nov 2019, from `https://bit.ly/2YaDfyW`

Walls et al. (2004). Assessing information system design theory in perspective: how useful was our 1992 initial rendition? *Journal of Information Technology Theory and Application (JITTA)*, *6*(2), 6.

Wang et al. (2016). An incentive mechanism with privacy protection in mobile crowdsourcing systems. *Computer Networks*, *102*, 157–171.

Wang et al. (2019). A survey on consensus mechanisms and mining strategy management in blockchain networks. *IEEE Access*, *7*, 22328–22370.

Warren. (2016). Strengthening research through data sharing. *New England Journal of Medicine*, *375*(5), 401–403.

Webster et al. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS quarterly*, xiii–xxiii.

Who. (2013). *Report of the situation of counterfeit medicines based on data collection tool who regions for africa and eastern mediterranean* [Internet web Page]. World Health Organization. Retrieved 08 may 2018, from `http://apps.who.int/medicinedocs/documents/s18385en/s18385en.pdf`

WHO. (2017). *A study on the public health and socioeconomic impact of substandard and falsified medical products* [Internet web Page]. World health Organization. Retrieved 08 may 2018, from `https://bit.ly/3aFMZ6V`

Who. (2017). *Who global surveillance and monitoring system for substandard and falsified medical products* [Internet web Page]. World health Organization. Retrieved 08 may 2018, from `https://bit.ly/35242PH`

Wieringa et al. (2012). Technical action research as a validation method in information systems design science. In *International conference on design science research in information systems* (pp. 220–238).

Winthereik et al. (2005). Ict and integrated care: some dilemmas of standardising inter-organisational communication. *Computer Supported Cooperative Work (CSCW)*, *14*(1), 43–67.

Wittich et al. (2014). Medication errors: an overview for clinicians. In *Mayo clinic proceedings* (Vol. 89, pp. 1116–1125).

Wood. (2014). *Ethereum: A secure decentralised generalised transaction ledger* [Internet Web Page]. Retrieved 04 dec 2018, from `http://gavwood.com/paper.pdf`

Wu et al. (2017). An efficient and secure identity-based authentication and key agreement protocol with user anonymity for mobile devices. *Wireless Personal Communications*, *94*(4), 3371–3387.

Wüst, K. & Gervais, A. (2018). Do you need a blockchain? In *2018 crypto valley conference on blockchain technology (cvcbt)* (pp. 45–54).

Xia et al. (2017a). Bbds: Blockchain-based data sharing for electronic medical records in cloud environments. *Information*, *8*(2), 44.

Xia et al. (2017b). Medshare: Trust-less medical data sharing among cloud service providers via blockchain. *IEEE Access*, *5*, 14757–14767.

Yang et al. (2015). A hybrid solution for privacy preserving medical data sharing in the cloud environment. *Future Generation Computer Systems*, *43*, 74–86.

Yang et al. (2021). Therapeutic errors captured by the new zealand national poisons centre: a retrospective audit. *Journal of Primary Health Care*, *13*(1), 63–69.

Yanwei et al. (2019). Efficient chosen-ciphertext secure hybrid encryption scheme tolerating continuous leakage attacks. *Journal of the Chinese Institute of Engineers*, *42*(1), 39–47. doi: 10.1080/02533839.2018.1547663

Yin et al. (2015). Big data for modern industry: challenges and trends [point of view]. *Proceedings of the IEEE*, *103*(2), 143–146.

Yue et al. (2016). Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. *Journal of medical systems*, *40*(10), 218.

Zareen et al. (2021). Blockchain and ipfs based service model for the internet of things. In *Complex, intelligent and software intensive systems: Proceedings of the 15th international conference on complex, intelligent and software intensive systems (cisis-2021)* (pp. 259–270).

Zawaly et al. (2019). Diagnostic accuracy of a global cognitive screen for M[aori and non-Māori octogenarians. *Alzheimer's & Dementia: Translational Research & Clinical Interventions*, *5*, 542–552.

Zhang et al. (2010). Security models and requirements for healthcare application clouds. In *Cloud computing (cloud), 2010 ieee 3rd international conference on* (pp. 268–275).

Zhang et al. (2015). An iot electric business model based on the protocol of bitcoin. In *Intelligence in next generation networks (icin), 2015 18th international conference on* (pp. 184–191). Paris, France.

Zhang et al. (2016a). Incentive mechanism for proximity-based mobile crowd service systems. In *Ieee infocom 2016-the 35th annual ieee international conference on computer communications* (pp. 1–9).

Zhang et al. (2016b). A secure system for pervasive social network-based healthcare. *IEEE Access*, *4*, 9239–9250.

Zhang et al. (2016c). Town crier: An authenticated data feed for smart contracts. In *Proceedings of the 2016 acm sigsac conference on computer and communications security* (pp. 270–282).

Zhang et al. (2017a). Applying software patterns to address interoperability in blockchain-based healthcare apps. *CoRR ArXiv*. Retrieved from `https://arxiv.org/abs/1706.03700`

Zhang et al. (2017b). Metrics for assessing blockchain-based healthcare decentralized apps. In *e-health networking, applications and services (healthcom), 2017 ieee 19th international conference on* (pp. 1–4). Dalian, China. doi: 10.1109/HealthCom.2017.8210842

Zhang et al. (2018a). FHIRchain: applying blockchain to securely and scalably share clinical data. *Computational and structural biotechnology journal*, *16*, 267–278.

Zhang et al. (2018b). Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. *Journal of medical systems*, *42*(8), 140.

Zhao et al. (2017). Lightweight backup and efficient recovery scheme for health blockchain keys. In *Autonomous decentralized systems (isads), 2017 ieee 13th international symposium on* (pp. 229–234). Bangkok, Thailand.

Zhao et al. (2018). Efficient key management scheme for health blockchain. *CAAI Transactions on Intelligence Technology*, *3*(2), 114–118.

Zheng et al. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In *Big data (bigdata congress), 2017 ieee international congress on* (pp. 557–564). Honolulu, HI, USA. doi: 10.1109/BigDataCongress.2017.85

Zheng et al. (2018). Blockchain-based personal health data sharing system using cloud storage. In *2018 ieee 20th international conference on e-health networking, applications and services (healthcom)* (pp. 1–6).

Zhong et al. (2003). Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks. In *Ieee infocom 2003. twenty-second annual joint conference of the ieee computer and communications societies (ieee cat. no. 03ch37428)* (Vol. 3, pp. 1987–1997).

Zhou et al. (2018). Mistore: a blockchain-based medical insurance storage system. *Journal of medical systems*, *42*(8), 149.

Zhu et al. (2008). A secure incentive scheme for delay tolerant networks. In *2008 third international conference on communications and networking in china* (pp. 23–28).

Zhuang et al. (2018). Applying blockchain technology for health information exchange and persistent monitoring for clinical trials. In *Amia annual symposium proceedings* (Vol. 2018, p. 1167).

Zyskind et al. (2015). Decentralizing privacy: Using blockchain to protect personal data. In *Security and privacy workshops (SPW), 2015 ieee* (pp. 180–184). San Jose, CA, USA.

Appendix A

Additional information here

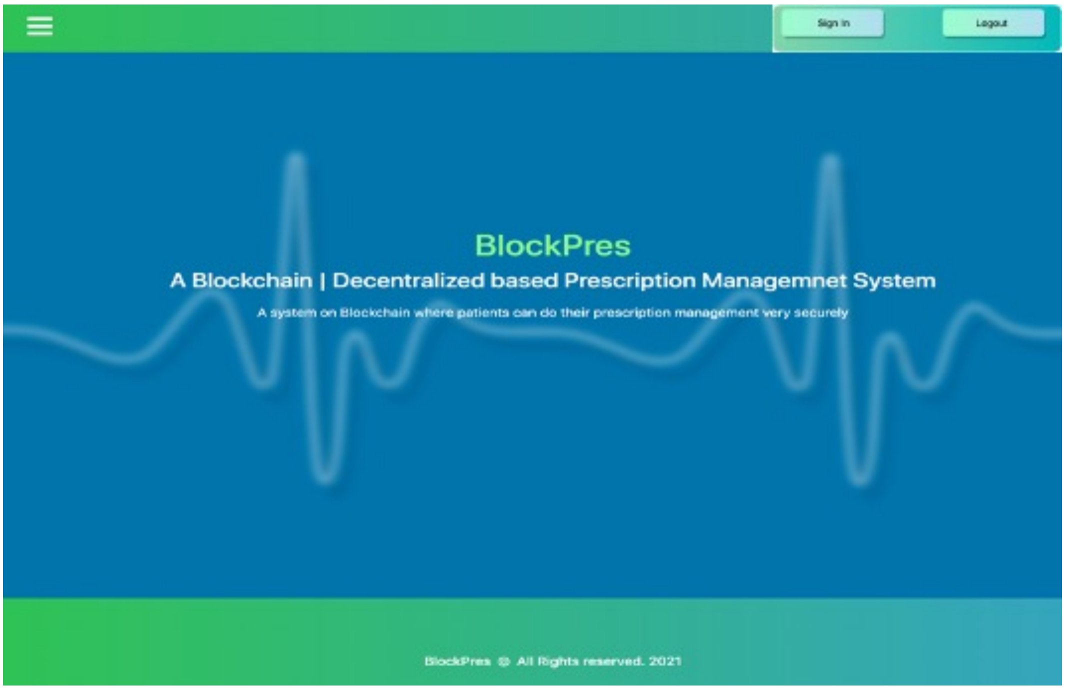
A.1 Introduction

This section presents BlockPres prototype developed based on framework and incentive mechanism. The prototype is evaluated in chapter 7. Below are presentation of the proposed BlockPres Artifact .

A.1.1 Prototype

Decentralised Application (Dapp) is developed based on the framework proposed in Chapter 5. The web browser is built with react.js. The DApp interacts with the smart contract by using the Ethereum network via a javascript API called Web3.js. The web browser push files by interacting with the IPFS network. The IPFS stores the files in the .txt file in the Dapp, uploaded by the medical entity with patients' permission. Figure A.1 and Figure A.2 presents the sign-in form where medical entities can login and use the system. The sign-up is not included as MOH and HealthNz can do this to register entities. Figure A.3 shows patients registration log; a healthcare provider can do this to enroll patients and provide the public and private keys. The receptionist forwards patients to a concerned doctor, and Figure A.4 where the doctor login and analyses the patient's condition and prescribe a prescription if it is a new patient. If the patients have a medical history, the doctor will request the concerned healthcare provider to access or share patients' records. The doctor then uploads the prescription to IPFS and store the file hash on the blockchain network. Also, send a prescription to the pharmacy. The doctor can see the patient record, patients address, timestamp, and IPFS link as shows in Figure A.5.

The Figure A.7 shows that the pharmacy login page where the pharmacy can see patients' prescription records and can send a permission request to patients and doctors. In Figure A.8,pharmacy sends permission request to patients and patients can login or scan QR code to give permission to pharmacy in Figure A.6. The patients can scan QR codes or log in to permit the pharmacy.



BlockPres

A Blockchain | Decentralized based Prescription Managemnet System

A system on Blockchain where patients can do their prescription management very securely

BlockPres © All Rights reserved. 2021

Figure A.1: BlockPres API

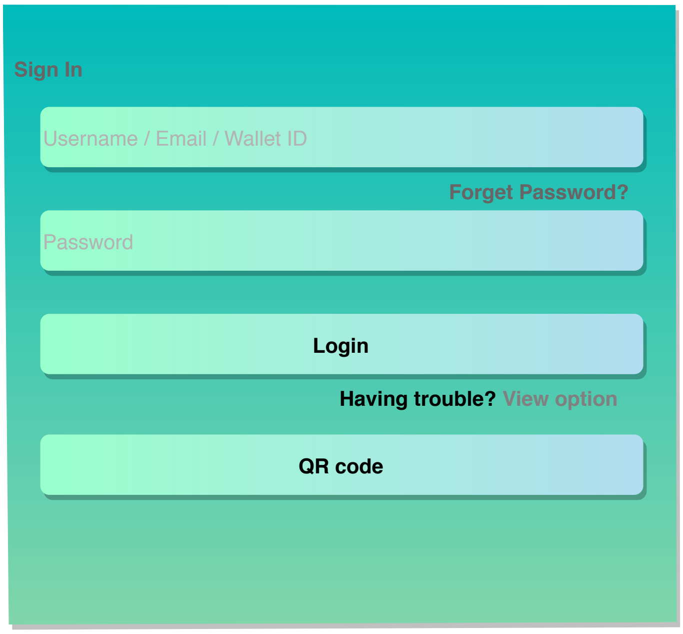


Figure A.2: Login Page

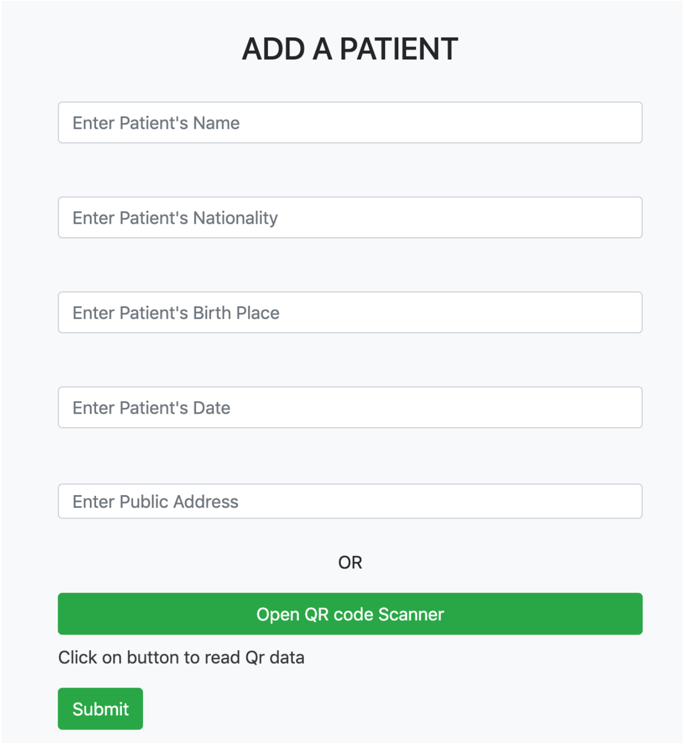
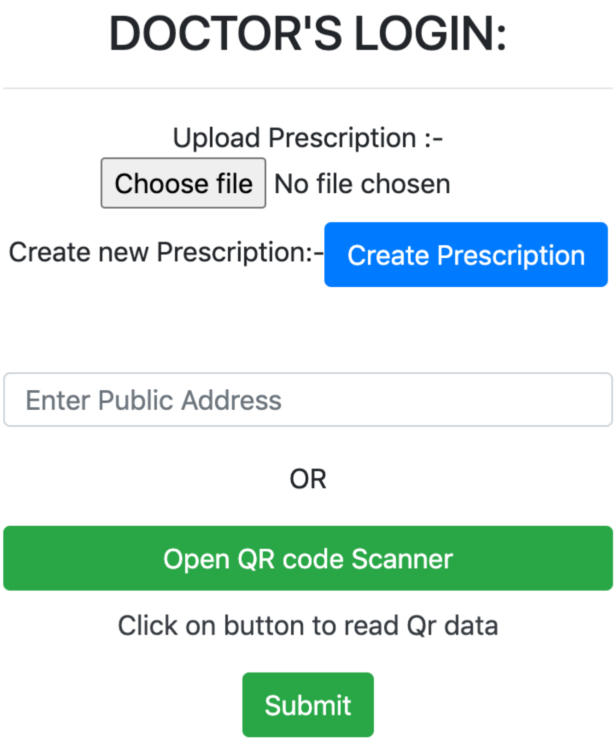


Figure A.3: Patients Registration Page



DOCTOR'S LOGIN:

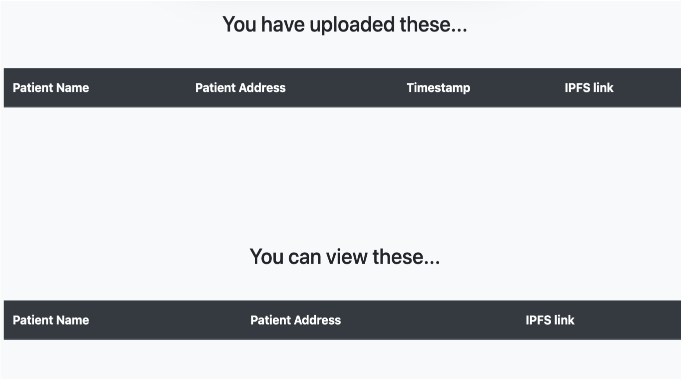
Upload Prescription :-

No file chosen

Create new Prescription:-

Click on button to read Qr data

Figure A.4: Doctor Login Page



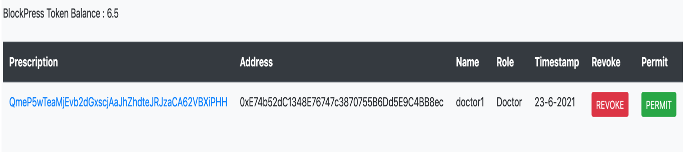
You have uploaded these...

Patient Name	Patient Address	Timestamp	IPFS link

You can view these...

Patient Name	Patient Address	IPFS link

Figure A.5: Information Log



BlockPress Token Balance : 6.5

Prescription	Address	Name	Role	Timestamp	Revoke	Permit
QmeP5wTeaMjEvb2dGxscjAaJhZhdteJRJzaCA62VBXiPHH	0xE74b52dC1348E76747c3870755B6Dd5E9C4BB8ec	doctor1	Doctor	23-6-2021	REVOKE	PERMIT

Figure A.6: Patients Permit and Revoke Permission

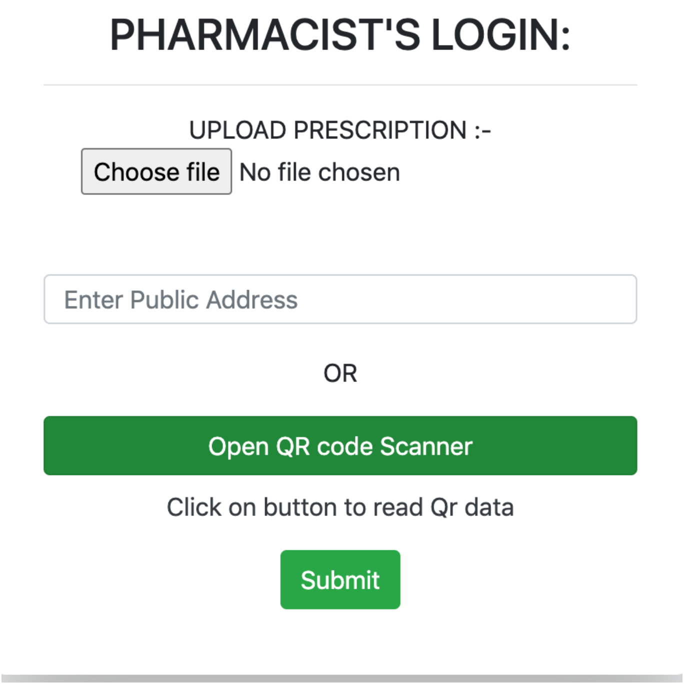


Figure A.7: Pharmacy Login Page

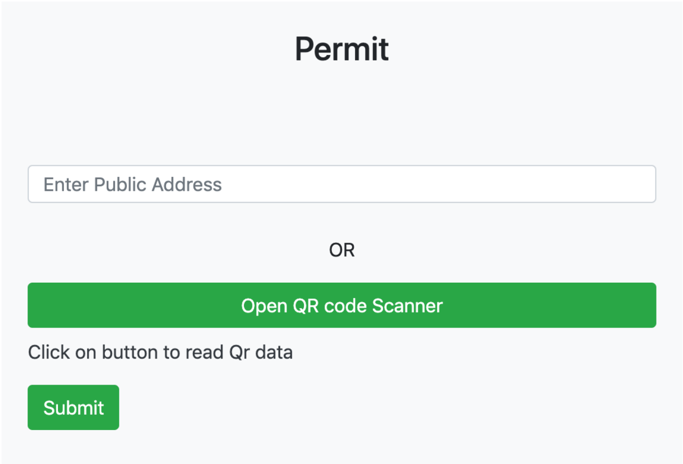


Figure A.8: Doctor and Pharmacy send Permission to patients Page