Privacy-aware efficient blockchain-based registration and verification system for vaccinated patients

V Tshipuke

orcid.org/0000-0003-2250-972

4

Dissertation accepted in fulfilment of the requirements for the degree Master of Computer Science at the

North West University

Supervisor: Prof Bassey Isong

Co-Supervisor: Mr Koketso Ntshabele

Co-Supervisor: Prof. Adnan Abu-Mahfouz (CSIR)

Graduation ceremony: May 2023

Student number: 34327320

Declaration

I, **Tshipuke V**, declare that "**Privacy-aware blockchain-based registration and verification system for vaccinated patients**" is my work which has never been presented for the award of any degree in any university. All sources of information used in this research have been deservedly acknowledged in the texts and references.

Signature: _______ _________________ Date: __23/01/23____________________

APPROVAL

Supervisor: **Prof Bassey Isong**
Department of Computer Science
Faculty of Natural and Agricultural Science
North-West University
South Africa

Signature: ________________________ Date: ________________________

Co-Supervisor: **Mr Koketso Ntshabele**
Department of Computer Science
Faculty of Natural and Agricultural Science
North-West University
South Africa

Co-Supervisor: **Prof. Adnan Abu-Mafhouz**
CSIR
Emerging Digital Technologies for 4IR (EDT4IR)
Pretoria, South Africa

Dedication

I dedicate this research work to my late father Pastor Tshipuke AR, for his contributions and encouragement towards me. His sacrifice was not in vain it yielded fruit. Thanking him so much. May his soul continue to rest in perfect peace.

Acknowledgement

First and foremost, I would like to thank my heavenly father for giving me wisdom and understanding. If it was not for God, I would not have made it but through His Spirit, He guided me until I completed my study.

Special thanks to my supervisor, Prof. Bassey Isong and my co-supervisors Mr Koketso Ntshabele along with Prof. Adnan Abu-Mahfouz (CSIR) for their tireless efforts and guidance towards the completion of this study.

I further want to acknowledge my family and fiancé for the sacrifices and support they gave me during this study, your encouragement during hard times helped me a lot.

Special gratitude goes to my mentors Apostle Nelson Msowoya and Pastor Tabitha Msowoya, thank you very much for your prayers and spiritual support you gave me, May God continue to use you.

I would also like to thank all the lecturers in the department of computer science for all their support and guidance, Thank you all.

Lastly, I would like to thank my sponsor CSIR for the financial support they gave me during the study, without your support it was not going to be easy, I greatly appreciate you.

Abstract

Healthcare systems are known to process large quantities of medical data almost daily, thereby increasing the risk of data being manipulated, stolen, or counterfeited. However, the global pandemic outbreak as a result of the Covid-19 virus has illuminated some of the present healthcare systems' limitations in responding to emergencies involving public health. With many governments rolling out vaccines and issuing vaccination-proof certificates globally, there has been an increase in counterfeit certification from unauthorized parties, making registering and verifying difficult. Therefore, this research study conducted a comprehensive literature review and employed the design science research methodology to design and develop an approach as a viable solution. A privacy-aware, secure vaccination management system was proposed to address the current challenge. The system utilizes blockchain smart contracts to save the details of the patient. Moreover, the stored data is encrypted using symmetric encryption, and the proposed system allows verification of the certificate using a quick response code.

Furthermore, we implemented the same system and integrated it with the traditional relational database to compare the effectiveness of the system running on it and the blockchain environments. Apache JMeter and Hyperledger Caliper were used to carry out a series of simulations to measure the performance and effectiveness of the solution. Evaluation parameters such as throughput, latency, response time, and the average time per transaction were used to assess the blockchain-based system's performance. The results indicate that the average response time was 132.24 ms, the throughput recorded 379.89 ms, the average latency recorded 204.60 ms, and the average time of transactions recorded was 10-12 seconds for 1000 transactions. Moreover, when comparing blockchain-based systems against the traditional database system, the results show that the traditional database is efficient in processing transactions but lacks data privacy and security strengths. In conclusion, this study strongly recommends integrating blockchain technology with the healthcare system to enhance the privacy and security of data being handled by healthcare systems and critical information systems.

Keywords: *Privacy, Security, Covid-19, Patient, Healthcare systems, Smart contract, QR code, Vaccination.*

Table of Contents

List of Figures

List of Tables

Definition of Concepts

Blockchain technology: is a distributed, unchangeable ledger that simplifies the recording of transactions and tracking of assets in a corporate network [1].

Internet of things: is the connectivity of computing devices embedded in ordinary items that allow them to send and receive data [2].

Nodes: A connection point capable of receiving, creating, storing, or transmitting data across dispersed network routes [3]

Smart Contracts: Computer protocols or if-and-then statements that are recorded in a blockchain and are performed when all of the predefined criteria are satisfied [4].

Healthcare: is the practice of preventing, diagnosing, treating, recovering from, or curing diseases, illnesses, injuries, and other types of physical and mental impairments in humans to maintain or improve their state of health [5].

Vaccination: the injection of a vaccine to assist the immune system in developing disease resistance [6].

Vaccine: is a biological molecule meant to protect people against pathogenic organisms[6].

Covid-19: An infectious disease caused by the SARS-CoV-2 virus [6].

Immunity passport: a document, whether physical or digital, attesting to the bearer's level of immunity to a dangerous disease [7].

Patients: any person who receives healthcare services from healthcare professionals [8].

System: a group of pieces that work together to form a single entity by adhering to a predetermined set of guidelines and interacting with one another [9].

Security: this is when a computer network is safeguarded from theft, damage to hardware and software, and interruption caused by unauthorized users, such as hackers[10].

Analysis: is defined as the process of extensively reading material to grasp it and provide accurate information and facts [11]**.**

Privacy: The concealing of information about an individual or group, or the capacity to control its disclosure [12].

Data: It is described as anything that provides statistics and facts; often, data are not organised in structured patterns [13].

Efficiency: The ratio of resources used (health inputs) to a certain measure of the valued health system outputs they generate [14]**.**

List of Acronyms

API:	Application Programming Interface
APP:	Application
ASE:	Advanced Standard Encryption
BT:	Blockchain Technology
BW:	Block Withholding
CSS:	Cascading Style Sheet
CSP:	Cloud Service Provider
Dapps:	Decentralized Applications
DFS:	Distributed File Storage
DoS:	Denial of Service
DSA:	Digital Signature Algorithm
ECC:	Elliptic Curve Cryptography
EdDSA:	Edwards-curve digital Signature Algorithm
EHR:	Electronic Health Record
EMR:	Electronic Medical Record
FAW:	Fork after withholding
FR:	Functional Requirements
ID:	Identity
IoMT:	Internet of Medical Things
IoT:	Internet of Things
IPFS:	InterPlanetary File System
LMDS:	Lambard Merkle Digital Signature
LMDSG:	Lamport Modified Digital Signature

NFR:	Non-Functional Requirements
OPD:	Outpatient Department
ORM:	Object Relational Mapping
P2P:	Peer to Peer
PBFT:	Practical Byzantine Fault Tolerance
PoA:	Proof of Authority
PoS:	Proof of Stake
PoW:	Proof of Work
QR:	Quick Response
RPM:	Remote Patient Monitoring
RSA:	Rivest–Shamir–Adleman
URL:	Uniform Resource Locator
VMS:	Vaccination Management System

Chapter 1

Introduction and Background

1.1 Chapter Outline

A brief overview of the research is presented in this chapter. The chapter discusses the research problem statement, underlying reasons as well as the objective and aims of the study. It also presents the research questions, outlines the contribution of this research, an overview of approaches for investigation and the organization of the overall dissertation.

1.2 Introduction

In many developing countries, patients are not finding it easy to get access to primary physicians or other caregivers as a result of the huge rise in the number of people seeking medical attention [15]. On the other hand, the healthcare sector has shown signs of improvement, and it is becoming more efficient as a result of the development of cutting-edge technologies such as the Internet of Things (IoT), which is enabled by wearable devices, sensors, blockchain and cloud computing, to name but a few. These technologies are helping the sector become more effective. Applications for these technologies include sickness prediction, pharmaceutical traceability, electronic medical records management, patient tracking, remote patient monitoring, and the fight against infectious illnesses like the Covid-19 epidemic [16], [17]. Not only has IoT improved the health sector, but it has also been implemented in various domains such as homes, transportation, agriculture, cities, telecommunication, traffic and so on [18]. Furthermore, the development of these technologies has made the majority of healthcare providers migrate from using conventional health systems to eHealth to change how information is governed and handled [19].

However, with multiple solutions offered by IoT and its integration into healthcare systems, current architectures are still failing to support the demand required by the growing data [20]. This is because current systems are based on a client-to-server architecture which relies on databases to store patient health details [21]. Healthcare systems are known to process large quantities of data every day thus, increasing the chances of exposure, manipulation and theft, furthermore, centralized systems require certain levels of trust [22]. Moreover, in developing countries such as South Africa, technology adoption is slow as they still rely on these centralized database-oriented traditional systems and these traditional systems are faced with several growing issues for example single-point failure, and denial of service and mostly rely on third parties to handle the patients' information, thereby rendering medical data less secure [17], [23]. The unanticipated outbreak of the pandemic known as Covid-19 has brought to light some of the limitations of the present healthcare system in its ability to respond to emergencies involving public health [24]. The first instance of Covid-19 was recorded in December 2019, and ever since then, the healthcare industry has been under pressure because of the increased demand for its services [25]. People from all around the globe are working diligently to discover the most effective solution to the problems presented by the Covid-19 epidemic, such as creating and testing vaccines, decreasing disease transmission, and promptly identifying viral carriers since coronavirus is highly infectious [24], [25]. This also accelerated the development of various technologies to assist with managing the outbreak of the virus, these include patient tracking applications, symptom identification and remote monitoring applications [26].

Taking into consideration such events, blockchain could be a solution in the health domain since it has demonstrated the ability to improve clinical trial data management by, among other things, reducing regulatory clearance delays and simplifying communication between multiple supply chain participants [23]. Furthermore, throughout the epidemic, the transmission of disinformation has grown dramatically, and existing platforms are unable to validate data, resulting in public fear and irrational behaviour. As a consequence of this, the development of a tracking system based on blockchain technology is essential if one is to ensure the dependability and reliability of information obtained by the general public and governmental entities [27], [20]. Other technologies such as Rivest-Shamir-Adleman(RSA), Advanced Encryption Standard (AES) and SHA-256 have been widely employed to improve healthcare data privacy and security in the past[28]. However, blockchain has shown to be more useful in healthcare as it enables the secured sharing of sensitive patient data among authorized parties while maintaining patient privacy and control over their data[29]. In its most basic form, a blockchain is an anonymous, append-only, distributed, and time-stamped data structure. It permits the formation of a decentralized peer-to-peer network which eliminates the requirement for a trusted authority and enables individuals who do not trust one another to interact with one another in a verifiable manner [30], [31]. Since new blocks may only be attached to the very last link in the chain, the blockchain provides immutable data storage (past transactions cannot be changed or erased). As a result, several blockchain-based solutions enable the safe transfer of digital assets among untrustworthy clients [32].

Blockchain technology is an exciting new technology that can change many businesses and peoples' way of life and, aside from cryptocurrency, it has the potential to assist numerous sectors to reduce inefficiency and surmount bottlenecks. For example, blockchain technology may accelerate the settlement of transactions, lower expenses, give transparency, editability, efficiency, income, and security and minimize transaction costs [33]. Since one of the super spreaders of Covid-19 is being in close contact with an infected patient many countries including South Africa are seeking ways to avoid the tight physical separation procedures required to limit the spread of serious diseases. Some countries, including the United States, Chile, Italy, the United Kingdom, and Germany, have advocated the usage of immunity passports, which are papers, either physical or digital, that verify whether a person has the Covid-19 virus or is reportedly resistant to it [34]. People possessing immunity passports may be released from physical constraints and permitted to return to work, education, and daily life. Immunity passports, on the other hand, pose serious scientific, practical, equitable, and legal issues [34], [35]

Given the current state of the healthcare sector in the sub-Saharan regions, for example, South Africa, it is worth investigating alternative technologies which will be efficient, secure and transparent while also limiting fraudulent and counterfeit vaccination proofs. Therefore, this study is focused on proposing and implementing a blockchain-based vaccination registration and verification system. Due to the characteristics offered by blockchain technology, an efficient verification system can be achieved.

1.3 Problem Statement

Due to the ongoing pandemic stemming from Covid-19 [16], several nations such as South Africa have proposed or developed different strategies to prevent or contain the widespread airborne diseases. The strategies include self-isolation, contact distancing and quarantine for people who were showing up mild symptoms [7]. Accordingly, many covid-19 mobile applications were developed and extensively publicized to help with the tackling of the virus during the first wave. These systems were mostly quarantine apps, contact tracing apps, symptom monitoring apps and information-providing apps that alerted users who came into physical contact with an infected person(s) [7]. However, these apps are not effective in achieving their goals. As such, the medical industry needs new technologies that will assist in the monitoring and controlling of the virus spread. Thus, data that is accurate and trustworthy is vital. But the currently used technology or apps lack a source of trustable and accurate data that may help to provide correct information about Covid-19 [36]. In addition, clinical laboratories and general hospitals can give information on patients affected by the Covid-19 epidemic, but the data may be false and erroneous since they are not managed, maintained or obtained following defined criteria [17],[37]. As several countries issue vaccines and develop vaccination-proof certificates to curb the menace, there is a pressing need to develop cost-effective systems to deliver and deploy vaccination certificates [7], [38]. Security and privacy in these systems must be the priority which most of the currently implemented systems did not focus on[35]. Moreover, medical data must be handled in a trustworthy and secure environment. As proof of vaccination is required in almost every travel destination to show that indeed the vaccine has been administered, there have been several counterfeit certificates and fraudulent claims of the vaccine having been administered [39], [40].

Given the stated challenges, this research proposes the development and deployment of a blockchain-based system to register and verify vaccinated patients via a quick response (QR) code-based application. This solution idea is not only limited to vaccination but also may be applicable in other areas such as voters' registration, transmission and storage of election results, Home Affairs records, etc.

1.4 Research Motivation

In South Africa, despite the growing technologies, there is still a slow rate of the adoption of new technologies which can help in healthcare. Most healthcare centres are still utilizing traditional paper-based methods to capture and manage medical records. During the vaccination period, after the patient was vaccinated paper-based proof was offered as a confirmation. However, this strategy is time-consuming since it requires a third party who manually organises the medical data and this approach poses a threat to patients' data since confidentiality and privacy might be compromised at any time. Another problem is that it can be counterfeited, duplicated or faked so there is a need to develop a secure vaccination proof with certain security measures that can be used to prove the authenticity of the vaccination.

One of the ways that this airborne disease can be controlled is by spending less time in a contaminated area [41]. There is a need for an efficient system that will verify that indeed the patient has been vaccinated and will limit people standing in queues trying to get verified and thus will reduce the spread of the disease. The current system which is being used to manage and govern the issuing of vaccine-proof certificates is centralized, which means if one system encounters a fault it affects the rest. Therefore, the above gaps in development strengthen our determination to design and implement a blockchain-based system to register and verify vaccinated patients.

1.5 Research Questions

To address the stated research problem, the following research questions (RQs) would be answered:

RQ1: What is the state-of-the-art practice of registering and verifying vaccinated patients and what technologies are effective in transforming the healthcare system?

RQ2: How can an efficient and secure vaccination verification system be designed?

RQ3: How can we implement the designed system in RQ2 to evaluate its performance and effectiveness?

1.6 Research Aim and Objectives

1.6.1 Research Aim

This research aims to design and implement a privacy-aware blockchain-based system for registering and verifying vaccinated patients.

1.6.2 Research Objectives

To answer the above-stated RQs and meet the research aim, the following research objectives (ROs) will be addressed:

RO1: Investigating the current technology trends used in registering and verifying patients as well as carrying out comprehensive literature studies on blockchain effectiveness and applications in the healthcare sector.

RO2: Designing a registration and verification passports system based on blockchain technology while preserving confidentiality and privacy.

RO3: Implementing and evaluating the performance and effectiveness of the designed system.

1.7 Methods of Investigation

In the context of this research, to meet the objectives and obtain valid and trustworthy results, the design scientific research [42] methodology was adopted. Design scientific research is a methodical procedure that involves creating artefacts to address issues, evaluating what was developed or what is functioning, and communicating the outcomes of these evaluations [42]. In this methodology, the artefacts that are built or assessed are classed as constructs, models, methodologies and instantiations. Therefore their study may lead to an improvement in theories as a consequence of the artefacts [42]. The methodology allowed the design, implementation, and simulation of the proposed artefact. Moreover, in every research study, choosing a research method is an essential step as methods are useful in answering research questions. In this research study, qualitative and quantitative data collection and analysis approaches were used as the data obtained contained two facets of data. This study's research design served as a pattern for describing how the identified problem was handled by fulfilling the objectives. Chapter 3 discussed in detail the research methodology and design.

1.8 Research Contribution

The main contribution of this study to knowledge is to:

1) Provide state-of-the-art practice for registering and verifying vaccinated patients and blockchain technology applications.
2) Design and develop an efficient, authentic, secure and privacy-aware technique for registering and verifying vaccinated patients using blockchain technology.
3) It will also contribute as a forerunner to new avenues that can be explored in the pursuit of advancement in healthcare systems and other related sectors.

The research aims to help developers in the consideration of creating more systems that are decentralized rather than centralized.

1.9 Research Organization

This research study is categorized into the following chapters:

Chapter 1: Introduction – In the research introduction, the underlying issue is detailed in-depth to create a comprehensive image of the problem areas. This chapter highlights the aim and the questions that may be asked to establish goals that will assist in reaching the stated objective.

This chapter additionally elaborates on the research's scope and research output produced by the study.

Chapter 2: Literature review – Discusses in detail current healthcare system approaches, implementations and challenges. Furthermore, it describes blockchain technology, its integration with the healthcare system, its architecture, and the solutions it can bring to the health sector. Finally, the related works were also discussed in this chapter.

Chapter 3: Research methodology and design – In this chapter, the research methodology was presented as well as the research tools and methods used in the research study. Data collection and analysis approaches were also outlined in this chapter.

Chapter 4: System analysis and design – This chapter details the system that is being proposed. It describes the system design, system architecture, and requirements specifications including functional and non-functional requirements. It explains the way the system functions and details different functional features in the system.

Chapter 5: System implementation and results –The implementation and simulation of the proposed system were presented in this chapter. System operations and interfaces were also shown in this chapter. Furthermore, this chapter presented the simulation results, discussions, and comparisons with other systems.

Chapter 6: Summary, conclusion, and recommendations- This chapter presents the conclusions based on results obtained in Chapter 5 and gives recommendations on what can be done to improve the system and future work.

1.10 Research Outputs

During this research, a few research papers were produced as follows:

1. A review paper entitled "Analysis of IoT-Blockchain Technologies Integration into Healthcare Ecosystem" was produced and has been accepted for publication in the 2022 ICMECE Interdisciplinary Conference on Mechanics, Computers, and Electrics.

2. A journal paper entitled "Blockchain-based Vaccination Management System" is currently being drafted and completed for submission to any suitable NWU-accredited journal.

1.11 Chapter Summary

This chapter introduced the healthcare system problems and how blockchain technology might be used to find solutions to those difficulties. The research purpose, objectives and method of the investigation were all articulated. Additionally, the research motivation, as well as the research contribution to knowledge, is presented in this chapter.

Chapter 2

Literature Review

2.1 Introduction

The effect of ongoing COVID-19 pandemic has substantially impacted the health sector as well as other sectors such as the economy, education, transportation and politics. The increase in the number of cases daily has prompted different governments to come up with different strategies to manage the exponential spread of the disease. Some of the strategies include wearing facial masks, sanitizing your hands and keeping a social distance [43]. Moreover, as these countries rolled out vaccines, there was a need to register, store and verify the data of vaccinated patients. Existing systems cannot handle multifunctional and lifelong records, and currently, the world is facing a problem of counterfeit certification since there are a lot of unlicensed issuers and it makes it hard to manage the process. However, these obstacles can be overcome by incorporating blockchain technology into healthcare systems [44], [45].

The number of applications that may benefit from blockchain technology is constantly growing. This fact leads to the ever-increasing research attention on the creation of blockchain-based healthcare applications. In these studies, new technologies may be categorized based on their objectives, such as efficient delivery of health records, secure storage of data and sharing of medical information among healthcare institutions. These objectives aim to bring solutions to emerging issues in healthcare ecosystems. A blockchain consists of a list of records that cannot be changed and have timestamps. These records are maintained by a group of computers that are not under the control of a single organization. This idea is based on Bitcoin, a digital currency that was made in 2008 by an unidentified individual or organization using the alias Nakamoto. Blockchain is just an ever-expanding record of transactions called "blocks". These blocks are joined and protected using cryptographic standards to form a "chain," which is where the term "blockchain" comes from [46], [47].

The blockchain allows transactions to be confirmed by an untrustworthy collection of participants, which increases the security of the transaction. A decentralized ledger that does not allow for changes to be made is transparent, secure and auditable is provided by this technology. The blockchain is entirely viewable, enabling access to all transactions from the system's inception, and it can be validated and aggregated at any moment by any entity. When utilizing the blockchain system, data is organized into a chain of blocks, with each block containing a collection of Bitcoin transactions that occurs at a specific point in time. The blocks are connected by a reference to the block that came before them [16], [47], [48]. In this chapter, a comprehensive literature review was done on IoT, Healthcare systems and Blockchain technology.

2.1.1 Chapter Outline

The literature study of blockchain technology was discussed in this chapter. The aim was to incorporate blockchain technology into healthcare systems to ensure the privacy and security of healthcare records. Furthermore, it explains the challenges and benefits of the above-mentioned technology and related works. The chapter begins with a brief introduction and lastly discusses the general overview of Blockchain technology as used in the healthcare domain.

2.2 State of the Healthcare System

In developing countries, health care is mostly based on what the patient's health was like in the past. So, information about a person's health history is a crucial part of giving good service. Existing healthcare systems, on the contrary, have a lot of problems with security, privacy, efficiency and the sharing of information between different healthcare groups which makes it hard to trust and use the data [49]. This section discusses the existing healthcare systems, their operations, approaches and their drawbacks.

2.2.1 Existing Health Care Systems Approaches

2.2.1.1 Paper-based approach

Technology has changed different aspects of life including the health sector, security, user experience and other areas of interest in the health sector have improved and those improvements were brought about by Electronic Health records and electronic medical records [50]. However, some countries are still relying on paper-based methods to store medical records. This medical record involves a health practitioner writing the details of the patient and filing the record [51]. This paper-based medical record system is ineffective, insecure, disorganized and susceptible to manipulation. It is also plagued with data duplication and redundancy, as each facility that the patient visits have several copies of the patient's medical records [50]. In the paper-based approach, a patient has to first go to an Out-Patient-Department (OPD) where they have to request their documents while waiting for the retrieval of their documents, sometimes the process can take a long time since files are too many and at times patients files are not found which leads to a new file being created thereby losing track of past patient records [52], [53].

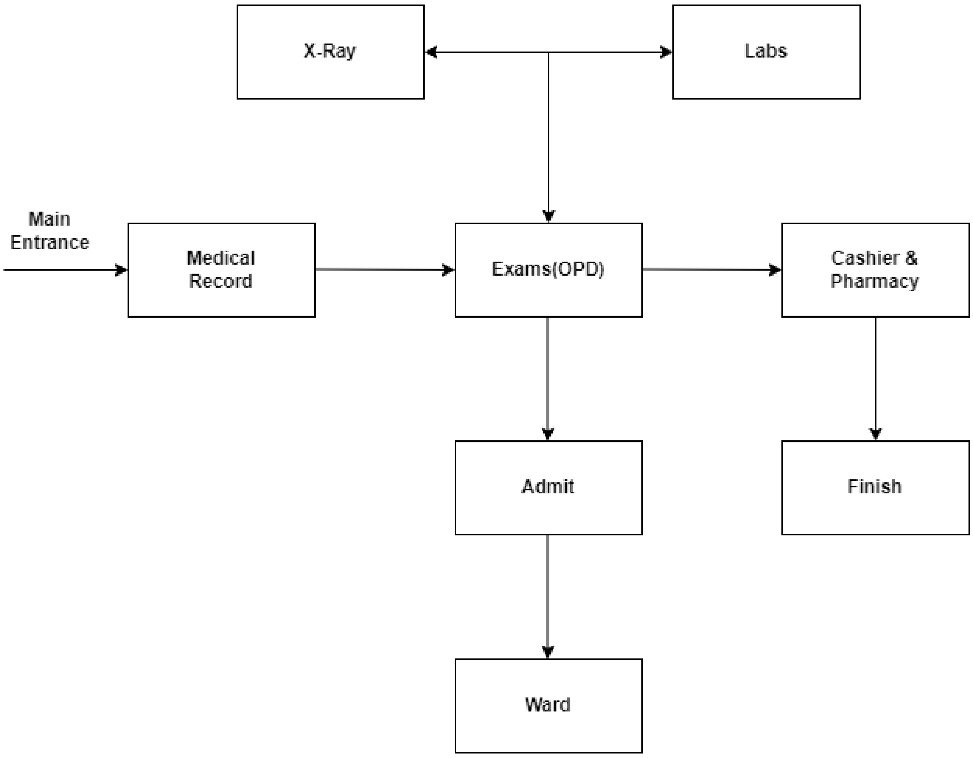


Figure 2.1: Relationship between OPD and other departments

B. Cloud-based approach

2.2.1.2 Cloud-based approach

Significant technological advances that are transforming the global health sector have been witnessed since the beginning of the 21st century. As a result of the migration from paper-based approaches to electronic health records, there has been a significant amount of change and transformation in healthcare systems [54]. Cloud computing is a new approach in digital technology that is widely employed in the healthcare business, and it permits not only the storage of medical data but also the transmission or interchange of medical data between parties [54]. The cloud-based approach consists of three different cloud models which are public, private and hybrid.

Public cloud model: This concept utilizes a shared infrastructure whose operation is determined entirely by a third-party service provider. This type of cloud system acquires its services from Cloud Service Providers (CSPs). Under this strategy, Electronic Health Records (EHRs) are typically shared between many organizations. The EHRs are extremely susceptible to different assaults and manipulations since they are kept on CSP-controlled off-premises servers. Despite the advantages that cloud computing has brought to the healthcare domain, there are still some issues with privacy and security [54], [55].

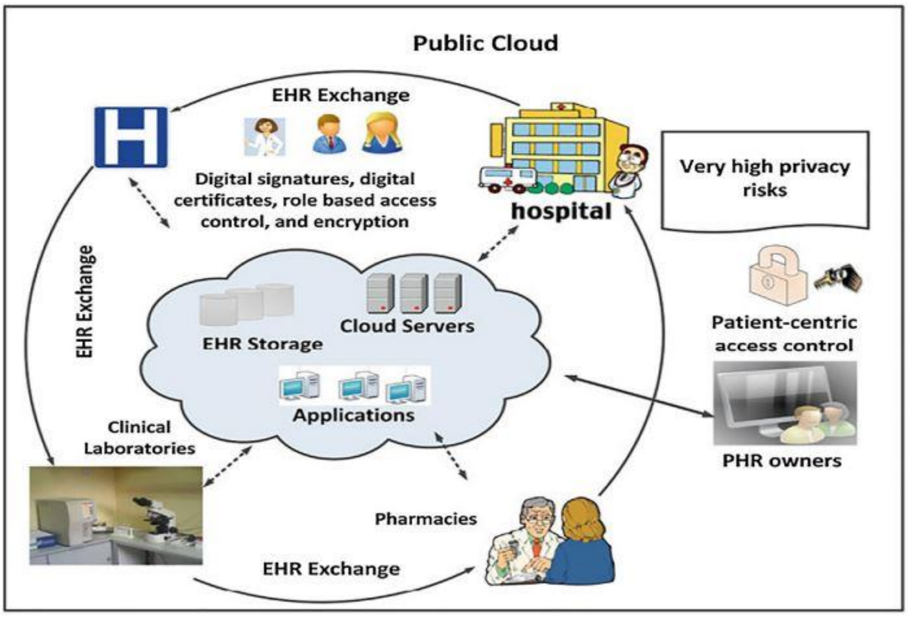


Figure 2.2: Public cloud model in the context of healthcare systems [54]

Private cloud model: This model is the most secure of all models, according to experts. Access to Electronic Medical Records (EMRs) in a private cloud is restricted to workers of healthcare facilities that are recognized as trustworthy and dependable [56]. The model as applied to the health sector is represented in figure 2.3

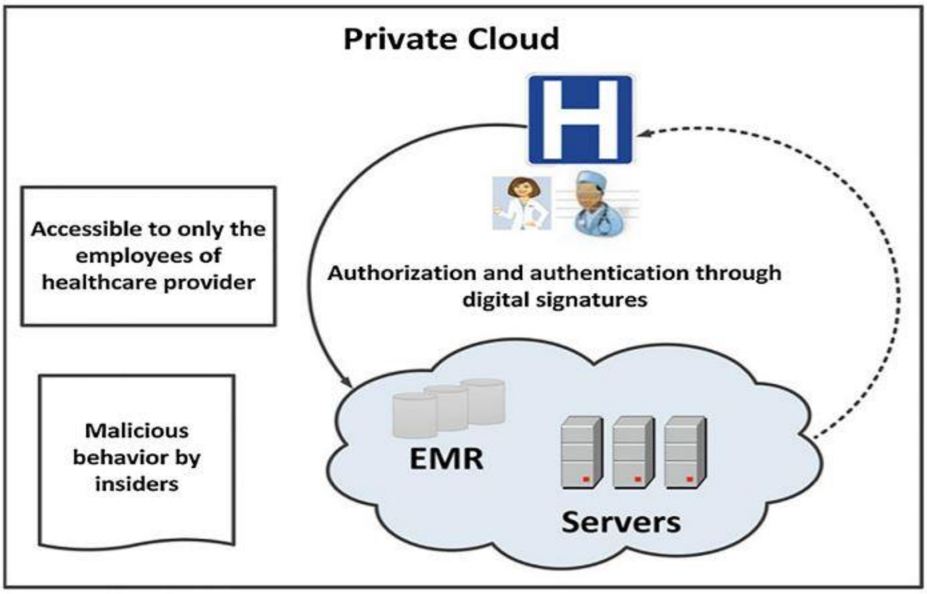

Private Cloud
Accessible to only the employees of healthcare provider
Malicious behavior by insiders
Authorization and authentication through digital signatures
EMR
Servers

Figure 2.3: Private cloud model in the context of healthcare [54]

Hybrid cloud model: This model combines both the feature of private and public clouds and is known to be highly advantageous. Healthcare providers with constrained and limited physical resources and a strong interest in utilizing legacy systems can utilize third-party services to store massive medical data without difficulty [54], [55]. The model is shown in Figure 2.4.

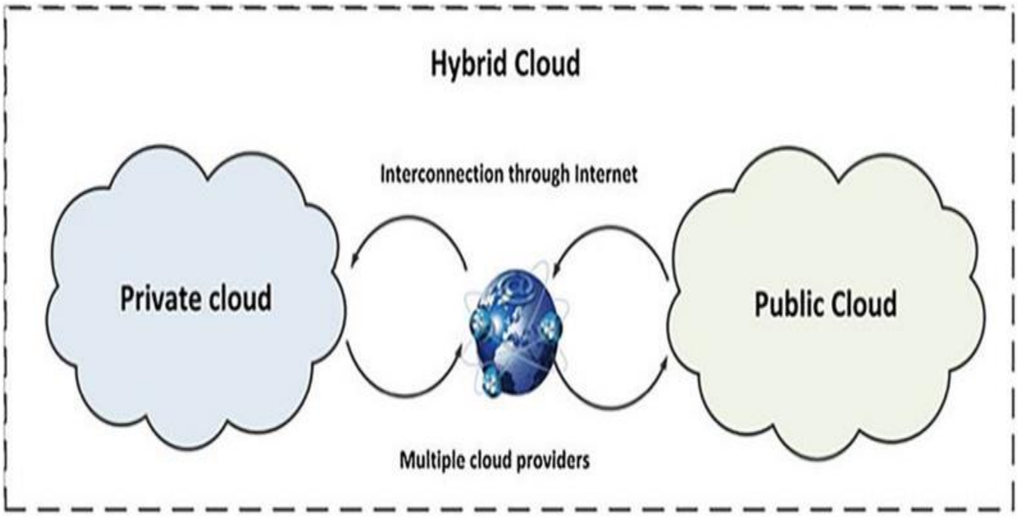


Figure 2.4: Hybrid cloud model in the context of healthcare [54]

Furthermore, despite the advantages that the cloud-based approach brings there are still several limitations with it. Security and system downtimes have long been considered obstacles to the cloud computing idea in the healthcare domain. This means that the availability of the system is still a challenge to this day [57]. Another major issue with the cloud-based approach in health is that it gives a reduced level of control over its architecture. This is a huge problem for companies, but service providers get rid of it by signing many contracts and offering guarantees [57]. Finally, cloud architectures are susceptible to several types of security attacks since most of them operate in an open and shared environment [58].

2.2.1.3 Traditional Database Approach

Most traditional health systems are still using centralized database architecture to store data, especially, in developing nations. However, these architectures have shown some weaknesses that lead to various cyber-attacks such as SQL injection [59]. This approach applies restrictions on data access according to the system's control mechanism. However, this system is susceptible if the system administrator allows unauthorized access then it will be compromised [60].

2.2.1.4 Comparison of Centralized and Decentralized architectures

Research has shown that approaches can be implemented on different architectures which can be classified as centralized and decentralized[61]. The architectures differ in terms of performance, security, redundancy, and trust. Table 2.1 shows the comparison between centralized architecture and decentralized architecture.

Table 2.1: Comparison of Centralized architecture vs Decentralized architecture

Ref		Decentralized architecture	Centralized architecture
[60]	Performance	Execution takes time	Immediate execution
[62]	Security	Uses cryptographic techniques	Traditional access control
[60]	Redundancy	Nodes have the latest copy	Copies are possessed by the central party only
[63]	Trust	No trusted party is required	A trusted party is required

2.2.2 Current Vaccination Registration and Verification Approach for Covid-19

In developing countries such as South Africa, both paper and cloud approach was utilized to register and verify vaccinated patients. After the vaccination of the patient, a paper-based card was given to the patient containing all vaccination details. The patient was required to present the card whenever verification was needed. However, the approach was not sufficient because a lot of counterfeit certificates and proof of vaccination were being made which then led to cloud migration where a system was developed known as the electronic vaccination data system (EVDS). It is a self-registration portal where vaccinated patients register their details and the government was able to track and monitor vaccines [64]. Due to its architecture, many problems arose such as being available due to the energy problems in the country as well as data accuracy as most of the people who were using the EVDS are not computer literate[61].

China also developed a contact tracing app that mainly focused on tracking individuals who tested positive for the Covid-19 virus. The developers of the app used sophisticated tracking and surveillance methods to track those patients. They anonymously tipped healthy individuals if they had been in contact with someone infected [40].

Furthermore, quarantine apps were also developed, and the concept was based on creating a virtual fence around individuals' houses so that they should not disobey the rules given by the authorities. If they disobey, authorities would be notified and legal actions would be taken. Taiwan uses the same geofencing technology to geofence persons who are obliged to self-isolate or quarantine at home. The geofencing application utilizes base station triangulation, which is less exact than GPS but offers a position within 300 meters. A social worker is appointed to check on quarantined patients twice each day via phone calls. If they are unresponsive, the police will visit their residence [40]. Moreover, Symptom monitoring apps were also developed, and the Apple company developed a web-based Covid-19 screening tool. Using a back-end algorithm, these applications inquire about the user's symptoms, including temperature, and whether the user is suspected of having COVID-19 it may be determined based on factors such as the user's recent trip, the sort of cough the user has, contact with an infected person, and so on. In most cases, these apps will offer the user step-by-step directions on what to do if it is thought that the user has been infected [65].

Despite the developed solutions to fight Covid-19, there is still a gap since most of the critical aspects such as security, privacy and storage have not been addressed. The current solutions focused more on providing information rather than addressing some of the challenges faced. This research study focuses on addressing those issues in the current healthcare domain.

2.3 Blockchain technology

2.3.1 Overview and architecture

Satoshi Nakamoto presented a brand-new idea in 2008 that he called "Bitcoin" to resolve the inherent trust concerns that were present in information networks. Bitcoin is a cryptocurrency whose value is maintained independently of centralized authority or any financial institution because it is maintained by a decentralized peer-to-peer (P2P) network of participants. It may be audited and verified. The decentralized digital currency known as bitcoin is supported by a technology known as a blockchain. The blockchain is a continuously growing ledger of data recordings, known as blocks, that are interconnected and safeguarded using cryptographic techniques [66]. Blockchain is known to be a transparent and secure information storage and distribution platform that runs independently of a centralized authority [67]. It consists of a series of blocks that are cryptographically joined. In the blockchain, the order of the blocks is crucial, which is why they are connected in a predetermined, immutable order specified by the time of the block's creation. The following information is contained within a block: the hash value of the block, the contents, and the hash value of the block that came before it [68].

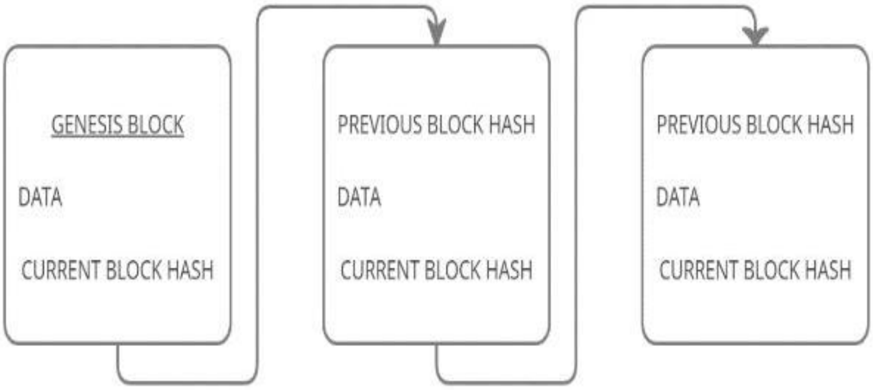


Figure 2.5: Blockchain Architecture [68]

A block is a record on the blockchain network that contains all the transactions that have been verified. As a consequence of this, any transaction that has not yet been verified will be added to a block. In addition, when a certain amount of time has passed, the blockchain will include a new block that is comprised of completed transactions, it must be validated by an individual known as a miner [64], [65]. A block's hash value is produced when the block is created; its value will change if the block's data is modified and it comprises the hash value of the preceding block as described in Figure 2.5 above [68]. The hash value is produced in such a manner that it is very hard to do reverse engineering on it; moreover, the hash is updated every minute if there is a change. Blockchain consensus mechanisms are used to approve and validate the tasks, only when the transaction has been approved does it then become a permanent part of the blockchain [69], [45].

2.3.2 Features of Blockchain

Blockchain as an emerging technology promises to bring a lot of solutions to some of the current problems because of its features. In this section, we presented some of the features of blockchain technology.

i. ***Decentralized:*** The fundamental characteristic of Blockchain implies that data may be captured, stored and updated on numerous computers rather than relying on a centralized node [70]. In a typical centralized transaction system, each transaction must be verified by and validated by a digital timestamp before it can be processed. According to the blockchain hierarchy, the public blockchain is known as a decentralized network, the consortium blockchain is slightly centralized, and the private blockchain is centralized and owned by a single entity. Because public blockchain is accessible to anybody anywhere in the globe, it has the potential to attract a large number of users from all over the world. Communities are extremely active as well. New public blockchains are created daily. Many different commercial applications might benefit from using blockchain for collaboration [41], [71], [72]

ii. ***Immutable:*** Decentralized blockchain networks record transactions in a distributed ledger that is checked by all peers, it becomes impossible to make changes to the public Blockchain. Alternatively, a modification may be made to a consortium and private blockchain ledger at the discretion of the dominant authority [71]. All blockchain records are retained in perpetuity and cannot be altered unless someone controls more than 51 per cent of the nodes at the same time [47], [70].

iii. ***Auditability:*** The consensus foundation allows every blockchain node to safely transfer or update data; the objective is to generate confidence from a single person to the whole system without the need for third parties to participate. All blockchain network transactions are kept in a digital decentralized ledger and validated using a digital timestamp. As a result, records may be examined and traced by acquiring access to any network node. For instance, on Bitcoin, all transactions can be tracked repeatedly. This increases the data state preserved by the blockchain's auditability and transparency. However, moving money back and forth across many accounts makes it very difficult to track down where the money came from in the first place [71], [70], [73].

iv. ***Distributed ledger:*** It can be described as a data structure that is reproduced across all of the network nodes and consists of an ordered list of transactions that have been aggregated and linked together in a block. This structure is called a block. The ledger maintains a record of all of the updates that have been made to the blockchain since it was first created. This application for Bitcoin makes use of a user account design that is analogous to that of traditional banking systems. In a blockchain designed for general purposes, several ledgers may be connected. Nevertheless, it is common practice in major organizations to provide each department with its ledger. Additionally, the ownership of a ledger might vary from being strictly regulated by a single authority to being openly accessible to the whole public [74], [75].

v. ***Consensus Determination:*** All nodes on a public blockchain, such as Bitcoin, may participate in the consensus process, but just a few nodes on a consortium blockchain are accountable for confirming a block. The delegates who will determine the confirmed block on the private blockchain will be chosen by a central authority. Many different consensus mechanisms may be found in blockchain systems. Communication-bound protocols such as Practical Byzantine Fault Tolerance (PBFT) and computation-bound mechanisms such as Proof of Work (PoW) are examples of the various types of mechanisms that fall under this category[72]. PBFT and PoW are two extremes, and other hybrid techniques seek to enhance the performance of these two extremes somewhere in the centre [74].

2.3.3 Types of Blockchain

This section presents different types of blockchain, as well as their comparisons, different blockchain consensus, applications and some of the challenges, which were also discussed in this section**.**

1) ***Public blockchain:*** Anyone may join a public blockchain, read or write on it, and take part in its consensus without needing the network administrator's prior approval. Even while public blockchains are decentralized, they may nevertheless be compromised by

invasions of privacy, greedy mining techniques, and attempts to gain control of 51 per cent of the network. The two public blockchains with the most users are Bitcoin and Ethereum. Together, they have more than 100 million users [70], [33], [71].

2) ***Consortium blockchain:*** A consortium blockchain indicates that the node with authority may be chosen ahead of time and that it typically involves partnerships. For example, in business-to-business partnerships, the data stored in Blockchain can either be made private or kept public, it can be regarded as being partially decentralized and it generally contains partnerships, among several other qualities; it is possible to perceive Blockchain as partially decentralized. For example, Hyperledger and R3CEV are both Blockchain consortiums that work together [70], [71].

3) ***Private blockchain:*** This blockchain network functions in a confined environment, for example, a private network, or is governed by a sole organization. Of which the peer-to-peer connection and decentralization are similar to the one used in the public blockchain but much smaller. The designer of a private Blockchain network is aware of who the participants are from the start. Because users enjoy complete anonymity on the public web, it is difficult to establish a permission-based system [76], [77].

2.3.3.1 Comparison of Blockchain Types

There are three major types of blockchain widely discussed public, private and consortium Blockchain. These types of blockchain technology differ in terms of security, cost, speed, consensus mechanism, and platforms. Table 2.2 shows the difference between the blockchain types.

Table 2.2: Comparison of blockchain types

Ref.	Consideration	Public Blockchain	Consortium Blockchain	Private Blockchain
[47], [66], [67]	**Security**	Because each block contains a copy of each transaction, it is extremely secure.	Provides confidentiality for transactions.	Access is restricted to certain individuals, and the system is deemed secure because all participants are recognized.
[33]	**Cost**	Cost is High	Cost is lower as compared to public blockchain	Cost is low

[78],[67], [69]	**Speed**	The speed is slow since transactions must be verified and synchronized with every node	The number of participants is limited which means high speed	Since it has a smaller number of nodes, it is effective and has high speeds
[79],[33]	**Consensus Mechanism**	Anyone can contribute throughout the consensus process.	The consensus process is governed by nodes that have been pre-selected.	The technique of consensus supports a large number of participants.
[78]	**Platform**	Ethereum	Ethermint, Multichain	Corda, Hyperledger Fabric

2.3.4 Blockchain Consensus Mechanisms

A fundamental advantage of the blockchain system is the technology that validates the block's dependability and trustworthiness without requiring a trusted central authority. To obtain a stable and trustworthy consensus in a decentralized distributed framework, consensus algorithms are utilized [66].

2.3.4.1 Proof of Work (PoW)

As it is associated with bitcoin, this is the most popularly used consensus algorithm. The PoW algorithm operates by searching for a value whose hashed representation begins with a certain amount of zero bits [80]. This is performed by adding a nonce, also known as a working increment, to the starting value and continuing to do so until the final hash starts with the specified amount of zero bits. This process is repeated until the final hash starts with the required number of zero bits. Once this nonce has been found and the proof of work has been accomplished, the block cannot be modified without repeating the work for that block as well as the work for any blocks that come after it [80], [67], [66].

2.3.4.2 Proof of Stake

Proof of Stake (PoS) is an alternative consensus technique created for public blockchains. PoS relies on the validator's ownership of the stake or the network's computational power rather than their ability to solve a cryptographic challenge [81]. There are validators instead of miners in the PoS. The PoS utilizes validators to propose, vote on, and generate new blocks in the network. The two methods for reaching a consensual agreement are the random technique and the Byzantine fault-tolerant approach [82], [66].

2.3.4.3 Practical Byzantine Fault Tolerant (PBFT) Consensus Algorithm

The practical Byzantine Fault Tolerant (PBFT) algorithm decreases the average response time by lowering the communication overhead required to operate under necessarily synchronous conditions, making it an attractive choice for Internet protocol communication systems [83], [84], [66]. The PBFT method consists of five steps: Request, Pre-preparation, Preparation, Commitment and Reply. Nodes must pass through these steps in PBFT to commit and operate in the network. PBFT will function correctly despite the presence of defective network nodes. During the request phase, the client is responsible for sending a request to the master node. During the pre-prepare phase, the master node is the one responsible for sending the request out to the other nodes, who determine whether or not to accept the request. If the nodes agree to the request to execute, they send the other nodes a prepared message. PBFT algorithms may also handle up to 80,000 messages per second, as demonstrated [85], [82], [81].

Table 2.3: Comparison of blockchain consensus algorithms

Category	**PoW**	**PoS**	**PBFT**
	Permissionless	Permissionless	Permissioned
Security	More Secure	Less Secure	Secure
Latency	Very High	Low	Low
Energy Consumption	Very High	Low	Low
Applications	Bitcoin, Ethereum	Peercoin	Hyperledger

2.3.5 Blockchain Applications

Figure 2.6 shows various applications of blockchain technology. his research study focuses on the areas where blockchain technology has been used in data management, security, and privacy.

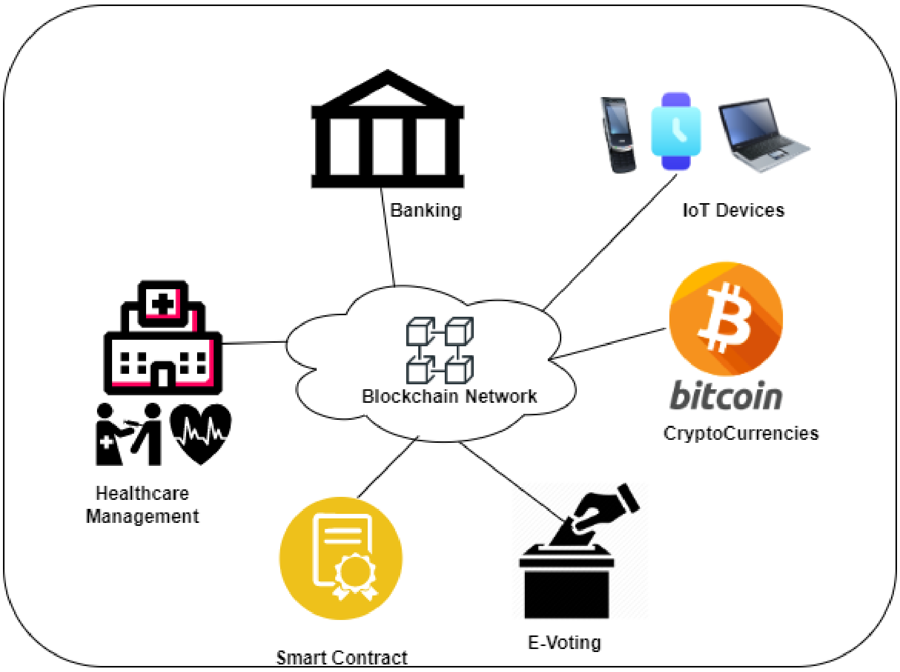


Figure 2.6: Blockchain application areas

Banking: Blockchain technology may completely change the banking and financial industries. A wide variety of financial organizations have been investigating the possible advantages that blockchain technology might provide for their operational procedures. The first-ever financial transaction to use blockchain technology was executed in 2016 between the Commonwealth Bank of Australia and Wells Fargo. There are currently several additional financial services that are conducted using blockchains, such as online payments and digital assets and 63% of central banks are conducting experiments with blockchain in the hopes of integrating it into their system following the completion of a successful trial of the technology [33].

Healthcare management: Current concerns with the healthcare management system include inconsistent data, duplicate information, as well as the incapacity of patients to have access to and take control of their data. When utilized appropriately, blockchain might alleviate several healthcare problems [33]. The objective of Blockchain is to record all sorts of transactions in a decentralized ledger that is independent of existing healthcare administration frameworks. It is accurate and unambiguous, saving time, effort and money, hence minimizing the amount of management effort required [76].

E-Voting: There is a widespread inability around the world, particularly among developing nations, to hold elections that are free and fair. Voting processes in firms, assemblies and even nations might all be made more open and transparent with the use of blockchain technology.

To promote free and fair elections and ensure the integrity of vote records, blockchain-based electronic voting systems have been investigated in around sixteen countries and the results showed that privacy and security in elections can be preserved [33], [86].

Cryptocurrencies: The functioning of Bitcoin, in addition to that of several other cryptocurrencies, such as Ether, is underpinned by the technology known as the blockchain. As of September 2020, Bitcoin and Ethereum have respective market capitalizations of $191 billion and $41 billion, while their respective values are $10,345 and $364. There are over 1200 distinct cryptocurrencies that are now active in the market. Litecoin, Ripple, Bitcoin Cash, Monero, Zcash and Dash are a few examples of alternative cryptocurrencies [33], [87].

Smart Contract: The term “smart contract” refers to a legally binding agreement between many entities that can be carried out with the assistance of computer-written instructions because it runs without giving the parties the option to cancel, the code ensures that there is no room for trust in the execution. Smart contracts assisted in the expansion of blockchain technology beyond cryptocurrencies and made it relevant to a vast array of applications, including healthcare, supply chain, the Internet of Things and business process management [33][74].

IoT Domain: The need for IoT devices to interact and exchange data without human intervention has sparked interest in using blockchain technology [33]. The Internet of Things (IoT) gadgets of today utilise cutting-edge technologies like computers, sensor networks, wireless communications and electronics in addition to contemporary management practices, which enable blockchain technology to be used [88]. For example, the ride-sharing transportation sector can utilize blockchain. It can create a peer-to-peer ecosystem. Therefore, it poses a threat to the monopoly of commercialized transportation services provided by corporations such as Uber, Careem, and Lyft. As a result, the economy will become more decentralized [88].

2.3.6 Challenges of Blockchain Technology

Although the blockchain's core concept is straightforward, its implementation presents several difficulties. This section highlights the most important consequences of its use, as determined by its users.

1) *Scalability and storage capacity:* The scalability and capacity of blockchain storage have been widely interrogated. In this approach, the chain is continuously increasing at

a pace of 1MB per block every 10 minutes in Bitcoin, and there are several versions of the chain stored among network nodes as the chain grows. Even though only full nodes (nodes that are capable of properly verifying transactions and blocks) store the whole blockchain, the storage requirements are high. As nodes grow in size, they use a growing quantity of system resources, limiting the system's scalability. A large chain hurts performance, such as increasing the synchronization time for new users [89], [33], [90].

2) *Cost of technology:* Using a new technology necessitates early expenditures on the part of both enterprises and consumers, including learning expenses associated with becoming acquainted with the system in general and the technology in particular. Regardless of the kind of blockchain, public sector respondents see blockchain adoption expenses as an investment in the long term when it comes to transaction and payment efficiency [91].

3) *Security Issues:* There have been claims of security problems and vulnerabilities in blockchain applications, particularly public blockchains, although blockchain technology is secure (primarily cryptocurrencies). Private and consortium blockchains provide a greater degree of security than public blockchains due to their restricted access. Among the ones that are reported the most frequently encountered security problems include malware attacks, fraud, denial of service (DoS), Sybil attacks, network and application vulnerabilities, and others. Loss of private keys may also result in severe security breaches and can be caused by criminal activities, accidents, or plain carelessness [33], [92], [76].

4) *Legal Issues:* The unavailability of a central authority, the unavailability of a minting organization, and, as a result, the complete absence of censorship in Bitcoin are both alluring and hazardous characteristics of the cryptocurrency. It is common for Bitcoin users to be accused of fraudulently misusing the network, and as a result, the technology is accused of encouraging or facilitating criminal behaviour. There has been a great deal of talk about Bitcoin sensitivity, the first decentralized cryptocurrency [33], [89].

5) *Interoperability:* According to the results of an extensive study, several industries are now interested in using blockchain technology. However, they are unable to interact and integrate due to the absence of a conventional protocol. In the blockchain industry, this is known as the absence of interoperability, and it has a detrimental effect on the

industry's growth. Therefore, rather than providing a wide range of practical solutions for a wide range of business models, Bitcoin continues to remain the dominant platform to put blockchain technology into action [71], [89], [33].

2.4 Blockchain Ethereum Smart Contract

Significant progress has been made in the implementation of smart contracts and the development of blockchain technology. In the 1990s, the term "smart contract" was utilized to describe the notion of a process for automated transactions that carry out the contractual obligations of an agreement [83]. As part of the transaction verification process, they are generated on the decentralized ledger and function independently. To generate the smart contract, a transaction on the Ethereum platform is required, this will then add the smart contract to the blockchain network. During this particular stage, a contract is issued a unique 160-bit identification address and its code is transferred to the blockchain network [93]. When properly constructed, a smart contract composes of a balance of contracts, a contract address, present executable code, and a contracting state. The security of smart contracts is dependent on how well the contract code is written, and the integrity of the blockchain may be seriously undermined if a fault is found in the implementation logic of the contract code [74]. Figure 2.7 shows a typical structure of a smart contract.

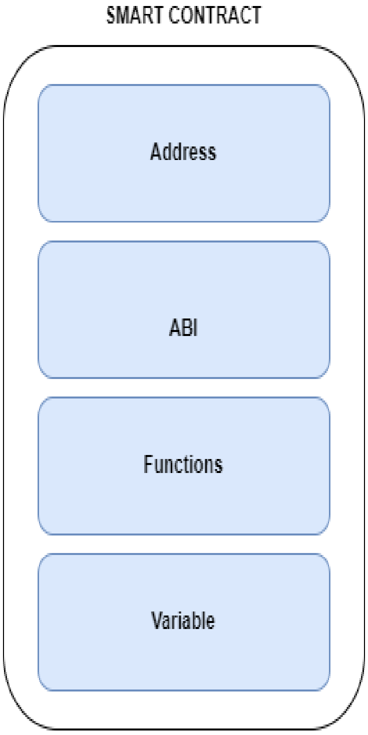


Figure 2.7: Smart Contract Structure

2.5 Blockchain Network Threats

Research has shown that there are several blockchain network threats. Table 2.4 discussed the threats and their definitions.

Table 2.4: Blockchain Network Threats

Threats	**Definition**
Greedy Mining Attack	In contrast to honest miners, dishonest miners release blocks selectively and promptly broadcast them to the network. This assault is initiated with the main purpose of obtaining an unfair pay out and causing honest miners to expend resources in the wrong direction [94], [95], [96].
Block Withholding attack (BW)	Blocks are removed during this kind of attack on mining pools. This prevents dishonest miners from publishing mined blocks, which in turn lowers the revenue of the pool [94].
Fork-after withholding attack (FAW)	The FAW attack incorporates aspects of both the BW and greedy mining methods, with the adversary splitting the computer resources at his disposal between mining for penetration and mining for innocent users [94].
Wallet security threats	Although password authentication is the predominant user authentication method, blockchain-based currencies employ private key-based authentication systems. To conduct transactions or access currency on a blockchain, users must hold both private and public keys[95][96].
51% attack	More than half of the system's processing power is under the control of the attacker (often a group of miners), hence this assault is also known as a majority attack. A malicious actor may invalidate any transaction block by seizing control of enough mining resources to halt the process [92], [95].

2.6 Cryptography Approaches

To ensure the ledger's integrity (the capacity to detect data tampering on the blockchain), blockchain systems employ advanced cryptographic algorithms. For this research, we have focused on two cryptography approaches which are mostly used.

2.6.1 Elliptic Curve Cryptography

Blockchain makes use of asymmetric cryptography, which necessitates the utilization of two unique keys (public and private) for encryption, decryption, and the creation of digital signatures. The production of key pairs and other activities, such as the digital signature, is carried out on the majority of blockchains with the assistance of an elliptic curve that is superimposed over a prime field [33]. In comparison to RSA and DSA, the implementation efficiency and level of security offered by elliptic curve cryptography (EC) are significantly higher. In addition to this, it is better suited to be used with devices that have restricted amounts of power, memory and bandwidth [33], [97]. Using EC cryptographic approach, blockchain technology ensures that all transactions are conducted securely while protecting all information and value storage. Therefore, anyone utilizing blockchain may be certain that anything recorded on the blockchain network is done so securely and lawfully [79].

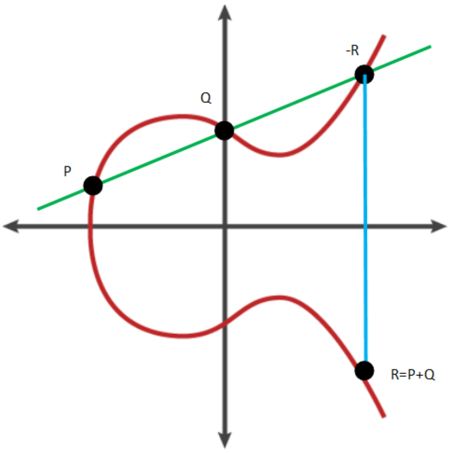


Figure 2.8: Elliptic curve cryptography[98]

The EC Cryptographic Signature technique kicks off with the generation of a pair of keys; subsequent steps involve the signing and verifying of transactions in the blockchain before they can be added to the block. The process of transaction signing requires the creation of a transaction in the form of a message. The message is then stored in the wallet program after being hashed and encrypted with each of the sender's transactions. The address is a Base58Check text encoding of a 160-bit message digest that was produced using SHA-256 and RIPEMD160 hashes [33], [79].

2.6.2 Digital Signature

In an untrustworthy environment, a digital signature that is built on asymmetric cryptography is often used for transaction authentication. To transfer transactions and check the authenticity of transactions, Blockchain relies on asymmetric cryptography. The sender utilizes his or her private key to digitally sign the transaction before it is broadcast over the P2P network. This happens before the transaction is published [99]. After the transaction has been sent, it is broadcast to all neighbouring nodes over the P2P network. In this kind of network, peers are treated with the same level of privilege as any other participant. After the transaction has been received by other nodes, the sender's public key is utilized to validate the validity of this received transaction following the specified block validation criteria [100].

2.6.3 Advanced Encryption Standard

The advanced encryption standard, known as symmetric cryptography, employs the usage of a similar key both for encryption and decryption processes. The length of the key that is being used is the determining factor for this specific use of AES encryption [101]. Encryption is done using a fixed data block that is 128 bits long. The Advanced Encryption Standard utilizes a block size of 128 bits for encryption and offers three distinct key sizes: 128, 256, and 192 bits. The block length is capped at 128 bits using the Advanced Encryption Standard, which employs the same three key size possibilities as before. The number of AES parameters is dependent on the length of the key. The Advanced Encryption Standard relies on transformations including substitution, permutation, mixing, and key addition to provide security. These transformations are used in every round of AES until the very last one [102].

2.6.4 Data Encryption Standard (DES)

The DES is one example of a symmetric algorithm. Through a series of complex operations, the DES algorithm transforms a string of plain text bits of a certain length into a string of cipher text bits of the same length. It used 64-bit blocks, with 8 of 16 bits utilized for parity checks. In each cycle of the DES algorithm, key bits and data bits are permuted, swapped, XOR’d and sent via the eight boxes. When running the DES algorithm, the eight boxes serve as lookup tables. Decryption is identical to encryption; however, it is performed in the other way [102], [101].

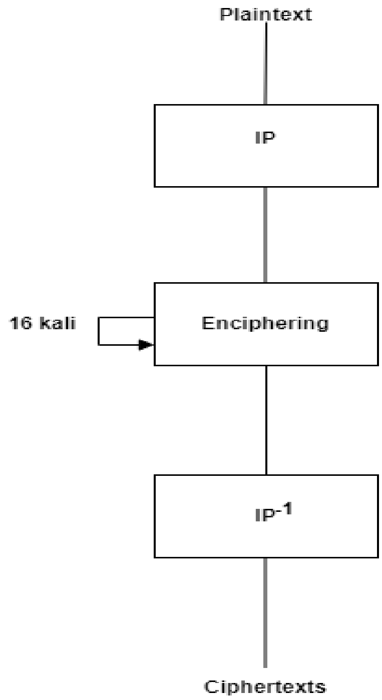


Figure 2.9: DES Global Algorithm

2.6.5 Rivest–Shamir-Adleman (RSA)

The RSA algorithm is largely regarded as the most trustworthy and secure encryption technology presently available. It allows for the use of high key sizes, which improves message encryption security by making it more difficult to decipher the encrypted message. RSA employs a public key for the encryption of the plaintext, which is known to all senders, while a private key is used for the decryption of encrypted data. RSA can overcome the issue of key distribution. However, because of how RSA was developed, it can only encrypt a limited quantity of plaintext at one time. For instance, in the case of a critical length of 2048 bytes, the maximum amount of plaintext that may be encrypted is 256. The benefit, however, is that it will be hard to decrypt using techniques that are already known when the critical size is huge [100], [102].

2.6.6 Merkle Trees

All the confirmed transactions are grouped into blocks, which are then mined and distributed. Up to the limit set by the block size restriction, multiple transactions can be included in a single block. Merkle trees, also known as hash trees, are the structures used to aggregate multiple transactions into a single block [103]**.** A Merkle tree is a tree-shaped data structure that is constructed via a bottom-up process. It can effectively summarize the combined transactions and check their legality. Each non-leaf node is created by computing its corresponding child nodes, starting with the leaf nodes (which are hashes of the original data) [95][103]. The leaf nodes are the site of origin [95].

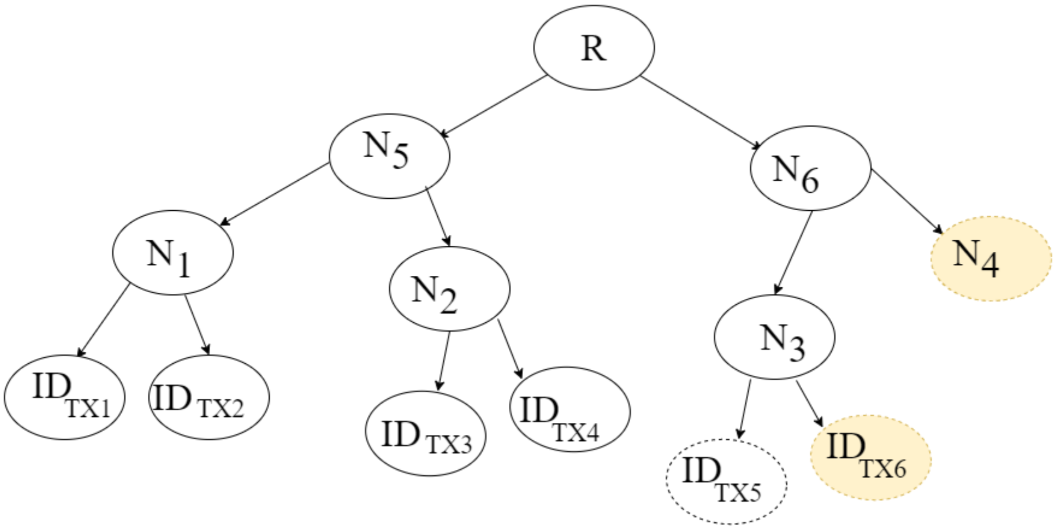


Figure 2.10: Merkle Tree within a block

2.6.7 Hashing Algorithms

The term "hash function" refers to any function that takes data of varying sizes and transforms it into data of a predetermined size [79]. The hash algorithm is the cryptographic approach that is used in Blockchain architecture more often than any other. The hash algorithm is used extensively inside Blockchain to create wallet addresses, maintain data integrity, encrypt data, calculate consensus, and connect blocks. To obtain a hash value in a reasonable time, it is feasible to compress data of any length into binary strings of a fixed length [79]. The features of a hash function include hiding, unidirectionality, puzzle friendliness, and collision resistance (it is difficult to determine the correct hash for a block, but simple to verify) [4].

2.7 Healthcare, IoT and Blockchain Technology

2.7.1 Overview

IoT is altering and simplifying manual processes to bring them into the digital era, acquiring amounts of data that yield unprecedented levels of information. This information is supporting the creation of smart applications, such as the enhancement of city administration and citizen quality of life through the digitalization of city services [89]. Therefore, the utilization of blockchain can supplement the IoT with trustworthy and secure data. IoT may considerably benefit from the functionality given by blockchain, which will also help in the development of existing IoT technologies. It is important to note that many research obstacles and unresolved concerns must be investigated before these two technologies may be utilized effortlessly.

2.7.2 IoT and Blockchain in Healthcare Benefits

Because of its significant qualities, such as item identification, governance, the growth of address space, authentication, and authorizing data privacy and security, several studies have recommended Blockchain Technology as a solution for a small number of Internet of Things devices [104].

Smart Contracts: The development of smart contracts is one of the most significant uses of blockchain technology. These contracts make it possible for an individual or an organization to create a legally binding document by using the blockchain system. To put it another way, smart contracts are essentially self-contained agents that make use of blockchain technology to encapsulate transactions and transform them into contracts or other legal documents. This enables smart contracts to be utilized to supply legal services to parties who are engaged in the transaction. They can be confirmed and tracked because they are composed of scripts that are saved using blockchain technology. Each script has its unique address, which enables the scripts to be tracked and validated. Smart contracts, which function in a decentralized fashion, make it possible to have fair commerce while also reducing the amount of player interaction [105], [92].

*Fraud Detection***:** The detection of fraudulent activity is just another use case for the technology behind blockchains. The practice of reviewing a document or other data system to see if the information has been altered in any way or whether there has been any other kind of dishonest behaviour constitutes fraud detection. Detecting fraud may entail stopping the insertion of fraudulent reviews into online review systems in the form of badmouthing and voting to stuff. This can be done by blocking certain IP addresses. Detecting fact-based fraud in the healthcare industry, such as the use of counterfeit certifications, is another aspect of it that may be involved [90].

Key Management: Several cryptographic techniques requiring the use of private and public keys are necessary to secure the data stored on the blockchain ledger. Blockchain technology, like any other sort of information-holding technology, needs the installation of measures to ensure security and privacy. Because blockchain data is kept open and accessible to all parties, most cryptographic procedures necessitate the usage of keys to allow those cryptographic processes to take place; hence, some kind of encryption/access control is necessary [90], [71].

Identity Verification: Aside from the healthcare field, numerous internet companies have discovered various techniques of identification verification. Many companies and governments already utilize passports and fingerprints to identify individuals. Although the government prepares and validates all papers, the blockchain offers an alternative to government-sponsored identity verification. Outside of these countries, blockchain may be used to validate a user's identity. One example is the use of blockchain technology to notarize weddings, birth documents, and corporate transactions, among other things. Using blockchain technology, a person may utilize the distributed ledger to authenticate his or her presence at a certain time and location, which would be validated by other people owing to the distributed nature of blockchain [90], [76].

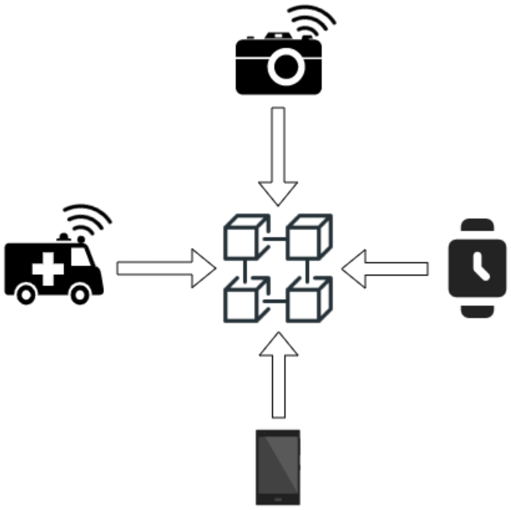


Figure 2.11: Blockchain-IoT integration approaches

2.8 Summary of Related Works

Several uses of blockchain technology in the medical sector, such as mobile health apps, monitoring devices, storing and sharing electronic media recordings, electronic health records (EHRs), insurance, and the storage of clinical trial data, are presently being researched. This section presents some of the work that has been done in the healthcare industry using blockchain technology.

2.8.1 Healthcare and Blockchain

This subsection discusses some of the existing works that utilized blockchain in the healthcare ecosystem.

Tripathi *et al*,[63] suggested an S2HS smart healthcare system approach based on blockchain to improve the security and integrity of smart health systems. Electronic health records, data from clinical trials, and other sensitive information acquired from a variety of sensors are encrypted and stored among several nodes in a blockchain network rather than in a centralized cloud. This allows for more decentralized access to the information. Only authorized parties, such as healthcare experts, insurance companies, pharmaceutical companies, and so on, can access these records, and they need the patient's consent to do so. When a clinician or doctor requests access to a patient's data, they must first notify the patient in real-time, and the data is only released if the patient consents to the disclosure.

Kumar *et al.* [31] presented a solution for the off-chain distributed storage of patient diagnostic reports using blockchain and interplanetary file systems (IPFS). The solution that was offered consisted of the implementation of a consortium blockchain-based architecture that can store medical information. IPFS has a version management technique, in which each report is connected with its hash value, and a peer may obtain a patient's medical report by utilizing the report's matching hash value. In addition, IPFS saves the hash values of all of the reports in a distributed fashion. In addition, IPFS provides users with a distributed file system (DFS), which makes it possible for users to store files and exchange them with one another. As part of this initiative, the hash of a patient's medical record is produced and then saved in a distributed ledger that is based on blockchain technology. This helps to make sure that the data is reliable and accurate.

Tarek *et al*. [106] suggested a secure inter-healthcare patient health records exchange architecture based on blockchain. The architecture that has been presented can identify and prevent harmful behaviour on electronic health records (EHRs) when they are both in transit and at rest. It may also certify the integrity and consistency of EHR queries and responses from other healthcare systems and provide them in an understandable format for all healthcare nodes.

Saha *et al*. [30] proposed a healthcare data management system on the blockchain framework. The suggested model is a multi-layered architecture in which various entities associated with the healthcare system would be represented by distinct components. The entities include patients, physicians, hospitals or clinics, medical records, etc. A consortium blockchain was used to implement the proposed solution.

Harris [21] proposed a blockchain solution to store covid-19 details. The solution entails storing and viewing patient status and transaction log information relevant to COVID-19 medical problems. This confidential information is only accessible to the relevant government and municipal authorities for monitoring and future action.

Saini *et al*. [107] provided a framework for the access control of smart contracts that were presented for cloud-based smart healthcare systems. In this method, electronic medical records (EMRs) are first encrypted utilizing the cryptographic functions of elliptic curve cryptography (ECC) and Edwards-curve digital signature algorithm (EdDSA), after which they are stored in the cloud, and their associated hashes are added to a blockchain. The viability of the suggested approach being implemented in a real-time smart healthcare system was shown by the assessment that was conducted. This would improve the level of security for patient-centric access control.

Thippeswamy *et al*. [108] proposed a blockchain-based approach for tracking medical reports. With this technique, the patients' medical records are maintained in a secure and distributed blockchain network. The patient is then granted a monopoly on his medical records, making the system more patient-centred. The system uses two-step authentication to provide security and privacy. Locally, the setup was completed using the ganache and metamask wallets.

Table 2.5: Summary of Blockchain in Healthcare

Ref.	Proposed Solution and Objective	Implementation	Consideration
[63]	S2HS-smart healthcare system approach based on blockchain	No	Data integrity, Security, Privacy, and Transparency
[31]	off-chain distributed storage of patient diagnostic reports using blockchain and interplanetary file systems (IPFS)	Yes: IPFS, Blockchain, Python flask	Consistency, Integrity, and Availability
[106]	The blockchain-based solution to facilitate scalable and secure inter-healthcare HER exchange	Yes: Blockchain, Smart contract	Security, Integrity, and Consistency
[30]	Healthcare data management system based on blockchain	Yes: Blockchain, FHIR Server	Transparency, Data replication, and availability
[21]	A low-cost Blockchain method for storing and viewing patient status and transaction log information	Yes: Blockchain, Hyperledger Fabric, Hyperledger Composer	Trust and Security

	relevant to their COVID-19 medical problems has been presented.		
[107]	Framework for the access control of smart contracts was presented for cloud-based smart healthcare systems	Yes: Blockchain, Cloud, ECC, EdDSA	User Verification, Access authorization, and misbehaviour detection
[108]	Blockchain-Based Medical Reports Monitoring System	Yes: Ethereum Blockchain, Ganache Truffle suite, Metamask wallets, Node Js	Security, Storage, and Authorization

2.8.2 Healthcare, Blockchain and IoT

Some of the related works that integrated IoT and blockchain into the healthcare ecosystems are discussed as follows:

Jafar [103] proposed a blockchain-assisted solution for medical IoT devices based on the Lamport Merkle Digital Signature (LMDS) to overcome security issues in the absence of a reliable third party to help solve security issues when a reliable third party is not involved. They advocated for the use of a blockchain-based cloud Internet of Things network and the integration of that network with patient and hospital health records. Authentication technologies such as LMDSG and LMDSV were used to protect medical data transmitted over the Internet of Things network. This proposed solution was safeguarded by a consensus mechanism, and it was tested using Cloud Sim 3.0 to ensure that it worked. Computing time and computational overhead were reduced by 25 per cent as a result of this strategy, while security was raised by 7 per cent.

Ammi *et al.* [109] proposed a custom blockchain architecture for safe smart house lightweight IoT. The proposed method considers the flow of data and performs the information exchange in the form of a transaction. Afterwards, the information that pertains to the transaction is saved on immutable blocks to preserve its integrity. This mapping technique will make it possible for the user to investigate any interactions that are not typical and will ensure the data integrity of the different transactions. Permissioned blockchain with the hyper ledger fabric platform was combined with the composer when developing this approach. The proposed solution was simulated, and the results have shown that using this blockchain-based paradigm may ensure that smart home users' important security and privacy requirements are met while retaining transparency and fostering interoperability.

Shukla *et al.* [110] proposed a Healthcare IoT identification and authentication utilizing an integrated fog computing-based blockchain architecture. The model focuses on storing IoT data on Fog nodes and master fog nodes rather than storing it on blockchain and cloud servers. The fog storage then organizes the patients' health data provided by healthcare IoT devices into comparable blocks that are linked with a unique block and the fog nodes are connected to the healthcare IoT. In a real-time situation, the ASE method was examined and analyzed, and the suggested technique was simulated using iFogSim.

Fotopoulus *et al.* [111] suggested a blockchain-enabled IoMT device authentication architecture. When the patient or clinic receives a new gadget, the strategy works. The device is then authorized and permitted to communicate with the system. To protect connections between devices and the IoT getaway or central system, each device is certified with a unique public or private key pair. The Hyperledger Aries Cloud Agent Python framework served as the foundation for the implementation.

Auja *et al.* [112] proposed the development of a decoupled blockchain technique for edge-envisioned IoT-Based Healthcare Monitoring. To separate the ledgers and block headers, the technique adopts a decoupled blockchain-based architecture, which reduces header production times and block preparation while ensuring security when transferring the obtained data. It is necessary to use an incremental tensor train approach to transport data from edge devices to a cloud server. This strategy reduces the overall amount of cloud storage space required while re-evaluating the same data with the least amount of error.

Attia *et al.* [113] suggested an IoT blockchain structure for healthcare monitoring based on a hyper-ledger structure. The approach is centred on remote monitoring of patients who have been discharged from the hospital and is intended to be monitored by medical personnel. Each patient is given a wearable device with sensors that can continually measure a specified set of parameters from a person's health condition. Data is then saved on a blockchain network using smart contracts.

Frikha *et al.* [67] proposed data management in healthcare and fitness utilizing an IoT-based Blockchain platform. The suggested method focuses on developing a patient-centred application for storing medical records. A patient must have a wearable device which can continually measure a predetermined set of parameters related to the patient's health state. The data is subsequently uploaded to a decentralized ledger. Their architecture was created in such a way that medical data confidentiality and access control are met. To meet the criteria, the method was built utilizing the Ethereum blockchain and smart contracts.

Ray *et al.* [114] proposed an electronic health record service strategy in the IoT-Blockchain Ecosystem. Patients' electronic health record data is sent to doctors using a private blockchain, and doctors' and patients' diagnostic HER data are communicated through the same infrastructure. Swarm exchange is crucial for assisting the functions in a secure and efficient bidirectional manner. The findings indicated that the proposed system functioned admirably in a variety of blockchain-IoT scenarios across a wide range of scenarios.

Yanez *et al.* [115] suggested a data allocation technique for Internet of Things systems based on blockchain. The development of a data controller that makes use of fuzzy logic forms the basis for this approach. To determine the RoA value, using this logic, context factors are extracted from each data request, data network and quality measure. This value is then used as a threshold measurement to assess whether or not a data request needs to be kept on the blockchain or allocated off-chain. This determination is made based on whether or not the value exceeds a certain threshold. Calculating the RoA required the use of MATLAB, which is a simulation tool.

Table 2.6: Summary of IoT Blockchain in Healthcare system

Ref.	Proposed Solution and Objective	Implementation	Consideration
[103]	Blockchain-assisted solution for medical IoT systems based LMDS for higher security.	Yes: CloudSim 3.0, LMDS, LMDSV, LMDSG, secured consensus technique	Immutability, privacy, authentication, data integrity and speed
[67]	IoT blockchain-enabled platform for a healthcare application for EHRs storage and examination using a hybrid e-health decentralization system to protect healthcare data.	Yes: Raspberry Pi 3, Ethereum Smart contracts, PoW and PoA.	Immutability, privacy, confidentiality, accountability, speed, transparency, decentralization, and energy consumption.
[116]	Blockchain framework for the security of EHR where data in the cloud is encrypted and sent to the blockchain integrated with LPWAN.	Yes: Blockchain, Cloud, LPWAN	Immutability, privacy, confidentiality, integrity and transparency
[117]	Blockchain-based smart contracts for protecting security and privacy issues of patient and sensors information and enhance on-time treatment	Yes: Raspberry Pi 3, body sensors, GSM module, GPS sensor.	Immutability, privacy, confidentiality, availability, transparency and integrity
[111]	Blockchain-based IoMT authentication framework using SSI for scalable and practical authentication for medical devices of various stakeholders	Yes: Hyperledger Aries and Ursa, Hyperledger Identity stack, SSI, Medical device, device vendor, Gateway vendor	Immutability, privacy, authentication, integrity

[20]	Decoupled blockchain-based schemes secure in-house health records transmitted from IoT devices to the edge nodes.	Yes: Blockchain, edge devices, incremental tensor train, Mhealth dataset	Immutability, privacy, integrity, speed and energy consumption
[113]	IoT blockchain structure for healthcare monitoring based on a hyper ledger structure	Yes: Hyperleder fabric, Smart Contracts	Immutability, privacy, authentication, integrity, accountability, and transparency
[108]	Integration of medical records into a distributed ledger using blockchain and a cryptographic hash for extra privacy protection.	Yes: React JS, Web3 Library, MetaMask, Ganache	Immutability, privacy, integrity and accountability
[118]	Blockchain-enabled mHealth system via wearable sensors for transparency, security, and privacy of remote monitoring healthcare data.	Yes: private Ethereum, IPFS distributed storage protocol	Immutability, privacy, data audit, authentication, data integrity, speed and accountability
[119]	A lightweight consensus technique and a decentralized patient software agent for the RPM system.	Yes: Blockchain, API gateway, IoT device gateway, IoT devices	Immutability, privacy, speed and energy consumption
[120]	BSDMF is based on IoMT for the security and privacy of transmitted patient healthcare data, scalable accessible healthcare data	Yes: Blockchain, IoMT devices, Cloud server	Immutability, privacy, authentication, transparency.
[121]	A secure IoT-based COVID-19 vaccine distribution system for effective tracking of vaccine units	Yes: Blockchain smart contracts	Immutability, privacy, authentication, integrity, availability, speed
[114]	BIoTHR: a blockchain and swarm exchange method to protect the privacy of healthcare data from IoT devices to a backend server.	Yes: GnuPG, IPFS, GOlang	Immutability, privacy security, transparency, interoperability, access control, availability, decentralization, pseudonymity, data aggregating, low cost

A literature review of the current existing technologies using blockchain in healthcare was carried out and it further described the existing challenges. Through literature review analysis we found that blockchain has the potential to improve the current healthcare technologies. However, most works done are mainly based on security, access control, data management and monitoring which leaves a gap to be filled in developing more decentralised systems with the help of this technology.

2.10 Chapter Summary

This chapter contained a comprehensive literature review of IoT blockchain technology in healthcare systems. Current existing technologies were also reviewed, and the benefits and disadvantages of blockchain technology as well as the architecture were reviewed in depth.

Chapter 3

Research Methodology and Design

3.1 Introduction

Several definitions of research exist. According to Thomas [122], research is the process of formulating hypotheses and then improving or discarding some of them in favour of others that are better supported. In practice, the researcher gathers information on instruments based on participant-completed questionnaires or recorded observations. In other terms, research is a systematic inquiry including the meticulous examination of materials and sources to generate new facts and conclusions [122], [123]. In the majority of scientific fields, research is utilized to understand and solve issues for the benefit of humanity. Just like other disciplines, research in Computer Science is very important as there is a need to contribute to the existing body of knowledge and to ensure the dynamism of the discipline and innovations.

To effectively carry out research in the academic setting, it is important to have a relevant methodology to outline the logical sequence that should be followed [124]. These logical steps include problem formulation, performing an extensive literature review/survey for comprehension, designing the construct and execution, demonstrating the solution's feasibility, solution evaluation, and conclusions as well as recommendations [5]. Moreover, to effectively achieve the ROs, research is also formulated based on the problem statement and relevant research methods selected to answer the RQs [125]. Methods refer to the processes of data collecting, approaches for detecting connections in the given data, research linkages and contributions to the specific area, as well as the evaluation of collected data for precision, accuracy, and consistency. In addition, methods are related to the evaluation of collected data for research linkages [126]. The outlined RQs are answered using various methods such as simulations, observations, model design, case studies and experiments [124]. Moreover, a suitable study research design is essential for reaching the anticipated research outcomes.

In the context of this research, the goal is geared at designing and implementing a privacy-aware, secure and efficient system to solve the problems of privacy and security in the current healthcare ecosystem. We utilized blockchain technology to achieve the intended goal. We defined the system's functions and designed its structure, thus, the system proposed must be able to carry out all its functions while protecting the data and being efficient. However, to effectively achieve our defined goal, suitable methodology and methods have to be chosen and followed until the research is completed. Figure 3.1 presents the research workflow in this research showing how the research evolved from inception to completion.

3.1.1 Chapter Outline

This chapter presents the research methodology and designs of the research. It starts with a short introduction and then discusses the research methodology in detail, design, methods, data collection, and data analysis. Also discussed are the tools and technologies used, research evaluation and ethical considerations.

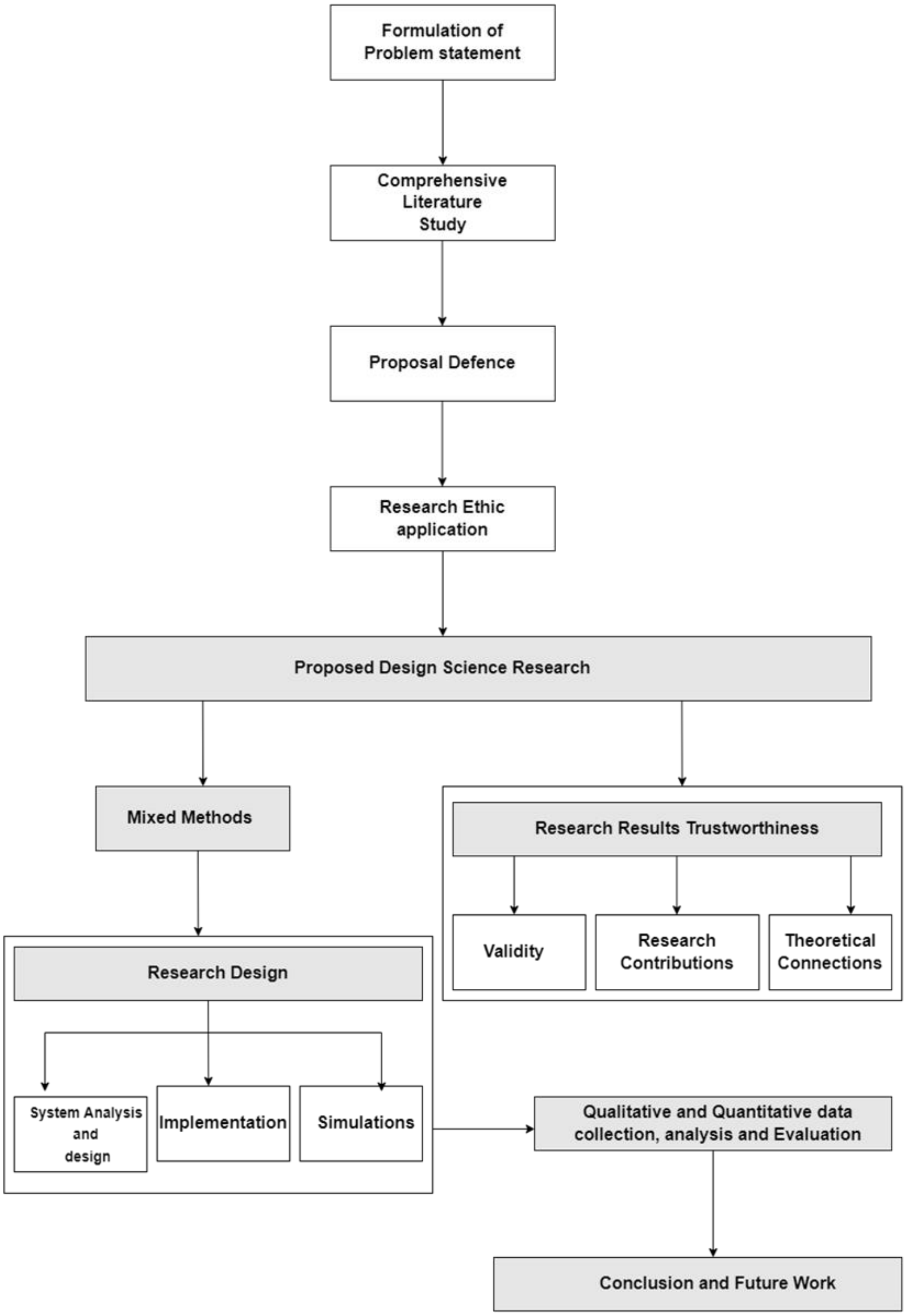

Formulation of Problem statement
Comprehensive Literature Study
Proposal Defence
Research Ethic application
Proposed Design Science Research
Mixed Methods
Research Results Trustworthiness
Validity
Research Contributions
Theoretical Connections
Research Design
System Analysis and design
Implementation
Simulations
Qualitative and Quantitative data collection, analysis and Evaluation
Conclusion and Future Work

Figure 3.1: Research workflow

As shown in Figure 3.1, this research started with the formulation of a relevant practical research problem statement after a preliminary literature study. This was to acquire insight into the existing issues linked with healthcare systems. Once a problem was identified, a comprehensive literature review/survey was launched to get a better comprehension of the research problem, approaches and suitable technologies. With the problem identified and proper background knowledge gained, the research proposal was written, submitted, approved, defended and ethics cleared. The actual research started by following the scientific methodology and the appropriate research methods selected to answer the RQs. The proposed system was analysed, designed and implemented. Data were collected using simulations and analysed then the results were presented. The solution was validated, and it is trustworthy and proven. Lastly, we provided a research contribution and its theoretical connections by evaluating and comparing it against the work done by other scholars in the literature. We then conclude, outline future works and submit the final dissertation.

3.2 Research Paradigms

A collection of perspectives and assumptions that are widely accepted within the research community concerning ontological, epistemological, and methodological concerns can be defined as a research paradigm [127]. A research paradigm also tackles epistemological concerns regarding how humans may know about reality. That is, how they can acquire knowledge about the world. Lastly, a research paradigm addresses methodological problems regarding viable ways to investigate reality and how to validate the knowledge obtained [127]. In the Computer Science discipline like other disciplines, research paradigms are very important because they help the researcher to grasp and explain perspectives on the nature of reality, the things that can be understood about it, and the processes involved in acquiring that knowledge [128]. Some of the research paradigms in the discipline of Computer Science are discussed next.

3.2.1 Positivism

The works of the French philosopher Auguste Comte were largely responsible for the rise to the popularity of the positivism type of philosophy at the beginning of the nineteenth century [129]. Positivism believes that reality exists independently of individuals. It is not mediated in any way by our senses and operates according to laws that cannot be altered. The ontological stance of realism is held by positivists. Positivists attempt to comprehend the social sphere similarly to how they comprehend the environmental universe [128]. Researchers go in as impartial observers to learn more about occurrences that take place independently of them. They do not affect or change the thing that is being observed. They will use words and symbols to describe things exactly as they are, without changing anything about the way things are [130].

3.2.2 Interpretivism

Interpretivism can be described as "a response to the undue dominance of positivism." The perspective on interpretation rejects the existence of a single, verifiable reality beyond our senses [128]. According to interpretive researchers, there is neither a universal truth nor a worldview. They perceive, interpret and comprehend based on their orientation reference and outline because they hold "the belief that uncommitted and disinterested impartiality is impractical and that reality or practicability of framework and backdrop is essential"[126, p3]. Interpretivism considers the world to be complicated and interpretable. The interpretation of findings might lead to issues concerning dependability [130].

3.2.3 Pragmatism

The pragmatic research approach maintains that conceptions are only significant to the extent that they are helpful to action. One of the pillars of pragmatics is "recognizing that there are numerous ways to do research and perceive the world, that no one perspective can ever provide a complete picture, and that there may be several realities" [128, p3]. The researcher's values drive the reflexive technique of inquiry that is inspired by doubt and a sense that something is amiss or out of place, and it is this process that restores confidence when the problem has been resolved [132]. Although mixed methods might be employed with any paradigm, pragmatism is typically regarded as the most prominent paradigm for mixed-methods social research. Pragmatists place the research topic and RQs at the core of their study and employ the techniques they deem most suitable for gaining the most meaningful insights from their research [130].

Therefore, within the scope of this investigation, we employed the pragmatic research paradigm since it allows the researchers to choose a variety of methods. The nature of this study required the use of mixed methods to obtain and validate the solution’s results.

3.3 Research Methodology

The term "research methodology" refers to a technique that may be used to answer or solve a research topic methodically. Thus, it may be defined as the process of learning how research is conducted scientifically [126], [133]. We studied the approach by analysing the many steps a researcher takes while examining his or her research subject, as well as the logic underpinning them. Choosing the right methodology is critical for giving guidance and openness in terms of research reporting methodologies and procedures used to illustrate how data was acquired, presented, evaluated and discussed ethically [126], [134]. Because of its compatibility with the pragmatic paradigm, the design science research approach was selected for this research and maintained throughout the study.

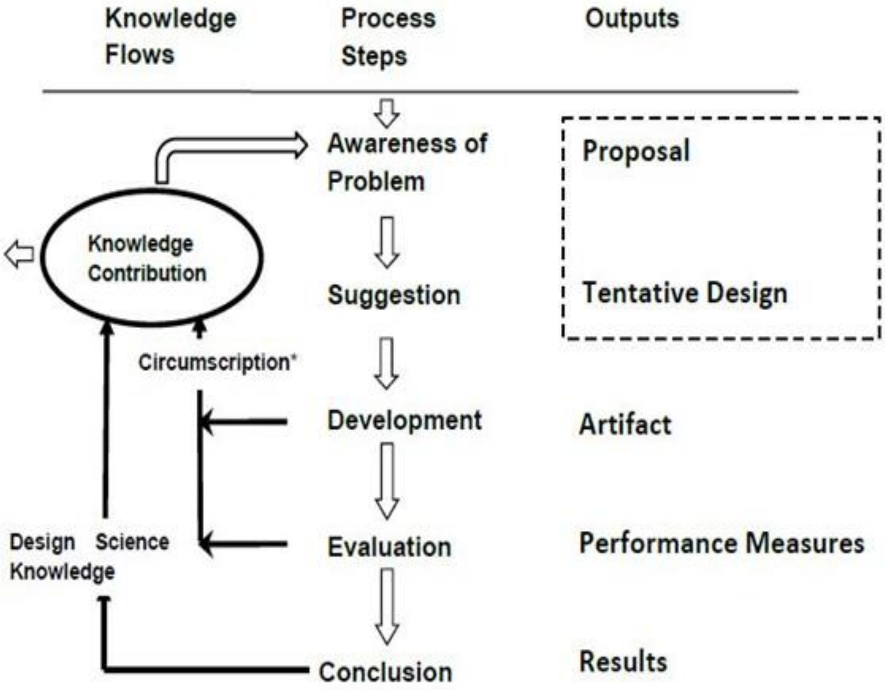


Figure 3.2: Design science research model[135]

3.3.1 The Design Science Research

Within the scope of this research, the design science research process model was adopted [135]. This is because this study involves the development of artefacts, and it engages primary activities to enhance and comprehend the behaviour of information systems. The design science research process produces artefacts such as system design techniques, languages, algorithms, and human/computer interfaces [135]. This also aligns with the pragmatic paradigm chosen for the research study since design science research employs various methods to evaluate information systems, and pragmatism allows a researcher to use a combination of different methods [136]. The design science research model is represented in Figure 3.2 and the phases involved are discussed as follows in line with this research:

a) *Awareness of the relevant research problem:* There are several ways of identifying a research problem in design research. In the current study, the research problem was identified through a preliminary literature review which assisted in investigating multiple factors around the research including but not limited to, existing blockchain technology in healthcare, an exploration into various approaches and the weaknesses that are found in those approaches.

b) *Suggestion:* Here an extensive literature review/survey was done to gain in-depth knowledge of the problem, the subject area, methods, technologies, etc. The knowledge gained assisted in the conceptualisation of the proposed system which has addressed most discovered research gaps and weaknesses. Different technologies and solution approaches were evaluated to check if they were suitable for the proposed system.

c) *Development:* A novel artefact was designed based on the knowledge obtained from a substantial literature review. This was to address the current problems at hand. In this study, a secure registration and verification system for vaccinated patients was developed using blockchain technology.

d) *Evaluation:* The simulation of the proposed solution was done; our approach was compared with the current systems and the results were published. Our approach showed satisfactory results and therefore can be recommended to be used.

e) *Conclusion:* Based on the solution evaluated, a real-world application is recommended since the performance and security were found to be better than the existing systems.

All the steps above were followed from the beginning to the end to accomplish the aim and goals stated in the first chapter.

Furthermore, this research study followed a mixed methodology of both quantitative and qualitative data collection as indicated by the research methodology used in this study. Quantitative approaches include the analysis of numerical data and often need the use of statistical tools to analyse the findings [126], [133]. This allows variables to be measured, and connections between them to be created. In qualitative research, a systematic investigation of social events that occur in natural settings is followed by the gathering and interpretation of data. These phenomena may contain, but are not confined to, how people view various elements of their own life, how people and/or groups behave, how entities work, and what role interactions have in the formation of relationships. However, these phenomena are not limited to these categories. Interviewing participants is the major procedure of data collection utilized in qualitative research. This method places the researcher in the role of the principal data collector. The researcher investigates not just the events themselves, but also the causes behind them and the impact they had on the persons under study [137], [138].

3.4 Research Design and Methods

3.4.1 Research Design

Research design is a general way of organizing different components of the study in a manner that will be logical and coherent [126] [127]. It also refers to the techniques or processes for integrating the various research components to reply to or answer the research question. It gives knowledge on how to apply a certain approach for data gathering and analysis in addressing or answering a research topic [123], [139]. The research design for this study is shown in Figure 3.3.

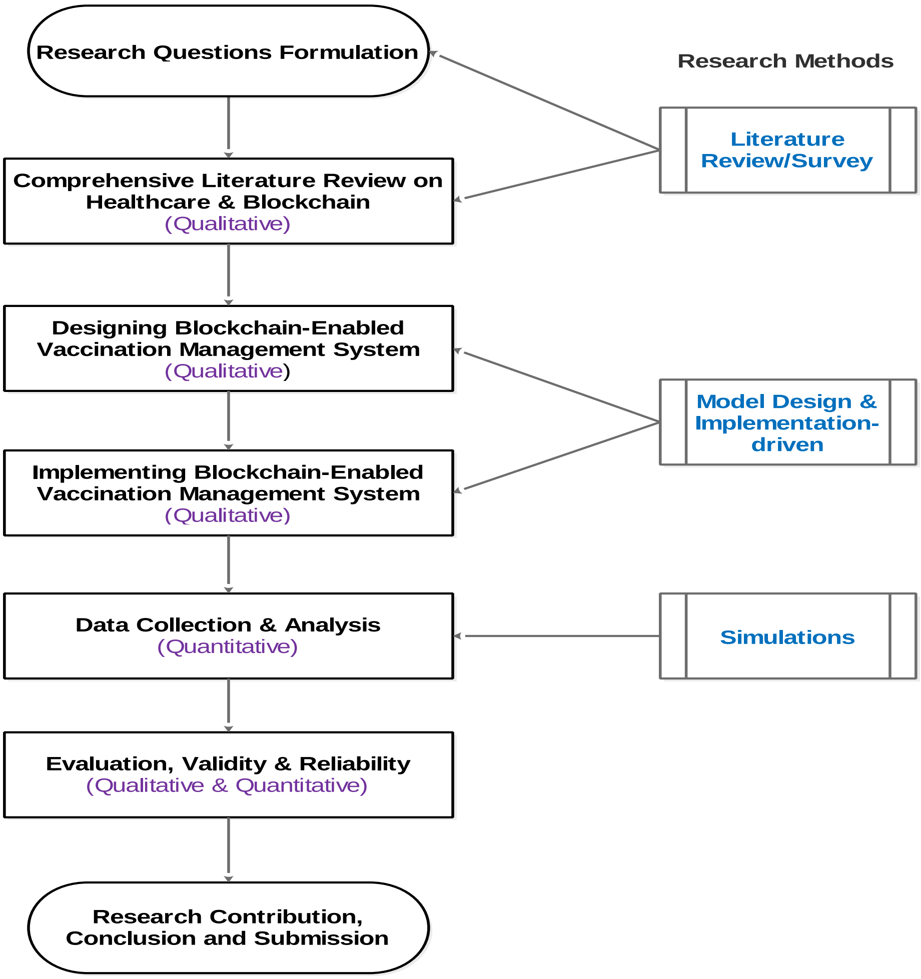

Research Questions Formulation
Research Methods
Literature Review/Survey
Comprehensive Literature Review on Healthcare & Blockchain
(Qualitative)
Designing Blockchain-Enabled Vaccination Management System
(Qualitative)
Model Design & Implementation-driven
Implementing Blockchain-Enabled Vaccination Management System
(Qualitative)
Data Collection & Analysis
(Quantitative)
Simulations
Evaluation, Validity & Reliability
(Qualitative & Quantitative)
Research Contribution, Conclusion and Submission

Figure 3.3: Research design and approaches

Figure 3.3 describes the research design and approach used in answering the RQs in this study. The research started by conducting a preliminary literature review to identify the research problem and formulated some RQs to address it. It was also designed to get a better comprehension of the current healthcare system and blockchain. After RQs were formulated and a comprehensive literature review performed, we then applied the knowledge gained to design a solution model which was implemented as a proof of concept to demonstrate the viability of the suggested solution. Moreover, to measure the effectiveness and performance of the developed artefact, numerous simulations were conducted to collect and analyze data. The results obtained were evaluated and validated to ascertain their reliability. Furthermore, the contribution of the research was determined, and a logical conclusion was drawn based on the evaluation.

3.4.2 Research Methods

Research methods are the strategies, techniques, and guidelines used to carry out an investigation and answer research questions [140]. This enables the measurement of variables and the subsequent establishment of their connections. Similar to Computer Science, particular methods are employed when doing research. The following techniques apply to addressing the research questions within the scope of this study:

A. *Literature Review:* To understand the depth of the problem at hand, an extensive literature review was carried out. Different research repositories such as IEEE Digital explore, Web Science, Science Direct *etc* were consulted to understand what other authors did, their approaches, solutions, methods and conclusions on integrating blockchain with healthcare systems. The research articles, journals and books conducted also led to a written article which reviewed the integration and use of blockchain technology in the healthcare ecosystem. This helped to answer RQ1 and RQ2 and it was done in Chapter 2

B. *Design and Implementation*: Using the knowledge obtained from the comprehensive literature review, we were able to come up with the requirement process as well as specify the requirements of which we outlined the functional and non-functional requirements. To demonstrate how the system works, system modelling was done which included the design of use case descriptions, use case diagrams and sequence diagrams. Finally, the study outlined the design of the system showcasing the system architecture, component design, algorithm design, privacy and security design of the system. This answered RQ2 and RQ3 and was done in Chapters 4 and 5.20

C. *Simulation:* To compare and evaluate our results with other scholars we simulated our proposed solution. The simulation was carried out using an *apache-JMeter 5.4.2* web load testing tool employing parameters such as throughput, latency, response time, and the average number of transactions per second vs the number of threads. The simulation was carried out using threads from 0 to 1000 to determine how the system responds. Furthermore, Hyperledger-Caliper was used to evaluate the blockchain performance using latency, throughput vs the number of transactions. This was done to compare our results with other scholars to validate the results and contribute to the body of knowledge. This answered RQ3 and it was done in Chapter 5.

3.5 Data Collection and Analysis

3.5.1 Data collection

Data collection is the systematic collecting and quantification of information on variables of interest to answer particular research questions, test hypotheses, and assess outcomes [141]. In the context of this research study, both primary and secondary data were collected [142]. The primary data was quantitative and was collected through simulations. The simulation involved testing different functionalities of the proposed simulation while recording the results and thereafter the average of the results was calculated so that the results can be consistent and accurate. However, secondary data was qualitative and was collected through scholarly articles (journals, articles and surveys). Different scholarly articles were consulted to understand the trends and provide clear insight into the problem at hand. This gave us direction for surveying the existing healthcare system challenges and identifying the present practical obstacle and providing a suitable solution to address them.

3.5.2 Data analysis

In the data analysis phase of any research endeavour, obtained data must be interpreted using logical and analytic reasoning to reveal patterns, trends and linkages for simple comprehension, it is often regarded as one of the most significant phases of the research process [126].

Quantitative analysis: It involves numerical, mathematical and statistical methods to analyse data [126]. This research study was utilized to help us understand the efficiency and effectiveness of the proposed solution through simulation results. Data were analysed to determine whether current problems can be solved, improved or solved by the solution as determined by this research. The data for analysis collected from simulations were presented in visualized graphs.

Qualitative analysis: Utilises an exploratory method to obtain an understanding of the recognized reasons and perspectives. The purpose is to recognize patterns and get a comprehensive grasp of the stated issue, proposed hypotheses and concepts [126]. It entails establishing connections and making academic contributions to identify patterns and future study areas. In this research study, this analysis gave us direction on how best we could identify and solve current healthcare system problems. Analysis was achieved by going through a literature review and tables were used to summarize and compare different findings from different authors.

3.6 Research Tools and Technologies

In the context of this research, two software programs were used in the analysis and development of the proposed solution. The software programs were Apache-JMeter 5.4.5 and Hyperledger calliper. These software programs were used to help us evaluate and present the research findings more understandably.

3.6.1 Apache-JMeter 5.4.5

The Apache JMeter program is open-source software that is a 100% java application that was built to assess functional behaviour and perform load testing. Its initial purpose was to test web applications, but it has now been extended to take on other test-related responsibilities as well. It is possible to use it to evaluate the performance of apps and online resources that are either static or dynamic on the web. It is possible to use it to simulate a high demand on a server, group of servers, network, or item to test the item's resilience or investigate the item's overall performance under a variety of different sorts of loads [143].

3.6.2 Hyperledger Caliper

When using the Hyperledger Caliper blockchain benchmarking tool, users can look at how well a blockchain implementation works by using a set of use cases that have already been set up. Hyperledger came up with this tool. Hyperledger Caliper will show how well the blockchain systems, Hyperledger Iroha, Hyperledger Burrow, Hyperledger Fabric, Hyperledger Besu, Hyperledger Sawtooth, Ethereum work and FISCO BCOS. At the moment, it can handle performance measures like Transaction/Read throughput, Success rate, Transaction/Read latency (minimum, maximum, average), and Resource consumption (CPU, memory, Network) [144].

3.6.3 Visual Studio Code

An example of a development process that is supported by the code editor known as Visual Studio Code is the process of debugging. Other development processes supported include task execution and version control. It makes an effort to provide just the tools that are required for a rapid code-build-debug cycle, allowing more complex processes to be handled by IDEs that have a greater number of capabilities, such as Visual Studio IDE[145]. In this research, visual studio code was used to write the entire code of the vaccination management system.

3.6.4 Remix IDE

Remix IDE is usable by users of all skill levels throughout the whole smart contract creation process. It has a wide collection of plugins with user-friendly interfaces and requires no installation. The integrated development environment is accessible in two forms (web app or desktop application) and as an extension to Visual code [146].

3.7 Research Evaluation, Validity and Reliability

The results acquired from the simulations were evaluated and a comparison with what other researchers had done was made to enable reliability. Furthermore, our proposed system showed great performance, and it provides more security to the data.

Evaluation: In this research study, the results were evaluated with what other scholars have found, this was to see if there is consistency with what other scholars have found. The parameters used for evaluation were latency, throughput, response time and the average number of transactions per second. The details of these parameters are presented in Chapter 5.

Validity: Validity describes the relationship between what the researcher intends to measure and what the researcher measured[124]. In the context of this study, validity was guaranteed because the researcher made sure that the instruments used in data collection were appropriate for answering the RQs.

Reliability: Reliability defines the accuracy of the researcher's method or how robust the method is [124]. In the context of this study, the researcher performed several simulations to compare results before making an actual conclusion. Also, the results obtained will be published to the scientific community for review and criticism.

3.8 Administration and Ethical Considerations

Before the commencement of the research study the department of Computer Science at the North-West University Mafikeng Campus follows certain procedures such as proposal writing, proposal defence, correction of the proposal writing and lastly submitting the research ethics clearance application. The proposal was successfully defended by the researcher, followed by correcting the proposal based on the comments made during the proposal defence. The corrections were submitted to the research committee and lastly, the research ethics application was submitted to the department for review. Ethical clearance was granted to the researcher to commence the study. There were no cases of ethics violations throughout the research.

3.9 Chapter Summary

This chapter explained the research method and design used in this study. The research methods and design were explained, which are the important parts of research, as well as the design science research methodology to meet the objectives of the suggested research study. Administration and ethical procedures were also discussed, outlining how the proposed research study would be done. Also, all of the steps that were taken in this research investigation were shown and discussed.

Chapter 4

System Analysis and Design

4.1 Introduction

The development of IoT has greatly increased the scope of connection that is possible between distant devices that are connected to the internet for information and access transfer. Moreover, IoT has changed and disrupted virtually every business on the planet, from education to supply chain management. IoT has also demonstrated outstanding success in the healthcare industry by streamlining diagnostic procedures and efficiently monitoring patients' activities [5]. However, with the benefits that come with IoT, the data that is processed in the healthcare domain is subject to various cyber-attacks that can give way to a single point of failure or ransomware attacks [147]. Therefore, data security and privacy are crucial aspects in the domain of healthcare as almost every day, huge amounts of healthcare records are processed and the more the data is processed the higher of risk cyber-attacks [147].

Presently, with several countries vaccinating and issuing vaccine certificates, most certificates are being faked and counterfeited which results in trust issues [148]. Therefore, there is a need of having effective measures in place which are efficient and secure to improve the privacy and security of healthcare data and also to bring back the trust and confidence in the authority [147], [148]. This research study presents the development of a vaccination management system (VMS) using blockchain technology. The system is developed to allow the registering authority to register vaccinated patients and their details will be stored on the smart contract deployed on the blockchain network. The proposed developed system also allows the patients to request their certificates and have their certificates scanned by the verification authority. The VMS aims to eliminate all the vulnerabilities such as data manipulation and fraud as well as reduce counterfeit certificates. Looking at the design approach of the VMS, the approach can be used to enhance security, privacy and transparency in other areas such as voting and registration of any kind. The proposed VMS is not only applicable to COVID-19 but to other forms of vaccination verifications such as yellow fever, TB, malaria, hepatitis, etc.

4.1.1 Chapter Outline

This chapter provides an analysis of the proposed system and its design. It starts with the requirements of the proposed system, its features, and the modelling. It then proceeds to the design in terms of architectural and component designs, including the database design. Lastly, we provided the overall operation of the system and the chapter summary.

4.2 System Analysis

System analysis is a crucial phase in software development that is done before the system is designed and implemented. As a major problem-solving approach, it requires a thorough grasp of the system's components, operation and interrelationships. This comprises an in-depth examination of the problem that must be solved and the most effective techniques for addressing the issue. In the case of the current system, the system analysis procedure is used to describe the functions of the system's components and the technologies that comprise the system's construction. It is also used to describe how the user interacts with system features.

4.2.1 Requirement process

With the literature review performed in Chapter 2 of this research, we found various scientific articles detailing the issue of data privacy and security in healthcare [149], [150], [4], [151], [152]; how data can be faked and manipulated with ease thereby compromising the authenticity of that health data [148], [153]. With vaccination certificates being issued at an alarming rate, and other healthcare activities that require registration of patients' information where confidentiality and integrity are highly required, this brings about a high demand for a system that is efficient, secure and that is verifiable. Therefore, since requirements are critical to systems quality, both functional (FR) and non-functional (NFR) requirements are important to realize the proposed system in this research to enhance the privacy and security of healthcare data.

To achieve the proposed system, the system's requirements were elicited based on the observation technique of requirements elicitation [154]. We carefully observed several current systems that were deployed in the healthcare environment, patients' dissatisfactions and research gaps in the literature. The requirements were essential because they served as a guide for establishing the system's functions and constraints, as well as the important components for the system to perform properly and accomplish its intended purpose to meet the objectives of this research.

4.2.2 Requirements specification

This subsection presents the requirements of the proposed system: FR and NFR. Requirements specification is the process of specifying system and user requirements [154]. These requirements must be clear, comprehensive, easy to understand and implementable. In the context of this research, FR and NFR were clearly stated since FR is the services that the system provides and how the system reacts after a certain input while NFR is the constraints on the services or functions delivered and on the development process [154]. This stage of the research was very critical because it is linked to the quality of the system and provided an in-depth understanding of users' needs to develop the proposed system that meets the research objectives. The core FRs and NFRs are presented in Figures 4.1 and 4.2 respectively.

Table 4.1: System FR

Functional Requirements:
FR1: The system shall allow valid users to register and have access to the system
FR1.1: The system shall create access tokens for each valid user to access the system
FR2: The system shall be able to generate a unique password for each user
FR3: The system shall generate a unique smart contract Id for each user
FR4: The system shall generate a QR Code
FR5: The system shall verify and validate registered users using QR-code

Table 4.2: System NFR

Non-Functional Requirements:
NFR1: The system shall be blockchain-enabled to enhance the privacy of patients using smart contract
NFR2: The system shall allow the collected patients' data to be encrypted and decrypted to enhance the security
NFR2.1: The user password shall be encrypted using the argon2 hash algorithm
NRF3: The access token shall be refreshed every 15 minutes.
NRF4: The system shall be available with 2 seconds of downtime.
NRF5: The system shall respond to user requests within a maximum of 2 seconds, a minimum of 3 seconds NRF6: The successful transaction submission to the blockchain shall happen within 0.5 seconds

4.2.3 System modelling

System modelling involves the creation of system models considered abstract with each model offering a unique perspective of the system [154]. In other words, it involves modelling the system using a graphical notation utilizing the Unified Modeling Language (UML) [154]. In the context of this research, we considered system modelling to be a crucial stage because it helped to model the requirements of the system and make it understandable from the research objectives' point of view as well as implementation perspectives. By using the use cases, actors, roles and other models, we demonstrated the system's many features and how the users interact with them as well as how they interact with system components based on their various roles. Moreover, it helped to reveal any limitations of the proposed system and in addressing them quickly before entering the next development phase.

A. Use a case diagram

Use cases constitute an abstract representation of events that may occur and impact the system, and they describe the system's behaviour in such instances [154]. This model assisted in defining the interaction of external entities or actors with the system. Therefore, in this research, the actors are system entities that may be internal or external to the system and interact with it. For the proposed system, the actors include the patients, registration, verification authorities, etc. who interact with the system to perform a task. This is presented in Figure 4.1

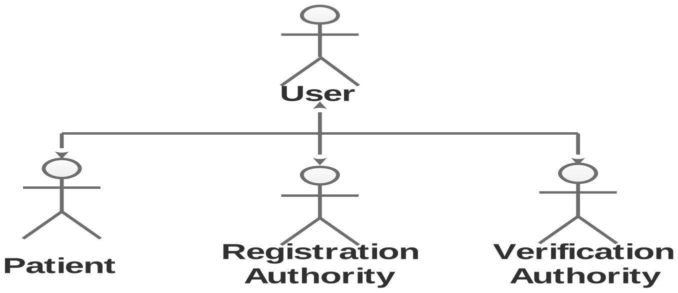


Figure 4.1: System actors

On the other hand, roles are the various tasks performed by each system's actors. Figure 4.2 presents a summary of the role of the actors in the proposed system.

Table 4.3: System actors' roles

Registration Authority	Patient	Verification Authority
- Register patients in the system - Invoked smart contract to store patients' information.	- Log in - Request, View, Download Certificate	- Verifies the certificate on the blockchain network using a QR code

Moreover, Figure 4.2 presents the system use case model which depicts the system's actors, use cases, and potential interactions.

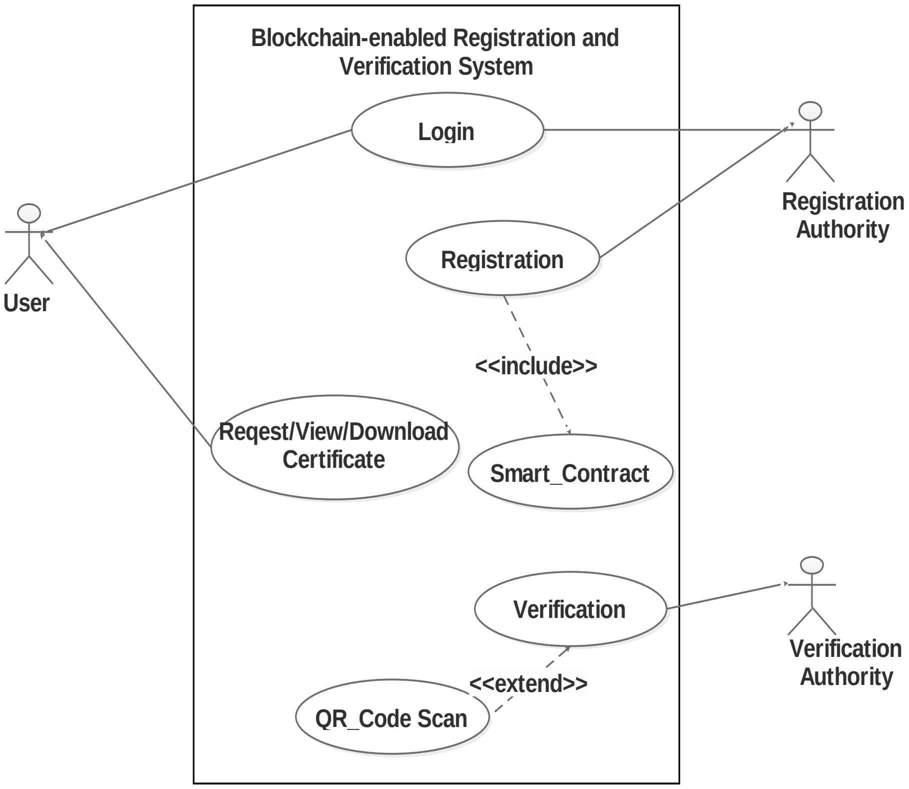


Figure 4.2: System use case model

4.2.4. Use case description

This subsection gives an analysis, or the use case description of the use case model presented in Figure 4.2. as presented, Table 4.4 describes the login use case, Table 4.5 describes registration, Table 4.6 describes the smart contract operation, Table 4.7 describes the patient request to view their certificate, and verification activity is shown in Table 4.8.

Table 4.4: System Login

Use Case Name	Login
Actor	User, Registering Authority, Verification Authority
Description	The user logs in to the system
Preconditions	The users should have valid login details
Postcondition	Access Granted
Normal Flow	1. To have access to the system, The registration authority must log in first. 2. For successful log-in (Patient), A page with an option to request a certificate is shown. 3. For a successful log-in (Verifier), A page with an option to scan the certificate will be displayed
Alternative Flow	1. Users enter login details. 2. The system will validate the user credentials entered. 3. No access is granted
Exceptions	The user entered the wrong email address or Passcode

Table 4.5: Patient Registration

Use Case Name	Registration
Actor	Registration Authority
Description	The user/patient is registered into the system
Preconditions	Unique Smart Contract Address ID assigned
Postcondition	Patient registered Successfully
Normal Flow	1. The Registration Authority enters the patient’s details. 2. The system verifies the unique smart contract ID. 3. The data is saved on the smart contract. 4. A vaccination hash is generated
Alternative Flow	1. The Registration Authority enters the patient’s details. 2. The system validates the smart contract's unique ID and account address. 3. Validation of the smart contract and account address fails, and the session is discarded
Exceptions	Invalid unique smart contract ID

Table 4.6: Deploying of smart contract

Use Case Name	Smart_Contract
Actor	Registration Authority
Description	The smart contract is deployed by the administrator to the blockchain network.
Preconditions	Registration Authority must be authorized and registered by relevant authorities
Postcondition	The smart contract is successfully deployed to the blockchain and the smart contract address in the blockchain is received
Normal Flow	1. The registration authority deploys the smart contract. 2. Checks whether the blockchain node is running. 3. If the node is running, the smart contract will be deployed, and the smart contract address will be assigned.
Alternative Flow	1. The registration authority deploys the smart contract. 2. The blockchain node not running. 3. Smart Contract will not be deployed
Exceptions	Not applicable

Table 4.7: Request/View Certificate

Use Case Name	Patient Request/View_ Certificate
Actor	Patient
Description	Users request the certificate
Preconditions	Patient Should Be Logged In
Postcondition	Access was granted for viewing the certificate
Normal Flow	1. After logging in the patient will enter their unique smart contract ID. 2. The system will validate if the unique smart contract ID exists in the smart contract. 3. The system will generate the QR Code based on the unique smart contract ID. 4. The system will allow the user to download the QR code.
Alternative Flow	1. After logging in the patient will enter their unique smart contract ID 2. The system will validate if the unique smart contract ID exists in the smart contract and blockchain network. 3. A unique smart contract ID does not exist. 4. No QR code generated
Exceptions	The user entered a wrong unique smart contract ID

Table 4.8: Verification

Use Case Name	Verification
Actor	Verification Authority
Description	Allows the certificate to be verified
Preconditions	Vaccination data must be stored on the smart contract
Postcondition	Certificate details on the blockchain
Normal Flow	1. The verification authority scans the QR Code. 2. The system searches the blockchain network for the for-patient vaccination details. 3. The system validates the QR code. 4. Details of registration are provided.
Alternative Flow	1. The verification authority scans the QR Code. 2. The system searches the blockchain network for patient vaccination details. 3. The system validates the QR Code. 4. No details will be provided.
Exceptions	Not applicable

4.2.5 Sequence of operations

Figure 4.3 presents the sequence of the suggested system using the sequence diagram. In this research context, we employed this model to show how the several actors in the proposed system interact with each other and other components to achieve the objective of the research.

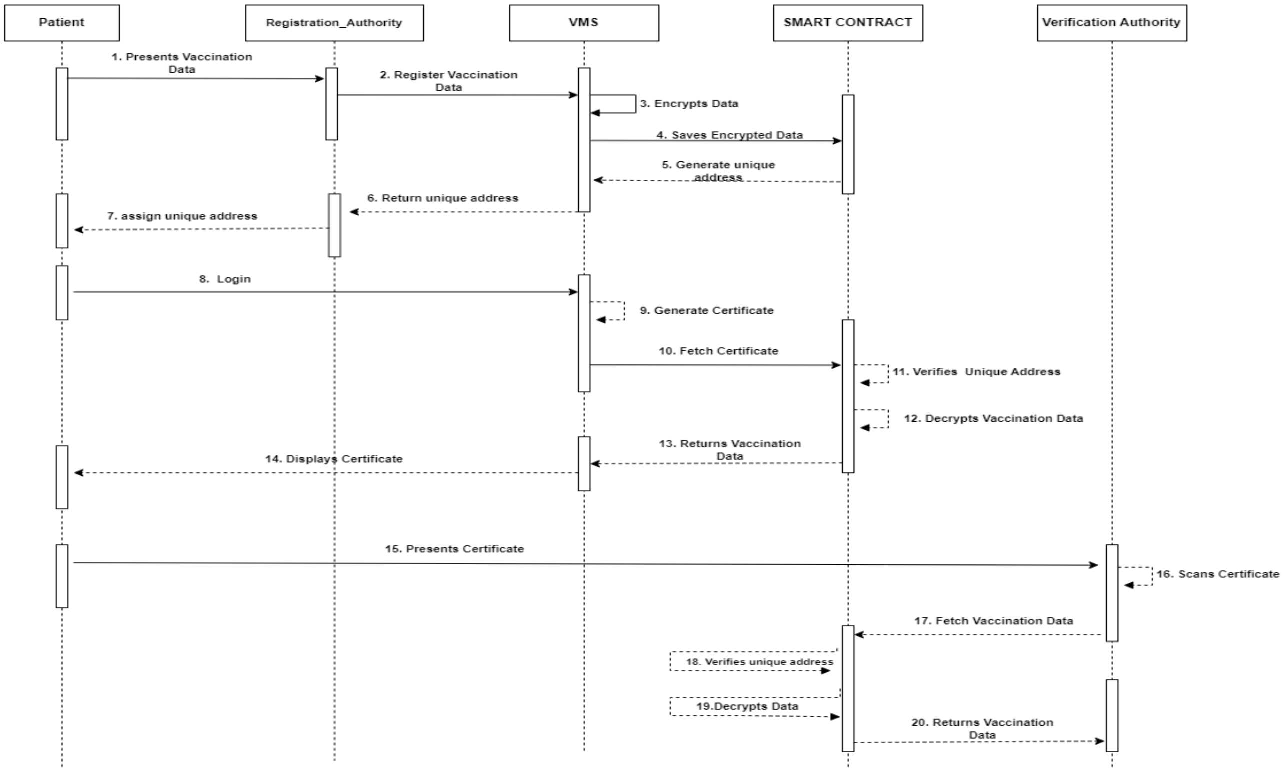


Figure 4.3: Blockchain registration and verification system process

As shown in Figure 4.3, the patient presents their vaccination details to the registration authority, who then logs in to the VMS and registers the patient's vaccination details. The VMS then encrypts the data and saves it to the smart contract, which is deployed on the blockchain network; then, a unique smart contract address is returned to the registration authority, which will assign it to the patient. A successful registration indicates that the patient is now part of the system and can log in and view their certificate. On the other hand, the verification authority is responsible for verifying the certificate's authenticity; the verification authority scans the QR code and validates it in the blockchain to check if the patient has been vaccinated. If the patient exists and is vaccinated, the important details will be retrieved from the blockchain network and displayed to the verification authority.

4.3 System Design

Software design is the critical stage of development immediately after the requirements have been collected and analyzed. Software design is the inventive process of determining which program components perform which functions [154]. Therefore, this section describes how the different software components together with their connections make the system produce the desired results. We presented our system design using the system architecture, components and algorithms.

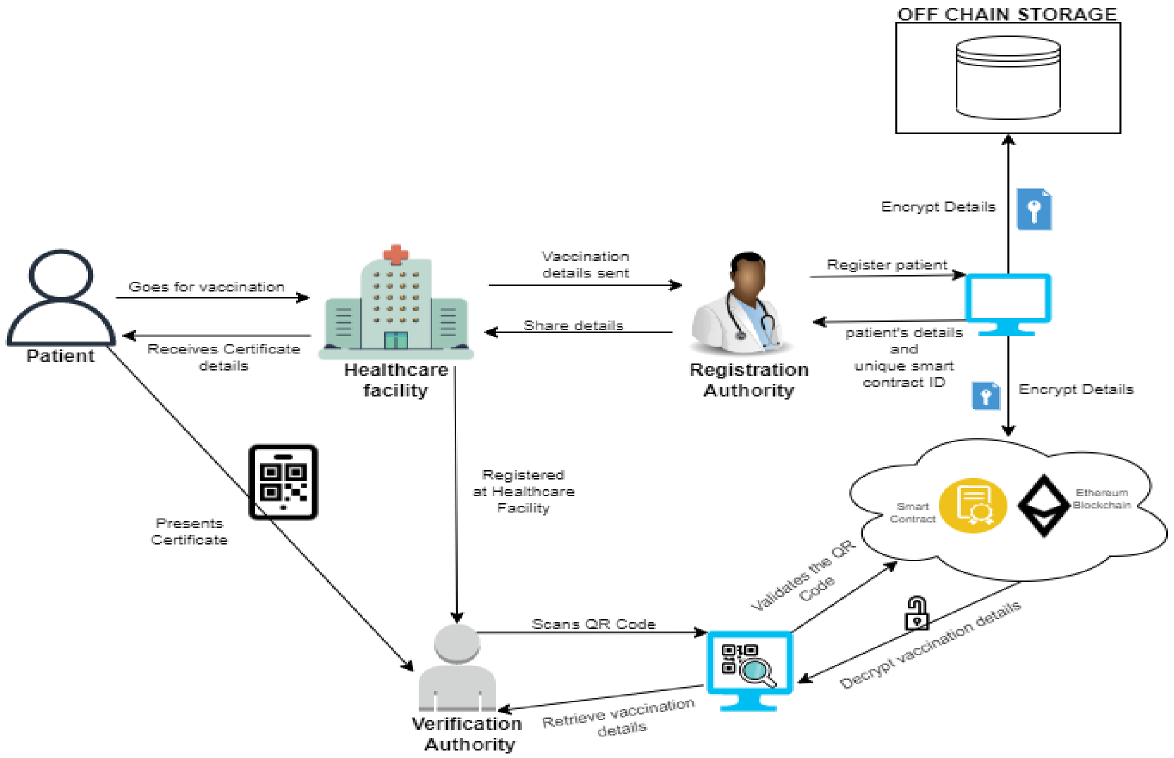


Figure 4.4: System architecture

4.3.1 System architecture

In the context of this research, system architecture presents the system's structure, components, and relationships among the components in the operating environment. It demonstrates the system's design under which it will meet its functional and non-functional requirements [154]. Figure 4.4 shows the proposed system architecture, illustrating each component as well as how it interacts with the others to accomplish the system's primary objective. Moreover, as shown in Figure 4.4, the smart contract shows the suggested way of securely storing the information on the blockchain network. Once the data is saved on the blockchain all other parties such as patients and verifiers can access it more securely. Blockchain technology is known for features such as data integrity, immutability, transparency, and availability. These features are implemented in the architecture shown in Figure 4.4.

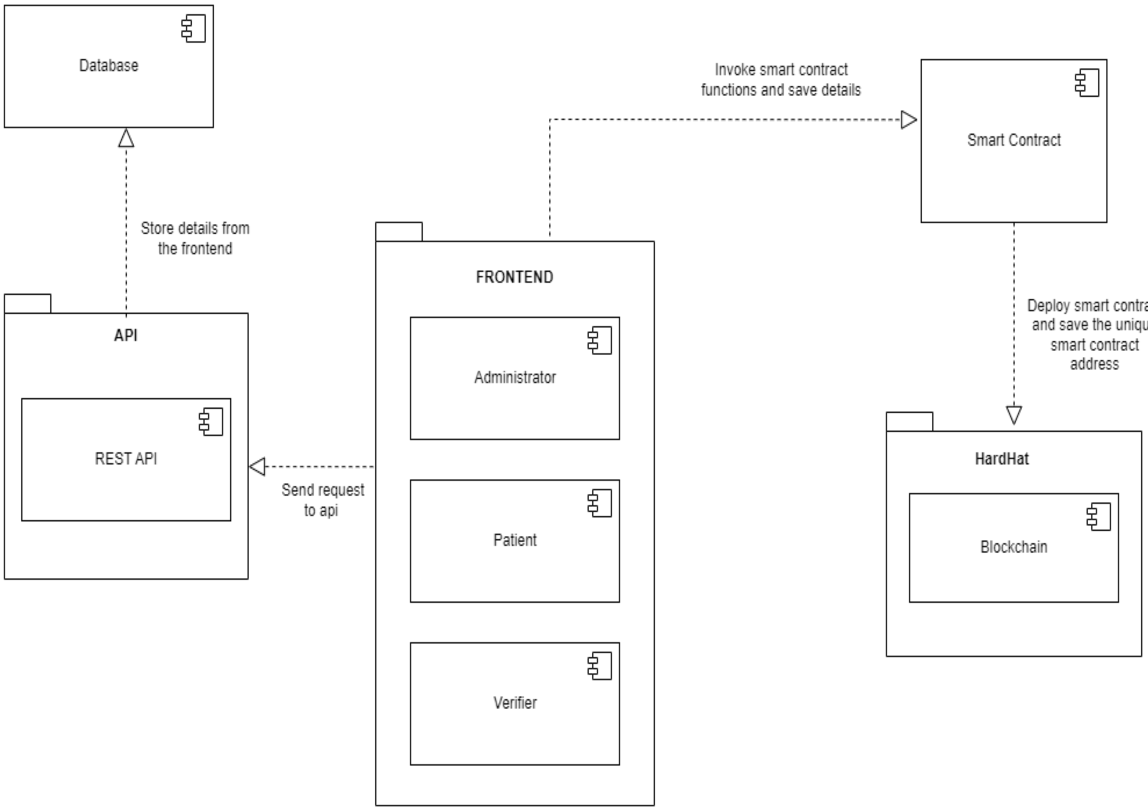

Database
Invoke smart contract functions and save details
Smart Contract
Store details from the frontend
FRONTEND
Administrator
Deploy smart contract and save the unique smart contract address
API
REST API
Send request to api
Patient
HardHat
Blockchain
Verifier

Figure 4.5: Proposed system component

4.3.2 System Component Design

Based on the system architecture presented in Figure 4.4, this subsection presents and describes the various identified components and sub-components used for designing and implementing the proposed system. This is presented in Figure 4.5.

4.3.2.1 Frontend

The components at the front end of the proposed system include:
Vaccine Administrator interface: This is the user interface that permits the administrator to enter each patient’s details and register the patient to the blockchain system. This is important because for the details to be reliable and trustworthy, there must be authorized personnel who are responsible for registering the patients.
Patient interface: This is the user interface responsible for the patient login and requests to view their certificate.

Verifier interface: To achieve verification, this user interface allows the verifier to scan the QR Code to confirm if the patient does exist in the blockchain system or not.

4.3.2.2 The Smart Contract

In the suggested system, the smart contract contributes significantly to its success. To achieve the objectives and aim of this study, secure and decentralized storage was proposed and required to store and retrieve patients' information efficiently. Due to the involvement of sensitive healthcare and personal data, unlike the existing systems, there is a need to ensure that the information is kept confidential, unchangeable and cannot be tampered with by third parties. To achieve this, we used a smart contract for the development based on the solidity programming language. The smart contract class diagram is shown in Figure 4.6.

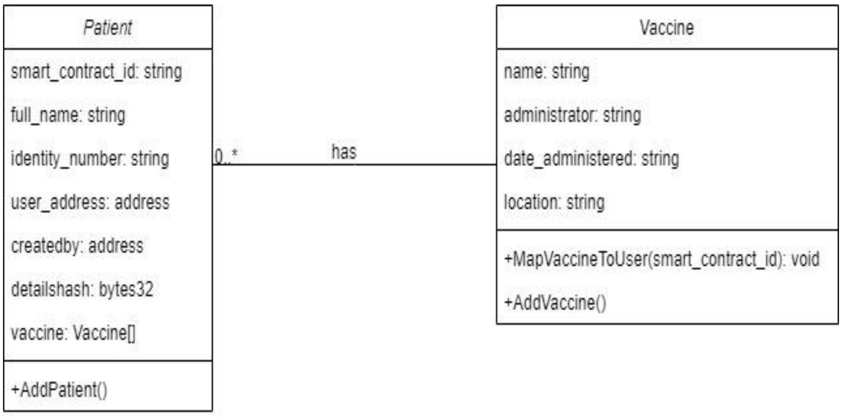


Figure 4.6: Smart contract class diagram

4.3.2.3 HardHat

To ensure effectiveness, we created a component that utilizes the Hardhat library, an Ethereum blockchain development environment. It can execute smart contracts written in solidity and allow the deployment, testing and debugging of solidity-based smart contracts without the need for a live environment. Hardhat can also be integrated with other applications and tools. Moreover, the command for running a hardhat node or server on a local machine is npx hardhat node, and to compile the smart contract, we used npx hardhat compile, while npx hardhat run scripts/sample-script.js --network localhost was used to deploy the smart contract to an address.

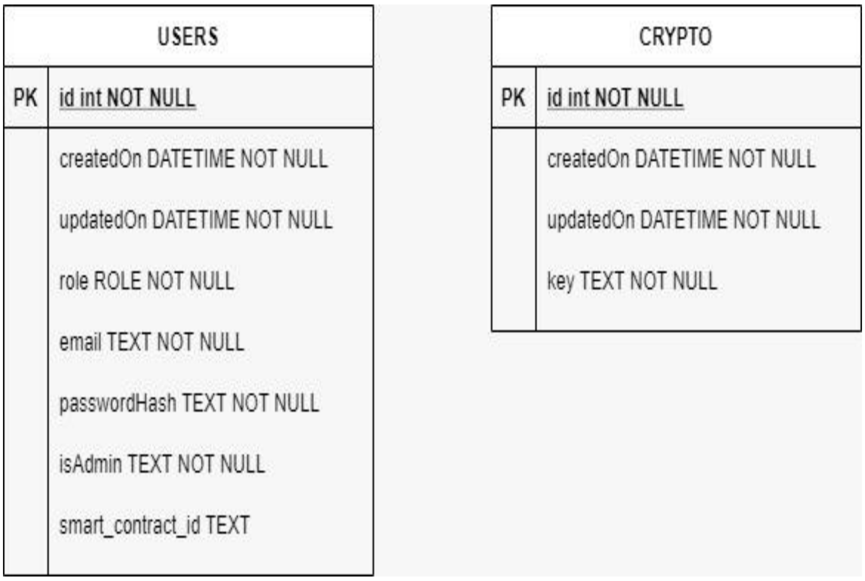
4.3.2.4 Application Programming Interface

Also, a RESTful Web Application Programming Interface (API) was used in this study to save login details to the database. This was used to minimize the high cost involved when a patient logs into the proposed system. The API is a kind of architectural design for an API that makes use of HTTP requests to access and utilise data. A request can be a GET, POST, DELETE, PATCH, or PUT which represents CRUD operation.

4.3.2.5 Database design

The database of the proposed system made use of an Object Relational Mapping (ORM) tool to map classes or models created using a language of choice by the developer such as JavaScript, C#, etc. The use of ORM in this study simplified the work of the development especially when a change in the class property structure of OOPLs occurs that requires an update of the virtual database.

In the context of the proposed system, the ORM is used in Prisma. Prisma provided us with a query builder which is auto-generated from the schema. Prisma has a hassle-free migration feature that automatically generates SQL database migrations that is customizable with a command as follows: *npx Prisma migrates* [155]. The *Prisma db push* allowed us to make changes to their databases without a need for generating migration files. This is shown in Figure 4.7.



USERS	
PK	id int NOT NULL
	createdOn DATETIME NOT NULL updatedOn DATETIME NOT NULL role ROLE NOT NULL email TEXT NOT NULL passwordHash TEXT NOT NULL isAdmin TEXT NOT NULL smart_contract_id TEXT

CRYPTO	
PK	id int NOT NULL
	createdOn DATETIME NOT NULL updatedOn DATETIME NOT NULL key TEXT NOT NULL

Figure 4.7: Class diagram for the database

4.3.3 Algorithm Design

This subsection describes the algorithm design of the various operations performed in the proposed system from the time that the patient is registered then encryption of the data, storing of the encrypted data on the smart contract deployed on the blockchain and database (off-chain), and how the user logs in to view their certificate and finally the algorithm for verification of the certificate.

4.3.3.1 Registration process

In this activity, a patient and their vaccination details are added to the system. Figure 4.8 present the algorithm for the activity. As shown in Figures 4.8 and 4.9, the **registration_authority** is the only entity authorized to register and add vaccine details about the vaccinated patient. Once the initial registration is done, the information or transaction is then updated on the smart contract deployed on the blockchain. In this case, the blockchain node will securely save the information for future usage or verification by appropriate authorities.

Algorithm 1: Registration of patient and vaccine details

Input: *unique smart contract ID, names, id number, vaccination date, vaccination administrator, vaccination location, vaccination name*

Output: *Transaction status object with a success message*

Steps:

1. Send a notification to metamask on the front end to give access to the application.
2. If the browser has no metamask installed, log the error on the browser console.
3. If metamask is installed, request to log into the account.
4. Give ethers and web3 library the Ethereum address from metamask.
5. Fill out the form on the frontend.
6. Use the deployed smart contract address to make a connection to the node using hardhat (blockchain on the localhost).
7. Make a call request to add the patient and vaccination details to the smart contract.
8. Ask the administrator to reject or confirm a transaction call.
9. If the administrator rejects the transaction, send a transaction fail status to metamask.
10. If the administrator confirms the transaction, add it to the smart contract.
11. Send a notification about the transaction with the transaction object containing block details.

Figure 4.8: Algorithm for patient registration

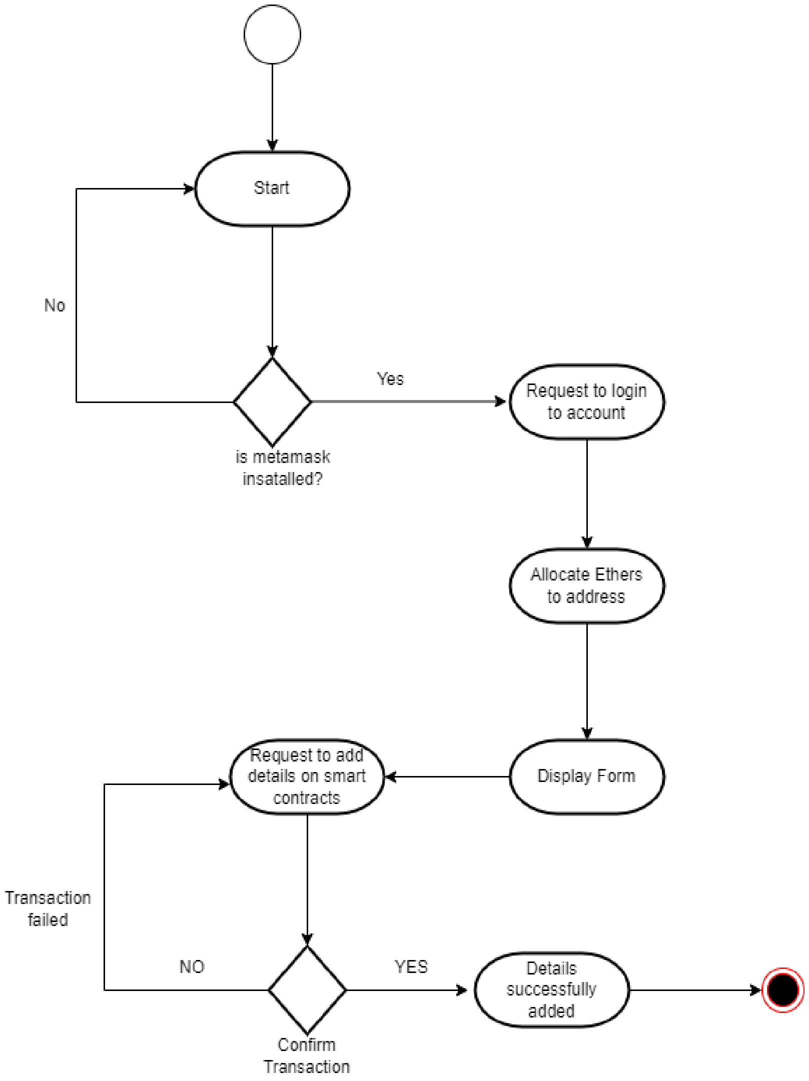

Start
No
Yes
Request to login to account
is metamask insatalled?
Allocate Ethers to address
Display Form
Request to add details on smart contracts
Transaction failed
NO
YES
Details successfully added
Confirm Transaction

Figure 4.9: Activity diagram representing the registration process

4.3.3.2 QR Code creation

In the proposed system, once a patient is registered to the system, a QR code must be created with a certificate for onward verification of authenticity. The algorithm for this activity is shown in Figure 4.10. In this case, a user or patient must be logged into the system using valid credentials created. Once access is granted, the patient or user must request a vaccination or registration certificate. Then by entering the unique smart contract ID the system will check if the smart contract ID exists. If it does, the QR-Code is then created returning the vaccination hash embedded in the QR-Code which is ready for download by the user. The description of the algorithm is shown in Figures 4.10 and 4.11.

Algorithm 2: Generating QR Code

Input: *Unique smart contract ID*

Output: *QR code*

Steps:

1. Check if the user has logged in.
2. If the user is not logged in, redirect the user to the login page.
3. Show the username on a certificate home.
4. Allow the user to enter their unique smart contract ID number.
5. Initiate a method call to the smart contract in the hardhat node (local blockchain).
6. Check if the unique smart contract id exists for any of the stored patients.
7. If the patient is not found, log the error on the node and browser console and alert the user on the browser page.
8. If the user is found, get the vaccination hash.
9. Generate the QR code.
10. Allow the user to download the generated image for future purposes.

Figure 4.10: Algorithm for QR-code generation

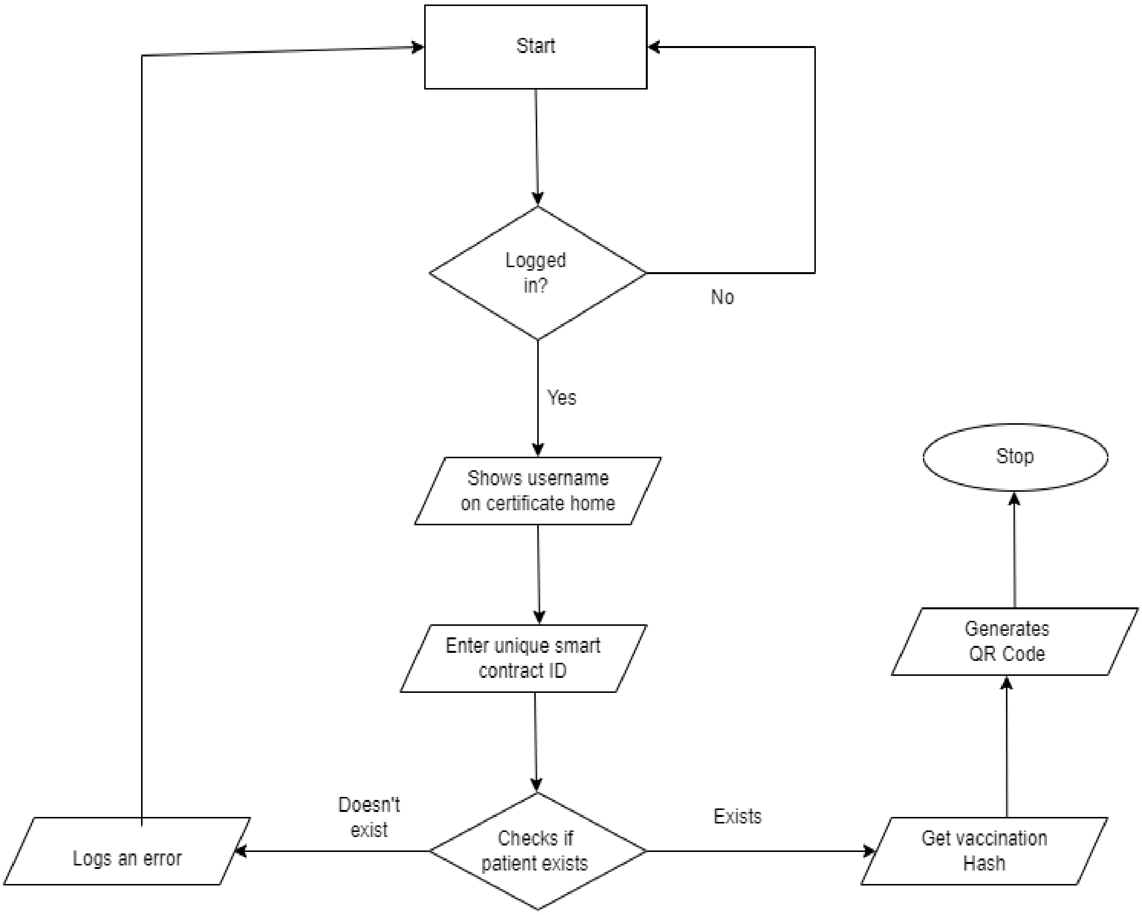


Figure 4.11: Flowchart representation of QR-code generation

4.3.3.3 Certificate verification

The verification of the certificate is an important aspect of the proposed system to ensure that the user is authentic. Figures 4.12 and 4.13 present the algorithmic process. To this end, the **verification_authority** must first log in to the system and request the use of a camera. Once permission is granted, the QR-Code on the certificate will be scanned using the camera. The extracted data stored in the QR code will then be converted into a string and saved into a local variable. Once that is done, a call to the smart contract will be initiated and the vaccination hash will be requested to get the stored data from the smart contract. If data is not available, it will log an error message indicating the QR Code is fake. But if the data is found, it will return all essential information of the user and the vaccination stored on the smart contract.

Algorithm 3: Vaccination certificate verification

Input: *QR code image*

Output: *Vaccine hash and user details*

Steps:

1. The verification authority must first log in.
2. Request camera use permission.
3. If web camera permission is not granted or the camera is not available, log the error.
4. Otherwise, scan the QR code image using the device's webcam.
5. Convert the data to a string and save it in a local variable.
6. Check if Metamask is connected and save the Ethereum account address of the verifier.
7. If the metamask is not connected, log the error.
8. Use the information to make a smart contract call from the front end.
9. Request for the vaccination hash.
10. Use the data from the QR code to get public user information.
11. If patient details are not found on the blockchain, then the QR code is fake, as data cannot be deleted once stored in the blockchain.
12. Alert the frontend that the node failed to retrieve the data since it does not exist.
13. Log the error on the node console.
14. Otherwise, print the user vaccination details as verification proof that the patient was vaccinated and the QR code is valid.

Figure 4.12: Algorithm for certification verification

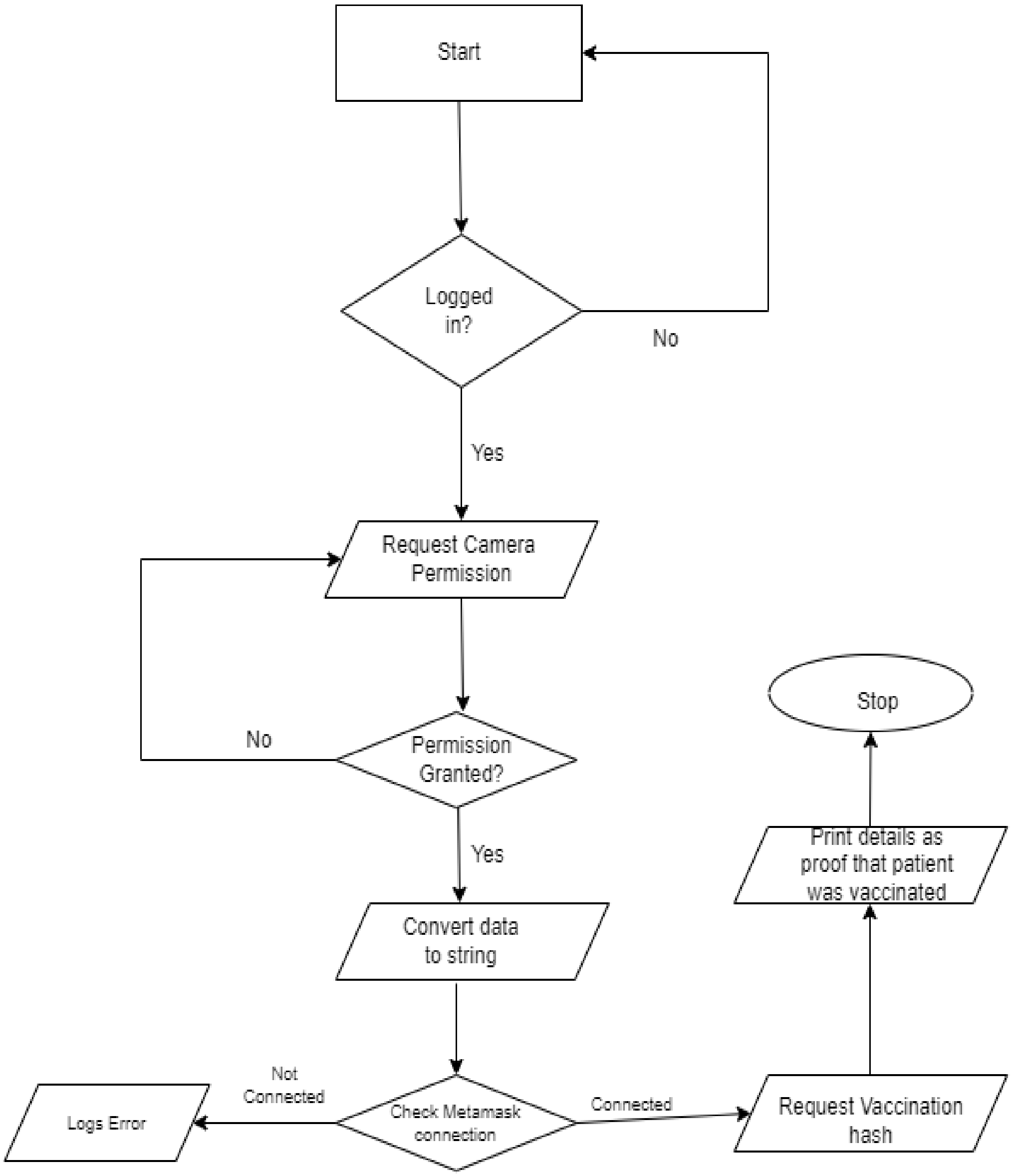


Figure 4.13: Flowchart representation of certificate verification

4.3.3.4 Smart contracts deployment

The blockchain-based smart contract is the core technology used in this proposed system to ensure transparency, integrity, confidentiality, privacy, immutability, etc. of patients' healthcare records. We employed a smart contract to store the sensitive data of patients. The algorithm of the activities involved is shown in Figures 4.14 and 4.15. Thus, for the smart contract to be deployed successfully the blockchain node must be running. When we want to compile the smart contract, we use the hardhat command. This causes the smart contract's API and bytecode to be generated. The compiler will then check if the contract is written properly, if there are any errors, it will throw an exception. If no errors are found, it executes the hardhat command to invoke the smart contract and generate an address that is returned to the console.

Algorithm 4: Smart Contract Deployment

Input: *Solidity smart contract file*

Output: *Smart contract address*

Steps:

1. Run hardhat node command: *npx hardhat node* to start the node server on a local host.
2. Run a hardhat command to compile the smart contract and generate the API and bytecode of the smart contract.
3. Check if the contract is properly written.
4. If the contract fails to compile throw an error.
5. Run a hardhat command to deploy the smart contract and generate an address.
6. Return the address to the console.

Figure 4.14: Algorithm for smart contracts deployment

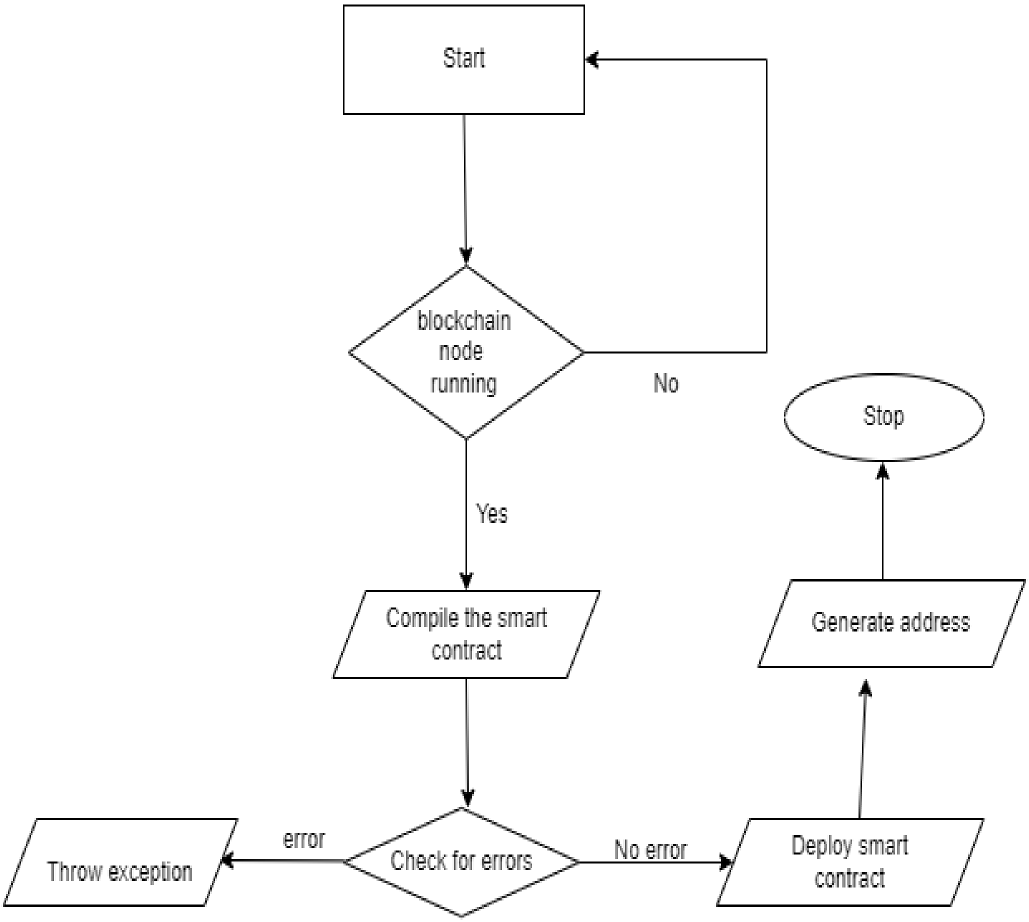
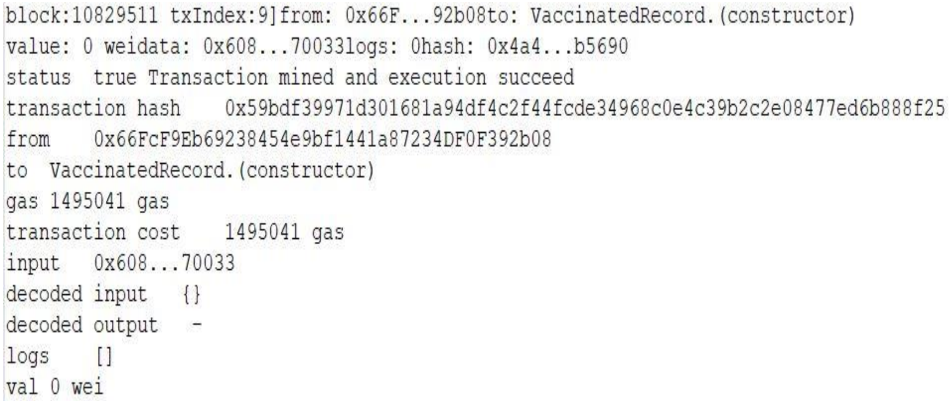


Figure 4.15: Algorithm to deploy smart contract



```
block:10829511 txIndex:9]from: 0x66F...92b08to: VaccinatedRecord.(constructor)
value: 0 weidata: 0x608...70033logs: 0hash: 0x4a4...b5690
status  true Transaction mined and execution succeed
transaction hash    0x59bdf39971d301681a94df4c2f44fcde34968c0e4c39b2c2e08477ed6b888f25
from    0x66FcF9Eb69238454e9bf1441a87234DF0F392b08
to  VaccinatedRecord.(constructor)
gas 1495041 gas
transaction cost    1495041 gas
input   0x608...70033
decoded input   {}
decoded output   -
logs    []
val 0 wei
```

Figure 4.16: Successful deployed smart contract

4.3.3.5 Database generation

Figure 4.17 and 4.18 represents the algorithm and flowchart for database generation in the proposed system. To achieve this, the Docker-compose.yml file must be available as input to create the docker container on the API project. Once done, the Prisma will be initialized in the API project and establish a connection to the database URL. The Prisma is then used to handle migrations and apply the migration to the database as well as push data if necessary. Finally, a running docker instance with a database on the desired port will be returned.

Algorithm 5: Database generation

Input: *Docker-compose.yml file*

Output: *Docker container with database image running*

Steps:

1. Create a Docker container using the Docker-compose.yml file on the API project.
2. Initialize Prisma in the API project and connect to the database URL.
3. Use Prisma to create migration for the models in the Prisma schema.
4. Apply the migration to the database and push data if necessary.
5. Return a running docker instance with a database on the desired port as per the docker-compose.yml configuration.

Figure 4.17: Algorithm for database generation

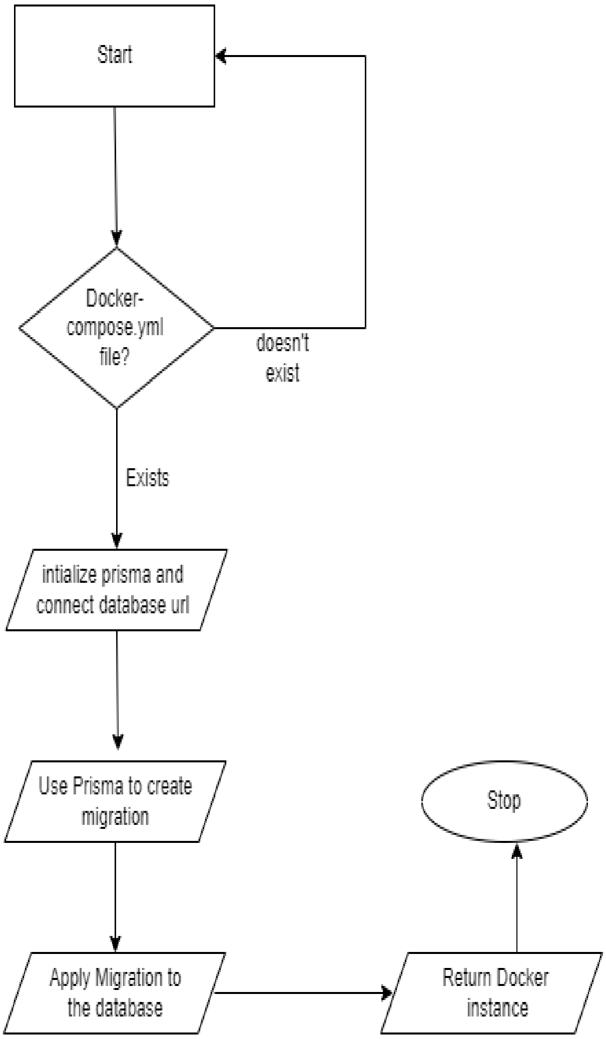

Start
Docker-compose.yml file?
doesn't exist
Exists
intialize prisma and connect database url
Use Prisma to create migration
Stop
Apply Migration to the database
Return Docker instance

Figure 4.18: Algorithm showing database generation

4.3.3.6 Symmetric data encryption and decryption

This study is focused on issues of privacy and security. Our priority was to ensure that patients' personal and healthcare information is always protected. Therefore, to enhance the security of the data, single-key encryption is used, and it is described in the algorithm in Figures 4.19 and 4.20. The **registration_authority** is required to log in and an access token will be created to make a post request to the API. The validity of the token will then be checked. If it is not valid, access will be denied and if it is valid, a 128-bit key will be generated and stored on the database and the plaintext will be encrypted using the generated key. Finally, a JSON object will be returned with a ciphertext.

Algorithm 6: Data Encryption

Input: *JSON object with patient plaintext data*

Output: *JSON object with ciphertext*

Steps:

1. Log in as a Registration_Authority.
2. Use the access token to make a post request to the API.
3. Check if the token is valid, if it is not valid deny access and throw an unauthorized HTTP exception.
4. If the token is valid, check for the user role, if it is not an admin denies access.
5. Generate a 128-bit key and store it in a database.
6. Encrypt the plaintext using the key.
7. Return a JSON object with ciphertext.

Figure 4.19: Algorithm for the data encryption process

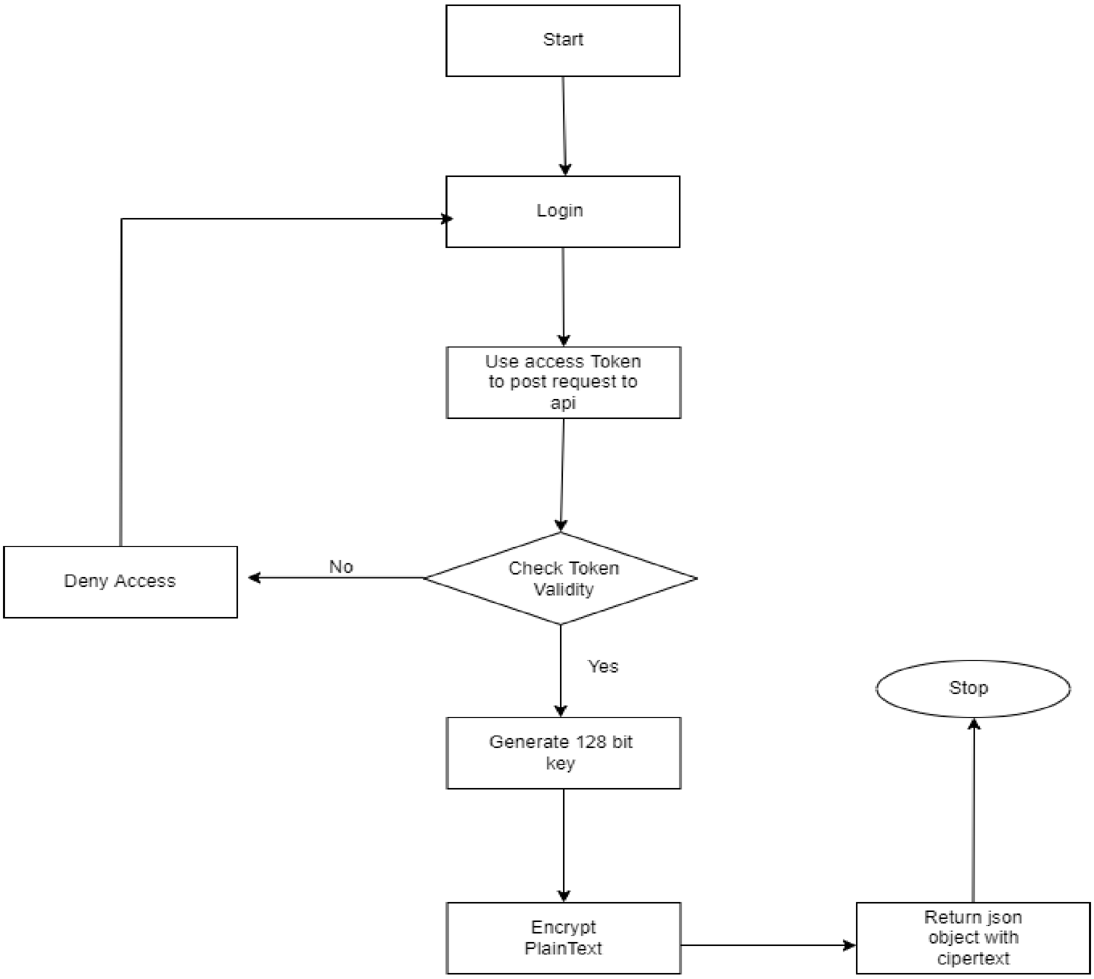


Figure 4.20: Flowchart representation of the data encryption process

Moreover, to decrypt the encrypted data, the **verification_authority** is the only entity with such responsibility. The algorithm involved in decrypting the encrypted data is presented in

Figures 4.21 and 4.22. In this case, the **verification_authority** must log in to the system and the authenticity and user role will be checked. If not a valid **verification_authority**, access will be denied, otherwise, access will be granted, and the 128-bit key will be used to decrypt the data and finally, the JSON object will be returned as plaintext.

Algorithm 7: Data Decryption

Input: *JSON with cipher text*

Output: *JSON with plaintext*

Steps:

1. Log in as verification_authority.
2. Check the authenticity and user role with an access token.
3. If the user is not known by the system or the role is not of a verification authority, deny access and throw an unauthorized HTTP exception.
4. Fetch the decryption key which is 128-bit.
5. Decrypt the data.
6. Return a JSON as plaintext.

Figure 4.21: Algorithm for data decryption

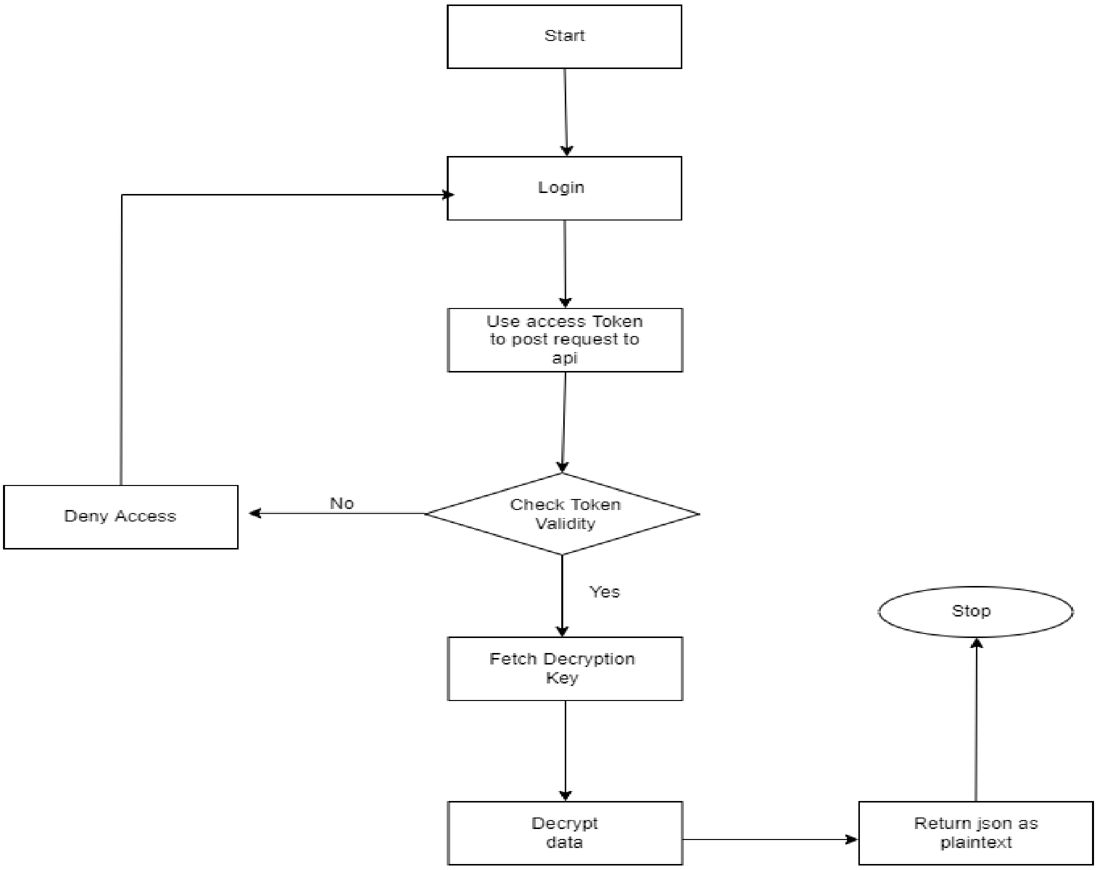


Figure 4.22: Flowchart representation of data decryption

4.4 Privacy and Security Design

4.4.1 Hashing algorithm

In terms of security, the system uses the argon2 algorithm [156]for password hashing which is generated automatically upon registration of the patient and thus reduces the chances of illegal logging into the system. Also, during the patient registration procedure, the system will produce a unique smart contract ID, which will be saved on the smart contract with the patient information to prevent the issuance of fake certificates. The unique smart contract ID will also be used to also generate the QR Code to verify that the patient is registered and vaccinated.

After registration, symmetric encryption is used to encrypt the data where both the registration authority and verification authority have the same key. The encryption was implemented using access tokens. This encryption minimizes the man-in-the-middle attacks and replays as the tokens are time-based and the information being transmitted is encrypted. Once the time session is finished a new token will be generated and sent to the API.

Argon 2 Hashing Algorithm:

Input: *Message string P*

Output: *string T bytes long*

Steps:

```
if T <= 64
        F'^T(B) = F^T(LE32(T)||B)
    else
        r = ceil(T/32)-2
        C_1 = F^(64)(LE32(T)||B)
        C_2 = F^(64)(C_1)
        ...
        C_r = F^(64)(V_{r-1})
        C_{r+1} = H^(T-32*r)(V_{r})
        F'^T(X) = W_1 || W_2 || ... || W_r || C_{r+1}
```

Figure 4.23: Argon2 Hash algorithm

4.4.2 Proof-of-Stake algorithm

The proposed solution employed the Ethereum local network which allows the development and testing of decentralized applications. However, to achieve privacy and security, this study employed a PoS consensus algorithm [157] on the Ethereum local network. Figure 4.25 shows the PoS algorithm used on the VMS while Figure 4.26 shows its sequence of operation.

```
Proof of Stake
    Input: Data in form of a transaction
    Output: Data stored in form of a mined transaction
    1. Send transaction requests with the private key.
    2. Node adds new transactions on the meme pool.
    3. Mining node combines all transactions to form a block.
    4. The miner broadcasts the final block.
    5. New block is validated and executed.
    6. unfulfilled transactions are removed from the local meme pool.
    7. Each block is evaluated, and state checksums are performed.
```

Figure 4.25: pseudocode for proof of stake implementation

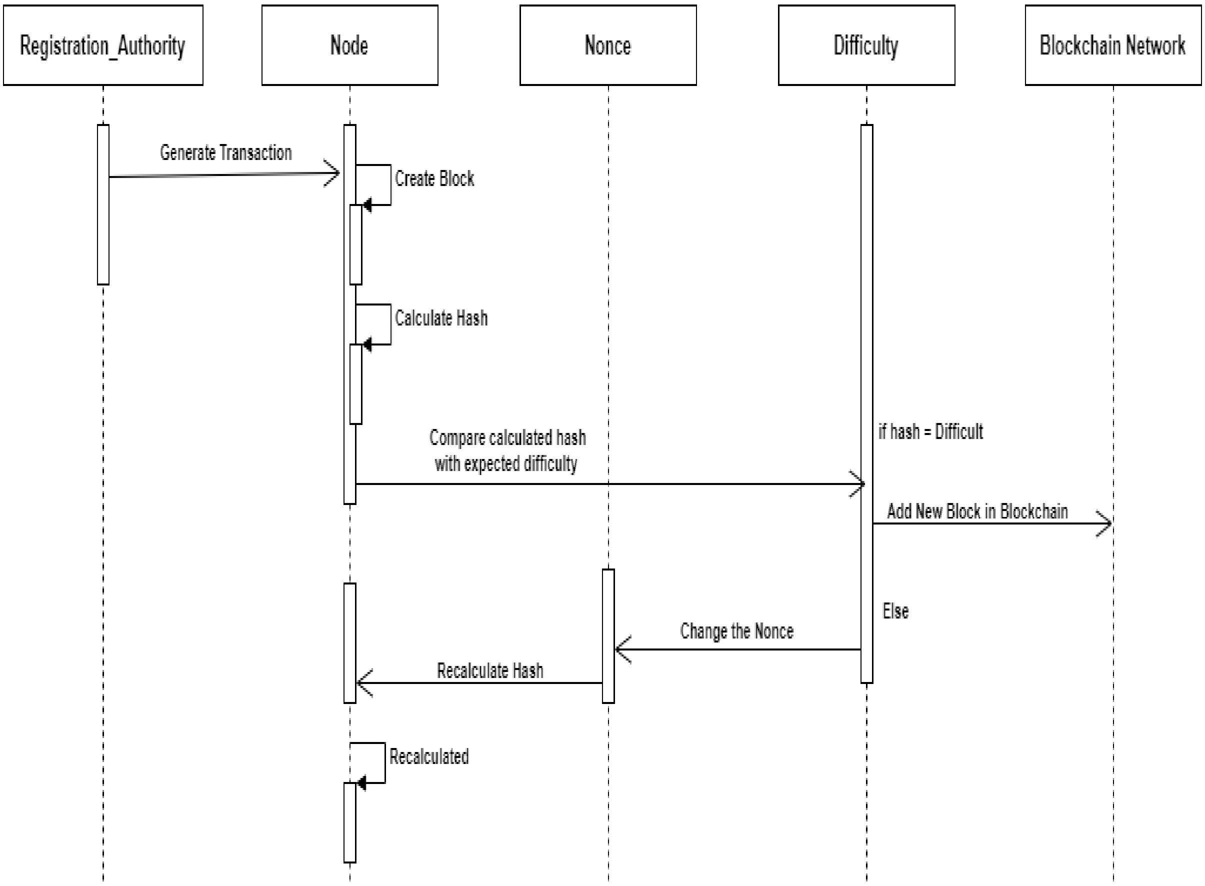


Figure 4.26: Proof of Stake operation in the system

Figure 4.26 demonstrates the operation of PoS in the system. To this end, the registration authority generates and sends the transaction to the node. The node performs further construction of the block, which also allocates a unique hash to each block. Next, the hash is compared to the anticipated difficulty. The block is added to the blockchain network if it meets the difficulty; otherwise, the nonce is modified, and new instructions are issued to recalculate the hash. The difficulty of the hash confers uniqueness and immutability on the data being recorded on the blockchain.

4.6 Chapter Summary

In this chapter, an analysis of the proposed system was provided outlining the system requirements, and the system design was performed to show how functions operate together with their components to achieve the objectives and the goal of the study.

Chapter 5

System Implementation and Results

5.1 Introduction

An overview of the proposed VMS's prototype implementation and the results thereof are presented in this section. The suggested VMS was designed in such a way that allows the registering authority to register the patient details, and then encrypt the data using symmetric encryption before saving it to the smart contract to protect the data. The data will then be saved securely on the smart contract where it will be accessed by a registered patient who will have to enter their credentials to gain access. After securely logging in, the patient will also be able to see and download their certificates. The system was also implemented in such a way that it allows for the verification of the certificate by just scanning the QR code generated by the system. Verification includes the decryption of the data. Various technologies such as ReactJs, MaterialUI, and CSS were used to design and style the interfaces.

In terms of blockchain and smart contract development, various libraries were used, such as Ethers and the web3 Library. These libraries were also discussed in this chapter. The implementation also consists of off-chain database storage which was developed using Prisma Studio. Moreover, an evaluation of the proposed VMS was done in this chapter using tools such as Apache Jmeter load testing tool and Hyperledger Caliper. The system was evaluated using parameters such as latency, throughput and response time. Lastly, a comparison with other current related systems was performed and the results were discussed.

5.1.1 Chapter Outline

The implementation of the proposed system is presented in this chapter, together with the results obtained and its evaluation. We provided screenshots depicting the system interfaces and the functionalities, simulation results and evaluation of the proposed system to make sure that the objectives of this research study were met. The basis of this chapter is to demonstrate the functionalities of the system and the operations of the implemented system.

5.2 Implementation

This section describes the system properties utilized to implement and execute the proposed system. To achieve the intended goal of the study several tools were used to build the system and the tools are categorized into a front end and back end.

5.2.1 System Properties

Table 5.1 Shows system properties that were used in implementing and conducting benchmark tests on the system.

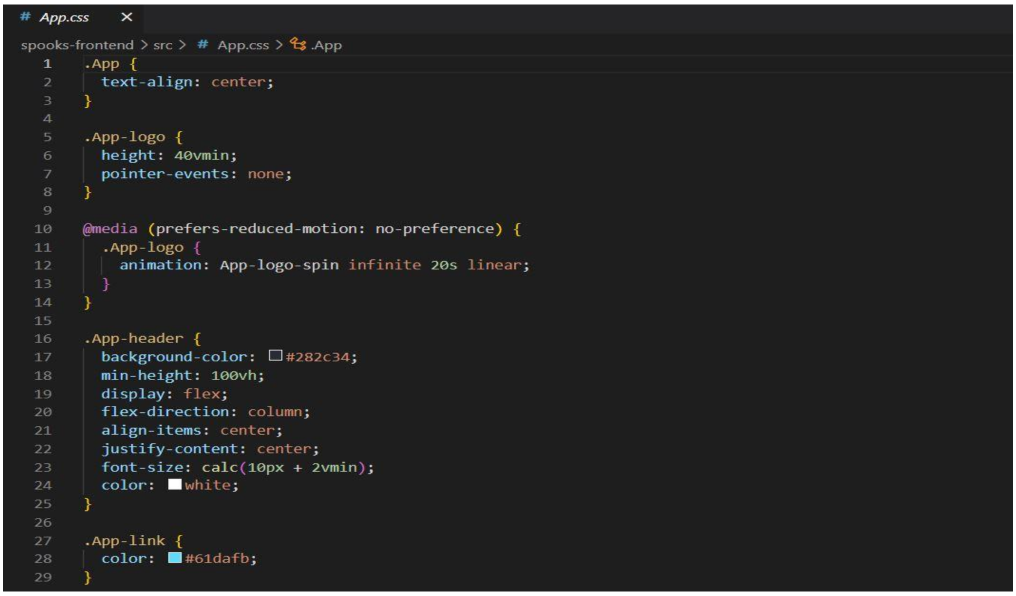
Table 5.1: System Properties

Parameter	Value
Software	Windows 10 Home, 64-bit operating system
	Apache-JMeter-5.4.3
	Hyperledger Caliper
Hardware	Hard Disk: 500GB
	RAM: 8GB
	Processor: Intel® Core ™ i5-8265U CPU @ 1.80 GHz

5.2.2 Front-end implementation

To implement the proposed system, the tools and technologies used at the front end are discussed in this subsection.

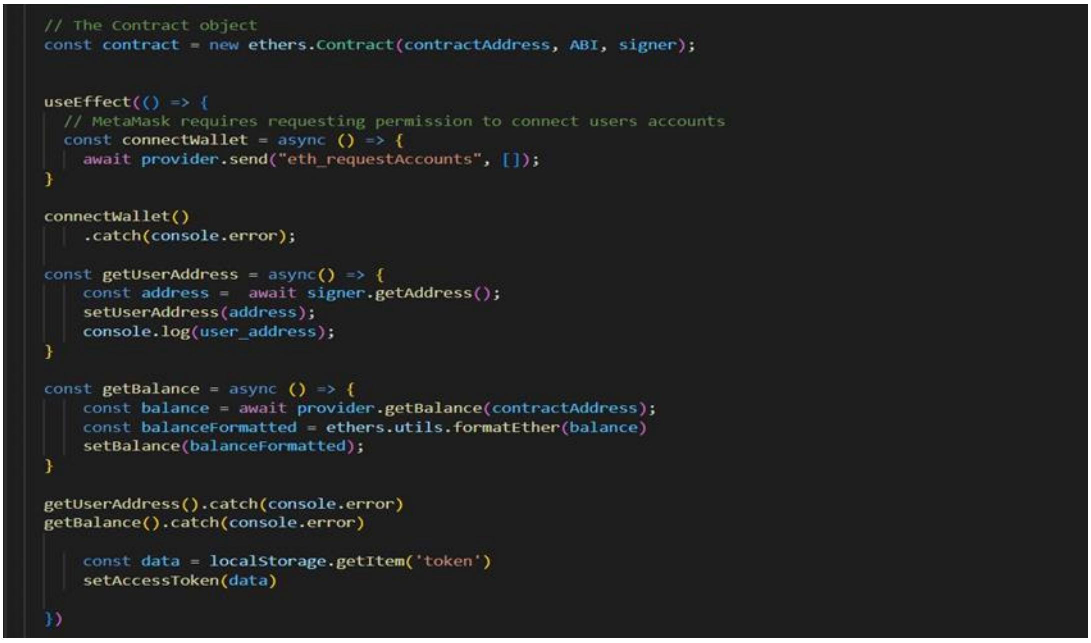
A. *ReactJs, Material UI and CSS:* React is an open-source and free JavaScript front-end framework for making user interfaces based on UI components. In this project, Reacts JavaScript was used to design the interface. To support Reactjs, we included the Material UI library to allow different in-built components to be imported as it saves a lot of time. Lastly, the front end used cascading styling sheet (CSS) to manually create the components and style the design form.



```css
.App {
  text-align: center;
}

.App-logo {
  height: 40vmin;
  pointer-events: none;
}

@media (prefers-reduced-motion: no-preference) {
  .App-logo {
    animation: App-logo-spin infinite 20s linear;
  }
}

.App-header {
  background-color: #282c34;
  min-height: 100vh;
  display: flex;
  flex-direction: column;
  align-items: center;
  justify-content: center;
  font-size: calc(10px + 2vmin);
  color: white;
}

.App-link {
  color: #61dafb;
}
```

Figure 5.1: CSS code

B. *WEB3.js and Ethers.js Libraries:* We utilized the web3.js framework in conjunction with the ethers.js package to provide effective communication between the front-end components and the smart contract. The two libraries allowed the researchers to listen and create events in the local Ethereum blockchain environment.



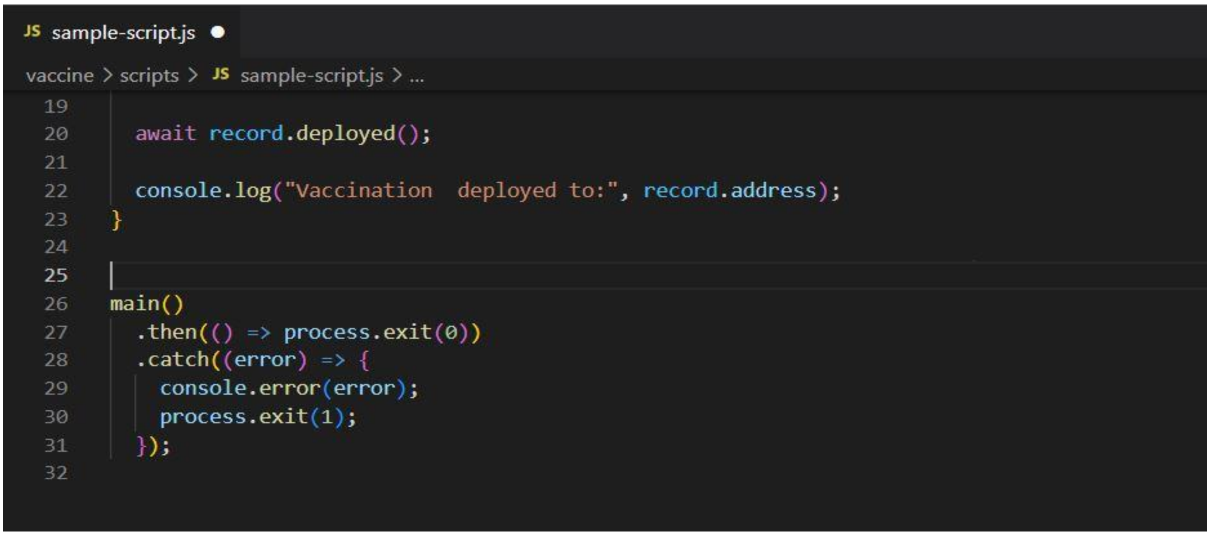
```
// The Contract object
const contract = new ethers.Contract(contractAddress, ABI, signer);


useEffect(() => {
  // MetaMask requires requesting permission to connect users accounts
  const connectWallet = async () => {
    await provider.send("eth_requestAccounts", []);
}

connectWallet()
    .catch(console.error);

const getUserAddress = async() => {
    const address =  await signer.getAddress();
    setUserAddress(address);
    console.log(user_address);
}

const getBalance = async () => {
    const balance = await provider.getBalance(contractAddress);
    const balanceFormatted = ethers.utils.formatEther(balance)
    setBalance(balanceFormatted);
}

getUserAddress().catch(console.error)
getBalance().catch(console.error)

    const data = localStorage.getItem('token')
    setAccessToken(data)

})
```

Figure 5.2: Web3.js and Ether.js library code

5.2.3 Back-end implementation

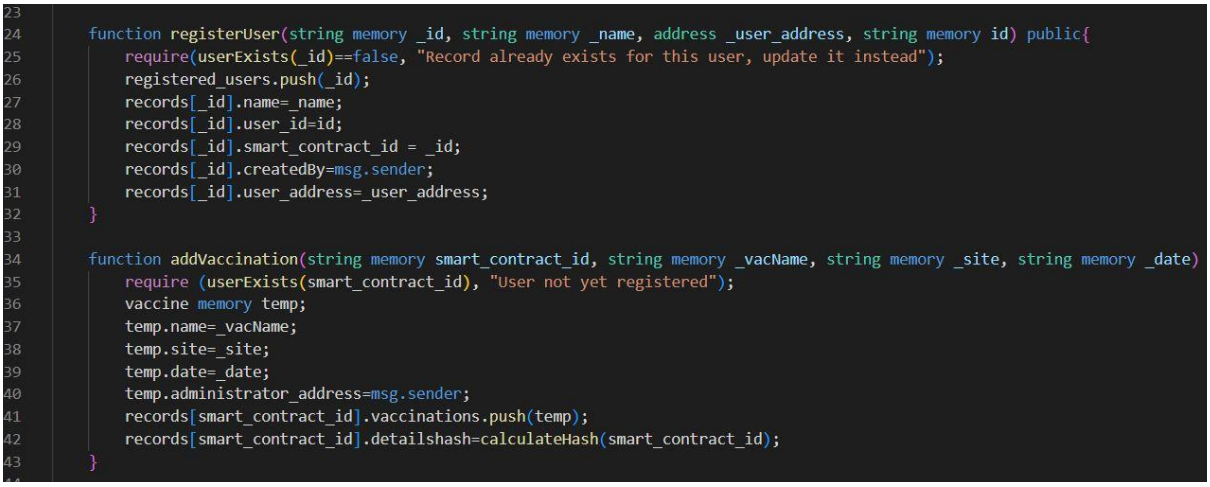
Some of the important tools used to create the back end of the system to ensure the objectives of this research are achieved are discussed as follows:

A. *Hardhat:* To effectively deploy, execute, debug, and test the smart contract in a local blockchain environment we used the HardHat library. This library creates a node on which our blockchains run. It records all the transactions with the smart contract and the front end.



```
  await record.deployed();

  console.log("Vaccination  deployed to:", record.address);
}


main()
  .then(() => process.exit(0))
  .catch((error) => {
    console.error(error);
    process.exit(1);
  });
```

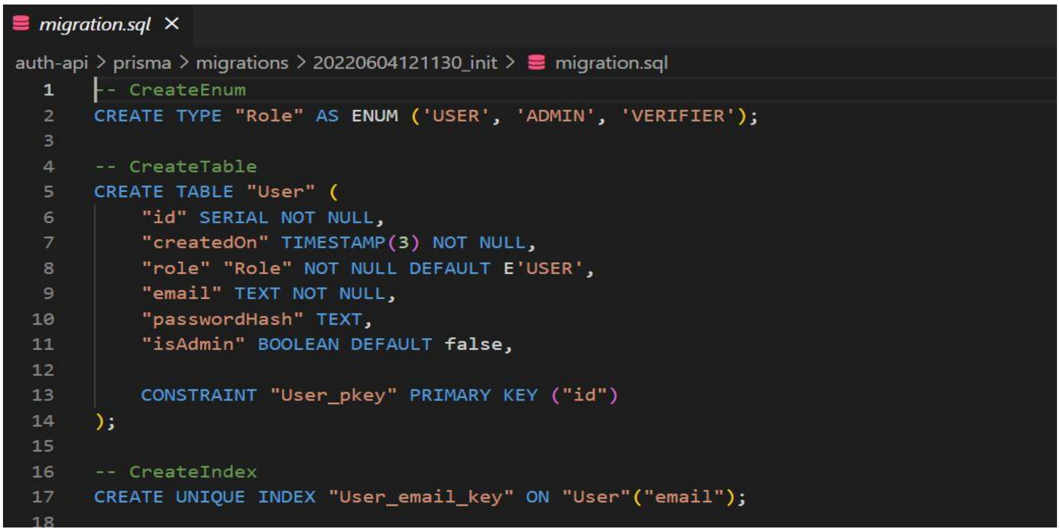
Figure 5.3: Hardhat code



```

    function registerUser(string memory _id, string memory _name, address _user_address, string memory id) public{
        require(userExists(_id)==false, "Record already exists for this user, update it instead");
        registered_users.push(_id);
        records[_id].name=_name;
        records[_id].user_id=id;
        records[_id].smart_contract_id = _id;
        records[_id].createdBy=msg.sender;
        records[_id].user_address=_user_address;
    }

    function addVaccination(string memory smart_contract_id, string memory _vacName, string memory _site, string memory _date)
        require (userExists(smart_contract_id), "User not yet registered");
        vaccine memory temp;
        temp.name=_vacName;
        temp.site=_site;
        temp.date=_date;
        temp.administrator_address=msg.sender;
        records[smart_contract_id].vaccinations.push(temp);
        records[smart_contract_id].detailshash=calculateHash(smart_contract_id);
    }
```

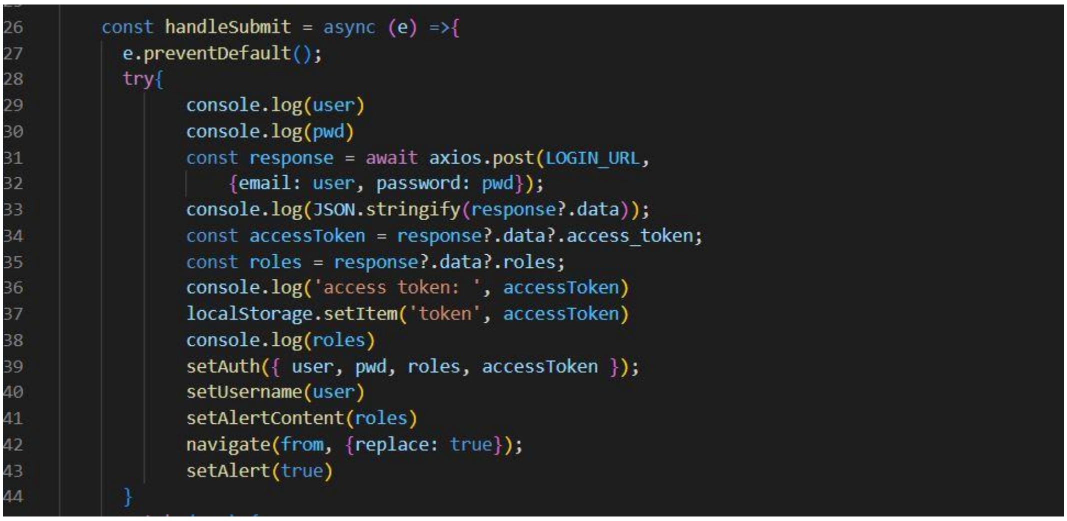
Figure 5.4: Smart contract method

B. *Rest API*, *Docker*, *Prisma and Argon2:* To manage the database, the API creates a container using docker. Docker is, by description, an Open-source containerization solution that enables programmers to package their applications as container-standard executable components. These components integrate the source code of an application with the OS libraries and dependencies required to execute the code in any context. Docker downloads a Postgres database image in our application so that Prisma may construct migrations and the API can save data to it. In the context of this research, the Prisma ORM creates a schema for the database.


migration.sql
auth-api > prisma > migrations > 20220604121130_init > migration.sql

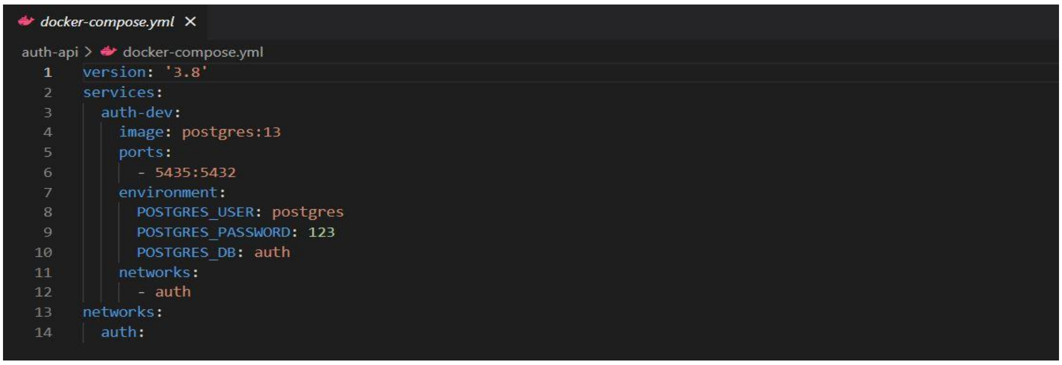
```sql
-- CreateEnum
CREATE TYPE "Role" AS ENUM ('USER', 'ADMIN', 'VERIFIER');

-- CreateTable
CREATE TABLE "User" (
    "id" SERIAL NOT NULL,
    "createdOn" TIMESTAMP(3) NOT NULL,
    "role" "Role" NOT NULL DEFAULT E'USER',
    "email" TEXT NOT NULL,
    "passwordHash" TEXT,
    "isAdmin" BOOLEAN DEFAULT false,

    CONSTRAINT "User_pkey" PRIMARY KEY ("id")
);

-- CreateIndex
CREATE UNIQUE INDEX "User_email_key" ON "User"("email");
```

Figure 5.5: Database generation code



```javascript
    const handleSubmit = async (e) =>{
      e.preventDefault();
      try{
            console.log(user)
            console.log(pwd)
            const response = await axios.post(LOGIN_URL,
                {email: user, password: pwd});
            console.log(JSON.stringify(response?.data));
            const accessToken = response?.data?.access_token;
            const roles = response?.data?.roles;
            console.log('access token: ', accessToken)
            localStorage.setItem('token', accessToken)
            console.log(roles)
            setAuth({ user, pwd, roles, accessToken });
            setUsername(user)
            setAlertContent(roles)
            navigate(from, {replace: true});
            setAlert(true)
      }
```

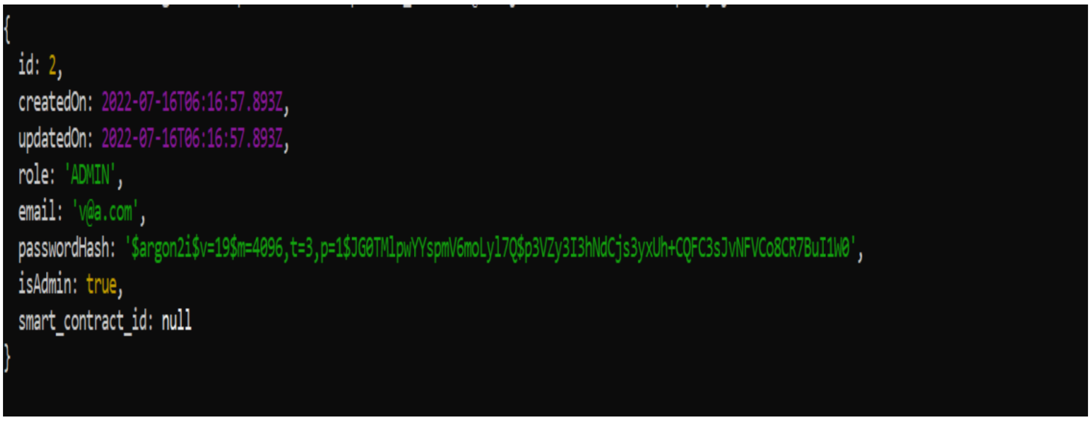
Figure 5.6: API code



```yaml
version: '3.8'
services:
  auth-dev:
    image: postgres:13
    ports:
      - 5435:5432
    environment:
      POSTGRES_USER: postgres
      POSTGRES_PASSWORD: 123
      POSTGRES_DB: auth
    networks:
      - auth
networks:
  auth:
```

Figure 5.7: Docker-compose code

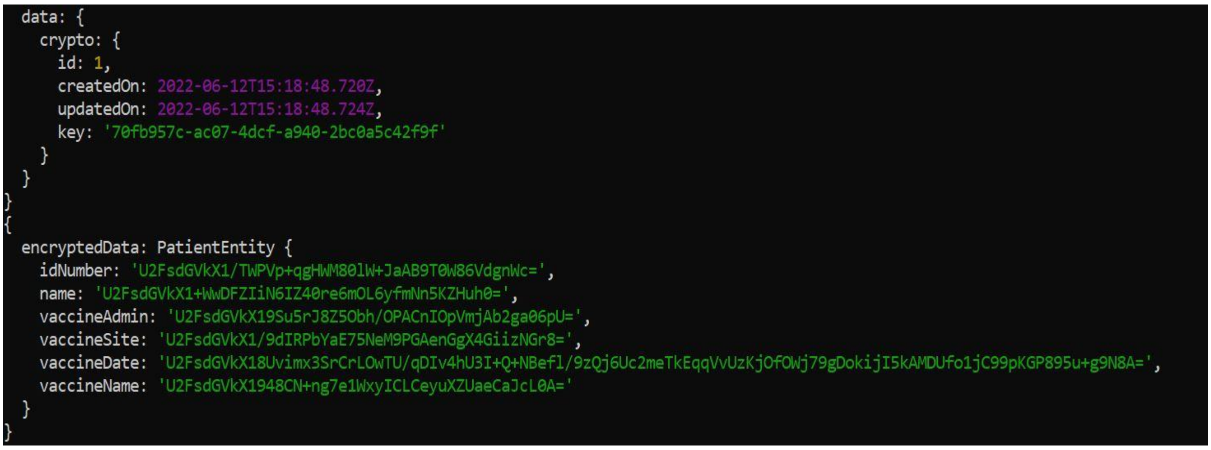
Moreover, for password hashing, an Argon2 cryptographic hashing algorithm [156]was used. This method improved the system's access control by preventing tradeoff attacks by using the cache and memory structure of more recent CPUs. This was made possible because of the algorithm [158].



```
{
  id: 2,
  createdOn: 2022-07-16T06:16:57.893Z,
  updatedOn: 2022-07-16T06:16:57.893Z,
  role: 'ADMIN',
  email: 'v@a.com',
  passwordHash: '$argon2i$v=19$m=4096,t=3,p=1$JG0TMlpwYYspmV6moLyl7Q$p3VZy3I3hNdCjs3yxUh+CQFC3sJvNFVCo8CR7BuI1W0',
  isAdmin: true,
  smart_contract_id: null
}
```

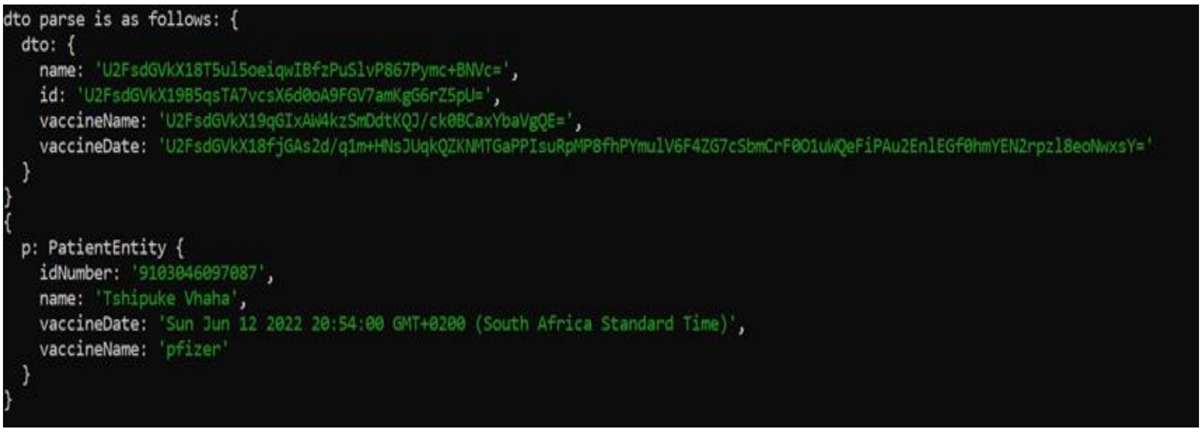
Figure 5.8: Argon2 password hashing

Finally, symmetric encryption was used to encrypt and decrypt the data. Figure 5.9 shows the encryption of the data and Figure 5.10 shows the decryption of the data. The encryption implementation was done to enhance the data security in the system.



```
  data: {
    crypto: {
      id: 1,
      createdOn: 2022-06-12T15:18:48.720Z,
      updatedOn: 2022-06-12T15:18:48.724Z,
      key: '70fb957c-ac07-4dcf-a940-2bc0a5c42f9f'
    }
  }
}
{
  encryptedData: PatientEntity {
    idNumber: 'U2FsdGVkX1/TWPVp+qgHWM80lW+JaAB9T0W86VdgnWc=',
    name: 'U2FsdGVkX1+WwDFZIiN6IZ40re6mOL6yfmNn5KZHuh0=',
    vaccineAdmin: 'U2FsdGVkX19Su5rJ8Z5Obh/OPACnIOpVmjAb2ga06pU=',
    vaccineSite: 'U2FsdGVkX1/9dIRPbYaE75NeM9PGAenGgX4GiizNGr8=',
    vaccineDate: 'U2FsdGVkX18Uvimx3SrCrLOwTU/qDIv4hU3I+Q+NBefl/9zQj6Uc2meTkEqqVvUzKjOfOWj79gDokijI5kAMDUfo1jC99pKGP895u+g9N8A=',
    vaccineName: 'U2FsdGVkX1948CN+ng7e1WxyICLCeyuXZUaeCaJcL0A='
  }
}
```

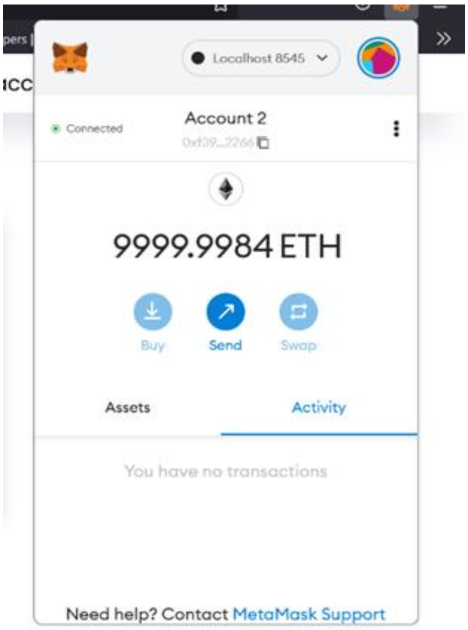
Figure 5.9: Encryption of data



```
dto parse is as follows: {
  dto: {
    name: 'U2FsdGVkX18T5ul5oeiqwIBfzPuSlvP867Pymc+BNVc=',
    id: 'U2FsdGVkX19B5qsTA7vcsX6d0oA9FGV7amKgG6rZ5pU=',
    vaccineName: 'U2FsdGVkX19qGIxAW4kzSmDdtKQJ/ck0BCaxYbaVgQE=',
    vaccineDate: 'U2FsdGVkX18fjGAs2d/q1m+HNsJUqkQZKNMTGaPPIsuRpMP8fhPYmulV6F4ZG7cSbmCrF0O1uWQeFiPAu2EnlEGf0hmYEN2rpzl8eoNwxsY='
  }
}
{
  p: PatientEntity {
    idNumber: '9103046097087',
    name: 'Tshipuke Vhaha',
    vaccineDate: 'Sun Jun 12 2022 20:54:00 GMT+0200 (South Africa Standard Time)',
    vaccineName: 'pfizer'
  }
}
```

Figure 5.10: Decryption of data

C. *Wallet:* In the context of this study, the metamask wallet was used to allow the researchers to access the Ethereum wallet through a browser. MetaMask is a bitcoin wallet that provides access to the decentralized applications environment of Web 3 (dapps) [159]. Metamask is used to display the gas price and how much Ethereum is available on the node to make a transaction. Gas price can be defined as the transaction fee on the blockchain of Ethereum. It is what users spend to validate or finish their transactions [159].



9999.9984 ETH

You have no transactions

Need help? Contact MetaMask Support

Figure 5.11: Metamask wallet

5.2.4 Evaluation parameters

To evaluate the efficiency of the implemented system, we used the Apache-JMeter load testing tool and Hyperledger-Caliper to test the transactions on the blockchain network. The Apache Software Foundation is responsible for the creation of the open-source testing application known as Apache-JMeter for use in load testing a client-server. Its advantage is that it provides reporting test results offline [160]. We focused on the parameters such as transaction latency, response time, throughput, and average time per transaction. Simulations were performed between 0 and 1000 users since we tested it on a local server.

Table 5.2: Evaluation metrics

Parameter	**Definition**
Transaction latency	It is the duration of time required to conduct a transaction over a network. It includes the time taken to submit the transaction and the reply from the server [85].
Response time	It is the amount of time taken by the system to process a request after receiving one [143].
Throughput	It is the number of completed transactions within a certain time frame [85].
Average time per transaction	It is the time taken to complete one transaction measured in seconds [85].
Number of transactions	It is the rate at which valid transactions are posted to the blockchain during a certain length of time [161].
Threads	A representation of users in a testing scenario [143].
Security	Protection of data and tools from malicious attacks and harm [10].
Privacy	The concealing of information about an individual or group, or the capacity to control its disclosure [12].

5.3 System Operations

The overall operations of the implemented proposed system were presented in this section. Figure 5.12 shows the overall process of the blockchain-based registration and verification system. The overall description of the vaccination operation described in figure 5.12 starts by running the node and then followed by deploying the smart contract. If the node is running without any errors, then the **registering_authority** will be permitted to register the **patient,** or else if the node is not running an error message will display alerting the administrator to restart the node. To successfully register the **patient**, the **registering_authority** must enter their valid credentials then authentication will take place. If the credentials are valid, then the system will allow the registration of the **patient** otherwise, it will show invalid credentials.

Upon successful registration the system allows the **patient** to log in with the issued credentials, these will be verified to check if the **patient** is indeed registered or not. If registered give access to request and view certificate else show invalid credentials. The requested certificate can be verified by the **verification_authority**. The verification authority must log in first using their credentials. If the credentials are correct then allow scanning of the QR Code and retrieve vaccination details, otherwise, deny access to log in and scan the QR code.

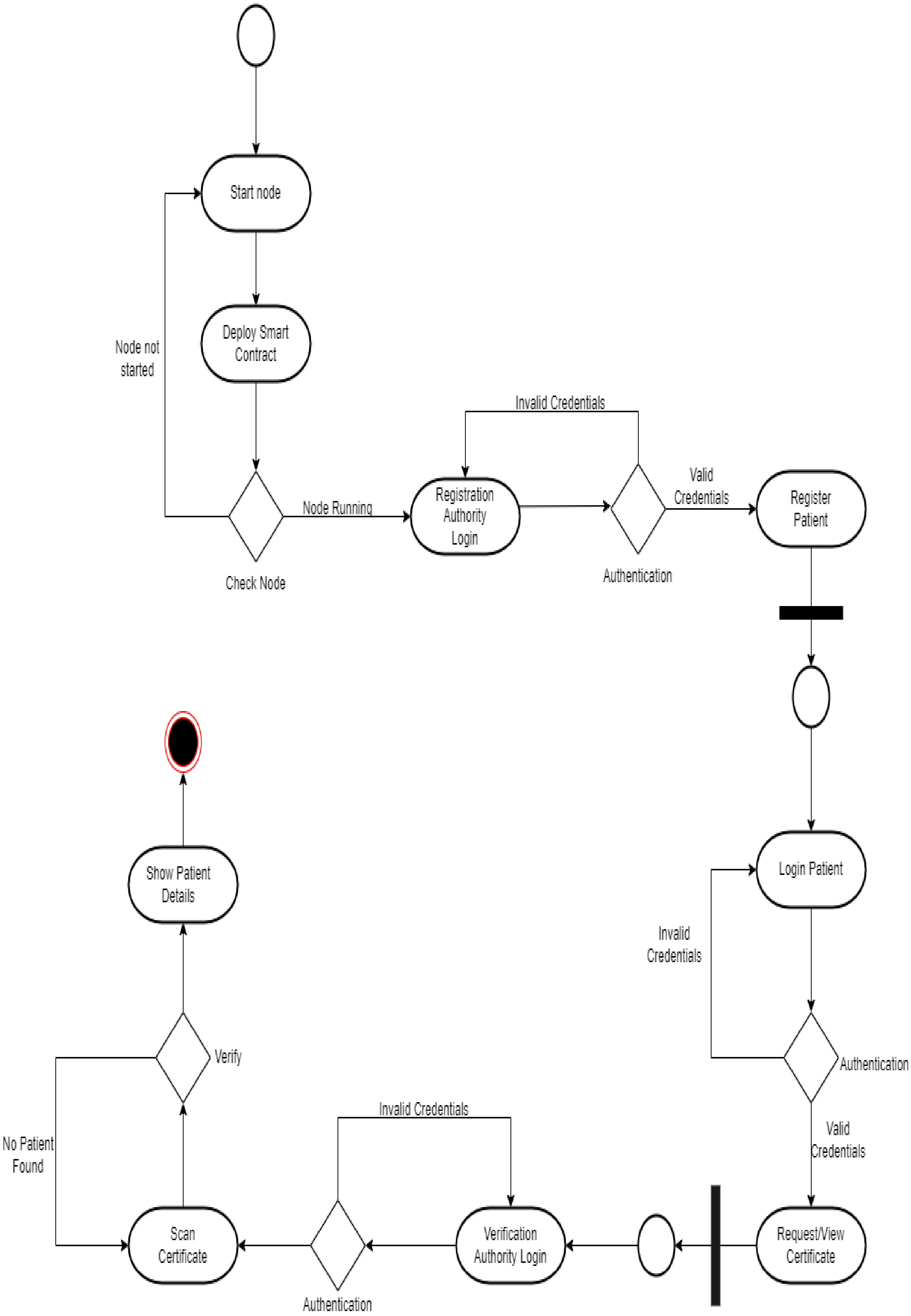


Figure 5.12: Smart contract enabled patient registration and verification process

5.4 System Interfaces

This section presents the overall VMS interfaces used in performing the operations of the proposed system.

5.4.1 Login

Figure 5.13 is the log-in page showing how different actors log in as per their roles in the system. The roles are **registration_authority**, **patient** and **verification_authority**, all entities must enter their email address and password to get authenticated and granted access to the system.

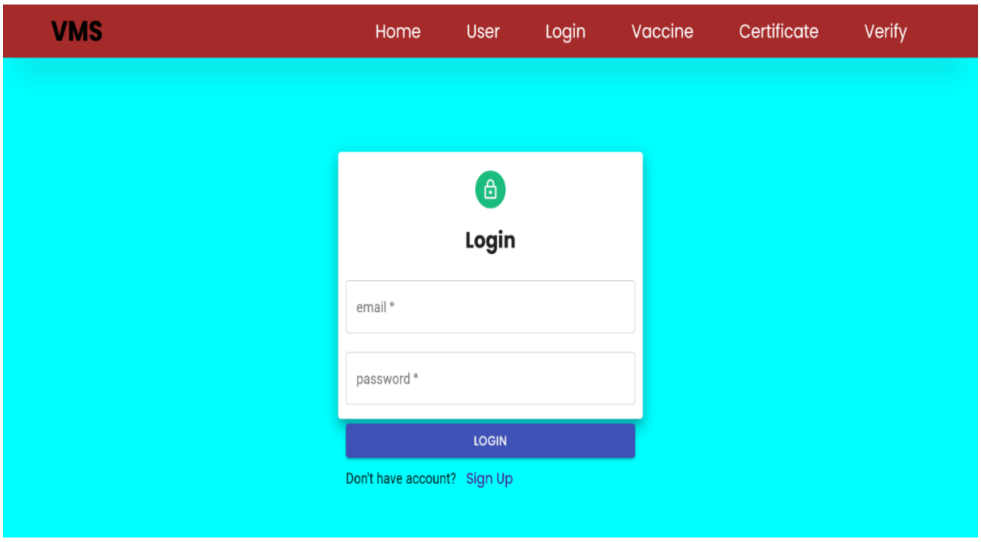


Figure 5.13: Login page

5.4.2 Registration

Figure 5.14 shows the **registration_authority** interface where a patient can register to the system. In this case, the **registration_authority** has to enter the patient's email address to create a new **patient** account in the system.

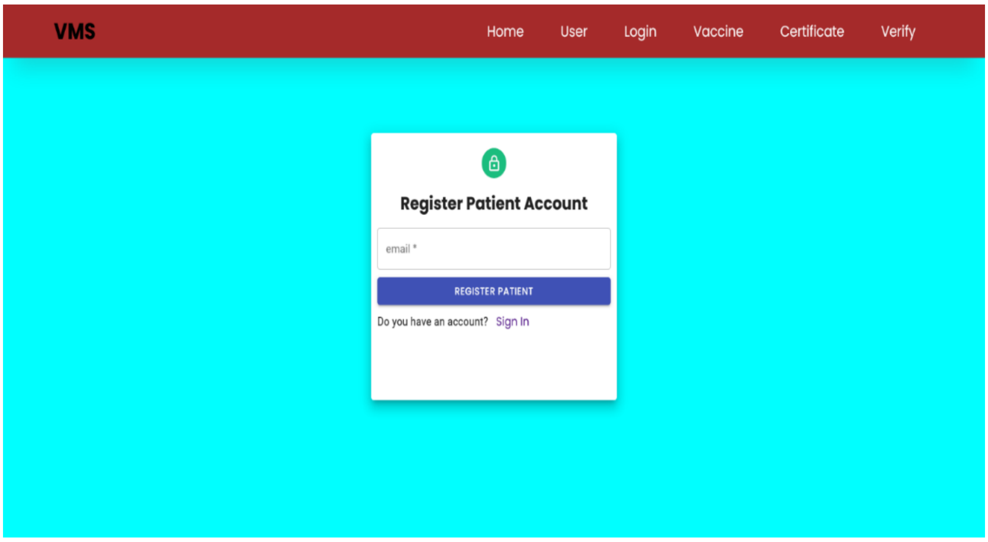
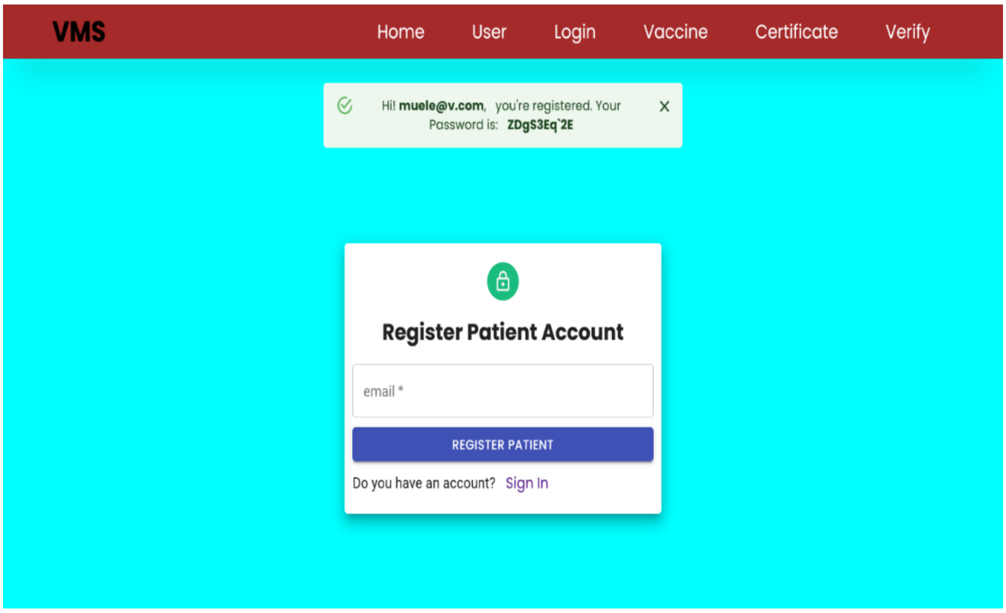


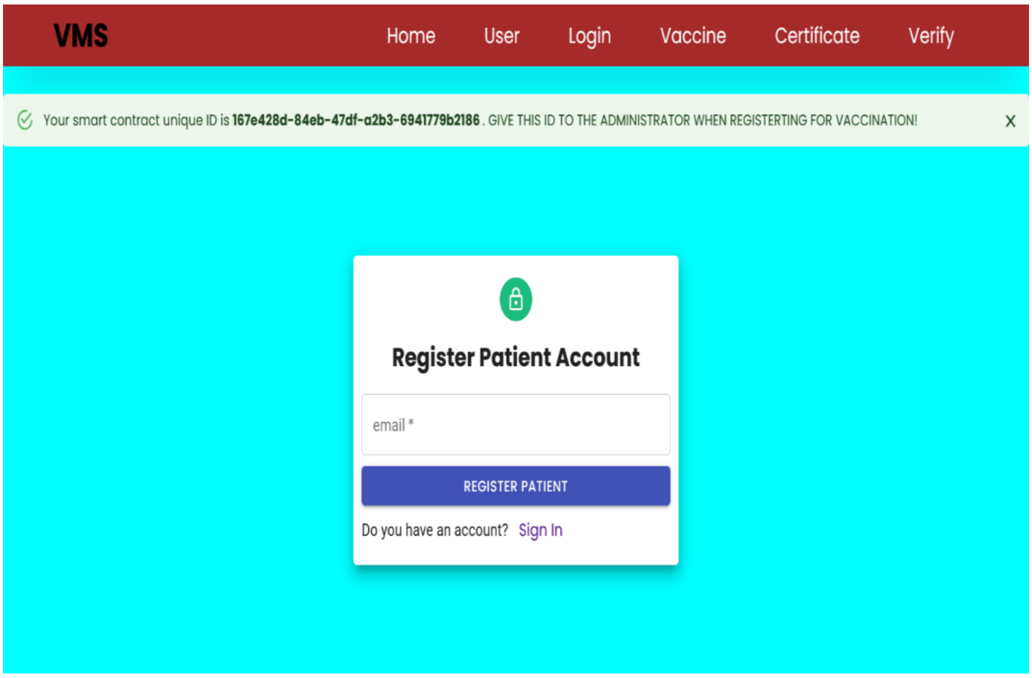
Figure 5.14: New patient registration



Hi! **muele@v.com**, you're registered. Your Password is: **ZDgS3Eq`2E**

Figure 5.15: Assigning password

Once there is a successful **patient** registration using the email address, the system will assign a unique password to the patient for future log-ins. This is captured in Figure 5.15. Moreover, the **unique smart contract ID** for the patient will automatically be generated during account registration. Figure 5.16 shows the **unique smart contract ID** to be used by the patient during the request for the certificate.



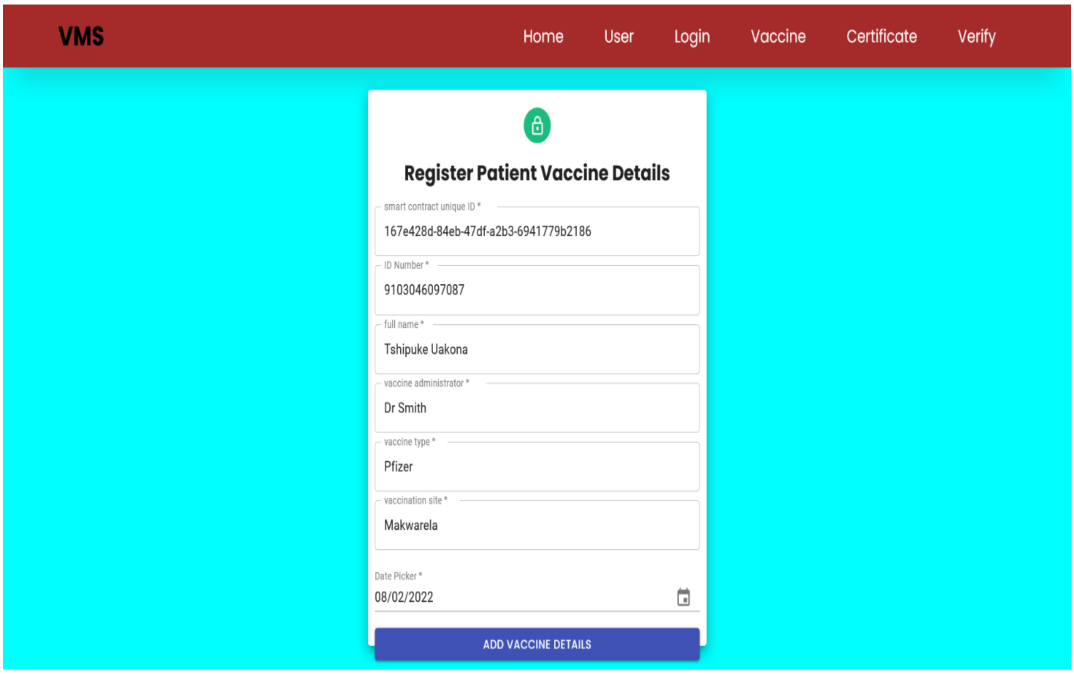
Your smart contract unique ID is **167e428d-84eb-47df-a2b3-6941779b2186** . GIVE THIS ID TO THE ADMINISTRATOR WHEN REGISTERTING FOR VACCINATION!

Register Patient Account

email *

Do you have an account?

Figure 5.16: Assigning unique smart contract ID



Register Patient Vaccine Details

smart contract unique ID *: 167e428d-84eb-47df-a2b3-6941779b2186

ID Number *: 9103046097087

full name *: Tshipuke Uakona

vaccine administrator *: Dr Smith

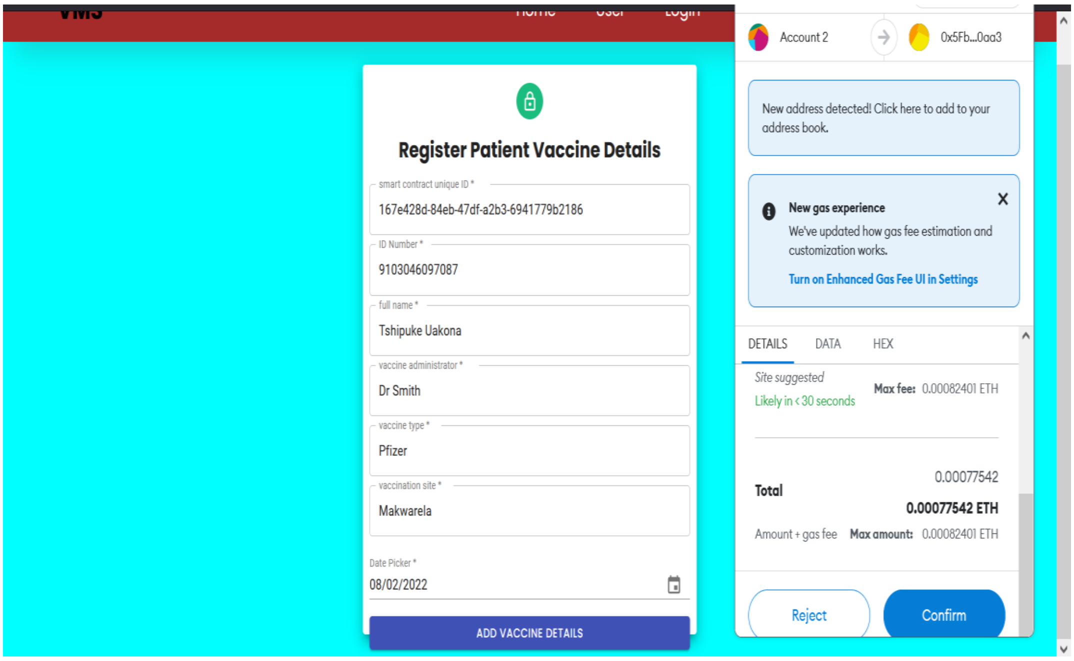
vaccine type *: Pfizer

vaccination site *: Makwarela

Date Picker *: 08/02/2022

Figure 5.17: Registration of patient vaccine details

Furthermore, Figure 5.17 presents the form that will be used by the **registration_authority** to enter the patient vaccination details when registering in the system. To this end, details such as *smart contract ID, ID number, full name, vaccination administrator, vaccine type, vaccination site* and *date* are required for a successful registration.



Register Patient Vaccine Details

smart contract unique ID * 167e428d-84eb-47df-a2b3-6941779b2186

ID Number * 9103046097087

full name * Tshipuke Uakona

vaccine administrator * Dr Smith

vaccine type * Pfizer

vaccination site * Makwarela

Date Picker * 08/02/2022

Account 2 → 0x5Fb...0aa3

New address detected! Click here to add to your address book.

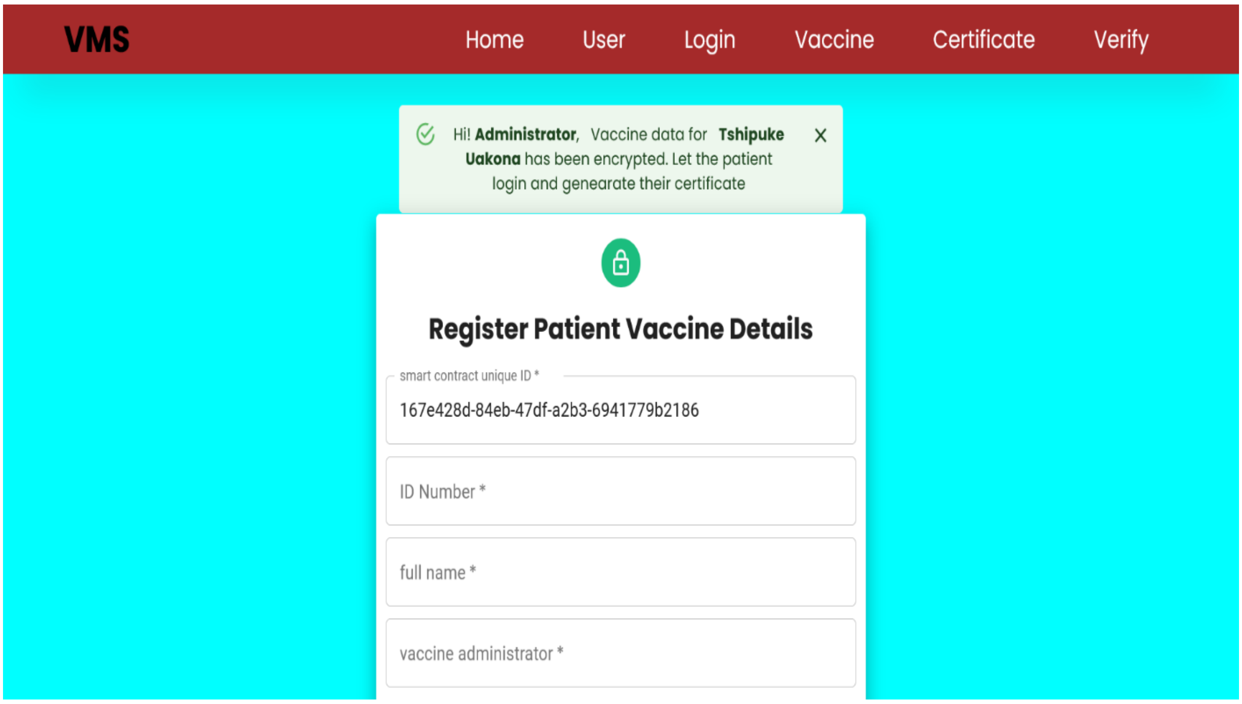
New gas experience
We've updated how gas fee estimation and customization works.
Turn on Enhanced Gas Fee UI in Settings

Site suggested
Likely in < 30 seconds
Max fee: 0.00082401 ETH

Total 0.00077542
0.00077542 ETH
Amount + gas fee Max amount: 0.00082401 ETH

Figure 5.18: Data confirmation

Also, Figure 5.18 shows how the VMS interacts with the smart contract. To this end, after the **registration_authority** enters all the details about a patient, a wallet confirmation will pop up so that the registration authority can confirm the transaction to the smart contract. Once confirmed, Figure 5.19 shows the successful registration of the patient into the VMS and the smart contract. Now the patient can log-in to request and view their certificate using the credentials assigned to them anytime, anywhere.



Hi! **Administrator**, Vaccine data for **Tshipuke Uakona** has been encrypted. Let the patient login and genearate their certificate

Register Patient Vaccine Details

smart contract unique ID * 167e428d-84eb-47df-a2b3-6941779b2186

ID Number *

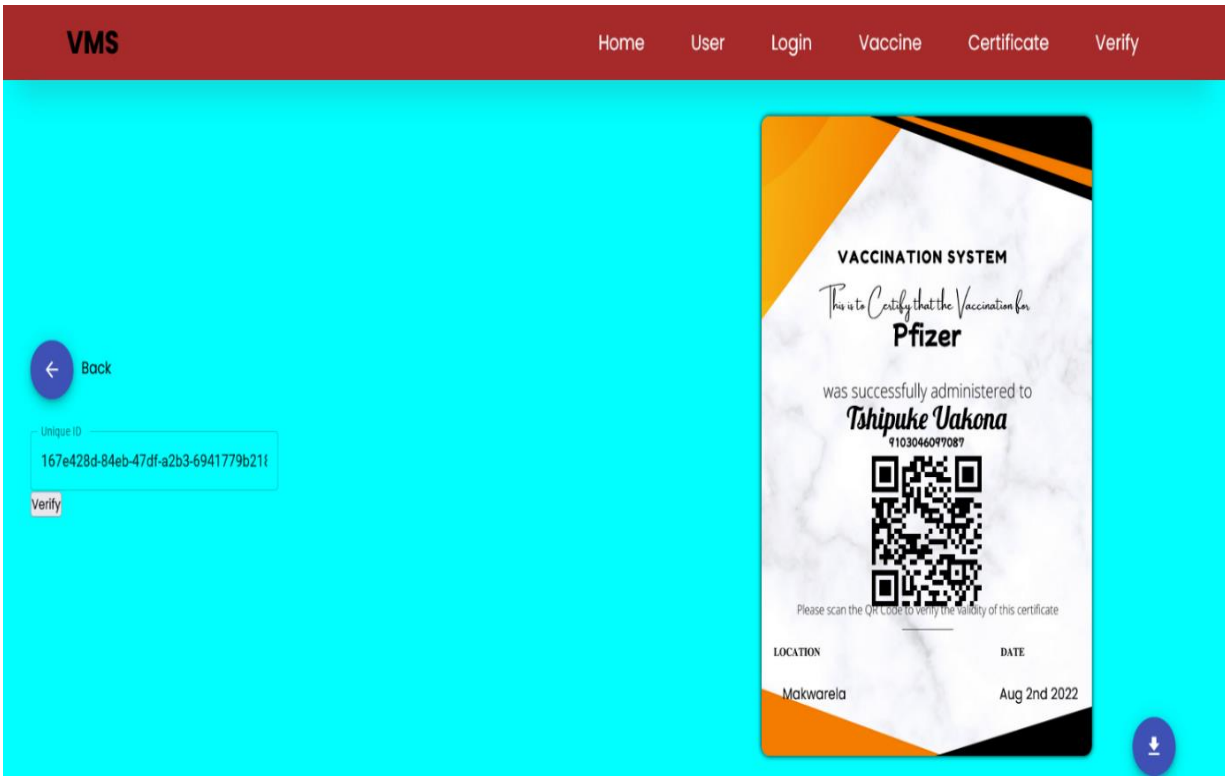
full name *

vaccine administrator *

Figure 5.19: Successful registration

5.4.3 Request and view the registration certificate

In the system proposed here, once there is a successful log-in for the patient, the form shown in Figure 5.20 will be displayed. Here the patient can request their certificate using their unique smart contract ID and can download their Certificate with a QR code to use during the verification stage.



Unique ID: 167e428d-84eb-47df-a2b3-6941779b21(

VACCINATION SYSTEM

This is to Certify that the Vaccination for

Pfizer

was successfully administered to

Tshipuke Uakona

9103046097087

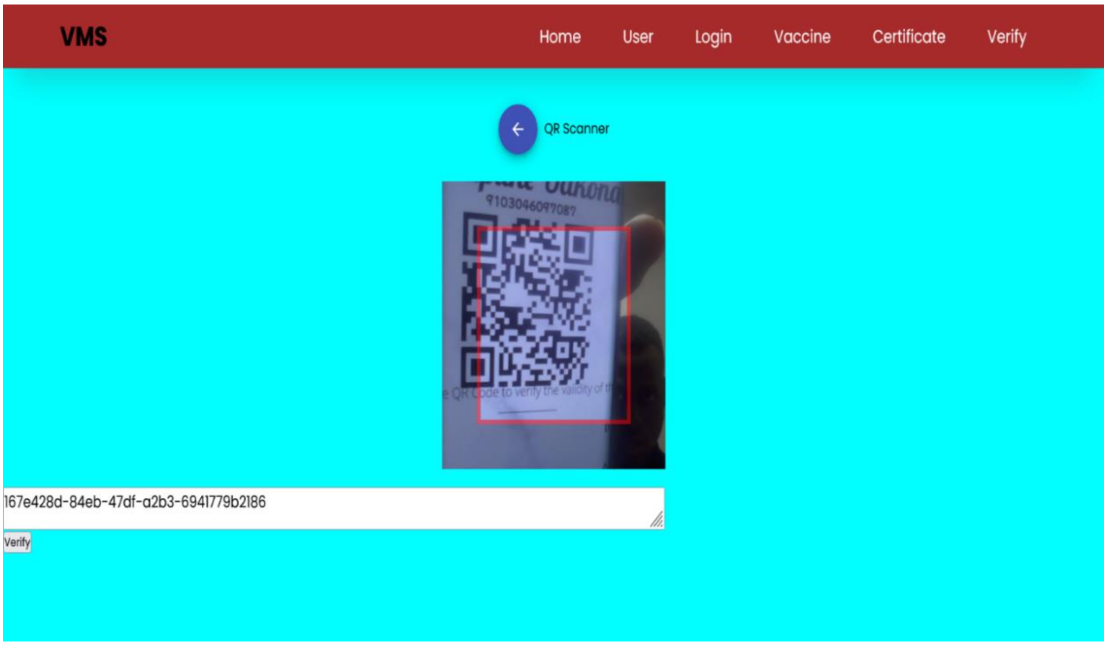
Please scan the QR Code to verify the validity of this certificate

LOCATION	DATE
Makwarela	Aug 2nd 2022

Figure 5.20: QR and certificate generation

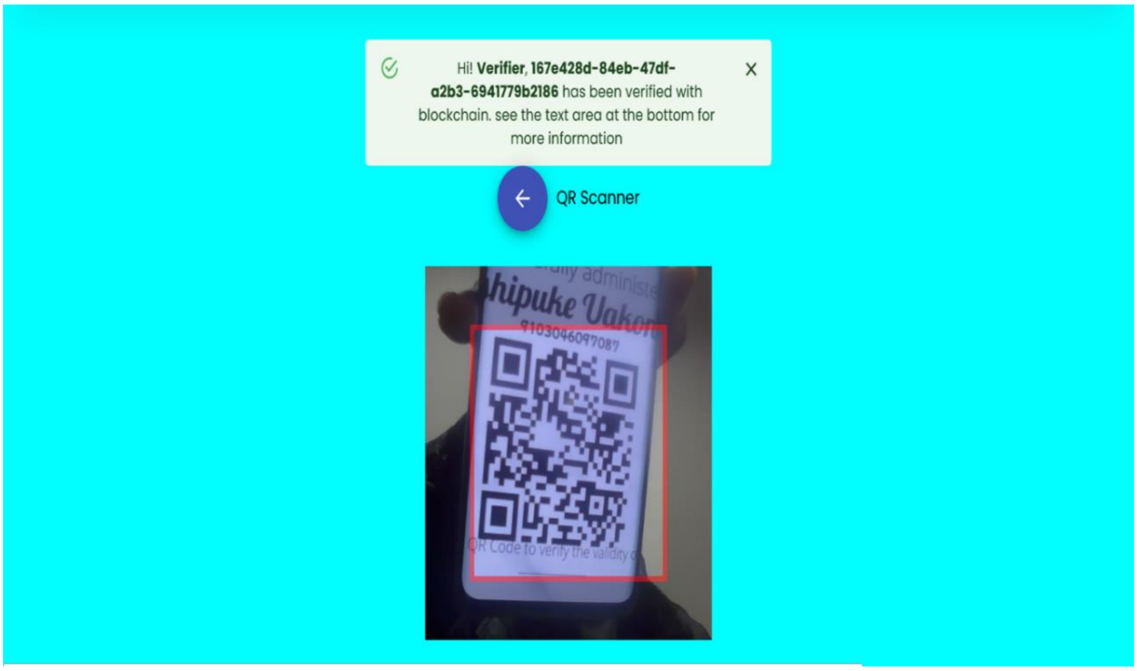
5.4.4 Certificate verification

As a core function of this proposed system, patient registration verification is very important to avoid fraudulent claims. Figure 5.21 shows how the **verification_authority** scans the QR code provided by the patient to verify its authenticity. In this case, upon scanning the QR code, all the details stored on the smart contract blockchain will be retrieved as proof that the patient has been vaccinated. This is captured in Figures 5.22 and Figure 5.23.



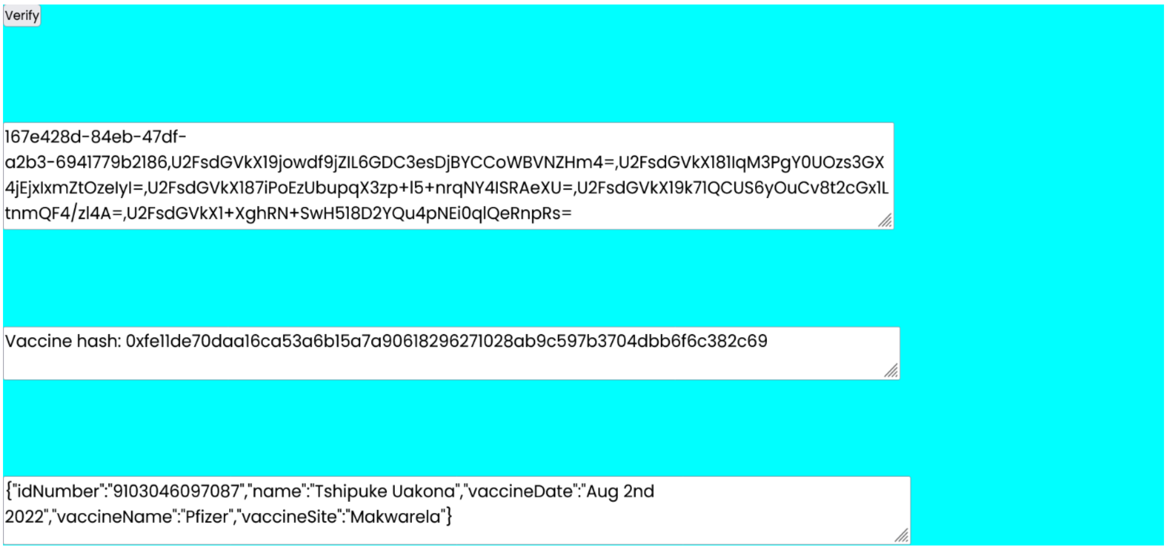
167e428d-84eb-47df-a2b3-6941779b2186

Figure 5.21: Scanning of the certificate using the QR code



Hi! **Verifier, 167e428d-84eb-47df-a2b3-6941779b2186** has been verified with blockchain. see the text area at the bottom for more information

Figure 5.22: Successful scanning of the certificate using QR Code



```
167e428d-84eb-47df-a2b3-6941779b2186,U2FsdGVkX19jowdf9jZIL6GDC3esDjBYCCoWBVNZHm4=,U2FsdGVkX181IqM3PgY0UOzs3GX4jEjxIxmZtOzeIyI=,U2FsdGVkX187iPoEzUbupqX3zp+I5+nrqNY4ISRAeXU=,U2FsdGVkX19k71QCUS6yOuCv8t2cGx1LtnmQF4/zl4A=,U2FsdGVkX1+XghRN+SwH518D2YQu4pNEi0qlQeRnpRs=
```

```
Vaccine hash: 0xfe11de70daa16ca53a6b15a7a90618296271028ab9c597b3704dbb6f6c382c69
```

```
{"idNumber":"9103046097087","name":"Tshipuke Uakona","vaccineDate":"Aug 2nd 2022","vaccineName":"Pfizer","vaccineSite":"Makwarela"}
```

Figure 5.23: Successful data retrieval from the blockchain

5.5 System Results

This section discusses the evaluation of the VMS using simulations to assess the effectiveness and performance of the system of VMS and the obtained results. In this study, JMeter was used to analyse the VMS server performance, we have taken 0-1000 threads with a ramp-up speed of one second. With the JMeter, the pace at which concurrent users attempt to use the system during a load test is the ramp-up speed [160]. The simulations were set up to determine the parameters discussed in Table 5.2 against the number of threads and transactions performed on the system – performance and effectiveness.

5.5.1 Response time

The response time is broken down by the number of threads that are run on the VMS and is shown in figure 5.24. The x-axis displays the total number of threads, while the y-axis displays the response time in milliseconds. According to the data shown in Figure 5.24, the amount of time required to respond likewise rises along with the number of threads. This indicates that the response time is directly proportional to the number of threads. The average response time of the simulation was calculated to be 132.24 ms.

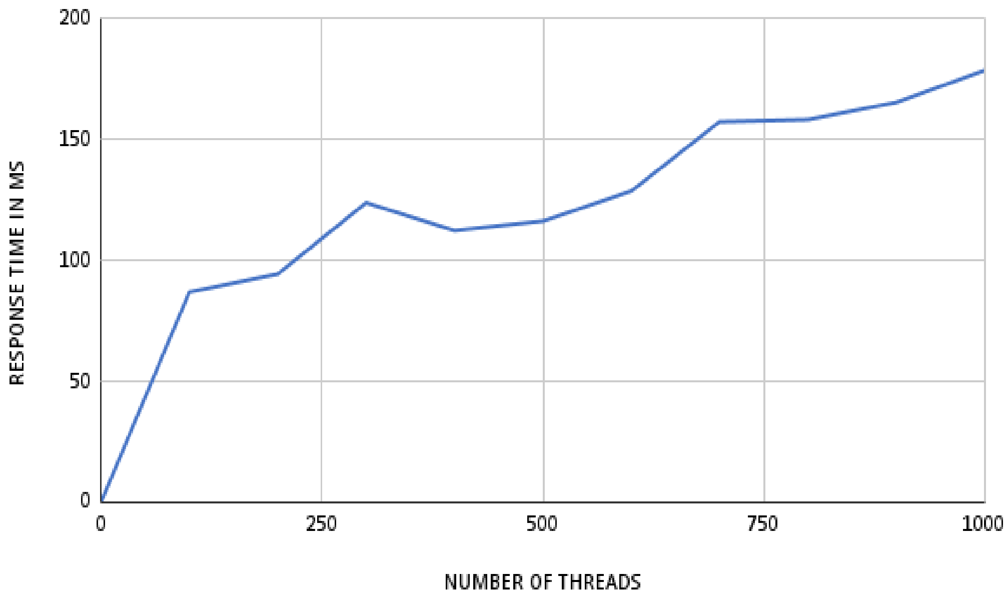


Figure 5.24: Response Time vs Number of Threads

5.5.2 Average throughput

Figure 5.25 presents the throughput in milliseconds over the number of threads carried out in the system. According to the graph shown in Figure 5.25, the throughput increases in direct proportion to the number of active threads. This shows that the system is running without any disruptions because throughput must increase as the number of threads increases[162].

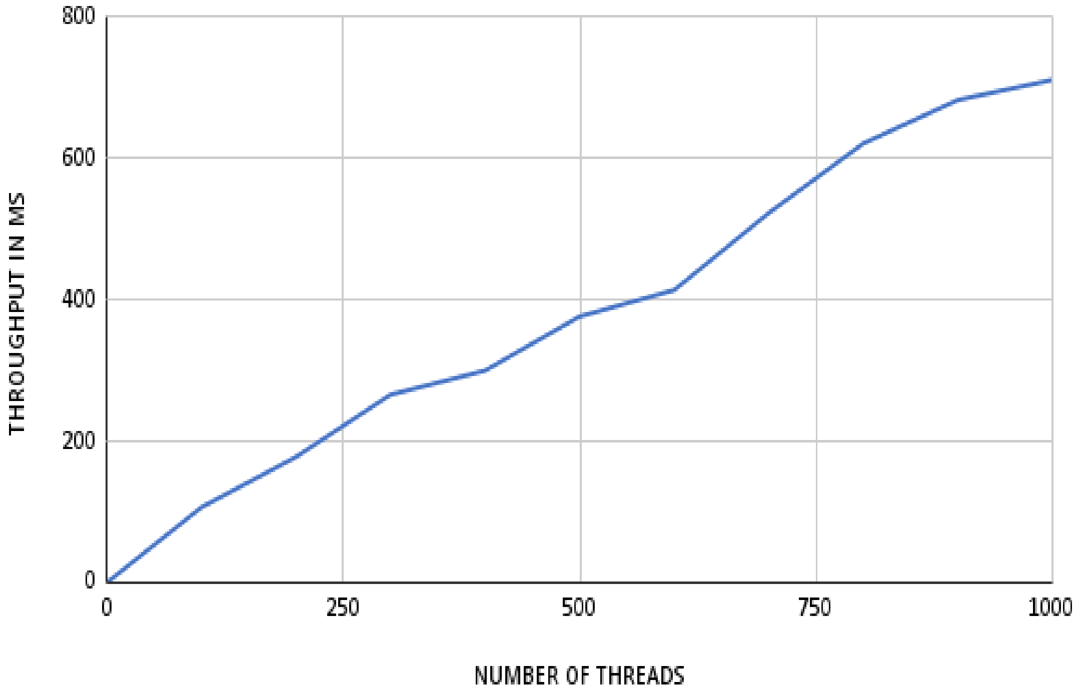


Figure 5.25: Throughput vs Number of threads

5.5.3 Average time

Figure 5.26 shows the average time per transaction in milliseconds against the number of threads performed. According to the graph in Figure 5.26, the average time per transaction increases as the number of threads increases. The proposed VMS was able to process 1000 transactions in about 10-12 seconds which is an indication that the system is efficient since it can handle a high volume of transactions in a relatively short amount of time.

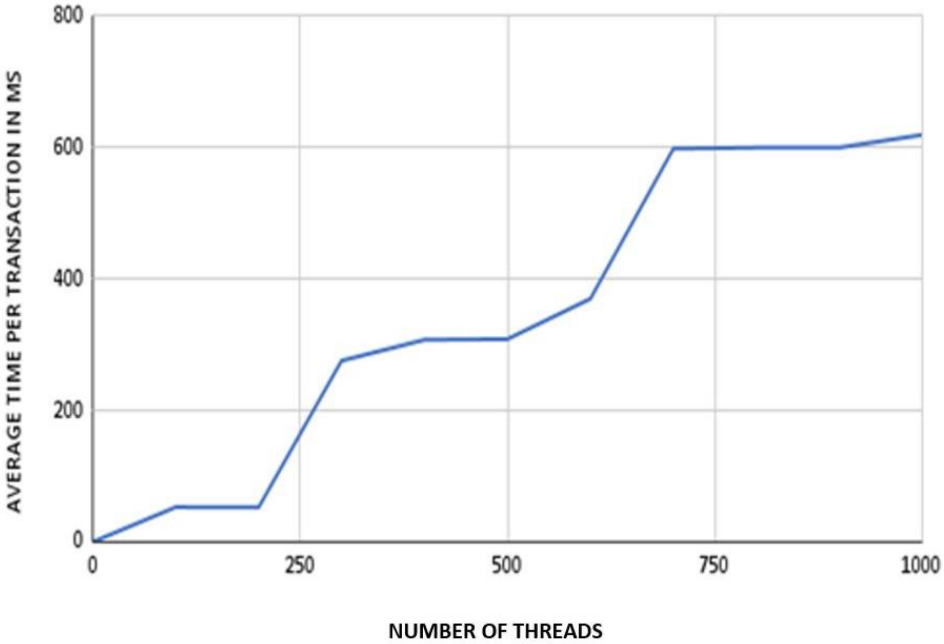


Figure 5.26: Average Time per transaction vs Number of threads

5.5.4 Latency

Figure 5.27 shows the latency in milliseconds vs the number of threads conducted in the VMS. According to the graph shown in Figure 5.27, the latency increases as the number of threads increases. However, once it reaches a certain peak it shows a straight line and starts to increase again. The average latency calculated was 204.60 milliseconds. One possible explanation for this is that the present designs of blockchain do not permit them to scale up to rates of several thousand transactions per second. Scalability remains an issue and should be considered when integrating IoT devices with Blockchain [66], [27].

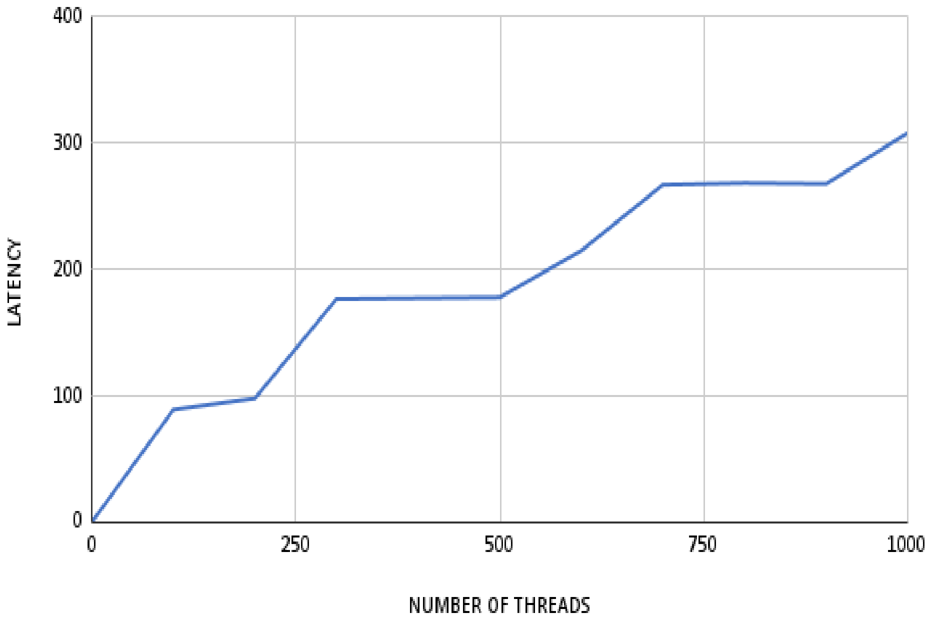


Figure 5.27: Latency vs Number of Threads

5.5.5 Hyperledger Caliper performance

The Linux Foundation presented the Hyperledger open-source blockchain project in December 2015. In addition to Hyperledger Fabric and Hyperledger Caliper, the Hyperledger project offers a variety of frameworks and tools. A Caliper is a performance assessment tool for blockchains that evaluates many blockchain systems based on their suitability for a variety of use cases. It generates reports that include performance indicators such as throughput and latency [163].

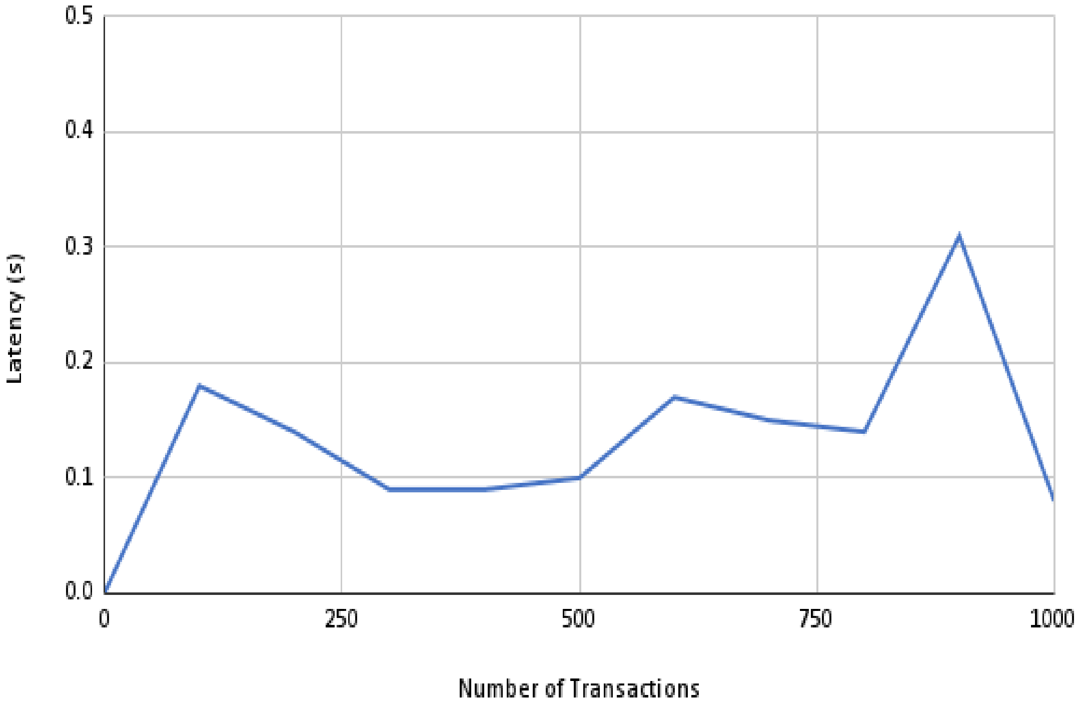


Figure 5.28: Patient registration latency vs Number of transactions

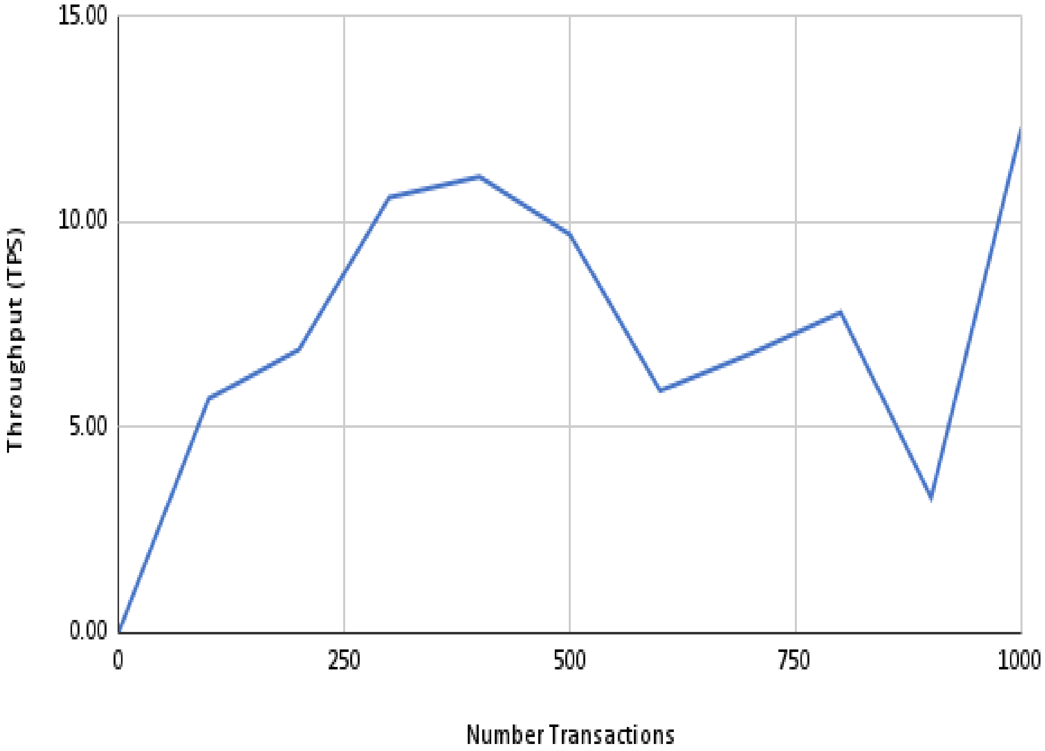


Figure 5.29: Patient registration Throughput vs Number of Transactions

In the simulations performed, the latency and throughput of registering the patient details were evaluated with a total number of 1000 transactions. Figure 5.28 and Figure 5.29 show the latency and throughput vs the number of transactions when registering a patient to the smart contract deployed on the blockchain network. The latency seems to increase when the number of transactions increases, however, between 250 and 800 transactions latency shows to be constant. Upon reaching 1000 transactions the latency starts to drop mainly because of the server limitation on which the simulations were being carried out. The average latency of the simulation was 0.114 seconds. The throughput shows an increase from 0 to 400 transactions then it decreases to a throughput of 4TPS level, as the transactions start to go over 850 the throughput decreases and then increases as it approaches 1000 transactions. Therefore, the throughput increases in proportion to the number of transactions but decreases when it reaches a certain threshold for the number of transactions. The average throughput of the simulation was 8.01 transactions per second. Blockchain still faces a challenge of scalability, since when the number of transactions increases they also increase computational requirements [153]. According to [66] Blockchain was not designed to store huge amounts of data so when integrating blockchain with IoT scalability issues must be considered.

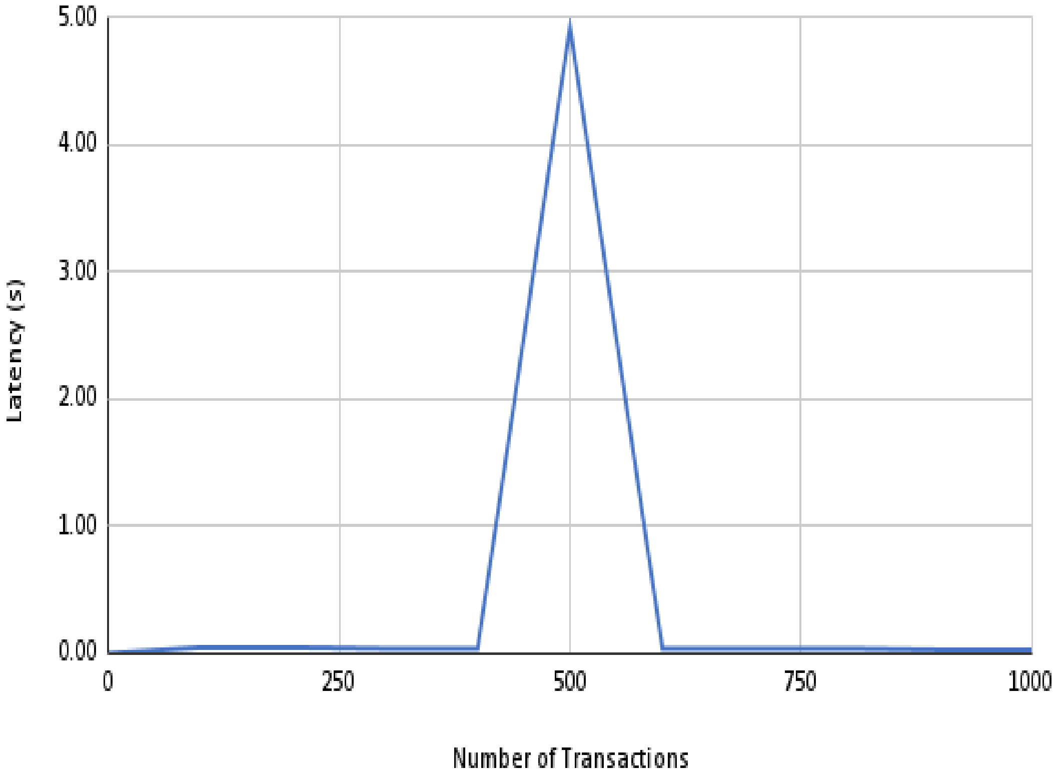


Figure 5.30: GetVaccinationHash Latency vs Number of Transactions

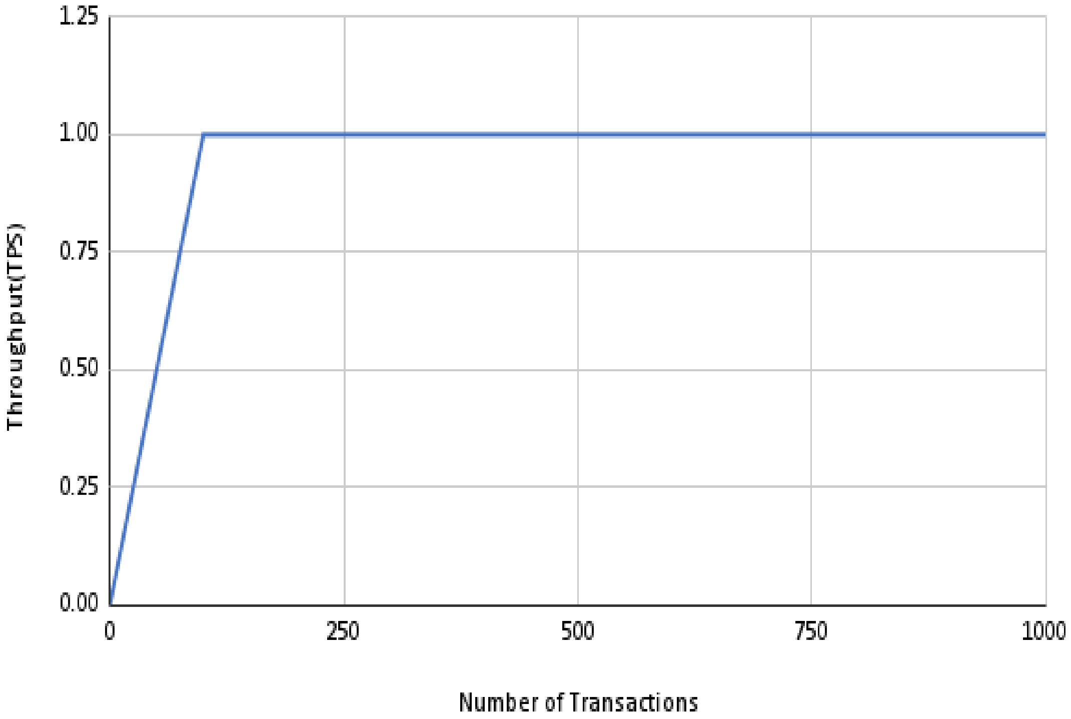


Figure 5.31: GetVaccinationHash Throughput vs Number of Transactions

Moreover, we also measured the latency and throughput of getting vaccinationHash. Figures 5.30 and 5.31 show the latency and throughput of getting the vaccination hash from the blockchain network. The simulation shows that the latency of getting the vaccination hash is constant however when the number of transactions gets to 450 the latency increases and reaches a certain peak decreasing to be constant again. The average latency of getting the vaccination hash from the blockchain is 0.0529s. Furthermore, the simulation results showed that the throughput increases as the number of transactions increases but when it reaches a certain number of transactions the throughput becomes constant. The average throughput was calculated to be 1 transaction per second.

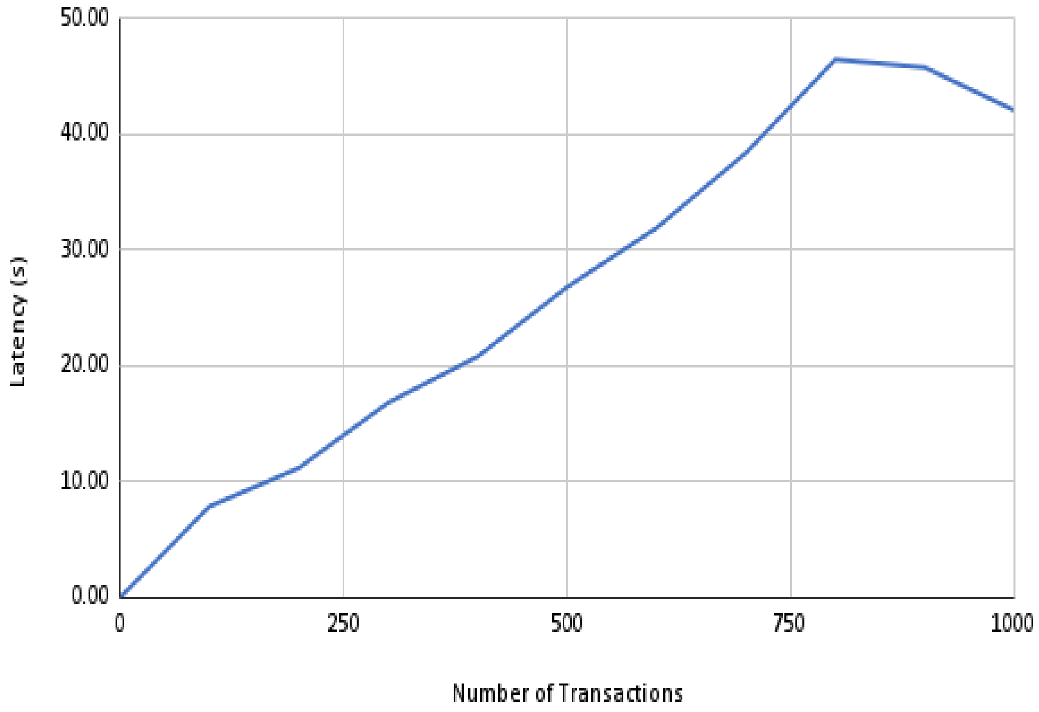


Figure 5.32: User registration latency vs Number of transactions

Finally, we measured the latency and throughput of registering the user on the blockchain's network smart contract.

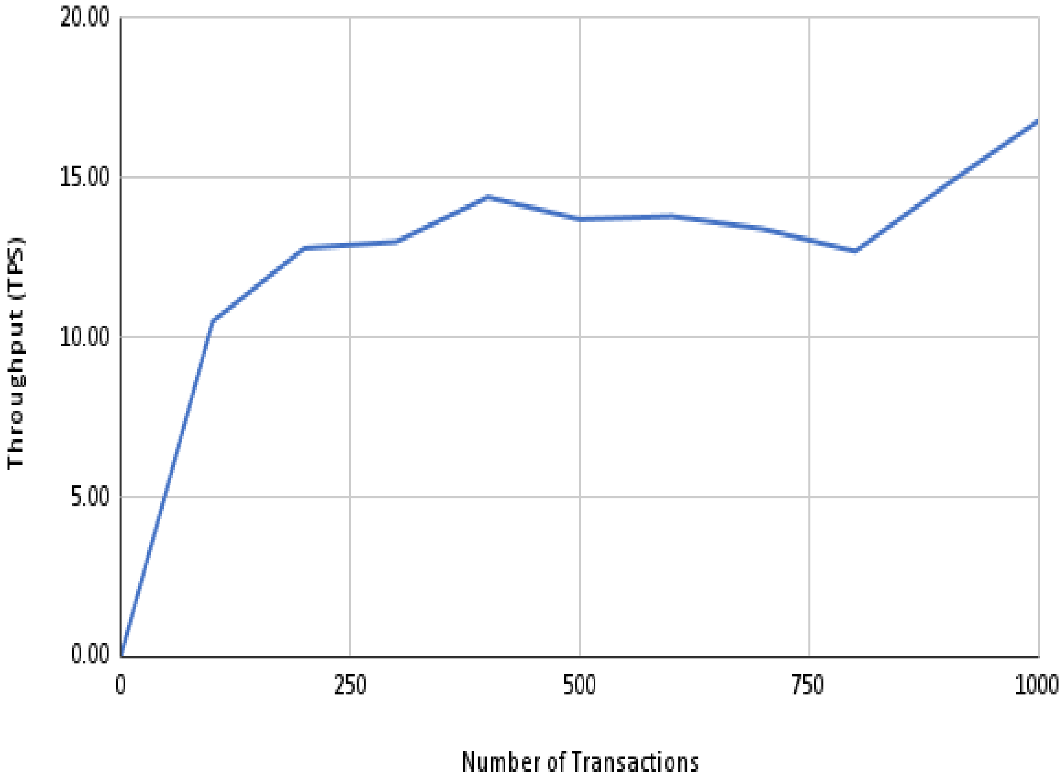


Figure 5.33: User registration throughput vs number of transactions

The latency and throughput of registering the user were presented in Figures 5.32 and 5.33. The results show that latency increases as the number of transactions increases. Therefore, we can say latency is directly proportional to the number of transactions. The average number calculated for the latency is 28.8 seconds. Furthermore, as the number of transactions increases the throughput showed an increase as well however when it reaches 300 transactions it starts to be constant with no change. The average throughput calculated is 13.59 transactions per second.

Table 5.3: Summary of performance metrics

Name	**Success**	**Fail**	**Send Rate(TPS)**	**Max Latency (s)**	**Min Latency (s)**	**Avg Latency (s)**	**Throughput (TPS)**
RegisterUser	1	0	Infinity	0.20	0.20	0.20	5.0
AddVaccination	1000	0	85.9	72.94	0.40	57.61	12.9
GetvaccinationHash	1000	0	1.0	0.09	0.04	0.04	1.0

5.6 Security Analysis

The enhancement of the security and privacy of patients' data was one of the goals of this study. As a result, we used blockchain technology because of its cryptographic foundation and blockchain networks are known to be highly safe, resilient and robust [152].

5.6.1 Privacy

For this study, the proposed solution was developed on the Ethereum blockchain which is a public blockchain. However, this solution can also be implemented on permissioned blockchain networks which will then enhance privacy. Blockchain is also known for its high level of privacy since it keeps its public keys anonymous [96], [164]. The VMS encrypts the data before it sends it to the smart contract which provides another layer of privacy.

5.6.2 Data integrity

The integrity of data is a vital component of security needs. Because of its cryptographic underpinnings, blockchain provides in-built integrity protection since it is tamper-proof. After data has been put on the blockchain network, it is almost difficult for anybody to tamper or modify it. As a result of the immutability of user access control roles and challenges that are issued to the user's private key, the system forbids any alterations to any of these aspects [152], [165], [166]. As such data integrity is well maintained in our system.

5.6.3 Availability

Another important security aspect is availability; our architecture ensures that all information appropriate to the verification and authentication procedures stored on the blockchain is always accessible. Each node replicates and updates the transaction data. The functionality of the network will not be affected in any way, regardless of whether a node was removed from it accidentally, intentionally, or for any other reason. As a direct result of this, our system is designed to provide a very high degree of availability [165], [166], [96].

5.6.4 Access control

Users are permitted to conduct transactions on the blockchain, and all users must be authenticated before they use the system. Access control is important because in our system only the **registering_authority** must register the user and the vaccination authority must verify the certificate. Therefore the system must not allow any illegal entities to submit transactions [152], [164].

5.6.5 Transparency

"Transparency" describes one of the features of the blockchain in which all nodes have access to the system’s records and where any alterations to those records are also visible to all nodes, allowing the blockchain network to be trusted. Due to the vast amount of computational power needed to make modifications to the blockchain network, it is thus impossible to criticise [147].

Table 5.4: Comparison with related works

Ref.	Application	Type of Blockchain	Performance	Security
[167]	Electronic Health Records	Consortium	When there are more outstanding transactions, mining becomes more time-consuming.	Access control Lists were used to manage different operations.
[168]	Vaccine supply and management	Ethereum	According to the authors, the transaction time was reasonable for real-world applications.	-
[165]	Certificate validation	Ethereum	The performance was satisfactory to meet the requirements.	IPFS (Interplanetary File system) Smart Contracts Self-Sovereign Identity.
[169]	Digital passports	Private Blockchain	-	Smart Contracts.
[170]	Medical Data Sharing	Hyper ledger Fabric	The network performance was similar to centralised systems.	Birthday attack model to prevent hash collisions.
[96]	Data Security and Privacy	Fortified Chain	The system has proved to deliver faster file transactions. The system maintains a local cache to reduce costs.	Tamper-proof public ledgers. Smart Contract.

[67]	Data management	Ethereum	-	Smart Contract.
[171]	Verification of data	Ethereum	Verification probabilities greater than 99.99% may be attained at a reduced price.	Smart Contract.
[46]	Medical Education	Ethereum	-	IPFS Smart Contracts.
[148]	Data storage and Monitoring	Ethereum	Performance was found satisfactory.	Smart Contract.
This research	Vaccine registration Verification Data privacy Data Security	Ethereum	The response time proved to be fast. As the number of transactions increases, latency also increases. Throughput also increases as the number of transactions increases.	Symmetric Encryption Smart Contracts Access Control.

5.7 System Comparison and Discussions

The centralization of data in the traditional system opens up a lot of possible corruption since authorities can modify data. Therefore, decentralized systems are needed to decrease fraudulent activities surrounding healthcare data. The identification of data-centralized traditional systems led to the implementation of the VMS. The VMS implementation runs on a local blockchain network, which allows registering of patient details and storing of vaccination details to the smart contract deployed on the blockchain then encrypts the data using symmetric encryption before the data is stored on the smart contract. Since healthcare institutions are known for processing large quantities of data almost every day, it increases the risk of cyber-attacks thus the VMS employs an encryption strategy which encrypts data before storing it making it a cyber-attack-resilient system. Some of the weaknesses of centralized systems compared to decentralized systems are discussed in [152]. The security analysis is done, and it shows that the VMS has enhanced data integrity, confidentiality, privacy and security. Similar results were observed from previous studies such as [67], [165], [171] which makes this consistent with previous studies.

The results of the simulations performed to test the efficiency of the VMS are presented in this chapter. The system was evaluated using parameters such as latency, throughput and response time. As compared to other implementations of previous studies such as [148] and [165] the performance was satisfactory. In addition, prior research confirms that the latency, response time and throughput all increase with an increasing number of transactions; however, these metrics show some variation between testing servers; this might be due to blockchain scalability problems. Table 5.4 gives a comparison of the research findings with related research in the literature. The results do show that the simulation results are consistent with other studies' findings. In light of the findings of the results and the analysis of this study, it is clear that blockchain technology has the potential to enhance the security, privacy, and efficiency of healthcare systems.

5.8 Comparison between the Blockchain-based System and Traditional Systems

5.8.1 Practical Comparison

This section discusses the comparison between the blockchain-based system and the traditional database system via a series of simulations. The goal was to examine and contrast the performance and effectiveness of both systems. In this case, we measured the response time, throughput, latency and average time per transaction vs the number of threads and represented the results using graphs.

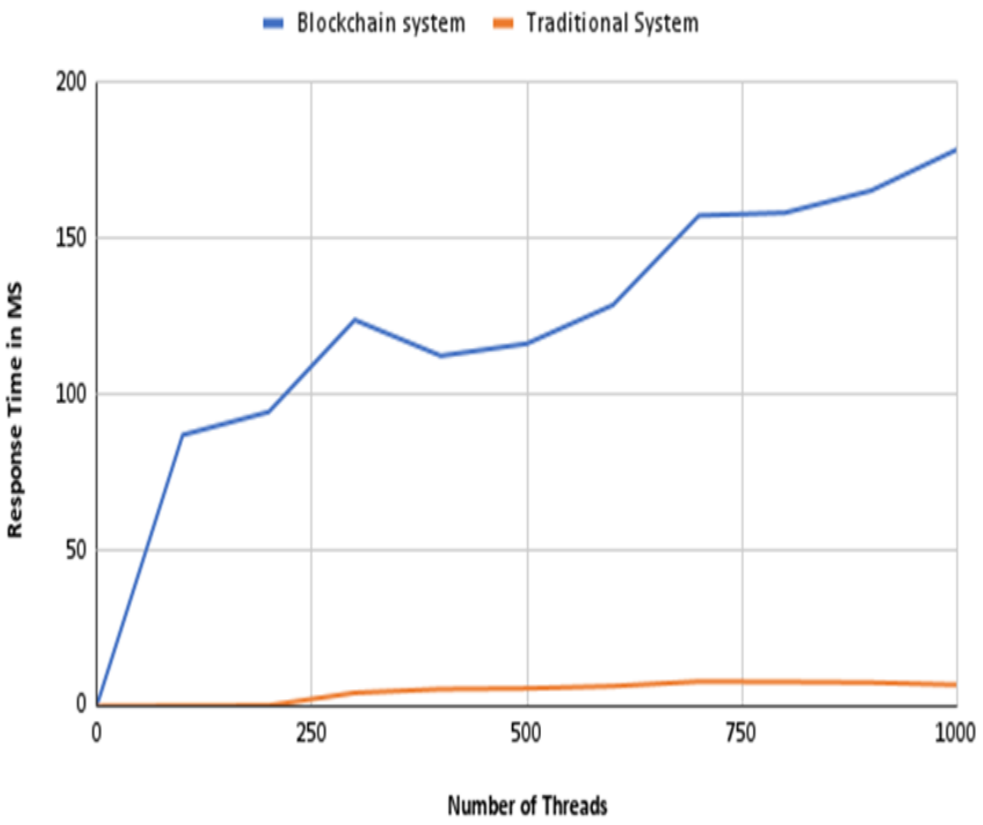


Figure 5.34: Response Time Vs Number of Threads

Figure 5.34 shows the response time of a traditional system and a blockchain-based system, the results show that an increase in the number of threads also leads to an increase in the response time. However, the traditional system has been shown to give a better response time as compared to the blockchain-based system. The reason for this could be that the blockchain system has to adhere to consensus mechanisms and the traditional system does not have any consensus mechanisms.

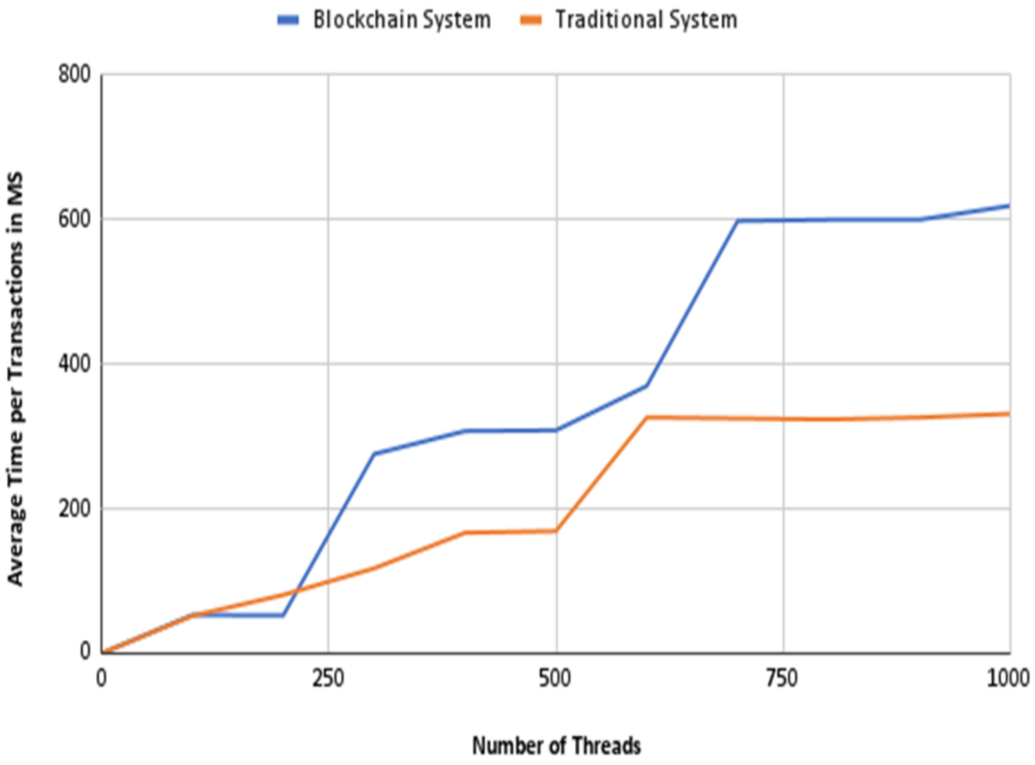


Figure 5.35: Average Time per Transaction vs Number of Threads

Figure 5.35 shows the average time per transaction between a traditional system and a blockchain-based system. The results show that the traditional system can process 1000 transactions in just 0.20 seconds while the blockchain-based system can process 1000 transactions in just about 10-20 seconds.

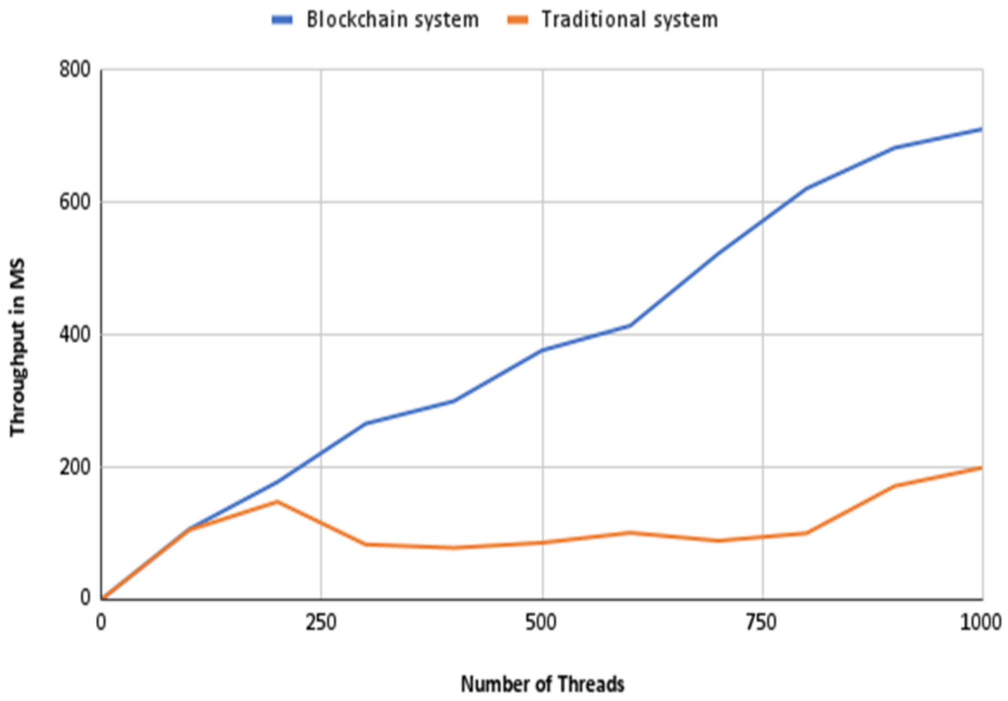


Figure 5.36: Throughput vs Number of Threads

Figure 5.36 shows the throughput of the traditional and blockchain-based systems. According to the results, the average throughput of the traditional system is less than that of the blockchain system. Though in both systems the throughput increases as the number of threads increases.

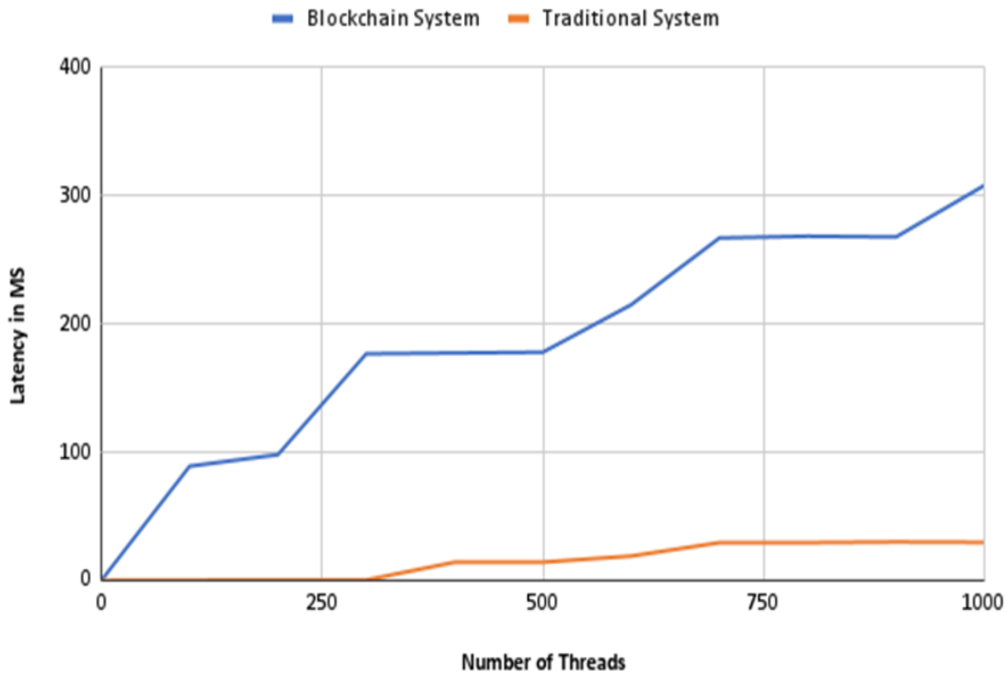


Figure 5.37: Latency vs Number of Threads

Figure 5.37 shows the latency of the traditional system and blockchain-based system, the results showed that the latency of the traditional system is less than that of the blockchain system. However, the relationship between the number of threads and the latency is directly proportional in both systems.

5.8.2 Theoretical comparison

The theoretical comparison of the blockchain-based system and a traditionally-based system in respect of the existing literature is presented in this section. To achieve this, parameters such as latency, throughput, response time security, privacy, transparency, availability, etc. were used. Table 5.5 presents the comparisons made.

Table 5.5: Theoretical comparison of the blockchain system and the traditional

Attribute	Blockchain-based system	Traditionally based system
Latency	High	Low
Response time	Execution takes time due to the consensus algorithm.	Immediate Execution.
Average time per Transaction	Executes 1000 transactions in 12 seconds.	Executes 1000 transactions in 0.20 seconds.
Throughput	High	Low
Data Integrity[166]	Tamperproof	No tamperproof
Data Security[60]	Cryptographic Methods such as ECC are employed. Symmetric Encryption is used to encrypt data.	SHA-256 Encryption is used.
Availability[96]	The system is always available since data is duplicated in different nodes.	A single point of failure is still a problem.
Access Control[152]	Cryptographic techniques are used.	Traditional access control methods.
Transparency[147]	Transparent to all on a public ledger.	Transparency is not maintained as data can be altered.
Privacy[164]	Consensus Algorithms are used to preserve privacy.	-
Data storage	Smart Contracts	SQL database

5.9 Chapter Summary

In this chapter, the results were presented. We were able to examine the effectiveness of blockchain technology as used in the VMS. Some of the benefits of employing blockchain technology in healthcare delivery systems were outlined and an evaluation of the proposed system with related works was presented. Furthermore, from the results, we can undoubtedly say that using blockchain technology in the healthcare system can be an advantage.

Chapter 6

Summary, Conclusion and Recommendations

6.1 Chapter Outline

The general summary, conclusion, recommendations, and future works was presented in this chapter. It summarizes in detail what was done to attain the purpose and objectives of the research. It also identifies the region that needs to be researched for future work.

6.2 Summary

In this research, the goal was to design and implement a privacy-aware efficient vaccination records management system that can register the vaccinated patient, encrypt their data, save the data on the smart contract implemented on the blockchain network and allow the certificate to be scanned using QR-code. The research was conducted in the following manner: In Chapter 1, the research was introduced and the background study on the proposed topic was carried out. Furthermore, the chapter outlined the goals, objectives, problem statement and research questions which were used to answer the research objectives. Additionally, the chapter goes on to briefly describe the research methodology utilized in this study. Chapter 2 focused on outlining the literature on healthcare systems, IoT and blockchain technology. Chapter 2 also explored different types of blockchain, threats to the blockchain network, challenges in the blockchain architecture and some of the benefits of integrating blockchain with healthcare systems. Chapter 3 outlined the methodology adopted in this study, as well as the research methods and the research design process while Chapter 4 discussed the system design and analysis, indicating, in detail, how different components of the system work together to accomplish the purpose of the research study. Chapter 5 outlined the results as well as the discussion based on the simulations performed to assess the efficiency and security of the proposed solution of the study. Finally, Chapter 6 summarized the entire research study, conclusions were drawn, and recommendations and future works were provided.

To meet the intended ROs, the following chapters provide answers to the specified RQs:

RQ1: What is the state-of-the-art practice of registering and verifying vaccinated patients and what technologies are effective in transforming the healthcare system?

RQ1 was answered in Chapter 2 where the researcher conducted an exhaustive literature study to evaluate the current work done in the healthcare system, IoT and blockchain technology. Though IoT was not directly involved in this research, its integration with blockchain in the healthcare ecosystems pave the way for blockchain utilization in this research. The literature study discussed challenges consisting of, but not limited to security, data privacy and efficiency as being faced by the current implemented approaches and what other authors have suggested for solving those challenges. Moreover, the literature study gave insight into how the vaccination management system can be designed to address current challenges.

RQ2: How can an efficient and secure vaccination verification system be designed?

RQ2 was answered in Chapter 2 and Chapter 4. An analysis of what other researchers have done in terms of efficiency, privacy and security of healthcare systems was done before concluding which approach to take for the design proposed in this study. Chapter 4 described how the system can be designed, this included and was not limited to the requirement process, requirements specifications, system modelling, system operation, algorithmic design and system architecture.

RQ3: How can we implement the designed system in RQ2 to evaluate its performance and effectiveness?

RQ3 was answered in Chapter 5. In this chapter, the system implementation presented was based on both software development and simulations to obtain the results. Parameters such as throughput, latency and response time were used to evaluate the performance of the system. The results obtained were then analysed and compared with other similar research in the literature. The study found our results to be consistent with other studies.

6.3 Conclusion

This research study showcases the employment of blockchain technology via the development of the vaccination management system. To achieve this, the researcher used smart contracts and encryption techniques to enhance the privacy and security of the system. To measure the efficiency and effectiveness of the system, simulations were also performed and evaluated against what others had done. Though blockchain technology is known for use in the financial sector, our findings in this study show that the integration of blockchain and the healthcare system is feasible to improve security and privacy. Chapter 5 section 5.6 detailed the security analysis that was done and led to this conclusion. Furthermore, Chapter 5 section 5.5 discussed the simulation results of the system. The results of the system showed that the throughput, latency and response time all increased in direct proportion to the number of transactions. This indicates that there is a directional proportionality in the relationship between the number of transactions and the throughput, latency and response time. However, the comparison between the blockchain-based system and the traditional database system showed that the traditional system responds much faster than the blockchain-based system although in terms of security theoretical evaluations showed that blockchain-based systems are more secure than the traditional system. Additionally, the results show consistency with the current literature since our results also indicate blockchain scalability issues. With the proposed solution, the researcher believes that if blockchain is integrated with healthcare systems as well as other systems, then security, privacy and trust can be achieved which means cyber-attacks and fake documents can be reduced.

6.4 Recommendations, Implications and Future work

A. Recommendations

The proposed solution in this research study brought about a more secure and efficient approach to handling data and information by employing different security techniques. Based on the findings of this research study, the researcher recommends the following to be done:

- The proposed solution should be implemented on a private blockchain and tested on a live server such as the Mainnet or Rinkeby Testnet so that results can be compared with what was found on the public blockchain and local server.
- More research studies should be done on the issue of blockchain scalability.
- Different data encryption algorithms should be employed in the vaccination management system and tested against cyber-attacks to make the system more secure.
- Different privacy models should be employed in the vaccination management system and tested against cyber-attacks to make the system more privacy-aware.

B. Implications

The primary objective of this research study was to implement a solution that will improve data security and privacy among healthcare systems. Furthermore, the solution provided by this study is not limited to improving healthcare systems but other sectors such as academic and voting institutions can benefit in terms of registration and verification of issued data. Moreover, security during data transmission can be improved using the data encryption techniques employed in the proposed solution thus will increase trust in data such as voter registration and election results transmission. Lastly, utilizing smart contracts can reduce fake and counterfeit documentation of birth certificates, marriage certificates and other identity documents.

C. Future Works

In future, the system should be implemented in a way that verifies whether the vaccine has been approved by pharmaceutical authorities as well verify the identity of the patient using the home affairs database as this will help to bring trust in different entities.

References

[1] W. Bodeis and G. P. Corser, "Blockchain adoption, implementation and integration in healthcare application systems," *Conf. Proc. - IEEE SOUTHEASTCON*, vol. 2021-March, pp. 2021–2023, 2021, doi: 10.1109/SoutheastCon45413.2021.9401885.

[2] G. S. Gunanidhi and R. Krishnaveni, "Improved Security Blockchain for IoT based Healthcare monitoring system," *Proc. 2nd Int. Conf. Artif. Intell. Smart Energy, ICAIS 2022*, pp. 1244–1247, 2022, doi: 10.1109/ICAIS53314.2022.9742777.

[3] A. Tandon, A. Dhir, N. Islam, and M. Mäntymäki, "Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda," *Comput. Ind.*, vol. 122, 2020, doi: 10.1016/j.compind.2020.103290.

[4] R. Poorni, M. Lakshmanan, and S. Bhuvaneswari, "DigiCert: A Secured Digital Certificate Application using Blockchain through Smart Contracts," *Proc. 4th Int. Conf. Commun. Electron. Syst. ICCES 2019*, no. Icces, pp. 215–219, 2019, doi: 10.1109/ICCES45898.2019.9002576.

[5] S. Chakraborty, S. Aich, and H. C. Kim, "A Secure Healthcare System Design Framework using Blockchain Technology," *Int. Conf. Adv. Commun. Technol. ICACT*, vol. 2019-Febru, pp. 260–264, 2019, doi: 10.23919/ICACT.2019.8701983.

[6] A. Sharma *et al.*, "Blockchain technology and its applications to combat COVID-19 pandemic," doi: 10.1007/s42600-020-00106-3/Published.

[7] D. Marbouh *et al.*, "Blockchain for COVID-19: Review, Opportunities, and a Trusted Tracking System," *Arab. J. Sci. Eng.*, vol. 45, pp. 9895–9911, 2020, doi: 10.1007/s13369-020-04950-4.

[8] M. U. CHELLADURAI, D. S. Pandian, and D. K. Ramasamy, "A Blockchain based Patient Centric EHR Storage and Integrity Management for e-Health Systems," *Heal. Policy Technol.*, p. 100513, 2021, doi: 10.1016/j.hlpt.2021.100513.

[9] "What is system? - Definition from WhatIs.com." https://www.techtarget.com/searchwindowsserver/definition/system (accessed Jul. 19, 2022).

[10] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Futur. Gener. Comput. Syst.*, vol. 107, pp. 841–853, 2020, doi: 10.1016/j.future.2017.08.020.

[11] M. Torky and A. E. Hassanein, "Integrating blockchain and the internet of things in precision agriculture: Analysis, opportunities, and challenges," *Comput. Electron. Agric.*, vol. 178, no. May, p. 105476, 2020, doi: 10.1016/j.compag.2020.105476.

[12] E. Toch *et al.*, "The Privacy Implications of Cyber Security Systems," *ACM Comput. Surv.*, vol. 51, no. 2, pp. 1–27, 2019, doi: 10.1145/3172869.

[13] "(No Title)," 2007, doi: 10.1002/asi.20508.

[14] S. Poorejbari and W. Mansoor, "Smart healthcare systems on improving the efficiency of healthcare services," *2019 2nd Int. Conf. Signal Process. Inf. Security. ICSPIS 2019*, pp. 1–4, 2019, doi: 10.1109/ICSPIS48135.2019.9045894.

[15] A. I. Sanka *et al.*, "Blockchain-Empowered Multi-Robot Collaboration to Fight COVID-19 and Future Pandemics," *IEEE Access*, vol. 8, no. 1, pp. 10474–10498, 2021, doi: 10.1109/ACCESS.2021.3051051.

[16] K. Azbeg, O. Ouchetto, S. J. Andaloussi, and L. Fetjah, “A Taxonomic Review of the Use of IoT and Blockchain in Healthcare Applications,” *IRBM*, vol. 1, 2021, doi: 10.1016/j.irbm.2021.05.003.

[17] W. Yang, E. Aghasian, S. Garg, D. Herbert, L. Disiuta, and B. Kang, “A Survey on Blockchain-Based Internet Service Architecture: Requirements, Challenges, Trends, and Future,” *IEEE Access*, vol. 7, pp. 75845–75872, 2019, doi: 10.1109/ACCESS.2019.2917562.

[18] K. Azbeg, O. Ouchetto, and S. J. Andaloussi, “BlockMedCare : A healthcare system based on IoT, Blockchain and IPFS for data management security,” *Egypt. Informatics J.*, vol. 23, no. 2, pp. 329–343, 2022, doi: 10.1016/j.eij.2022.02.004.

[19] M. Sookhak, M. R. Jabbarpour, N. S. Safa, and F. R. Yu, “Blockchain and smart contract for access control in healthcare: A survey, issues and challenges, and open issues,” *J. Netw. Comput. Appl.*, vol. 178, no. July 2020, p. 102950, 2021, doi: 10.1016/j.jnca.2020.102950.

[20] G. Rathee, A. Sharma, H. Saini, R. Kumar, and R. Iqbal, “A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology,” *Multimed. Tools Appl.*, vol. 79, no. 15–16, pp. 9711–9733, 2020, doi: 10.1007/s11042-019-07835-3.

[21] P. Harris, “Blockchain for COVID-19 Patient Health Record,” *Proc. - 5th Int. Conf. Comput. Methodol. Commun. ICCMC 2021*, no. Iccmc, pp. 534–538, 2021, doi: 10.1109/ICCMC51019.2021.9418443.

[22] S. A. Goswami, “Internet of Things : Applications,” pp. 47–50, 2019.

[23] T. K. Mackey *et al.*, “‘Fit-for-purpose?’ - Challenges and opportunities for applications of blockchain technology in the future of healthcare,” *BMC Med.*, vol. 17, no. 1, pp. 1–17, 2019, doi: 10.1186/s12916-019-1296-7.

[24] A. Kalla, T. Hewa, R. A. Mishra, M. Ylianttila, and M. Liyanage, “The Role of Blockchain to Fight against COVID-19,” *IEEE Eng. Manag. Rev.*, vol. 48, no. 3, pp. 85–96, 2020, doi: 10.1109/EMR.2020.3014052.

[25] E. Of, “S Ustainable D Evelopment of C Ritical,” *Textb. Influ.*, vol. 24, no. 8, pp. 0–63, 2014, [Online]. Available: http://dx.doi.org/10.1002/9781118636817.ch20%5Cnhttp://onlinelibrary.wiley.com/doi/10.1002/9781118636817.ch20/summary%5Cnhttp://onlinelibrary.wiley.com/store/10.1002/9781118636817.ch20/asset/ch20.pdf?v=1&t=hxhpa5tb&s=c7ecd88d68ad5408bbcee1986b3da261fb63d2.

[26] W. Y. Ng *et al.*, “Review Blockchain applications in health care for COVID-19 and beyond : a systematic review,” *Lancet Digit. Heal.*, vol. 3, no. 12, pp. e819–e829, 2021, doi: 10.1016/S2589-7500(21)00210-7.

[27] Y. Himeur *et al.*, “Blockchain-based recommender systems: Applications, challenges and future opportunities,” *Comput. Sci. Rev.*, vol. 43, p. 100439, 2022, doi: 10.1016/j.cosrev.2021.100439.

[28] M. Aun, “A Secure BlockChain Framework for IoT Healthcare,” 2022.

[29] B. A. Kumar, T. Mohanraj, S. Shahulhammed, and R. Santhosh, “A study of blockchain technologies and health care systems,” *Proc. 4th Int. Conf. IoT Soc. Mobile, Anal. Cloud, ISMAC 2020*, pp. 265–267, 2020, doi: 10.1109/I-SMAC49090.2020.9243529.

[30] S. Saha, A. Majumder, T. Bhowmik, A. Basu, and A. Choudhury, “A Healthcare Data Management System on Blockchain Framework,” *2021 Int. Conf. Smart Gener. Comput. Commun. Networking, SMART GENCON 2021*, pp. 1–5, 2021, doi: 10.1109/SMARTGENCON51891.2021.9645890.

[31] R. Kumar, N. Marchang, and R. Tripathi, “Distributed Off-Chain Storage of Patient Diagnostic Reports in Healthcare System Using IPFS and Blockchain,” *2020 Int. Conf. Commun. Syst. NETworkS, COMSNETS 2020*, pp. 1–5, 2020, doi: 10.1109/COMSNETS48256.2020.9027313.

[32] M. S. Ferdous, M. J. M. Chowdhury, and M. A. Hoque, “A survey of consensus algorithms in public blockchain systems for crypto-currencies,” *J. Netw. Comput. Appl.*, vol. 182, no. February, p. 103035, 2021, doi: 10.1016/j.jnca.2021.103035.

[33] A. I. Sanka, M. Irfan, I. Huang, and R. C. C. Cheung, “A survey of breakthrough in blockchain technology: Adoptions, applications, challenges and future research,” *Comput. Commun.*, vol. 169, no. December 2020, pp. 179–201, 2021, doi: 10.1016/j.comcom.2020.12.028.

[34] A. L. Phelan, “COVID-19 immunity passports and vaccination certificates: scientific, equitable, and legal challenges,” *Lancet*, vol. 395, no. 10237, pp. 1595–1598, 2020, doi: 10.1016/S0140-6736(20)31034-5.

[35] L. Ricci, D. Di Francesco Maesa, A. Favenza, and E. Ferro, “Blockchains for covid-19 contact tracing and vaccine support: A systematic review,” *IEEE Access*, vol. 9, pp. 37936–37950, 2021, doi: 10.1109/ACCESS.2021.3063152.

[36] T. Singhal, “A Review of Coronavirus Disease-2019 (COVID-19),” *Indian J. Pediatr.*, vol. 87, no. 4, pp. 281–286, 2020, doi: 10.1007/s12098-020-03263-6.

[37] M. Filali Rotbi[1], S. Motahhir[2], and A. El Ghzizal[1], “Blockchain technology for a Safe and Transparent Covid-19 Vaccination.”

[38] K. K. F. Tsoi, J. J. Y. Sung, H. W. Y. Lee, K. K. L. Yiu, H. Fung, and S. Y. S. Wong, “The way forward after COVID-19 vaccination: Vaccine passports with blockchain to protect personal privacy,” *BMJ Innov.*, vol. 7, no. 2, pp. 337–341, 2021, doi: 10.1136/bmjinnov-2021-000661.

[39] C. M. Angelopoulos, A. Damianou, and V. Katos, “DHP Framework: Digital Health Passports Using Blockchain -- Use case on international tourism during the COVID-19 pandemic,” 2020, doi: 10.1111/j.1365-2966.2005.08922.x.

[40] H. John Leon Singh, D. Couch, and K. Yap, “Mobile Health Apps That Help With COVID-19 Management: Scoping Review,” *JMIR Nurs.*, vol. 3, no. 1, p. e20596, 2020, doi: 10.2196/20596.

[41] Who, “Changes from the previous version,” 2020, [Online]. Available: https://www.who.int/publications/i/item/considerations-in-adjusting-public-health-and-social-measures-in-the-context-of-covid-19-interim-guidance.

[42] R. Weber, *Design-science research*. 2018.

[43] R. Budiono and M. C. Z. Candra, “Managing COVID-19 Test Certificates Using Blockchain Platform,” *Proc. 2021 Int. Conf. Data Softw. Eng. Data Softw. Eng. Support. Sustain. Dev. Goals, ICoDSE 2021*, pp. 1–5, 2021, doi: 10.1109/ICoDSE53690.2021.9648482.

[44] T. T. Huynh, T. Tru Huynh, D. K. Pham, and A. Khoa Ngo, “Issuing and Verifying

Digital Certificates with Blockchain," *Int. Conf. Adv. Technol. Commun.*, vol. 2018-Octob, pp. 332–336, 2018, doi: 10.1109/ATC.2018.8587428.

[45] P. Dutta, T. M. Choi, S. Somani, and R. Butala, "Blockchain technology in supply chain operations: Applications, challenges and research opportunities," *Transp. Res. Part E Logist. Transp. Rev.*, vol. 142, no. August, p. 102067, 2020, doi: 10.1016/j.tre.2020.102067.

[46] J. Rathod, A. Gupta, and D. Patel, "Using Blockchain Technology for Continuing Medical Education Credits System," *2020 7th Int. Conf. Softw. Defin. Syst. SDS 2020*, pp. 214–219, 2020, doi: 10.1109/SDS49854.2020.9143876.

[47] S. Brotsis, K. Limniotis, G. Bendiab, N. Kolokotronis, and S. Shiaeles, "On the suitability of blockchain platforms for IoT applications: Architectures, security, privacy, and performance," *Comput. Networks*, vol. 191, no. March, p. 108005, 2021, doi: 10.1016/j.comnet.2021.108005.

[48] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "Continuous Patient Monitoring with a Patient Centric Agent: A Block Architecture," *IEEE Access*, vol. 6, pp. 32700–32726, 2018, doi: 10.1109/ACCESS.2018.2846779.

[49] H. G. Abdul-Rahman, "University of Ghana http://ugspace.ug.edu.gh School Of Public Health College Of Health Sciences University Of Ghana Development Of Patient Record Management System For Yendi Health Centre By Hassanatu Gomdah Abdul-Rahman This Health Informatics Practicum," no. 10636998, 2018.

[50] A. Shahnaz, U. Qamar, and A. Khalid, "Using Blockchain for Electronic Health Records," *IEEE Access*, vol. 7, pp. 147782–147795, 2019, doi: 10.1109/ACCESS.2019.2946373.

[51] P. Patil, M. Sangeetha, and V. Bhaskar, "Blockchain for IoT Access Control, Security and Privacy: A Review," *Wirel. Pers. Commun.*, vol. 117, no. 3, pp. 1815–1834, 2021, doi: 10.1007/s11277-020-07947-2.

[52] S. D. Kulkarni, V. Roshni, S. Varshitha, M. V. Sandeep, T. Monish, and V. Venkataraman, "Modelling the patient flow in an out Patient Department (OPD) of a hospital using simulation techniques," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 1059, no. 1, 2021, doi: 10.1088/1757-899X/1059/1/012041.

[53] M. Zakirul *et al.*, "Blockchain and Big Data to Transform the Healthcare," 2018, doi: 10.1145/3224207.3224220.

[54] S. Chenthara, K. Ahmed, H. Wang, and F. Whittaker, "Security and Privacy-Preserving Challenges of e-Health Solutions in Cloud Computing," *IEEE Access*, vol. 7, pp. 74361–74382, 2019, doi: 10.1109/ACCESS.2019.2919982.

[55] O. Ali, A. Shrestha, J. Soar, and S. F. Wamba, "Cloud computing-enabled healthcare opportunities, issues, and applications: A systematic review," *Int. J. Inf. Manage.*, vol. 43, no. July, pp. 146–158, 2018, doi: 10.1016/j.ijinfomgt.2018.07.009.

[56] R. Ganiga, R. M. Pai, M. Pai, and R. K. Sinha, "Private cloud solution for Securing and Managing Patient Data in Rural Healthcare System," *Procedia Comput. Sci.*, vol. 135, pp. 688–699, 2018, doi: 10.1016/j.procs.2018.08.217.

[57] M. Javaid, A. Haleem, R. P. Singh, S. Rab, R. Suman, and I. H. Khan, "Evolutionary trends in progressive cloud computing based healthcare: Ideas, enablers, and barriers," *Int. J. Cogn. Comput. Eng.*, vol. 3, no. February, pp. 124–135, 2022, doi:

10.1016/j.ijcce.2022.06.001.

[58] Y. Al-Issa, M. A. Ottom, and A. Tamrawi, “EHealth Cloud Security Challenges: A Survey,” *J. Healthc. Eng.*, vol. 2019, 2019, doi: 10.1155/2019/7516035.

[59] D. K. Taylor Hardin, “Blockchain in Health Data Systems: a Survey,” *Education*, vol. 6, pp. 135–160, 2019.

[60] M. J. M. Chowdhury, A. Colman, M. A. Kabir, J. Han, and P. Sarda, “Blockchain Versus Database: A Critical Analysis,” *Proc. - 17th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. 12th IEEE Int. Conf. Big Data Sci. Eng. Trust. 2018*, pp. 1348–1353, 2018, doi: 10.1109/TrustCom/BigDataSE.2018.00186.

[61] T. Gabriel, A. Cornel-Cristian, M. Arhip-Calin, and A. Zamfirescu, “Cloud Storage. A comparison between centralized solutions versus decentralized cloud storage solutions using Blockchain technology,” *2019 54th Int. Univ. Power Eng. Conf. UPEC 2019 - Proc.*, 2019, doi: 10.1109/UPEC.2019.8893440.

[62] A. I. Sanka and R. C. C. Cheung, “A systematic review of blockchain scalability: Issues, solutions, analysis and future research,” *J. Netw. Comput. Appl.*, vol. 195, no. October 2021, doi: 10.1016/j.jnca.2021.103232.

[63] G. Tripathi, M. A. Ahad, and S. Paiva, “S2HS- A blockchain based approach for smart healthcare system,” *Healthcare*, vol. 8, no. 1, p. 100391, 2020, doi: 10.1016/j.hjdsi.2019.100391.

[64] C. Hofisi, L. C.-I. J. Of, and U. 2021, “Challenges and Opportunities of South Africa’s Electronic Vaccination Data System in the Provision of COVID-19 Vaccines,” *Scholar.Lifescienceglobal.Com*, pp. 1474–1480, 2021, [Online]. Available: https://scholar.lifescienceglobal.com/pms/index.php/ijcs/article/view/8428.

[65] R. P. Singh, M. Javaid, A. Haleem, and R. Suman, “Internet of things (IoT) applications to fight against COVID-19 pandemic,” *Diabetes Metab. Syndr. Clin. Res. Rev.*, vol. 14, no. 4, pp. 521–524, 2020, doi: 10.1016/j.dsx.2020.04.041.

[66] S. Saxena, B. Bhushan, and M. A. Ahad, “Blockchain based solutions to secure IoT: Background, integration trends and a way forward,” *J. Netw. Comput. Appl.*, vol. 181, no. December 2020, p. 103050, 2021, doi: 10.1016/j.jnca.2021.103050.

[67] T. Frikha, A. Chaari, F. Chaabane, O. Cheikhrouhou, and A. Zaguia, “Healthcare and Fitness Data Management Using the IoT-Based Blockchain Platform,” *J. Healthc. Eng.*, vol. 2021, no. ii, 2021, doi: 10.1155/2021/9978863.

[68] P. Varma Kakarlapudi, Q. H. Mahmoud, and Q. A. Systematic, “healthcare A Systematic Review of Blockchain for Consent Management,” 2021, doi: 10.3390/healthcare.

[69] T. Rathee and P. Singh, “A systematic literature mapping on secure identity management using blockchain technology,” *J. King Saud Univ. - Comput. Inf. Sci.*, no. xxxx, 2021, doi: 10.1016/j.jksuci.2021.03.005.

[70] M. Niranjanamurthy, B. N. Nithya, and S. Jagannatha, “Analysis of Blockchain technology: pros, cons and SWOT,” *Cluster Comput.*, vol. 22, no. s6, pp. 14743–14757, 2019, doi: 10.1007/s10586-018-2387-5.

[71] A. A. Monrat, O. Schelén, and K. Andersson, “A survey of blockchain from the perspectives of applications, challenges, and opportunities,” *IEEE Access*, vol. 7, pp. 117134–117151, 2019, doi: 10.1109/ACCESS.2019.2936094.

[72] T. Hewa, M. Ylianttila, and M. Liyanage, “Survey on blockchain based smart contracts: Applications, opportunities and challenges,” *J. Netw. Comput. Appl.*, vol. 177, no. February 2020, p. 102857, 2021, doi: 10.1016/j.jnca.2020.102857.

[73] D. Berdik, S. Otoum, N. Schmidt, D. Porter, and Y. Jararweh, “A Survey on Blockchain for Information Systems Management and Security,” *Inf. Process. Manag.*, vol. 58, no. 1, p. 102397, 2021, doi: 10.1016/j.ipm.2020.102397.

[74] B. Bhushan, P. Sinha, K. M. Sagayam, and A. J, “Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions,” *Comput. Electr. Eng.*, vol. 90, no. July 2019, p. 106897, 2021, doi: 10.1016/j.compeleceng.2020.106897.

[75] H. Wang, Z. Zheng, S. Xie, H. N. Dai, and X. Chen, “Blockchain challenges and opportunities: a survey,” *Int. J. Web Grid Serv.*, vol. 14, no. 4, p. 352, 2018, doi: 10.1504/ijwgs.2018.10016848.

[76] A. Haleem, M. Javaid, R. P. Singh, R. Suman, and S. Rab, “Blockchain technology applications in healthcare: An overview,” *Int. J. Intell. Networks*, vol. 2, pp. 130–139, Jan. 2021, doi: 10.1016/J.IJIN.2021.09.005.

[77] J. Bernal Bernabe, J. L. Canovas, J. L. Hernandez-Ramos, R. Torres Moreno, and A. Skarmeta, “Privacy-Preserving Solutions for Blockchain: Review and Challenges,” *IEEE Access*, vol. 7, pp. 164908–164940, 2019, doi: 10.1109/ACCESS.2019.2950872.

[78] I. Makhdoom, M. Abolhasan, H. Abbas, and W. Ni, “Blockchain’s adoption in IoT: The challenges, and a way forward,” *J. Netw. Comput. Appl.*, vol. 125, no. September 2018, pp. 251–279, 2019, doi: 10.1016/j.jnca.2018.10.019.

[79] A. Pieroni, N. Scarpato, and L. Felli, “Blockchain and IoT convergence—a systematic survey on technologies, protocols and security,” *Appl. Sci.*, vol. 10, no. 19, pp. 1–23, 2020, doi: 10.3390/app10196749.

[80] M. Z. L.M. Bach, B. Mihaljevic, “Comparative Analysis of Blockchain Consensus Algorithms,” pp. 1545–1550, 2018.

[81] S. M. H. Bamakan, A. Motavali, and A. Babaei Bondarti, “A survey of blockchain consensus algorithms performance evaluation criteria,” *Expert Syst. Appl.*, vol. 154, 2020, doi: 10.1016/j.eswa.2020.113385.

[82] S. S. Panda, B. K. Mohanta, U. Satapathy, D. Jena, D. Gountia, and T. K. Patra, “Study of Blockchain Based Decentralized Consensus Algorithms,” *IEEE Reg. 10 Annu. Int. Conf. Proceedings/TENCON*, vol. 2019-Octob, pp. 908–913, 2019, doi: 10.1109/TENCON.2019.8929439.

[83] Z. Zheng *et al.*, “An overview on smart contracts: Challenges, advances and platforms,” *Futur. Gener. Comput. Syst.*, vol. 105, pp. 475–491, 2020, doi: 10.1016/j.future.2019.12.019.

[84] U. Bodkhe, D. Mehta, S. Tanwar, P. Bhattacharya, P. K. Singh, and W. C. Hong, “A survey on decentralized consensus mechanisms for cyber physical systems,” *IEEE Access*, vol. 8, pp. 54371–54401, 2020, doi: 10.1109/ACCESS.2020.2981415.

[85] P. G. Vishnu Gopal and G. Mathew, “Blockchain Based Verification of Vehicle History for Pre-owned Vehicle Industry,” *ICCISc 2021 - 2021 Int. Conf. Commun. Control Inf. Sci. Proc.*, 2021, doi: 10.1109/ICCISc52257.2021.9484896.

[86] M. Mircea, M. Stoica, and B. Ghilic-Micu, “Analysis of the Impact of Blockchain and

Internet of Things (BIoT) on Public Procurement," *IEEE Access*, vol. 10, pp. 63353–63374, 2022, doi: 10.1109/access.2022.3182656.

[87] R. A. Canessane, N. Srinivasan, A. Beuria, A. Singh, and B. M. Kumar, "Decentralised Applications Using Ethereum Blockchain," *5th Int. Conf. Sci. Technol. Eng. Math. ICONSTEM 2019*, pp. 75–79, 2019, doi: 10.1109/ICONSTEM.2019.8918887.

[88] U. Majeed, L. U. Khan, I. Yaqoob, S. M. A. Kazmi, K. Salah, and C. S. Hong, "Blockchain for IoT-based smart cities: Recent advances, requirements, and future challenges," *J. Netw. Comput. Appl.*, vol. 181, no. February, p. 103007, 2021, doi: 10.1016/j.jnca.2021.103007.

[89] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Futur. Gener. Comput. Syst.*, vol. 88, no. 2018, pp. 173–190, 2018, doi: 10.1016/j.future.2018.05.046.

[90] K. Khujamatov, E. Reypnazarov, N. Akhmedov, and D. Khasanov, "Blockchain for 5G healthcare architecture," *2020 Int. Conf. Inf. Sci. Commun. Technol. ICISCT 2020*, 2020, doi: 10.1109/ICISCT50599.2020.9351398.

[91] E. Toufaily, T. Zalan, and S. Ben Dhaou, "A framework of blockchain technology adoption: An investigation of challenges and expected value," *Inf. Manag.*, vol. 58, no. 3, p. 103444, 2021, doi: 10.1016/j.im.2021.103444.

[92] H. M. Hussien, S. M. Yasin, N. I. Udzir, M. I. H. Ninggal, and S. Salman, "Blockchain technology in the healthcare industry: Trends and opportunities," *J. Ind. Inf. Integr.*, vol. 22, no. November 2020, p. 100217, 2021, doi: 10.1016/j.jii.2021.100217.

[93] B. Hu *et al.*, "A comprehensive survey on smart contract construction and execution: paradigms, tools, and systems," *Patterns*, vol. 2, no. 2, p. 100179, 2021, doi: 10.1016/j.patter.2020.100179.

[94] M. A. Jan *et al.*, "Security and blockchain convergence with Internet of Multimedia Things: Current trends, research challenges and future directions," *J. Netw. Comput. Appl.*, vol. 175, no. May 2020, p. 102918, 2021, doi: 10.1016/j.jnca.2020.102918.

[95] E. Zaghloul, T. Li, M. W. Mutka, and J. Ren, "Bitcoin and Blockchain: Security and Privacy," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10288–10313, 2020, doi: 10.1109/JIOT.2020.3004273.

[96] B. S. Egala, A. K. Pradhan, V. Badarla, and S. P. Mohanty, "Fortified-Chain: A Blockchain-Based Framework for Security and Privacy-Assured Internet of Medical Things with Effective Access Control," *IEEE Internet Things J.*, vol. 8, no. 14, pp. 11717–11731, 2021, doi: 10.1109/JIOT.2021.3058946.

[97] "Elliptic Curve Cryptography - KeyCDN Support." https://www.keycdn.com/support/elliptic-curve-cryptography (accessed Jul. 13, 2022).

[98] A. Khatoon, P. Verma, J. Southernwood, B. Massey, and P. Corcoran, "Blockchain in Energy Efficiency: Potential Applications and Benefits," doi: 10.3390/en12173317.

[99] S. Shi, D. He, L. Li, N. Kumar, M. K. Khan, and K. K. R. Choo, "Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey," *Comput. Secur.*, vol. 97, 2020, doi: 10.1016/j.cose.2020.101966.

[100] P. Matta, M. Arora, and D. Sharma, "A comparative survey on data encryption Techniques: Big data perspective," *Mater. Today Proc.*, vol. 46, pp. 11035–11039, 2021, doi: 10.1016/j.matpr.2021.02.153.

[101] Rismayani and C. Susanto, “Using AES and des Cryptography for System Development File Submission Security Mobile-Based,” *2020 8th Int. Conf. Cyber IT Serv. Manag. CITSM 2020*, 2020, doi: 10.1109/CITSM50537.2020.9268805.

[102] V. Verma, P. Kumar, R. K. Verma, and S. Priya, “A Novel Approach for Security in Cloud Data Storage Using AES-DES-RSA Hybrid Cryptography,” *2021 IEEE Int. Conf. Emerg. Trends Ind. 4.0, ETI 4.0 2021*, 2021, doi: 10.1109/ETI4.051663.2021.9619274.

[103] J. A. Alzubi, “Blockchain-based Lamport Merkle Digital Signature: Authentication tool in IoT healthcare,” *Comput. Commun.*, vol. 170, no. April 2020, pp. 200–208, 2021, doi: 10.1016/j.comcom.2021.02.002.

[104] S. A. ElRahman and A. S. Alluhaidan, “Blockchain technology and IoT-edge framework for sharing healthcare services,” *Soft Comput.*, vol. 4, no. Lueth 2015, 2021, doi: 10.1007/s00500-021-06041-4.

[105] T. McGhin, K. K. R. Choo, C. Z. Liu, and D. He, “Blockchain in healthcare applications: Research challenges and opportunities,” *J. Netw. Comput. Appl.*, vol. 135, no. September 2018, pp. 62–75, 2019, doi: 10.1016/j.jnca.2019.02.027.

[106] O. Ajayi, M. Abouali, and T. Saadawi, “Secured Inter-Healthcare Patient Health Records Exchange Architecture,” *Proc. - 2020 IEEE Int. Conf. Blockchain, Blockchain 2020*, pp. 456–461, 2020, doi: 10.1109/Blockchain50366.2020.00066.

[107] A. Saini, Q. Zhu, N. Singh, Y. Xiang, L. Gao, and Y. Zhang, “A smart-contract-based access control framework for cloud smart healthcare system,” *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5914–5925, 2021, doi: 10.1109/JIOT.2020.3032997.

[108] M. N. Thippeswamy, B. M. Sai Kiran, P. R. Tanksali, M. Hegde, and P. R. Naik, “Block chain based medical reports monitoring system,” *Proc. 4th Int. Conf. IoT Soc. Mobile, Anal. Cloud, ISMAC 2020*, pp. 222–227, 2020, doi: 10.1109/I-SMAC49090.2020.9243573.

[109] M. Ammi, S. Alarabi, and E. Benkhelifa, “Customized blockchain-based architecture for secure smart home for lightweight IoT,” *Inf. Process. Manag.*, vol. 58, no. 3, 2021, doi: 10.1016/j.ipm.2020.102482.

[110] S. Shukla, S. Thakur, S. Hussain, J. G. Breslin, and S. M. Jameel, “Identification and Authentication in Healthcare Internet-of-Things Using Integrated Fog Computing Based Blockchain Model,” *Internet of Things (Netherlands)*, vol. 15, p. 100422, 2021, doi: 10.1016/j.iot.2021.100422.

[111] F. Fotopoulos, V. Malamas, T. K. Dasaklis, P. Kotzanikolaou, and C. Douligeris, “A Blockchain-enabled Architecture for IoMT Device Authentication,” *2nd IEEE Eurasia Conf. IoT, Commun. Eng. 2020, ECICE 2020*, pp. 89–92, 2020, doi: 10.1109/ECICE50847.2020.9301913.

[112] G. S. Aujla and A. Jindal, “A Decoupled Blockchain Approach for Edge-Envisioned IoT-Based Healthcare Monitoring,” *IEEE J. Sel. Areas Commun.*, vol. 39, no. 2, pp. 491–499, 2021, doi: 10.1109/JSAC.2020.3020655.

[113] O. Attia, I. Khoufi, A. Laouiti, and C. Adjih, “An IoT-Blockchain architecture based on hyperledger framework for healthcare monitoring application,” *2019 10th IFIP Int. Conf. New Technol. Mobil. Secur. NTMS 2019 - Proc. Work.*, 2019, doi: 10.1109/NTMS.2019.8763849.

[114] P. P. Ray, B. Chowhan, N. Kumar, and A. Almogren, “BIoTHR: Electronic Health

Record Servicing Scheme in IoT-Blockchain Ecosystem," *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10857–10872, 2021, doi: 10.1109/JIOT.2021.3050703.

[115] W. Yanez, R. Mahmud, R. Bahsoon, Y. Zhang, and R. Buyya, "Data Allocation Mechanism for Internet-of-Things Systems With Blockchain," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3509–3522, 2020, doi: 10.1109/JIOT.2020.2972776.

[116] M. T. Quasim, A. A. E. Radwan, G. M. M. Alshmrani, and M. Meraj, "A blockchain framework for secure electronic health records in healthcare industry," *Proc. Int. Conf. Smart Technol. Comput. Electr. Electron. ICSTCEE 2020*, pp. 605–609, 2020, doi: 10.1109/ICSTCEE49637.2020.9277193.

[117] H. L. Pham, T. H. Tran, and Y. Nakashima, "A Secure Remote Healthcare System for Hospital Using Blockchain Smart Contract," *2018 IEEE Globecom Work. GC Wkshps 2018 - Proc.*, 2019, doi: 10.1109/GLOCOMW.2018.8644164.

[118] D. D. Taralunga and B. C. Florea, "A blockchain-enabled framework for mhealth systems," *Sensors*, vol. 21, no. 8, pp. 1–24, 2021, doi: 10.3390/s21082828.

[119] A. Bhawiyuga, A. Wardhana, K. Amron, and A. P. Kirana, "Platform for integrating internet of things based smart healthcare system and blockchain network," *Proc. - 2019 6th NAFOSTED Conf. Inf. Comput. Sci. NICS 2019*, pp. 55–60, 2019, doi: 10.1109/NICS48868.2019.9023797.

[120] A. Abbas, R. Alroobaea, M. Krichen, S. Rubaiee, S. Vimal, and F. M. Almansour, "Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things," *Pers. Ubiquitous Comput.*, 2021, doi: 10.1007/s00779-021-01583-8.

[121] M. S. Mortensen, "D Evelopment of a C Ampylobacter V Accine for P Oultry," *Textb. Influ.*, vol. 24, no. 11, pp. 1–5, 2021, [Online]. Available: http://dx.doi.org/10.1002/9781118636817.ch20%5Cnhttp://onlinelibrary.wiley.com/doi/10.1002/9781118636817.ch20/summary%5Cnhttp://onlinelibrary.wiley.com/store/10.1002/9781118636817.ch20/asset/ch20.pdf?v=1&t=hxhpa5tb&s=c7ecd88d68ad5408bbcee1986b3da261fb63d2.

[122] C. G. Thomas, *Research Methodology and Scientific Writing 2nd editions*, vol. 2, no. 1. 2021.

[123] S. Robinson, *Research Methodology*, vol. 50, no. 2. 2011.

[124] M. B. • J. Hansson and B. O. • B. Lundell, *Thesis Projects: A Guide for Students in Computer Science and Information Systems Second Edition*, vol. 7, no. 2. 1967.

[125] C. Dawson, "Introduction to Research Methods," *How To Content*, vol. 53, no. 9, pp. 1689–1699, 2013.

[126] W. J. Creswell and J. D. Creswell, *Research Design: Qualitative, Quantitative adn Mixed Methods Approaches*, vol. 53, no. 9. 2018.

[127] P. Johannesson and E. Perjons, *An introduction to design science*, vol. 9783319106. 2014.

[128] A. A. Rehman and K. Alharthi, "An introduction to research paradigms. International," *J. Educ. Investig.*, vol. 3, no. 8, pp. 51–59, 2016.

[129] P. K. Kankam, "The use of paradigms in information research," *Libr. Inf. Sci. Res.*, vol. 41, no. 2, pp. 85–92, 2019, doi: 10.1016/j.lisr.2019.04.003.

[130] J. Wilson, “Essential of Business Research,” vol. 44, no. 8, pp. 7250–7257, 2011, doi: 10.1088/1751-8113/44/8/085201.

[131] G. Goldkhul, “Pragmatism vs interpretivism in qualitative information systems research,” *Eur. J. Inf. Syst.*, vol. 21, no. 2, pp. 135–146, 2012.

[132] M. N. K. Saunders, P. Lewis, and A. Thornhill, *“Research Methods for Business Students” Chapter 4: Understanding research philosophy and approaches to theory development*, no. January. 2019.

[133] M. Balnaves and P. Caputi, *Introduction to Qualitative Research Methods: An Investigation Approach*. 2001.

[134] P. D. Leedy and J. E. Ormrod, *Practical Research Planning and Design 11th Edition*, vol. 6, no. 11. 2015.

[135] B. Kuechler and S. Petter, “D Esign S Cience R Esearch in,” no. 1, pp. 1–66, 2012, doi: 1756-0500-5-79 [pii]\r10.1186/1756-0500-5-79.

[136] A. Hevner *et al.*, “A pragmatic approach for identifying and managing design science research goals and evaluation criteria To cite this version : HAL Id : hal-02283783 Managing Design Science Research Goals and,” 2019.

[137] H. Noble and J. Smith, “untitled _ Enhanced Reader.pdf,” *Clinical Infectious Diseases*. 2015.

[138] R. Kumar, *h c r a Rese ology d o h Met a Rese ology d t*. 2011.

[139] L. M. H. W.Paul Vogt, Dianne C.Gardener, *When to use what research design*, vol. 17, no. 3. 2014.

[140] P. Delamont and S. Atkinson, *SAGE qualitative research methods. Vol I-IV*. 2010.

[141] M. E. Buchanan, “Methods of data collection,” *AORN J.*, vol. 33, no. 1, 1981, doi: 10.1016/S0001-2092(07)69400-9.

[142] Thomas P. Vartanian, *Secondary data analysis*. 2011.

[143] “Apache JMeter - User’s Manual: Glossary.” https://jmeter.apache.org/usermanual/glossary.html (accessed Jul. 07, 2022).

[144] “GitHub - hyperledger/caliper: A blockchain benchmark framework to measure performance of multiple blockchain solutions https://wiki.hyperledger.org/display/caliper.” https://github.com/hyperledger/caliper (accessed Jul. 18, 2022).

[145] “Documentation for Visual Studio Code.” https://code.visualstudio.com/docs (accessed Jul. 18, 2022).

[146] “Welcome to Remix’s documentation! — Remix - Ethereum IDE 1 documentation.” https://remix-ide.readthedocs.io/en/latest/ (accessed Jul. 18, 2022).

[147] W. M. A. Al-Rubaye and S. Kurnaz, “Blockchain and Smart Contracts to Improve Dental Healthcare for Children in Primary School,” *2021 Int. Conf. Adv. Comput. Appl. ACA 2021*, pp. 62–67, 2021, doi: 10.1109/ACA52198.2021.9626789.

[148] S. S. Nabil, M. S. A. Pran, A. A. Al Haque, N. R. Chakraborty, M. J. M. Chowdhury, and M. S. Ferdous, “Blockchain-based Covid Vaccination Registration and Monitoring,” 2021, [Online]. Available: http://arxiv.org/abs/2109.10213.

[149] M. Araag, M. Mandar, N. Prashant, and S. Shamna, “IRJET- Secure Approach for

Medical Record using Blockchain Technology," *Irjet*, vol. 8, no. 5, pp. 2940–2943, 2021.

[150] M. Parameswari, A. M. M, M. Akilesh, and N. Aravind, "A Block Chain Technology based Data Security in Medical Report for Healthcare," pp. 3625–3629, 2020.

[151] P. Bradish, S. Chaudhari, M. Clear, and H. Tewari, "CoviChain: A Blockchain Based COVID-19 Vaccination Passport," pp. 1–6, 2021, [Online]. Available: http://arxiv.org/abs/2112.01097.

[152] H. R. Hasan *et al.*, "Blockchain-Based Solution for COVID-19 Digital Medical Passports and Immunity Certificates," *IEEE Access*, vol. 8, no. December, pp. 222093–222108, 2020, doi: 10.1109/ACCESS.2020.3043350.

[153] T. McGhin, K. K. R. Choo, C. Z. Liu, and D. He, "Blockchain in healthcare applications: Research challenges and opportunities," *J. Netw. Comput. Appl.*, vol. 135, no. January, pp. 62–75, 2019, doi: 10.1016/j.jnca.2019.02.027.

[154] I. Sommerville, *TENTH edition Tenth Edition*. 2016.

[155] Prisma, "Prisma Documentation." https://www.prisma.io/docs/.

[156] "What is Argon2? - argon2-cffi 21.3.0 documentation." https://argon2-cffi.readthedocs.io/en/stable/argon2.html (accessed Jan. 19, 2023).

[157] S. Yan, "Analysis on Blockchain Consensus Mechanism Based on Proof of Work and Proof of Stake," pp. 464–467, 2022, doi: 10.1109/ICDACAI57211.2022.00098.

[158] "GitHub - P-H-C/phc-winner-argon2: The password hash Argon2, winner of PHC." https://github.com/P-H-C/phc-winner-argon2 (accessed Jul. 16, 2022).

[159] "What is MetaMask? How to Use the Top Ethereum Wallet - Decrypt." https://decrypt.co/resources/metamask (accessed Jul. 06, 2022).

[160] R. Abbas and Z. Sultan, "Comparative Analysis of Automated Load Testing Tools : Apache JMeter, Microsoft Visual Studio (TFS) , Load Runner, Siege," pp. 39–44, 2017.

[161] "ABOUT HYPERLEDGER," Accessed: Jul. 16, 2022. [Online]. Available: https://wiki.hyperledger.org/groups/pswg/performance-and-scale-wg.

[162] M. Kuzlu, M. Pipattanasomporn, L. Gurses, and S. Rahman, "Performance analysis of a hyperledger fabric blockchain framework: Throughput, latency and scalability," *Proc. - 2019 2nd IEEE Int. Conf. Blockchain, Blockchain 2019*, pp. 536–540, 2019, doi: 10.1109/Blockchain.2019.00003.

[163] W. Choi and J. W. K. Hong, "Performance Evaluation of Ethereum Private and Testnet Networks Using Hyperledger Caliper," *2021 22nd Asia-Pacific Netw. Oper. Manag. Symp. APNOMS 2021*, pp. 325–329, 2021, doi: 10.23919/APNOMS52696.2021.9562684.

[164] A. Chowdhary, S. Agrawal, and B. Rudra, "an Educational Certificate Verification," pp. 916–921, 2021.

[165] M. Abubakar, P. McCarron, Z. Jaroucheh, A. Al Dubai, and B. Buchanan, "Blockchain-based Platform for Secure Sharing and Validation of Vaccination Certificates," *Proc. - 2021 14th Int. Conf. Secur. Inf. Networks, SIN 2021*, 2021, doi: 10.1109/SIN54109.2021.9699221.

[166] K. S. Malik, D. Rani, C. Science, P. C. L. S. Govt, and C. Karnal, "IoT System with Blockchain for Data Security and Protection : A Review," *Int. Res. J. Eng. Technol.*, pp.

1572–1580, 2021.

[167] M. Ghadamyari and S. Samet, “Decentralized electronic health records (DEHR): A privacy-preserving consortium blockchain model for managing electronic health records,” *ICT4AWE 2020 - Proc. 6th Int. Conf. Inf. Commun. Technol. Ageing Well e-Health*, no. Ict4awe, pp. 193–198, 2020, doi: 10.5220/0009398101990204.

[168] Y. Madhwal, Y. Yanovich, and I. Chumakov, “CoVID-19 Vaccination Certificate Supply Verification Based on Blockchain,” *ACM Int. Conf. Proceeding Ser.*, pp. 88–93, 2021, doi: 10.1145/3510487.3510500.

[169] K. Chandra and M. Mushtaq, “Digital_Passport_and_Visa_Asset_Management_Using_Private_and_Permissioned_ Blockchain,” *arXiv Prepr. arXiv2107.06849*, 2021, [Online]. Available: https://arxiv.org/abs/2107.06849.

[170] E. J. de Aguiar, A. J. dos Santos, R. I. Meneguette, R. E. De Grande, and J. Ueyama, “A blockchain-based protocol for tracking user access to shared medical imaging,” *Futur. Gener. Comput. Syst.*, vol. 134, pp. 348–360, 2022, doi: 10.1016/j.future.2022.04.017.

[171] M. H. Chinaei, H. Habibi Gharakheili, and V. Sivaraman, “Optimal Witnessing of Healthcare IoT Data Using Blockchain Logging Contract,” *IEEE Internet Things J.*, vol. 8, no. 12, pp. 10117–10130, 2021, doi: 10.1109/JIOT.2021.3051433.