**BINDURA UNIVERSITY OF SCIENCE EDUCATION**

**FACULTY OF SCIENCE AND ENGINEERING**

**DEPARTMENT OF COMPUTER SCIENCE**

# A Blockchain-Based Health Journal For Sharing Medical Records Between Different Health Providers

**BY**

**TINOTENDA CHIDENGE**

**B211157B**

***This dissertation is submitted in partial fulfilment of the requirements of the Bachelor of Science Honors Degree in Software Engineering.***

## DECLARATION FORM

I, Tinotenda Chidenge, do hereby declare to the best of my knowledge to Bindura University of Science Education that this dissertation is my original work and all materials and academic sources of information other have been duly acknowledged. I also declare that this current work has not been submitted to any other academic institution for the purposes of an academic merit.

Chidenge

..T.CHIDENGE.. ……………… 30../..06../2025….

STUDENT SIGNATURE DATE

..W.Kanyongo…. ……………… 04../..07../2025….

SUPERVISOR SIGNATURE DATE

…P.CHAKA…….. ………………….. 04…/07../2025….

CHAIRPERSON SIGNATURE DATE

# DEDICATION

I dedicate this academic work to those who have inspired and motivated me throughout my academic pursuits.

## ACKNOWLEDGEMENTS

First and foremost, I would like to thank God Almighty for granting me the strength, wisdom, and perseverance to complete this research this research journey. Without His guidance, none of this would have been possible. I am sincerely grateful to my supervisor, Dr Kanyongo, for their continuous support, guidance, and encouragement throughout this study. Your insights, patience, and feedback were instrumental in shaping this research and bringing it to completion. My heartfelt thanks go to the lectures and staff of the Computer Science department, who provided a strong academic foundation and valuable input during my studies. I also appreciate the support of my colleagues and classmates, whose collaboration and discussion enriched my understanding of the subject. Special appreciation goes to my family and BUSE ASA for their unwavering love, prayers, and encouragement throughout my academic journey. Your belief in me gave me the strength to keep pushing forward. Lastly, I would like to acknowledge the participants and stakeholders who contributed to the system testing and evaluation phase. Your involvement added real-world value and depth to this research. To everyone who contributed in one way or another thank you.

## ABSTRACT

Reversing the prevalent problems of data fragmentation, security vulnerabilities, and limited interoperability in traditional electronic health record (EHR) systems in environments like

Zimbabwe, this research proposes a blockchain-enabled health journal. This study aimed to design and implement a blockchain-powered health journal that would facilitate secure, patient-oriented sharing of health records across different types of healthcare providers. Through the implementation of a design science research approach, the methodology involved the development of a decentralized application utilizing Ethereum blockchain for transaction immutability and smart contracts, and InterPlanetary File System (IPFS) as an off-chain encrypted data storage. Cryptographic hashing (SHA-256) was applied to guarantee data integrity and authenticity. Key findings indicate the utilization of a decentralized architecture successfully, sustaining good security, tamper-evident record storage, and open data sharing. The system was able to effectively grant patients full ownership over their health data, with dynamic access control. Smart contracts were successfully automated to control access rules, applying permissions and enabling secure authentication. Moreover, the system had a level of interoperability that enabled healthcare providers to access patient records across institutions using a common blockchain infrastructure. User testing was very high in terms of control mechanisms and usability, with 66.7% of users being able to work independently without support. A surprise critical result, however, revealed a data integrity match of 66.7% between submitted and retrieved data, indicating a severe flaw in the current off-chain data management or data retrieval process that is antithetical to the underlying promise of blockchain immutability. These results hold deep implications for software engineering, affirming blockchain as industry-shaping technology for safe and patient-centered health information systems. In validating the theoretical benefit of decentralization and smart contract automation, the work also identifies significant engineering challenges, specifically to provide end-to-end data integrity in combining on-chain and off-chain storage. Future studies must aim at bridging the gap in data integrity, continuing to enhance overall system usability towards universal acceptance, accurate performance benchmarking, and rigorously confirming regulatory compliance to continue advancing the practical adoption of secure, blockchain-based healthcare solutions.

**Table of Contents**

## Table of Figures

# CHAPTER 1: PROBLEM IDENTIFICATION

## 1.1 Introduction

In recent years, blockchain technology has emerged as a transformative tool across various industries, including healthcare. Blockchain technology is a decentralized and distributed digital ledger that securely records transactions across multiple nodes, ensuring that the data is immutable and transparent. (Zhang e t al., 2023). This innovative technology has gained traction in various sectors, particularly in healthcare, where it offers a promising solution for sharing medical records among different health providers. By utilizing blockchain, healthcare organizations can enhance data security, improve interoperability, and streamline the sharing of patient information (Kuo, et al., 2017). Its ability to enhance data integrity, traceability, and access control makes it particularly suitable for managing sensitive information such as medical records.

The healthcare industry faces significant challenges related to date management, including issues such as data fragmentation, security risks and limited interoperability among electronic health record (EHR) systems (Mhlanga & Chikanda, 2020). Traditional HER systems often operate in silos, making it difficult for healthcare provider to access comprehensive patient information when needed. Blockchain technology addresses these challenges by creating a secure and unified platform for sharing medical records, ensuring that patient data is accurate, up-to-date and accessible across various healthcare settings (Iyer, et al., 2021). These issues are particularly pronounced in Zimbabwe where a significant portion of healthcare facilities relies on paper-based systems or disconnected electronic systems, leading to delays in treatment and suboptimal patient care (Chigora & Mutisi, 2018).

Blockchain technology, with its decentralized architecture, offers enhanced security and transparency compared to traditional centralized systems (Nakamoto, no date). Its immutability ensures the integrity and authenticity of medical records, reducing the risk of data tampering and unauthorized access (Tapscott *et al.*, 2016). Several studies have explored the potential of blockchain in healthcare, demonstrating its feasibility for secure and efficient data sharing (Azizi, et al., 2019) (Chen, et al., 2018) .

The proposed system will leverage the unique features of blockchain technology to address the challenges of data fragmentation, ensure data security and privacy, and improve interoperability among healthcare providers within Zimbabwe. Unlike traditional systems, blockchain ensures that patient data is immutable and accessible only to authorized parties, thereby enhancing trust and coordination in healthcare delivery (Daraghmi, et al., 2019).

## 1.2 Background of Study

Medical records management has been a challenge to many healthcare systems the world over, and Zimbabwe is no exception. Good medical recordkeeping is fundamental to diagnosis, continuity of care, and proper resource management. However, the traditional systems, in particular, the paper-based systems, have been proven incapable of solving the emerging demands in modern healthcare (Chilunjika & Uwizeyimana, 2024). Advanced technologies, such as blockchain, might revolutionize the management of medical records by ensuring security, interoperability and accessibility (Antonio & Nhapi, 2022) (Baguma, et al., 2019).

Previous studies have explored the potential of blockchain technology to address global healthcare issues, such as fragmented data systems and security breaches (Kuo, et al., 2017). Their research highlights blockchain's decentralized nature, which allows secure and tamperproof storage of medical records, ensuring data integrity and patient privacy. This foundation is crucial in contexts like Zimbabwe, where healthcare systems often face resource constraints.

Zimbabwe's healthcare system struggles with inefficiencies, particularly in rural areas, over 60% of healthcare facilities in Zimbabwe rely on paper-based systems, which are prone to errors, loss, and duplication (Chigora & Mutisi, 2018). These inefficiencies hinder the delivery of quality care and burden an already strained system.

Researches made emphasized the role of technology in addressing Zimbabwe's healthcare challenges (Mhere & Mapuranga, 2021). They noted that HER had been piloted in some urban centers but faced challenges, including poor internet connectivity, high costs and resistance to change. These findings underscore the need for a robust, cost-effective solution like blockchain which can operate in resource-limited settings.

Some scholars have documented the potential of blockchain in healthcare, particularly for secure sharing of medical records between providers (Daraghmi, et al., 2019). Their studies found that blockchain reduce s redundancies, enhances data accuracy, and ensures that patient information is accessible only to authorized individuals. This aligns with Zimbabwe's need for a system that addresses data fragmentation and improves interoperability.

Zimbabwe's healthcare sector has taken steps towards digitization with systems such as Impilo Electronic Health Record system being implemented to centralize patient information. (Ministry of Health and Child

Care, 2024) While this initiative has improved data availability within specific institutions, it remains a centralized system, making it prone to security vulnerabilities and operational inefficiencies. Moreover, interoperability between various healthcare providers remains limited, complicating the ability to deliver coordinated care.

Globally, blockchain applications in healthcare have shown promising results in enhancing data security and patient-centricity. For example, Estonia has successfully implemented a blockchain-based health records system to facilitate secure and interoperable data exchange among healthcare providers. Such systems not only improve data accessibility but also empower patients to control their medical information (Techzim.co.zw, 2022)

In Zimbabwe, blockchain technology remains underexplored in the healthcare sector. Despite ongoing discussions and pilot projects, there is limited adoption of this technology for health information management. This research aims to fill this gap by designing a blockchain-based health journal system that integrates data from multiple healthcare providers, ensuring secure, efficient, and patient-centered management of health records.

## 1.3 Statement of the problem

Medical records management and sharing in Zimbabwe pose serious challenges to the healthcare sector. Most of the available EHR systems are centralized and often face problems of fragmented data, insecurity of data, and limited interoperability among different healthcare providers; these problems limit quality patient care and restrict healthcare professionals from access to patient information. Many healthcare facilities in Zimbabwe operate on disparate systems that do not communicate with each other. This fragmentation leads to incomplete patient's records, making it difficult for healthcare providers to obtain a holistic view of a patient's medical history (Chikanda & Matiza, 2019). Moreover, healthcare facilities in Zimbabwe still rely on paper-based record systems, which are prone to loss, damage, and inefficiency, over 40% of patient files in rural hospitals are misplaced or lost annually, leading to a lack of continuity in patient care (Gomba, et al., 2020). This is particularly problematic for chronic disease management, where historical records are critical for effective treatment. Zimbabwe's referral system is disjointed, with minimal communication between primary healthcare facilities and tertiary hospitals. A study revealed that more than 50% of referrals are accompanied by incomplete or inaccurate patient information, leading to delays in diagnosis and treatment (Moyo & Zinyemba, 2022). For instance, urban hospitals often have to repeat diagnostic tests because rural facilities cannot provide accurate records, increasing costs and wasting resources. Centralized systems are often targets for cyberattacks, and the lack of robust cybersecurity measures in Zimbabwean healthcare institutions raises concerns about patient data breaches. This situation diminishes patient trust and discourages individuals from sharing their health information (Munyoro, et al., 2021). The inability of different healthcare systems to share data seamlessly results in delays in patient care. Healthcare providers often spend excessive time retrieving patient information from various sources, which can be detrimental in emergency situations (Mhlanga & Chikanda, 2020). Patients in Zimbabwe typically have limited access to their health records, which reduces their ability to participate actively in their healthcare decisions. This lack of engagement can lead to poorer health outcomes and decreased satisfaction with the healthcare system (Chisi & Nyoni, 2022). Implementing a blockchain-based health journal could transform the healthcare system by reducing data fragmentation, ensuring secure access to patient information and improving healthcare outcomes across the country.

## 1.4 Research Objectives

1. To design and implement a blockchain based journal that enables secure, decentralized and interoperable sharing of medical records between different health providers.

2. To explore how a blockchain based health journal can empower patients with greater control over their medical records and facilitate informed consent for data sharing.
3. To integrate smart contracts into the blockchain based health journal to automate patient consent management and access control for medical records.

### 1.5 Research Questions

1. How can blockchain technology be used to ensure security, integrity and authenticity of medical records shared between health providers.
2. How can blockchain based health journal facilitate better communication and collaboration between patients and healthcare providers.
3. In what ways do smart contracts enhance the efficiency and transparency of patient consent processes compared to traditional methods.

### 1.6 Research Propositions/ Hypothesis

The implementation of a blockchain-based health journal will significantly improve the efficiency, security, and interoperability of medical record sharing between different healthcare providers by:

1. Enhancing data security by reducing unauthorized access to medical records.

2. reducing the time required to share medical records between healthcare providers.

3. improving patient satisfaction by enabling better coordination and continuity of care.

4. reducing errors associated with fragmented or missing patient data during referrals.

## 1.7 Justification/ Significance of the study

The research on a blockchain-based health journal for sharing medical records between different healthcare providers aims to address critical challenges in healthcare systems, particularly in Zimbabwe:

### 1.7.1 Significance to Individuals

Patients facilitates access to their healthcare history, leading to improved healthcare choices and customized treatment. Health care providers allow greater efficiency in accessing patients' records with less error and test duplication. Researchers and academics provide accurate, tamper-evident data for clinical research.

### 1.7.2 Significance to Policy Makers

Regulatory compliance which improves such frameworks as GDPR and HIPAA by ensuring secure data management. Health system improvement supports the healthcare digital transformation to provide more coordinated care. Fraud prevention reduces medical fraud and insurance fraud by ensuring data integrity.

### 1.7.3 Significance to Practice

The research ensures interoperability which simplifies record-sharing between hospitals, clinics, and specialists. Data privacy and security also takes advantage of blockchain's decentralization and encryption to prevent unauthorized access. The proposed system also improve efficiency by reducing paperwork, administrative costs, and delay in patient care.

### 1.7.4 Significance to Theory

This study bridges blockchain and healthcare informatics adding to the scholarly body of knowledge on blockchain's function in sharing medical data. Decentralized systems in health enriches theoretical discussion on decentralized health systems for security and effectiveness.

## 1.8 Assumptions

The research on a blockchain-based health journal for sharing medical records between different healthcare providers operates under the following assumptions:

1. It is assumed that blockchain technology can be effectively integrated into the existing healthcare infrastructure in Zimbabwe, even in resource-constrained settings.

2. Basic internet connectivity will be available at most healthcare facilities, enabling the operation of a blockchain-based system.
3. It is assumed that healthcare providers will input accurate and reliable patient data into the system, ensuring the integrity of medical records.
4. Healthcare providers and other stakeholders will be willing to adopt the blockchain-based health journal, recognizing its potential to address inefficiencies and improve healthcare delivery.
5. The government and relevant regulatory bodies will support the implementation of blockchain technology in the healthcare sector by providing the necessary policies and guidelines.

### 1.9 Limitations/ Challenges

1. Blockchain is still evolving and there may be technical limitations that affect scalability, security and usability of the proposed system.
2. Medical records are often stored in different formats and systems, which can make it challenging to standardize and share data across different health providers.
3. The proposed system may not be compatible with existing healthcare systems and infrastructure which can limit its adoption and effectiveness.

### 1.10 Scope/ Delimitation of the Research

The research focuses on exploring the feasibility, design, and implementation of a blockchain-based health journal for sharing medical records among different healthcare providers. The research is centered on Zimbabwe, particularly addressing the challenges faced by healthcare providers in both urban and rural areas regarding medical record management and sharing. The study examines the use of blockchain technology as the foundational infrastructure for developing a secure, decentralized, and interoperable system for medical records. It explores the integration of blockchain with existing healthcare systems and potential applications in resource-limited settings. The research focuses on primary users such as healthcare providers (hospitals, clinics, and specialists), patients, and policymakers. It examines how blockchain can facilitate better communication and coordination among these groups.

### 1.11 Definition of Terms

1. Blockchain- decentralized, digital ledger that records transactions across a network of computer in a secure and transparent manner.

2. Technology- application of scientific knowledge for practical purposes.

3. Journal- is a record of events, experiences or transactions kept on a regular basis

4. Data- facts or other information collected for reference.

5. Patient- an individual who receives medical care, treatment or services from a healthcare provider.

6. Medical record- collection of documented information about a patient's medical history, including diagnoses, treatments, medications, test results.

# CHAPTER 2: LITERATURE REVIEW

## 2.1 Introduction

Literature review is a critical analysis of existing research, theory and findings on a specific topic. It is utilized to summarize, evaluate and synthesize the scholarly literature in order to place a study into context, establish knowledge gaps and create a theoretical framework for research(Hart *et al.*, 1999). Literature review helps scholars to limit their research questions, justify their study and locate their work in academic literature(Hart *et al.*, 1999). In this section the researcher is going to give details of theoretical literature, empirical evidence and the research gaps.

## 2.2 Theoretical Literature

### 2.2.1 Blockchain Theory

Blockchain theory originates from a distributed, decentralized ledger system documenting transactions in an unbreakable and transparent way without depending on a central controller(Nakamoto, no date). Blockchain theory is based on the cryptography, consensus algorithm and decentralization to maintain data as immutable and tamper-proof(Swan and Swan, 2015). One of the fundamental theories upon which blockchain is founded is distributed ledger technology, which describes how digital ledgers are distributed across numerous nodes in a network(Pilkington et al., 2016). In contrast to the conventional centralized databases, blockchain has a consensus mechanism be it proof of work or proof of stake to validate transactions, thus enhancing security and fewer intermediaries' reliance(Tapscott *et al.*, 2016). Theoretically, blockchain adheres to trust less systems theory, where it is presumed that transactions could be secure and verifiable without parties having to trust each other. This has particular application in such industries as finance, healthcare and supply chain management where data integrity and security are critical(Yermack and Yermack, 2017). In healthcare, recent studies have explored the possibility of blockchain enhancing data security, interoperability and patient privacy. For instance, systematic review indicated immense potential of blockchain in clinical research, including its role in improving data management and access control(Cihan *et al.*, 2025).

### 2.2.2 Health Information Exchange (HIE) Theory

Health information exchange refers to the structured electronic sharing of health-related information among healthcare organizations. Theoretical foundations of health information exchange are multifaced, drawing from various disciplines to address complexity of healthcare data interoperability(Kruse *et al.*, 2018). The core aim of the study is to enable secure, seamless, and efficient sharing of medical records between different health providers exactly what HIE theory promotes. Traditional HIE systems face issues like centralization, interoperability, and lack of patient control. By using blockchain, there is decentralization which allows each health provider to interact with a common system without needing a central authority; smart contracts which ensure that only authorized users can view or modify records. And patients can control who accesses their data that is granting or revoking doctor access, reinforcing the HIE principle of patient-centered care.

1. Adaptive Structuration Theory (AST)

   AST examines the adaptation and adoption of technologies within organizations, emphasizing the interplay between advanced technologies and social structures. AST has been used in the context of HIE to examine the diffusion and assimilation of HIE systems within healthcare organizations, highlighting how organizational structures and processes influence the use of such technologies (Gefen et al., 2023). This study entails a decentralized, technology-intensive platform with social interactions among multiple actors (patients, doctors, hospitals). AST is particularly relevant because it explains how these actors adopt and adapt the blockchain-based system over time. The blockchain platform introduces new structures: immutable records, decentralized access, smart contracts and role-based permissions, these structures define how users interact with the medical data, who controls access, and how trust and data integrity are maintained.
2. Normalization Process Theory (NPT)

   NPT deals with social processes that facilitate or hinder the implementation of novel technologies into usual practice. In a recent research, NPT was employed in assessing barriers to the continued use of Electronic Health Records (EHRs) and HIE capability, unveiling difficulties like interoperability issues and user engagement that affect the normalization of HIE in clinical practice (Snyder *et al.*, 2024). The study introduces a new digital innovation, a blockchain-based system that revolutionizes the exchange, access, and maintenance of medical records. NPT allows for inquiry into the conditions under which this system will be adopted and sustained in routine health care processors across multiple providers.

3. Unified Theory of Acceptance and Use of Technology (UTAUT)

   UTAUT offers a model for explaining user acceptance of information systems. A mixed-method study used UTAUT to assess user acceptance of HIE solutions and found that performance expectancy, effort expectancy, and facilitating conditions have a significant impact on clinicians' intention to use HIE technologies(Dharmayat and Mastellos, 2021). UTAUT explains the following why and how various users (doctors, patients, nurses, admins) will accept or resist implementing the blockchain-based health journal. Users will adopt the system if they believe it improves data sharing, speeds up access to records, and enhances health quality.

4. Social Exchange Theory and Diffusion of Innovations Theory

   These theories have been combined in order to examine the determinants influencing the attitudes of healthcare providers in regards to the relative advantages and disadvantages of using HIE. The model from this combination suggests that it is crucial to look at these attitudes in a way that will promote the adoption and continued use of HIE systems(Zhang and Zhang, 2017). Social Exchange Theory explains human relationships and interactions as a result of cost-benefit analysis. People engage in interaction if they believe the benefits are more than the costs. Health professionals and patients will utilize the blockchain system if they believe it offers more value for example more data security, control and coordination compared to the costs (time to learn, technological complexity).

### 2.2.3 Patient Centre Care Theory

Patient-Centered Care (PCC) emphasizes treating patients as active partners in healthcare by them respecting their preferences, ensuring transparent communication and enabling shared decision making(Makubalo *et al.*, 2020). Blockchain-based health journal system realizes these principles by allowing patients to control access to their health records through smart contracts and decentralized consent mechanisms(Haddad *et al.*, 2023). This empowers patients to grant or revoke access, boosting autonomy and trust, while the transparency and immutability of blockchain mean they can track who is accessing their data critical for PCC driven communication and transparency(Hylock *et al.*, 2019; Makubalo *et al.*, 2020). By enabling secure, cross provider sharing of records, the system enables coordinated, continuous care and averts fragmentation, enhancing patient outcomes(Haddad *et al.*, 2023). Hence, the blockchain solution aligns with PCC by bringing together patient empowerment, trust, transparency and seamless care coordination.

### 2.2.4 Data Governance Theory

Data governance theory is a procedure, policy, and system that facilitates effective management, quality, privacy, and security of data across an organization. The theory forms the basis of data-driven decision-making, regulatory compliance, and risk management(Lis *et al.*, 2021). The theory is based on accountability, transparency, and stewardship of data, ensuring that data is properly managed and used responsibly(Khatri *et al.*, 2010). The blockchain-based health journal must align with strong data governance principles, especially given the sensitive nature of medical records.

1. Information Governance (IG)

   Information governance (IG) applies processes and policies to control data assets to ensure regulatory compliance, as well as ethical use of data. IG is more than IT governance because it encompasses handling data within its broader domains including legal and ethical ones(Smallwood and Smallwood, 2014). The study's ability to provide transparent and verifiable audit trails aligns with the IG principle of accountability, allowing tracking of all data interactions. As such, the proposed blockchain-based solution exemplifies how emerging technology can enforce robust information governance while trust and patient autonomy in healthcare.

2. Data Stewardship

   Data stewardship theory concentrates on responsibility and the role of particular individuals (data stewards) in managing data integrity and compliance with regulations. Current research has determined that good data stewardship practices enhance data quality and reduce data breach risks(Abraham et al., 2023). The study enforces data governance policies such as consent tracking, role-based access control and compliance with healthcare regulations, fulfilling key data stewardship that ensures health information is managed ethically and securely across healthcare providers.
3. Decision rights and Accountability

   This theory is concerned with who has to be in charge of and in command of data assets. In recent times, a study published brought forth that organizations where decision rights models are well articulated have better results for data governance and increased compliance with data governance regulations such as GDPR and HIPAA(Alhassan *et* *al.*, 2019). This study operationalizes the principle of assigning decision making authority and enforcing accountability through technology, ensuring that data handling is both responsible and transparent.

4. Data trust and Ethics Framework

   Data Trust and Ethics Framework is a framework that emphasizes the responsible governance of data by ensuring principles such as trust, transparency, consent, privacy and fairness during data collection, access and use(Floridi *et al.,* 2016). In healthcare, where patient data collected and stored is highly sensitive, ethical data management is critical to preserving public trust and satisfying legal and ethical obligations. The proposed blockchain-based health journal system directly supports this framework by providing secure, transparent, and consent driven access to medical records. Blockchain's immutability and auditability also enhance transparency and accountability, two pillars of ethical data stewardship. Besides, by decreasing centralized control and limiting the possibility of unauthorized access or misuse, the proposed system fosters a trusted data sharing environment(Haddad *et al.,* 2023). Thus, the proposed system infiliates the Data Trust and Ethics Framework by embedding privacy, fairness and patient empowerment into its technological core, ultimately advancing ethical health data practices beyond institutional boundaries.

### 2.2.4 Electronic Health Record

Electronic Health Records (EHRs) are computerized duplicates of patients' paper charts, designed to have the information immediately available and safe to the prescribed users (HealthIT.gov, 2024). Patient-focused, real-time records integrate a patient's medical history, including demographics, progress notes, medicines, vital signs, immunizations, laboratory tests, and radiology reports, into a single electronic collection, easy and efficient to provide inclusive healthcare (CMS, 2024). This study proposes a blockchain-based system to manage and share medical records which is, in essence, an advanced EHR system with decentralized features.

1. Technology Acceptance Model (TAM)

   TAM posits that perceived ease of use and perceived usefulness play a strong role in influencing users' acceptance and adoption of technology. For EHRs, TAM has been applied in research to conceptualize healthcare professionals' acceptance, with the contention that ease of use and perceived advantages are key determinants of EHR acceptance(Sadoughi *et al.*, 2019). TAM helps assess whether end-users (doctors, patients, nurses, admins) will adopt the blockchain-based journal. Users will likely adopt the system if they see it improves efficiency, accuracy, or privacy of data sharing. In this study, TAM was used to evaluate user feedback during testing or pilot implementation for example does the patient find it easy to share data with their doctor ? Does the doctor find it useful in making timely decisions?

2. Diffusions of Innovations (DOI)

   This theory investigates why, how, and at what rate new ideas and technology are diffused throughout cultures. It has been applied to research the adoption of EHRs, examining the relative advantage, compatibility, complexity, trialability, and observability of the diffusion process(Sadoughi *et al.*, 2019). DOI explains how new technologies like blockchain are adopted over time within a social or institutional setting. This theory explains how hospitals and clinics might gradually adopt your system starting with innovators and early adopters for example tech-savvy providers.

3. Socio-Technical Systems

   This theory is concerned with how technology and humans interact within an organizational setup. In the deployment of EHR, it emphasizes the importance of balancing technological systems with organizational structure and people so that there can be effective integration(Kemp *et al.*, 2024). This theory ensures the system integrates well with people, roles, and healthcare workflows.

4. Unified Theory of Acceptance and Use of Technology

   UTAUT integrates elements of several models to predict user intentions to use technology as well as actual usage behavior. Research employing UTAUT in EHRs has identified performance expectancy, effort expectancy, social influence, and facilitating conditions as significant predictors of EHR adoption among healthcare professionals(Sadoughi *et al.*, 2019).

## 2.3 Empirical Literature

An innovative blockchain-based system for efficient and secure management of Electronic Health Records (EHRs) was introduced, the solution was put forward to address fundamental challenges in healthcare data management, including interoperability, patient agency, and data security(Azaria *et al.*, 2016). The system utilized blockchain technology to create a decentralized network, thus evading a central authority. This system ensures that medical records are duplicated on multiple nodes, enhancing the resilience and security of data(Azaria *et al.*, 2016). All access to a patient's medical data is recorded on the blockchain, based on an immutable record of all access and modification. This feature enhances transparency and accountability because patients and providers can track the history of medical records accurately(Azaria *et al.*, 2016). Smart contracts are employed by the system to manage permissions and data sharing. Patients can dynamically grant and revoke permission over their medical records so that only the permitted individuals can read or write sensitive information(Azaria *et al.*, 2016). The system is also designed to function in harmony with already existing healthcare data storage systems. By interfacing with providers' already existing databases, the system offers interoperable data exchange without calling for a complete overhaul of the already existing systems(Azaria *et al.*, 2016). To encourage adoption and support the blockchain network, the study proposes an incentive model whereby medical researchers can join the network as miners. In return for providing computational resources, they are given access to anonymized medical information for research, fostering a win-win relationship between medical advancement and data security(Azaria *et al.*, 2016). The system empowers the patients since it grants them control over their medical data, allowing them to determine access rights and guaranteeing their autonomy in making medical decisions. The blockchain, being decentralized, and the cryptographic techniques safeguard the medical records from unauthorized manipulation and access(Azaria *et al.*, 2016). By providing one platform for sharing data, the system reduces the friction that occurs while sharing medical records among different healthcare providers, and hence leading to more coordinated and efficient patient care(Azaria *et al.*, 2016). Despite the success in demonstrating secure and decentralized access, high transaction costs on Ethereum made the system impractical for real world use(Azaria *et al.*, 2016).

In addition researchers discussed the possibility of blockchain technology in transforming Health Information Exchange (HIE) systems, they presented an in-depth review of the characteristics of blockchain and its suitability in the biomedical and healthcare fields(Kuo *et* *al.*, 2017). The authors pointed out the decentralized nature of blockchain, which removes the necessity for a central authority. This structure makes it impossible for data to be altered retroactively after data is input, and health record integrity is maintained. Blockchain employs cryptography to protect data(Kuo *et al.*, 2017). The research emphasized that this security system can protect sensitive patient information from improper use and data leakage. The study acknowledged that while blockchain is one platform, interoperability across different healthcare systems remains a significant challenge. Data formats and protocols should be standardized in order to allow for free exchange of information(Kuo *et al.*, 2017). The researchers explained that blockchain network scalability is a problem, especially with the large volumes of data that are produced in healthcare. They suggested that future research needs to enhance blockchain systems for effective management of big-scale health data(Kuo *et al.*, 2017). The study discussed the complexities of implementing blockchain technology in existing healthcare regulations, such as HIPAA in the US(Kuo *et al.*, 2017).

FHIRChain is a blockchain-based framework for enhancing the security and scalability of clinical data sharing, the solution aims to resolve the issue of data silos in healthcare that typically undermine efficient information exchange and collaborative clinical decision-making(Zhang *et al.*, 2018). FHIRChain encapsulates the Health Level Seven Fast Healthcare Interoperability Resources (HL7 FHIR) standard to facilitate seamless interoperability among heterogeneous healthcare systems. This integration enables efficient and accurate sharing of clinical data across platforms(Zhang *et al.*, 2018). Through the utilization of blockchain technology, FHIRChain enables a decentralized network of clinical data management, this eliminates the need for centralized authorities, reducing single points of failure and enabling data to be more resilient(Zhang *et al.*, 2018). The system employs cryptographic techniques inherent in blockchain to secure patient data and also access controls and authentication mechanisms ensure that sensitive information is only viewed by authorized entities, hence ensuring patient privacy(Zhang *et al.*, 2018). FHIRChain suggests digital health identities to authenticate data sharing participants, this element streamlines the verification process, ensuring that data viewing and alterations are done by verified users(Zhang *et al.*, 2018). To demonstrate FHIRChain's real-world applicability, the scholars showcased a case study on its application in collaborative decision-making for remote cancer care. In this application scenario, different healthcare professionals and specialists securely accessed and shared patient data utilizing the FHIRChain system(Zhang *et al.*, 2018). The decentralized framework facilitated real-time collaboration, leading to more informed treatment decisions and improved patient outcomes(Zhang *et al.*, 2018).

The research article "OmniPHR: A distributed, interoperable, blockchain-based personal health record architecture"  addresses an extremely critical challenge in healthcare today: the isolation of patient health records(Roehrs *et al.*, 2019). Patient health information tend to be spread out among various healthcare providers, clinics, and hospitals. Such inability to see everything in one place makes the delivery of healthcare inefficient and likely to result in errors(Roehrs *et al.*, 2019). The current Electronic Health Record (EHR) systems are typically not very interoperable, and therefore, it is hard to share patient data among various providers. Usually, patients do not exercise much control over their own health information, bringing privacy concerns(Roehrs *et al.*, 2019). The researchers introduce OmniPHR, a distributed system that utilizes blockchain technology to build an interoperable and secure personal health record system. Blockchain's nature of decentralization guarantees data integrity and security, and smart contracts can automate the control of access and data exchange(Roehrs *et al.*, 2019). OmniPHR seeks to solve interoperability issues by making data exchange effortless between various health providers irrespective of their current systems. The framework gives patients greater control over health data, giving them the capacity to control access and share it with authorized providers(Roehrs *et al.*, 2019). The system is distributed, hence the data is not kept in one location, so it is more secure, and system up time(Roehrs *et al.*, 2019). The research demonstrated that blockchain can be employed to create a distributed and interoperable PHR system. The performance testing identified that the proposed architecture can support a large data volume and transaction volume with acceptable response times(Roehrs *et al.*, 2019). The research highlighted the potential of OmniPHR in driving patient control over their health data and enhancing the provision of healthcare(Roehrs *et al.*, 2019).

ACTION-EHR system is a blockchain-instantiated Electronic Health Record (EHR) system to strengthen patient-centered sharing and management of data, and specifically radiation cancer treatment(Dubovitskaya *et al.*, 2020). ACTION-EHR uses smart contracts to implement data-sharing transactions, these are provided as Representational State Transfer (REST) Application Programming Interfaces (APIs), enabling open interaction between the blockchain network and outside applications, including web portals for patients and healthcare providers(Dubovitskaya *et al.*, 2020). The system utilizes the Health Level Seven Fast Healthcare Interoperability Resources (HL7 FHIR) standard to represent shared EHR data. This choice promotes interoperability, which enables seamless integration with existing hospital EHR systems and supports uniform data exchange formats(Dubovitskaya *et al.*, 2020). ACTION-EHR empowers patients by providing control of medical data, patients can grant or refuse access to their records with the assurance that they are entirely engaged in healthcare information management(Dubovitskaya *et al.*, 2020). The researchers created a prototype for ACTION-HER, the system was tested in a distributed environment with deidentified patient data, demonstrating its utility for application in real-world healthcare settings(Dubovitskaya *et al.*, 2020). As more healthcare data becomes available, it is a continuous challenge to maintain the scalability of the blockchain network in providing large-scale data sharing without any degradation in performance. However, integrating ACTION-EHR into existing healthcare regulatory frameworks, e.g., HIPAA in the US, needs to be done carefully to avoid a compromise on patient privacy and security of data. Encouraging adoption of this new system by both healthcare providers and patients involves the need to overcome potential resistance to change and simplifying the use of the system and delivering value to existing processes. ACTIONEHR represents a significant step forward in patient-centered healthcare data management. With blockchain technology and standards of compatibility, it offers a secure and efficient platform for the sharing of EHRs and possibly improving cooperative care and cancer patient outcomes and more generally.

MedShard: Electronic Health Record Sharing using Blockchain Sharding, this study introduces a transaction based sharding technique to enhance the scalability and efficiency of electronic health record sharing using blockchain technology (Hashim *et al.*, 2021). The key finding is that the proposed sharding method outperforms standard blockchain techniques by eliminating cross-shard communication, thereby improving the number of appointments processed, consensus latency, and throughput(Hashim *et al.*, 2021). The research addresses the scalability bottleneck in blockchain networks, which arises from the consensus mechanism and ledger replication by partitioning the network into smaller shards and processing transactions in parallel, the proposed technique significantly enhances network performance (Hashim *et al.*, 2021). The study contributes to resolving the scalability issue in healthcare blockchain and provides a more efficient solution for secure EHR sharing among various entities(Hashim *et al.*, 2021). Specifically, it scales out healthcare blockchain-based systems using sharding, eliminates cross-shard communication overhead, and uses Proof-of-Authority (PoA) for consensus within the shards. The transaction-based shard formation, based on a patient's ID, ensures that previously visited caregivers participate in the shard, removing the need for patients to keep track of their visits(Hashim *et al.*, 2021). The research acknowledges that while sharding has been explored in other domains, its application in healthcare blockchain is relatively new(Hashim *et al.*, 2021). However, the research did not consider associated security threats, emergency case handling, EHRs management and efficient patient record updates, and also room did not explore different consensus algorithms and shard formation methods to optimize performance further(Hashim *et al.*, 2021).

Patient-Centered Blockchain-Based Electronic Health Record Management (PCEHRM) system designed to allow patients to manage their healthcare records across multiple stakeholders while ensuring privacy and control without a centralized infrastructure(Haddad *et al.*, 2023). The system uses an Ethereum blockchain and InterPlanetary File System (IPFS) for secure, distributed storage of medical metadata and to ensure record immutability. A key component is the Ethereum smart contract, termed the patient-centric access control protocol, which facilitates trustworthy access control(Haddad *et al.*, 2023). The study demonstrated that the PCEHRM system enables stakeholders (patients, labs, researchers) to obtain patient-centric data securely and in a distributed manner through a web-based interface, testing in a Windows environment, using Truffle to compile a smart contract prototype and deploying on Ethereum with Web3, validated the framework's efficiency and practicability(Haddad *et al.*, 2023). Evaluation focused on medical data storage costs for IPFS on the blockchain and execution time relative to the number of peers and document sizes, with findings indicating the proposed strategy was efficient and practicable (Haddad *et al.*, 2023). The research identifies that current EHR systems often lack adequate interoperability and security, presenting privacy and scalability issues and also that existing blockchain-based solutions have shortcomings, such as storing medical records in third party databases or on-chain, which raises concerns about data breaches, privacy, and scalability(Haddad *et al.*, 2023). The PCEHRM addressed these gaps by giving patients complete control over their health records, storing data securely via IPFS, and using smart contacts to manage access permissions (Haddad *et al.*, 2023). The system enhances privacy, security, confidentiality and scalability, while also improving data integrity and auditability. The research failed to implement the system on a public blockchain and integrate AI to aid clinicians in analyzing diagnostic data and communicating with patients(Haddad *et al.*, 2023).

MedShare, a blockchain-enabled framework for solving key problems in privacy-preserving and secure medical data sharing(Wang *et al.*, 2021). The research discussed the possibility of decentralized ledger technology for enabling data security, patient control, and interoperability among healthcare networks by leveraging advantages of cryptographic methods that is encryption and zero-knowledge proof and smart contracts, MedShare guaranteed that sensitive patient records were not exposed during their utilization while allowing auditable access by health professionals and researchers with authorization(Wang *et al.*, 2021). One of the most significant contributions of the study was that it was patient-centered, restoring control of information to individual patients from centralized organizations, which aligns with contemporary data protection laws such as GDPR and HIPAA(Wang *et al.*, 2021). In contrast to conventional systems, MedShare leveraged the blockchain immutability to establish immutable audit trails, thus enhancing transparency and accountability of information transactions(Wang *et al.*, 2021).

Other scholars studied how smart contracts enable secure sharing of health data for a mobile cloud based e-health system's, in which their main goal was development of a secure and efficient framework for sharing electronic health records using blockchain technology and smart contracts within a mobile cloud environment (Chinnasamy *et al.*, 2023). They address the critical need for trustworthy access control in e-health systems, where the risk of unauthorized access and data breaches is high(Chinnasamy *et al.*, 2023). The proposed system combines blockchain's security features with the distributed storage capabilities of the Interplanetary File System (IPFS) to overcome limitations of traditional cloud-based solutions. The authors demonstrate that their system offers enhanced security, data integrity, and confidentiality while maintaining practicality through lightweight architecture and low network expectancy (Chinnasamy *et al.*, 2023). The research identifies several gaps in existing EHR sharing models, including a reliance on centralized systems with single points of failure, scalability for handling large datasets, and insufficient attention to access control and data privacy. Current methods often assume complete trustworthiness of cloud service providers, which is not always the case in portable cloud environments. The authors address these gaps by proposing a decentralized, blockchain-based system that eliminates the need for a central authority and provides fine-grained access control through smart contracts(Chinnasamy *et al.*, 2023). The use of smart contracts for managing permissions and enforcing privacy policies is a key takeaway that is applied in this study. The integration of IPFS for distributed storage can help address the scalability issues associated with storing large volumes of medical records on the blockchain. By building upon these findings, this study can further refine and optimize blockchain-based solutions for secure and efficient medical record sharing among healthcare providers.

Moreover researchers went on to explore the potential of blockchain technology to address the daunting challenges facing the management of health information in the public health sector in Zimbabwe(Chilunjika and Uwizeyimana, 2024). The research highlights that Zimbabwe, like most developing countries, is faced with problems in health information management. These include issues like dependence on porous, largely paper-based systems, vulnerability to data manipulation, limited access to essential health information, delays in information reporting(Chilunjika and Uwizeyimana, 2024). There is a dire need to ensure the integrity and security of health records, in a way that they are not tampered with without authorization or compromised. The primary aim of their research was to explore how blockchain technology can be leveraged to overcome these health information management issues in Zimbabwe(Chilunjika and Uwizeyimana, 2024). The researchers adopted a qualitative desk research approach, that is, they looked at existing literature and information to establish the promise of blockchain in this context(Chilunjika and Uwizeyimana, 2024). Blockchain's inherent immutability can discourage interference with health records, hence data integrity. Blockchain has the ability to facilitate secure and controlled sharing of health data among concerned stakeholders(Chilunjika and Uwizeyimana, 2024). The technology can enhance accountability and transparency in some critical healthcare functions, such as finance and procurement(Chilunjika and Uwizeyimana, 2024). Lastly, the research identifies the potential of blockchain to facilitate the delivery of higher quality health services. The research also identifies the significant challenges that can confront the adoption of blockchain in Zimbabwe, which include: poor ICT infrastructure, lack of skilled personnel, data security and privacy issues, potential resistance to change, usability issues(Chilunjika and Uwizeyimana, 2024). The authors urge policymakers to commission further research to have a full understanding and evaluation of the value of blockchain technology in Zimbabwe's context(Chilunjika and Uwizeyimana, 2024).

"A Blockchain-based Patient Portal for Mental Health Management" fulfils the vital need for secure and private management of mental health data(Jhamba *et al.*, 2024). Mental health information is extremely confidential, and traditional patient portals are susceptible to unauthorized access and leakage of information. The nature of mental illnesses requires more privacy and security(Jhamba *et al.*, 2024). The researchers identified the problem that existing systems are not robust enough to protect sensitive patient information and patients require more control over their mental health records(Jhamba *et al.*, 2024). The authors propose a blockchain-based patient portal to offer increased security and confidentiality for mental health information, blockchain's decentralized and immutable nature provides a tamper-proof history of patient information(Jhamba *et al.,* 2024). Blockchain technology makes patient records tamper-proof and ensures data integrity. The system uses cryptographic techniques to protect sensitive patient information(Jhamba *et al.,* 2024). Smart contracts are used to enforce access control automation and ensure that only approved parties have access to patient information. The research uses on-chain database storing hashes and the actual medical record of a patient and an off-chain solution handling encryption of each user's medical record(Jhamba *et al.*, 2024). Employing consensus algorithms such as Byzantine Fault Tolerance for data privacy and security and Comparative Analysis Research Methodology, allowed the researchers to evaluate the feasibility and performance of their proposed system compared to current patient portal systems(Jhamba *et al.,* 2024).

### 2.4 Research Gaps

Despite the growing interest in blockchain technology, there is lack of empirical studies on the feasibility, effectiveness and user acceptance of blockchain based health journal. This implies that there is need to investigate the factors that influence healthcare providers' adoption and use of blockchain based health journals.

### 2.5 Chapter Summary

Although blockchain-based EHR systems such as those proposed by Azaria et al. (2016) and promise decentralization, immutable audit trails and enhanced patient control, significant barriers persist. A major issue is interoperability, as many healthcare organizations struggle to integrate blockchain with legacy EHR platforms and adopt universal standards. Scalability also remains a constraint: public blockchains often cannot handle high transaction volumes without sacrificing performance. Furthermore, compliance with regulations such as GDPR and HIPAA is complex due to blockchain's immutable nature and distributed structure, requiring specialized design choices to reconcile legal requirements. Finally, adoption barriers including entrenched legacy systems, high implementation costs and limited technical expertise among stakeholders continue to hamper real-world deployment. Addressing these intertwined challenges is essential for developing a truly interoperable, scalable, compliant, and user-centric blockchain-EHR solution.

# CHAPTER 3: RESEARCH METHODOLOGY

## 3.1 Introduction

This chapter gives the research approach employed in this study with the objective of creating and validating a blockchain-based health journal for secure and efficient sharing of medical documents between different healthcare practitioners. The methodology outlines the research design, system development strategy, and requirements analysis methods employed. As the need for secure, transparent, and interoperable healthcare data systems increases, blockchain technology offers a decentralized and tamper-evident means to improve medical record management. The current study utilizes a proper methodology to design, develop, and assess the effectiveness of a blockchain-based system to overcome problems like data privacy, interoperability, and unauthorized access.

### 3.2 Research Design

A research design is the overall plan that is used to coordinate the various elements of a study in a logical and coherent way to optimally address the research issue. It sets out the agenda for data collection, measurement, and analysis(Huqa Arbale and African Journal Of Empirical Research, 2024). The research design forms the basis for deciding how to conduct the research, the research method, sampling methods, and data collection and analysis tools. In software development, research design would more commonly involve theoretical formulation and practical application, especially in applying approaches like Design Science Research (DSR) for developing and testing new technological artifacts.

This study adopts a DSR methodology, which is highly appropriate for the development and testing of technological artifacts aimed at addressing real-world issues. DSR offers a prescriptive process entailing the construction, demonstration, and testing of artifacts to ascertain their applicability and rigor(Delport et al., 2024). The six main steps in the DSR process are Problem identification and motivation, Definition of solution objectives, Design and development, Demonstration, Evaluation and Communication(Delport et al, 2024). The six steps above were used in applying and executing the suggested blockchain-based health journal system. Validity has been accorded more importance in DSR with recent advances, with a framework that classifies validity into criterion, causal, and context-related types, thereby offering a systematic solution to maintaining the credibility of findings in DSR(Larsen et al., 2025). This framework was deemed important in strengthening the rigor of artifact evaluation in the setting of this study. Furthermore, the imperative to deal with various forms of validity namely instrument, technical, design, purpose, and generalization to support the robustness of DSR artifacts(Kroop, 2025). Combining these elements ensures that the developed system not only functions optimally but also meet the intended objectives in the healthcare context.

The adoption of DSR is justified by the study's objective to design a functional blockchain system that addresses issues in medical records sharing, such as interoperability, privacy, and data security. Moreover, DSR supports the refinement of the artifact in an iterative way depending on user feedback, thereby making sure the ultimate solution matches the actual-world requirements of medical practitioners(Delport et al, 2024).

### 3.3 Requirements Analysis

Requirement analysis is one of the essential stages in the system development life cycle (SDLC) in which end users' and stakeholders' expectations and requirements are gathered, recorded, and analyzed to direct the system's design and implementation. It is a process that ensures the system under development conforms to both functional and non-functional requirements and achieves the desired objectives of the project(Pressman *et al.*, 2016). The process plays a central role in determining the system's functionality that is expected (functional requirements), how it should behave (non-functional requirements), and under which constraint or limitation it should run (Sommerville, 2015). In the context of this study, there was a thorough requirement analysis in terms of document examination, review of existing electronic health systems, and examination of data privacy legislation. This was carried out so that the blockchain-based health journal is in line with user requirements and regulatory demands.

#### 3.3.1 Functional Requirements

**Functional requirements** describe the specific behaviors, functions, and services that the system must perform(Pressman *et al.*, 2016). They define what the system should do and include features such as user authentication, data entry, record retrieval, and communication between different healthcare providers. These requirements directly contribute to achieving the system's main objectives.

The core features that the blockchain-based health journal must provide:

User Authentication and Access Control: patients, doctors, and healthcare providers should have role-based access using secure authentication (smart contracts).

Decentralized Storage and Ledger: medical records should be stored securely using blockchain for decentralized access.

Smart Contract Implementation: automate access permissions, data sharing, and patient consent management.

Audit Trail & Transparency: provide an immutable history of all transactions to ensure accountability.

Data Encryption and Privacy Protection: use cryptographic techniques to secure patient data.

Scalability & Performance Optimization: Ensure the system can handle multiple transactions efficiently.

Emergency Access: Allow temporary access to medical records in case of emergencies.

### 3.3.2 Non-Functional Requirements

**Non-functional requirements** specify the system's operational qualities and constraints. They define how the system should perform, focusing on attributes such as performance, security, reliability, usability, and scalability(Glinz and Glinz, 2007). These define the quality attributes of the system:

Security and Privacy: Ensure compliance with HIPAA, GDPR, and other regulations.

Reliability: The system should provide high uptime and fault tolerance.

User Experience: The interface should be user-friendly for both patients and healthcare providers.

Scalability: The system should be capable of handling a growing number of records and transactions.

Low Latency: Medical record retrieval and updates should be fast and efficient.

Availability: the system must be available 24/7, to ensure that medical records are always accessible.

### 3.3.3 Software Requirements

| | |
|---|---|
| Blockchain Platform | Ethereum, Ganache, Metamask |

| | |
|---|---|
| Smart Contract Development | Solidity and Truffle<br>Truffle Suite and Remix IDE |
| Backend Development | Node.js + npm<br>Express.js<br>IPFS (InterPlanetry File System) |
| Frontend Development | React.js, Ether.js or Web3.js, HTML, Material UI, JavaScript<br>OpenSSL, SHA-256<br>JSON Web Token |

### 3.3.4 Hardware Requirements

| | |
|---|---|
| Server Requirements | Processor: Intel Xeon or AMD Ryzen 7 (8+ cores)<br>RAM: 16GB or higher<br>Storage: SSD (1TB+) for fast data access<br>Internet: High-speed broadband |
| Blockchain Node Requirements | Node Computers: Each healthcare provider may need a node with:<br>CPU: Intel Core i7 or higher<br>RAM: 8GB or higher |

| | |
|---|---|
| | Storage: 512GB SSD minimum |

### 3.4 System Development

The systems development process followed in this study aligns with the SDLC principles and is supported by the DSR approach to facilitate the design and development of the blockchain-based health journal system. The SDLC supports a systematic process to facilitate organized planning, development, testing, and implementation of information system (Sommerville, 2015).

This section outlines the key phases involved in the system development process:

Planning- during this phase, the objectives, scope, and resources of the system were clearly defined. Planning involved identifying the key stakeholders primarily healthcare providers and patients and understanding their needs. This step also included feasibility analysis, project scheduling, and risk identification.

Requirement gathering was done through literature review, and analysis of existing healthcare systems. The requirements were categorized into **functional** and **non-functional** types to guide the design(Pressman *et al.,* 2016). Special attention was given to privacy, regulatory compliance and access control mechanisms.

System Designing- in this phase, the architecture and design specifications of the system were developed. A modular design approach was adopted to separate the front-end (user interface), back-end (server logic), and blockchain layer. Technologies used include: react.js for the front-end, node.js for the server-side logic, Ethereum blockchain (smart contracts) for storing access logs and verifying record integrity and IPFS (InterPlanetary File System) for storing encrypted medical records off-chain.

The implementation phase involved coding the system modules according to the design specifications. The smart contracts were written in Solidity and deployed to a local Ethereum test network (Ganache). The front-end and back-end were integrated using REST APIs. Security features such as user authentication, access control, and end-to-end encryption were embedded during development to ensure compliance with health data protection standards.

System testing was carried out in a controlled environment to evaluate the correctness, performance, and security of the application. The testing strategy included: unit testing of each module, integration testing between the blockchain, server, and interface and user acceptance testing with selected healthcare professionals to assess usability and functional completeness. Smart contracts were tested for vulnerabilities using tools like Remix IDE.

### 3.4.1 System Development Approach

In this study, the development of the blockchain-based health journal system followed a hybrid system development approach, combining the principles of DSR**,** Agile methodology, and the Prototyping model. This integrated approach was selected to ensure academic rigor, stakeholder-centered development, and practical validation of the system in real-world healthcare contexts.

The DSR framework served as the basic methodological structure for the study. DSR is especially well suited for research in the information systems field, where the principal aim is to develop and assess innovative artifacts that solve intricate, genuine problems(Hevner *et al.*, 2004). In this study, the main artifact was a blockchain-based health journal system, which was developed to ensure the far superior interoperability, security, and accessibility of medical records that all health care providers need in order to serve their patients. Following the DSR structure allowed for the systematic accomplishment of several essential task clusters, which were defined as phases for the investigation. Those phases, in order, were: problem identification and motivation; objective setting; designing and developing the artifact; demonstrating the artifact and communication of evaluation results.

While the full Agile methodology is often applied in software development, this study adopted an Agile-inspired iterative approach, this involved dividing the development process into multiple refinement cycles, allowing for frequent review, evaluation and improvement of the system in line with the objectives. Each development phase was followed by a reflection period in which adjustments were made based on insights and system testing results. This iterative cycle is consistent with Agile principles of continuous improvement and responsiveness. By embedding Agile concepts within the DSR cycle, the study maintained methodological flexibility.

Prototyping was used in this study not just as a software engineering technique, but as a core research method for exploring, validating and refining the design of the system. This approach aligns with the goals of DSR, which emphasizes building and evaluating artifacts as part of the research process(Peffers *et al.*, 2007). Two types of prototypes were developed: low-fidelity prototypes, such as interface sketches and wireframes, were used to gather early feedback on layout and workflow; high-fidelity functional prototypes which incorporated actual system features, including user authentication, data encryption and blockchain integration. These prototypes were iteratively refined based on objectives, making them essential tools for design validation and theory-building. In this way, prototyping served both a practical development function and a methodological role in the research, supporting user engagement and empirical evaluation(Pressman *et al.*, 2016).

## 3.5 System Design

System design refers to the process of defining the architecture, components, modules, interfaces, and data of a system in order to satisfy stated requirements (Sommerville, 2015). System design was the principal activity in this study where user and functional requirements were translated into a structured solution that supports secure, interoperable and efficient exchange of medical data among different healthcare providers through the use of blockchain technology. The design process was layered and modular in its nature, enhancing maintainability, scalability and system security. The major goal was to ensure the system satisfies functional requirements such as data sharing, access control, and updates of records as well as non-functional requirements such as privacy, reliability and usability.

### 3.5.1 System Architecture

The architecture is a hybrid system combining a centralized frontend using React, a decentralized backend using smart contracts and local testing tools like Ganache and on-chain interactions via Metamask. The separation of roles and access is handled both in the smart contract (on-chain) and in react route protection (off-chain) to offer a robust security model.

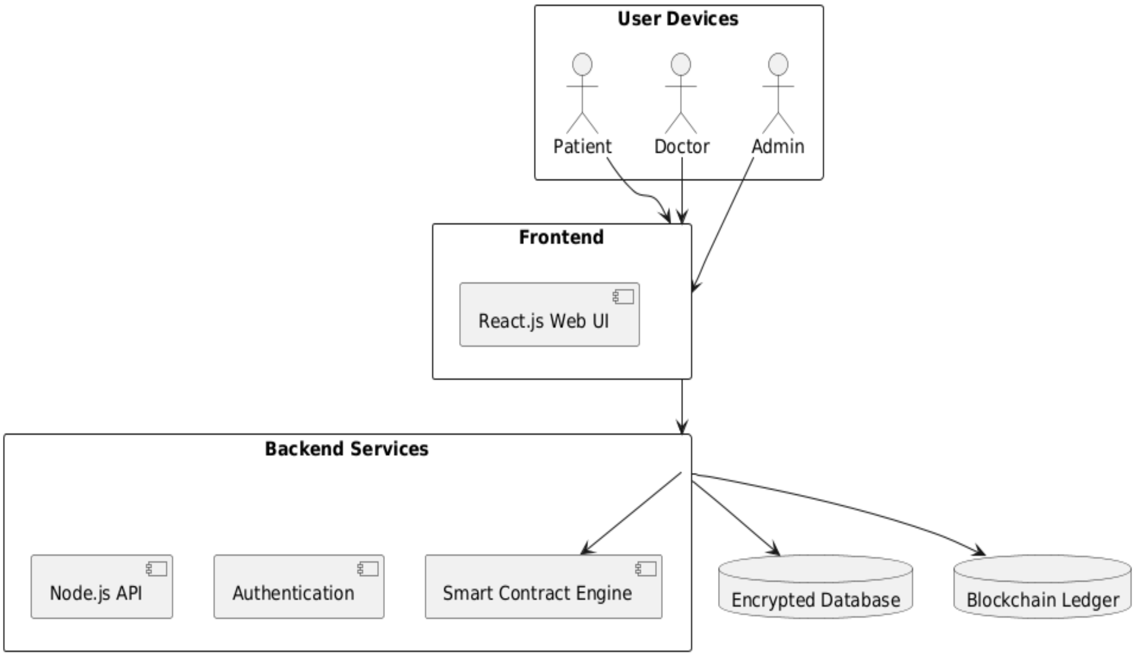


Figure 1: System Architecture

This architectural view breaks the system into key components and shows how they interact:

User Devices: Patients, doctors, and administrators interact with the system through web-enabled devices.

Frontend (React.js): Handles all user interactions and send requests to the backend.

Backend Services (Node.js): Processes requests, handles authentication, enforces access control, and connects to other modules.

Smart Contract Engine: Interacts with the blockchain to log and verify hashes of medical records.

Encrypted Database: Stores sensitive medical data in an encrypted format, separate from the blockchain.

Blockchain Ledger: Stores immutable record hashes to ensure data integrity, provide traceability, and support audit trails.

### 3.5.2 Use Case Diagram

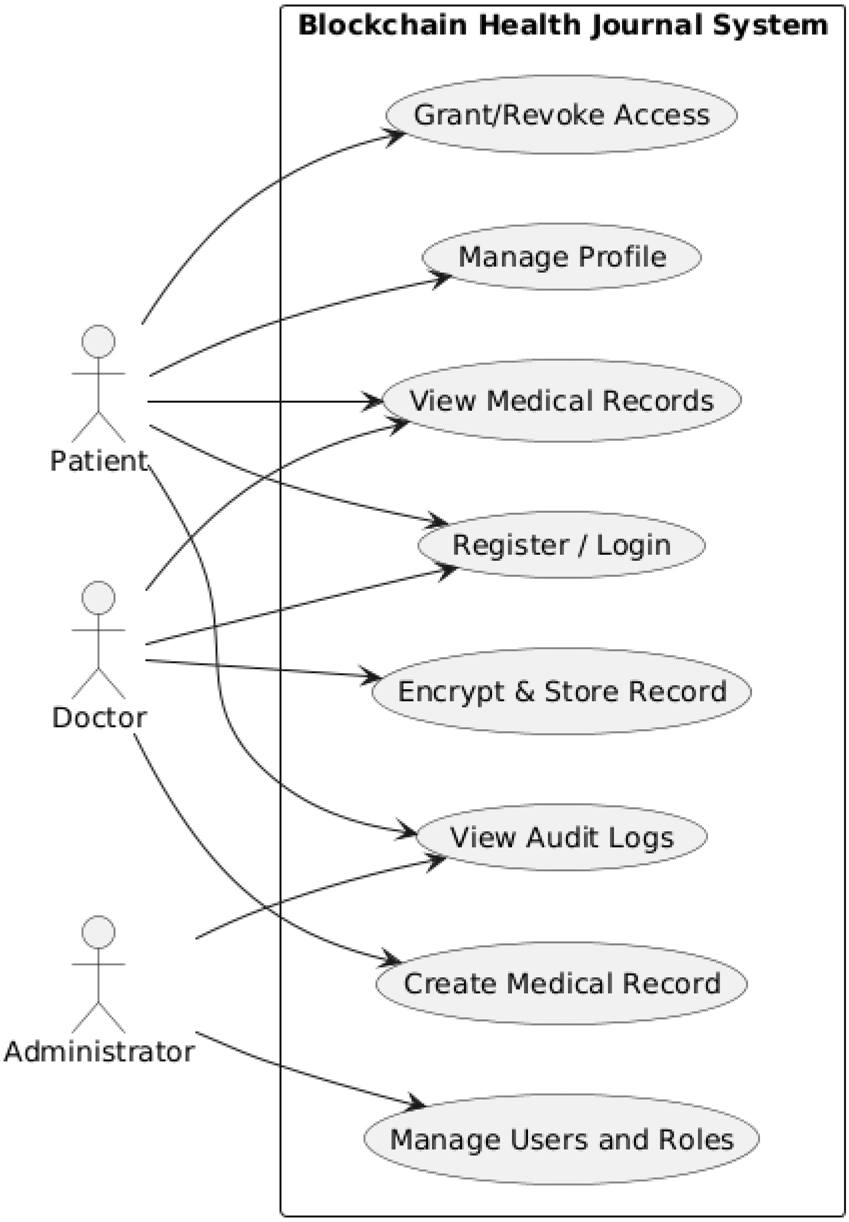


Figure 2: Use Case Diagram

The Use Case Diagram visualizes how different user roles interact with the blockchain-based health journal system to accomplish various goals.

Patient

Register and logs into the system.

Views personal medical records.

Grants access to specific doctors.

Doctor

Logs into the system.

Requests access to patient records.

Views patient data (if access granted).

Administrator

Manages user accounts.

Monitors system performance and security.

Assigns or  revokes access privileges.

### 3.5.3 Data Flow Diagram Level 1

DFD (Data Flow Diagram) Level 1 offers a broader view of the system by identifying the major processes, external entities and data stores, without going into too much technical detail.

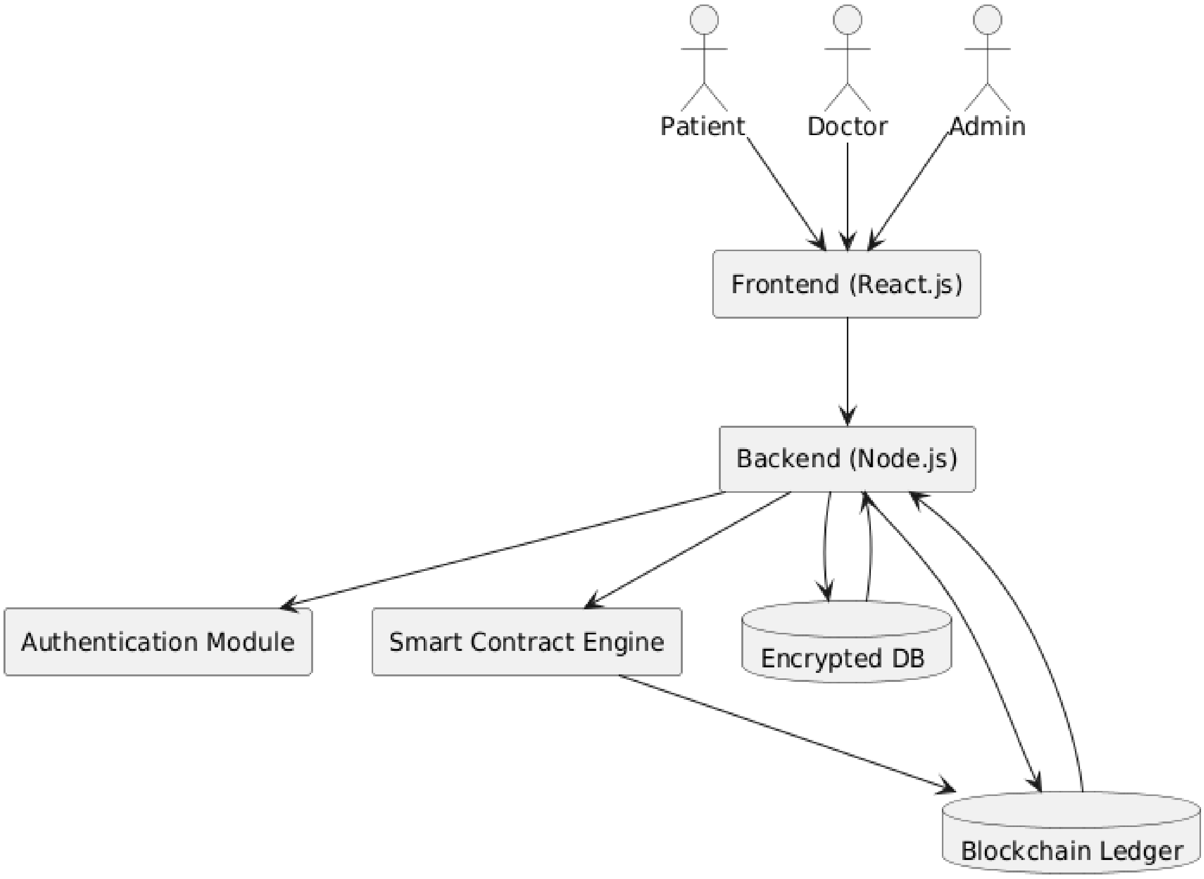


Figure 3: Data Flow Diagram Level 1

External Entities

Patient: Initiates actions such as registration, login, uploading, and accessing their own medical records.

Doctor: Requests to view patient medical records.

Admin: Manages user roles and monitors system security.

Processes

User Authentication: Verifies login credentials submitted by patients, doctors or admins.

Medical Record Management: Handles uploading, encrypting and saving medical records.

Smart Contract Execution: Generates hashes and interacts with the blockchain to store and verify record integrity.

Access Control: Checks if a doctor or patient has permission to access specific medical records.

Data Stores

Encrypted Medical Records Database: Stores encrypted patient data for long-term use.

Blockchain Ledger: Stores hashes of medical records for auditability and tamper evidence.

Data Flows

From patients/doctors to the web interface.

From the interface to the backend processes for encryption, verification, and storage.

From the backend to data stores (blockchain).

Retrieval flows when records are requested.

### 3.5.4 Sequence Diagram

The sequence diagram illustrates how different components interact during a patient's typical session:

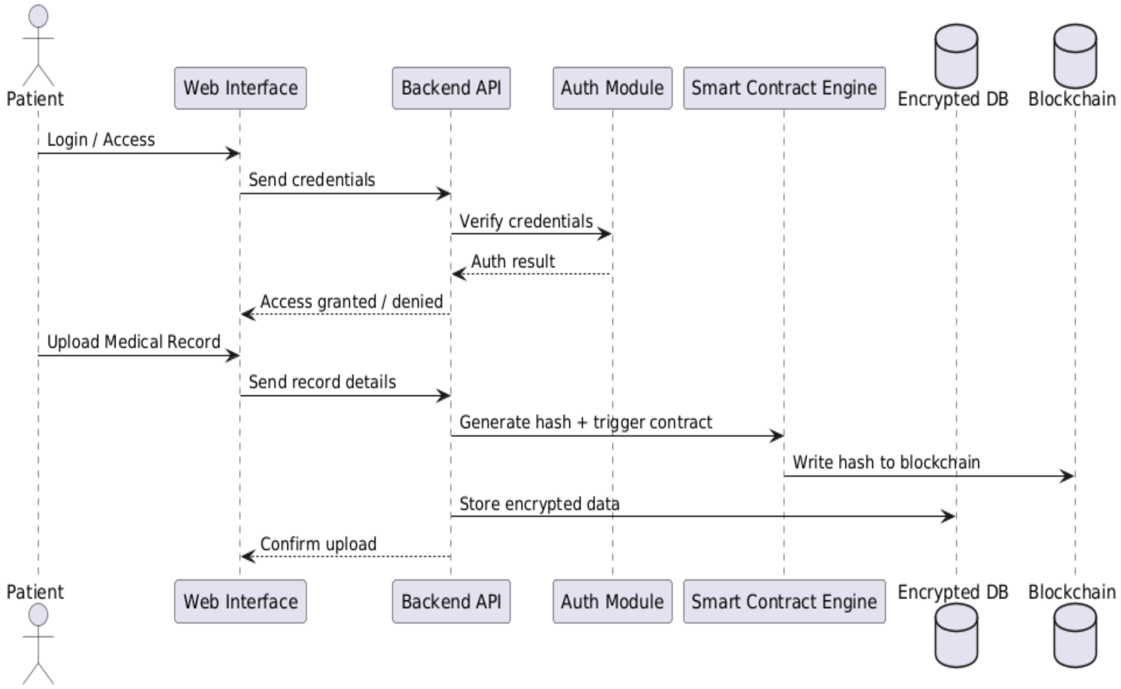


Figure 4: Sequence Diagram

Login Flow:

The patient initiates the login process via the web interface. Credentials are passed to the backend API, which then contacts the authentication module. If validated, access id granted.

Upload Flow:

Once authenticated, the patient can upload a medical record. The backend generates a hash of the record using cryptographic methods, and a smart contract is triggered. The smart contract records the hash on the blockchain for tamper-proof verification. Simultaneously, the encrypted medical record is securely stored in the off-chain database. The user receives confirmation upon success.

### 3.5.5 Data Flow Diagram Level 2

This diagram detail how data moves through the system during key actions:

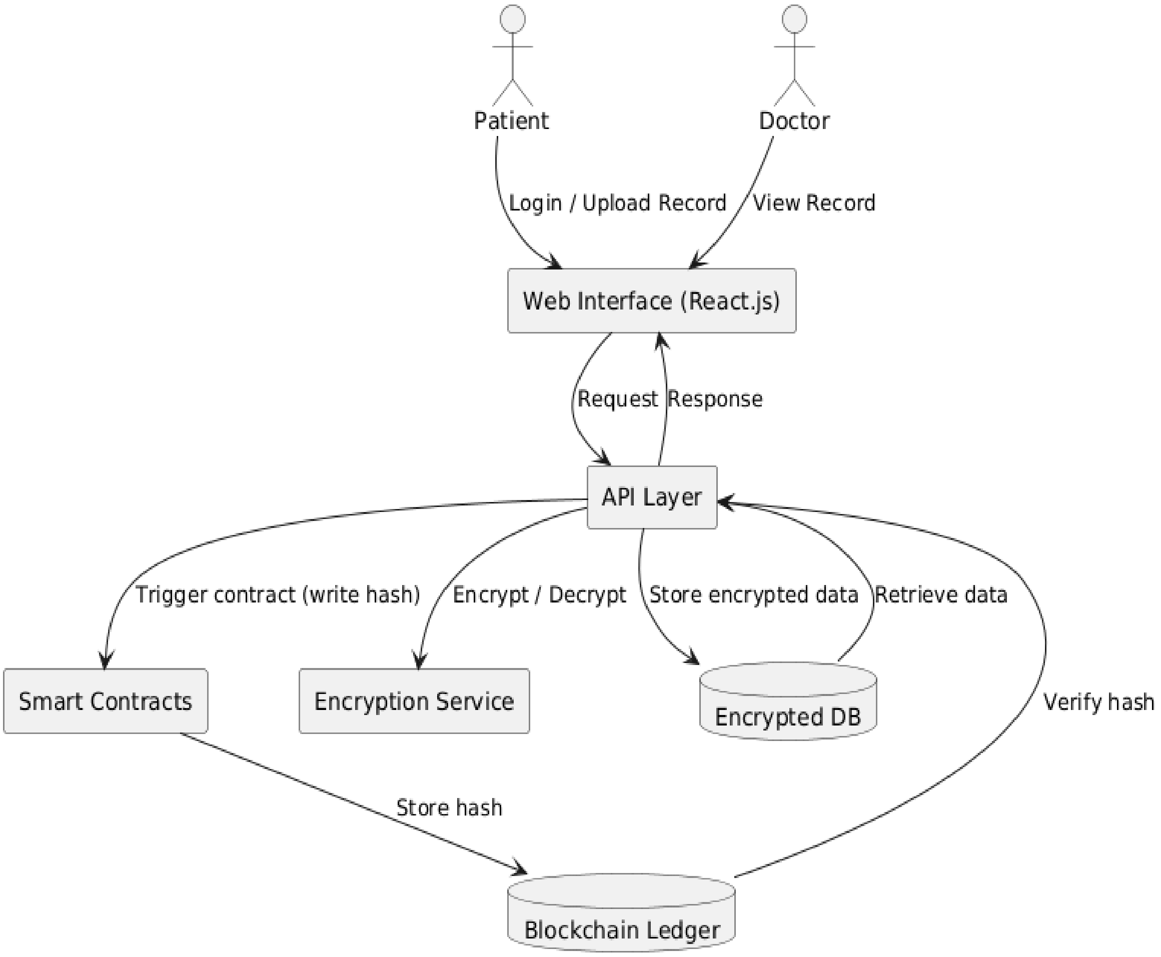


Figure 5: Data Flow Diagram Level 2

Patient Interaction:

Patients use the web interface to log in or upload records. Data flows through the API layer.

Encryption:

Before storage, the API communicates with an encryption module to ensure records are unreadable to unauthorized users.

Blockchain Integration:

A smart contract is invoked to write a unique hash of each medical record to the blockchain. This ensures data integrity and transparency.

Data Storage and Retrieval:

The encrypted record is saved in the database. When data is requested (by a doctor), the blockchain is used to verify its integrity before delivering it to the user.

### 3.5.6 System Flowchart

The flowchart demonstrates the logic and decision points in the user journey:

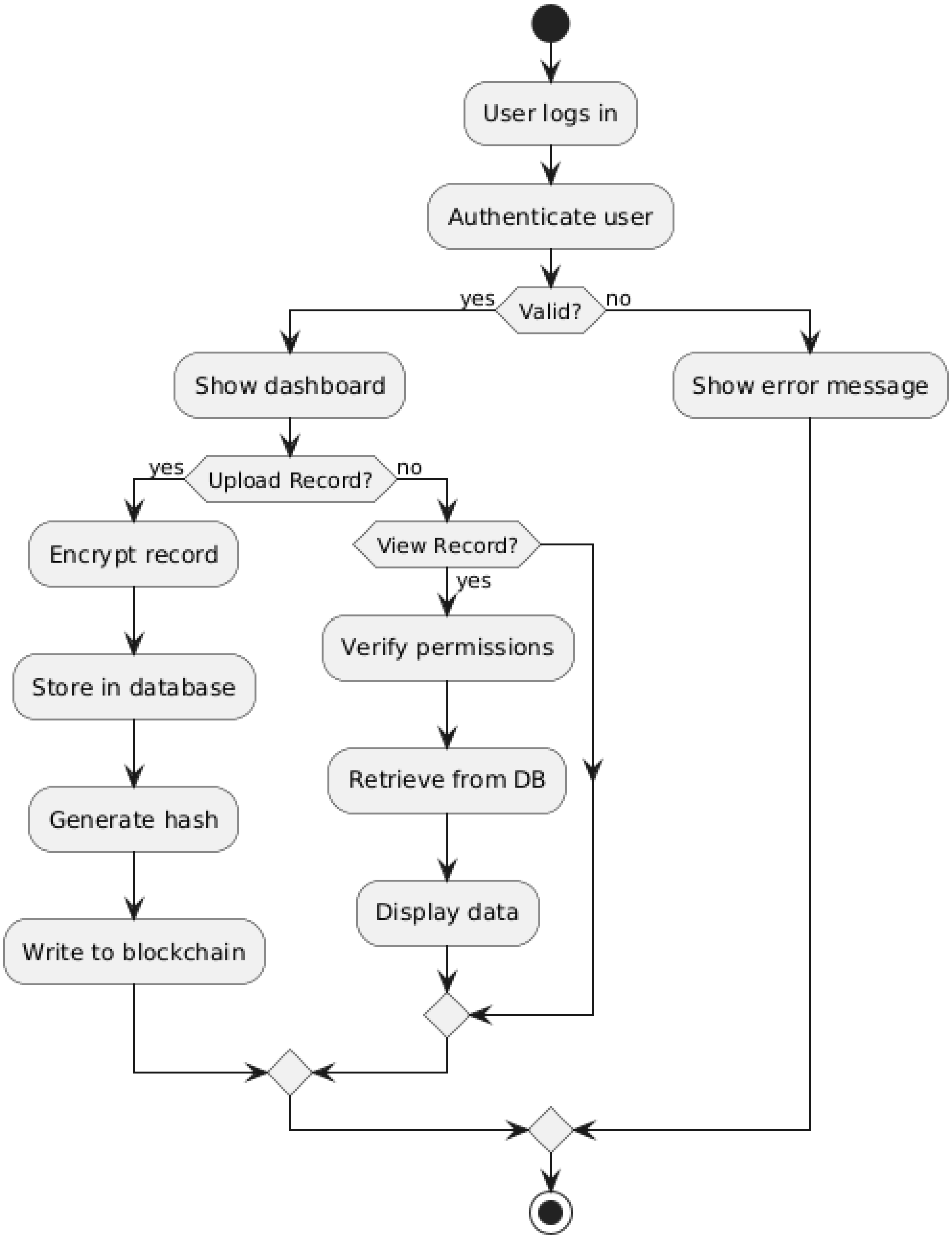


Figure 6: System Flow Chart

Login Process:

The user is authenticated before proceeding. If authentication fails, an error message is shown.

Post Login Options:

Usera are directed to their dashboard where they can choose to upload or view medical records.

Upload Record Flow:

If uploading, the record is first encrypted, stored in the database and its hash is written to the blockchain.

View Record Flow:

The system checks access permissions before fetching the encrypted data from the database. If valid, the record is decrypted and presented.

### 3.6 Data Collection

The project uses secondary data such as existing patient record structures and workflows in hospital systems to model the UI and smart contract logic. No personal patient data was used. Data for testing and evaluation was synthesized to simulate real-world scenarios.

### 3.7 Ethical Considerations

No real patient data was used in the study. The system is designed with privacy and data protection principles in mind. The use of blockchain ensures tamper-evident storage, while role-based access protects sensitive health information.

### 3.8 Chapter Summary

In conclusion, this chapter has outlined the research methodology employed to investigate the development of a blockchain based health journal for sharing medical records among different healthcare providers. The insights gained from this research methodology will serve as a foundation for addressing the core objectives of the study, ultimately contributing to the design of secure, efficient, and patient-centric health journal. The findings from this methodology will guide the subsequent phases of development and implementation.

# CHAPTER 4: DATA PRESENTATION, ANALYSIS AND PRESENTATION

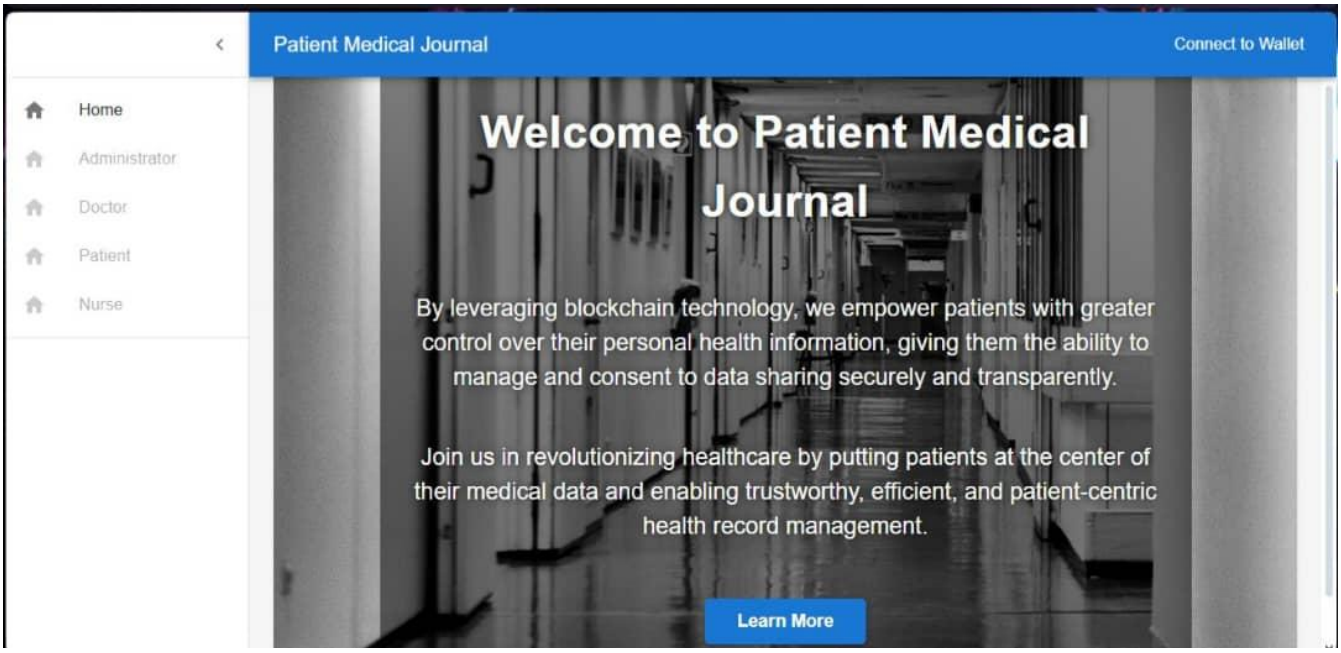
## 4.1 Introduction

This chapter reports the outcome of the implementation and evaluation of the proposed system in this research. The analysis is organized to reflect the study's main objectives and to indicate how the system addresses crucial issues in health information sharing. The first objective involved the design and implementation of a secure, decentralized, and interoperable platform for sharing medical records. Consequently, this chapter provides information from system functionality testing, user interaction assessments, and performance benchmarks that show how the blockchain structure enhances data protection and facilitates frictionless interoperability between various healthcare providers. The second aim examined the capability of blockchain in empowering patients with control over their medical information. User survey data and user feedback are reported to assess usability and the extent to which patients can see, control, and grant others access to their healthcare records in alignment with the concept of patient-centered care and informed consent. Lastly, the third goal was concerned with smart contract integration to enable automating access control and consent. This chapter includes a description of the operation of smart contracts within the system, with test results illustrating the accuracy and efficiency of automated access approvals based on patient defined rules. Generally, this chapter provides both quantitative and qualitative data to evaluate the system's performance, user satisfaction and alignment with the intended design goals. Each part is structured to link conclusions to the research objectives, presenting a lucid analysis defending the study's aim.

## 4.2 Implemented System

### 4.2.1 System Components

The frontend is the user interface that patients, doctors, and admins use. It's developed with React.js and provides pages and components like Patient Dashboard, Medical Records Viewer and Access Granting Panel.

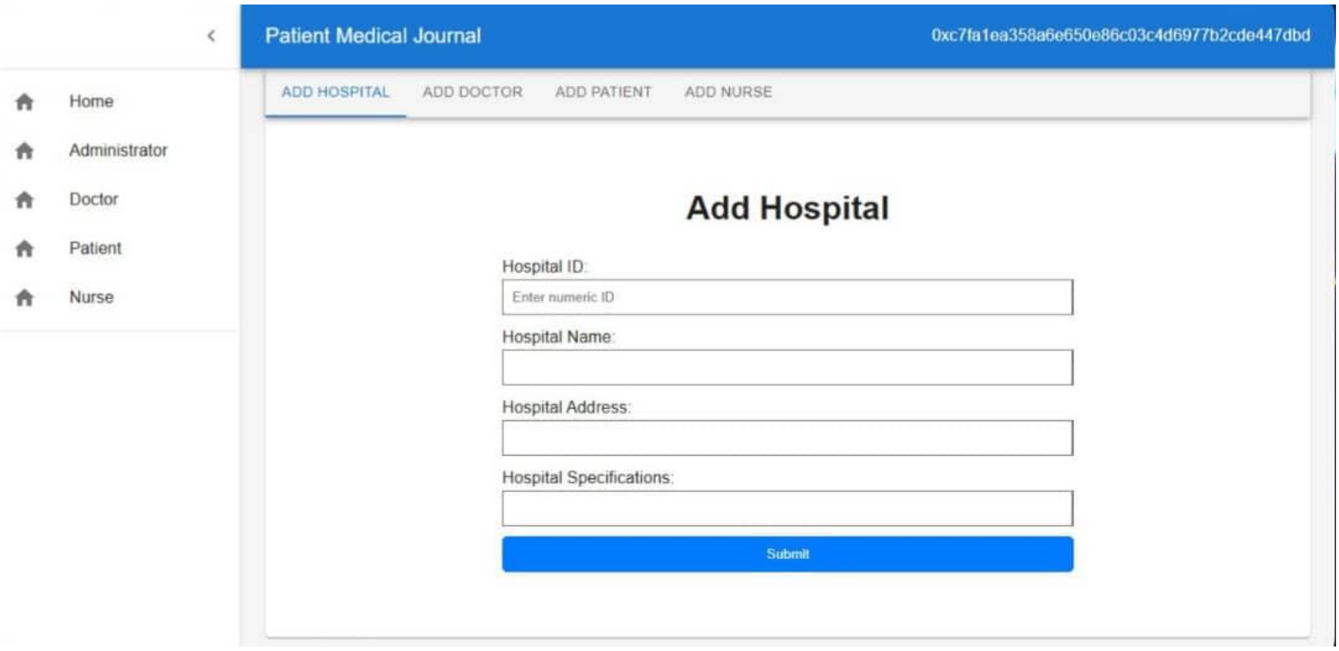


Welcome to Patient Medical Journal

By leveraging blockchain technology, we empower patients with greater control over their personal health information, giving them the ability to manage and consent to data sharing securely and transparently.

Join us in revolutionizing healthcare by putting patients at the center of their medical data and enabling trustworthy, efficient, and patient-centric health record management.

Figure 7: Landing Page



Add Hospital

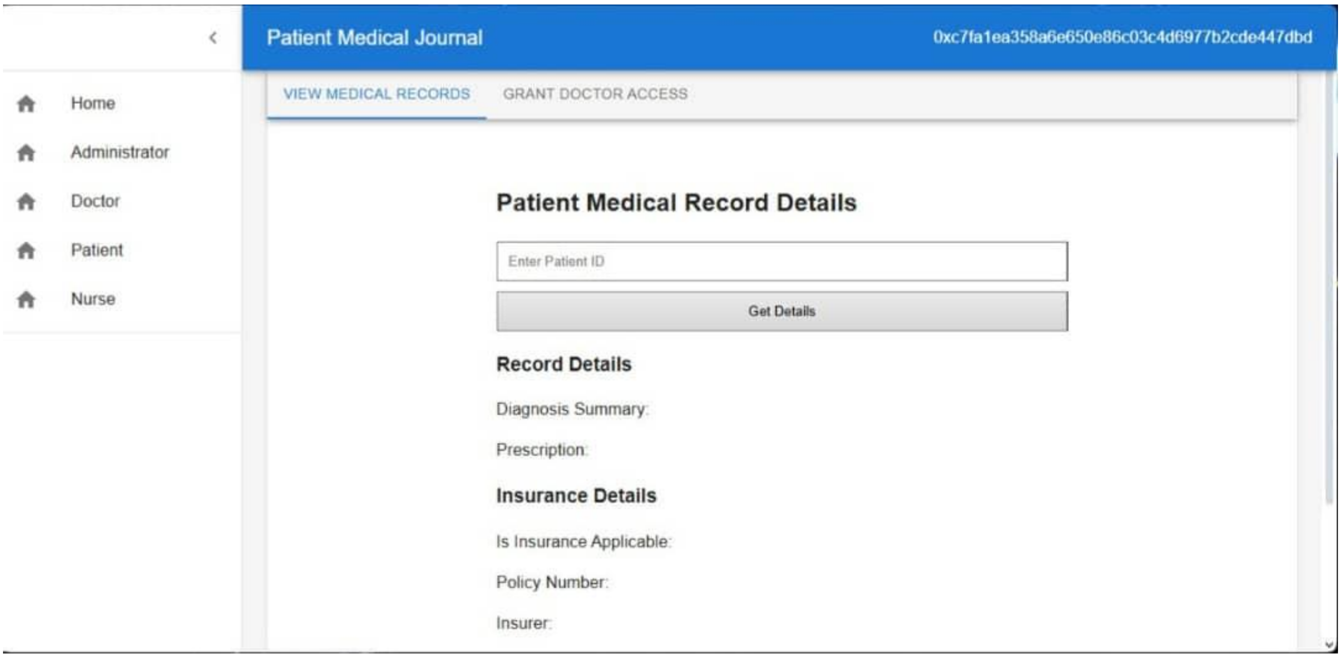
Hospital ID: Enter numeric ID

Hospital Name:

Hospital Address:

Hospital Specifications:

Figure 8: Admin Dashboard


Patient Medical Journal

0xc7fa1ea358a6e650e86c03c4d6977b2cde447dbd

VIEW MEDICAL RECORDS | GRANT DOCTOR ACCESS

- Home
- Administrator
- Doctor
- Patient
- Nurse

**Patient Medical Record Details**

Enter Patient ID

Get Details

**Record Details**

Diagnosis Summary:

Prescription:

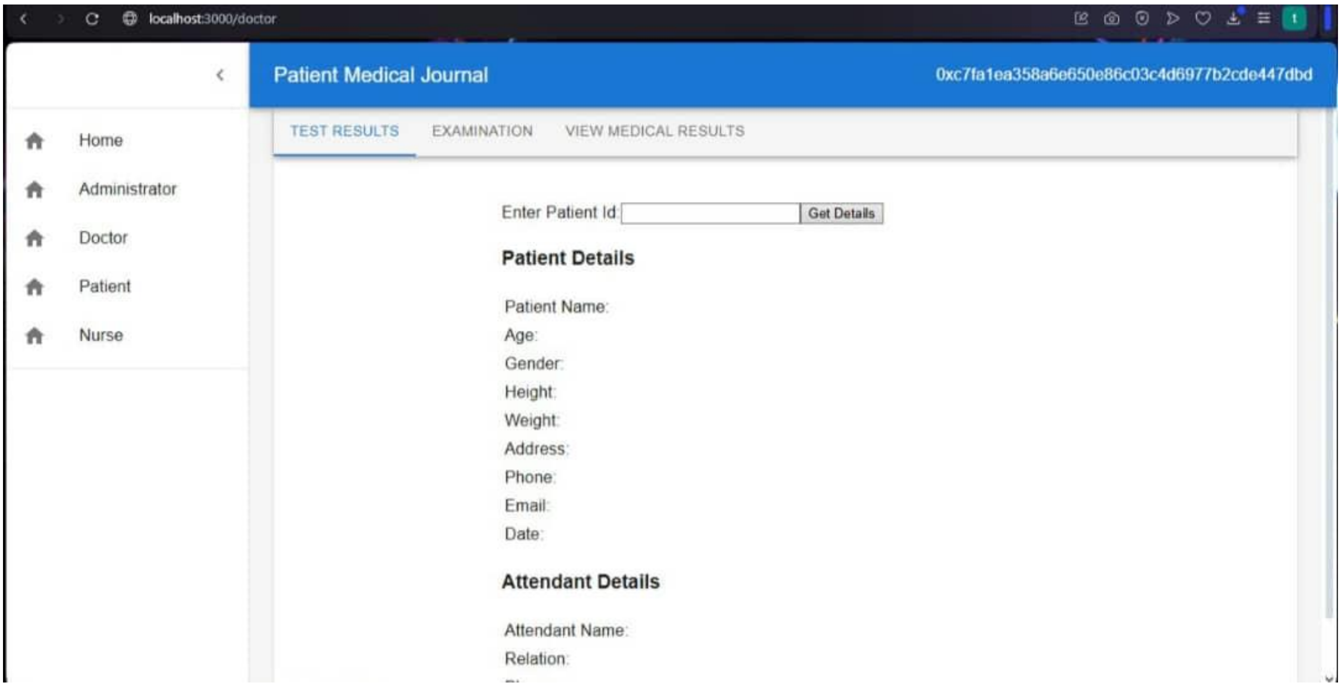
**Insurance Details**

Is Insurance Applicable:

Policy Number:

Insurer:

Figure 9: Patient Dashboard


localhost:3000/doctor

Patient Medical Journal

0xc7fa1ea358a6e650e86c03c4d6977b2cde447dbd

TEST RESULTS | EXAMINATION | VIEW MEDICAL RESULTS

- Home
- Administrator
- Doctor
- Patient
- Nurse

Enter Patient Id: Get Details

**Patient Details**

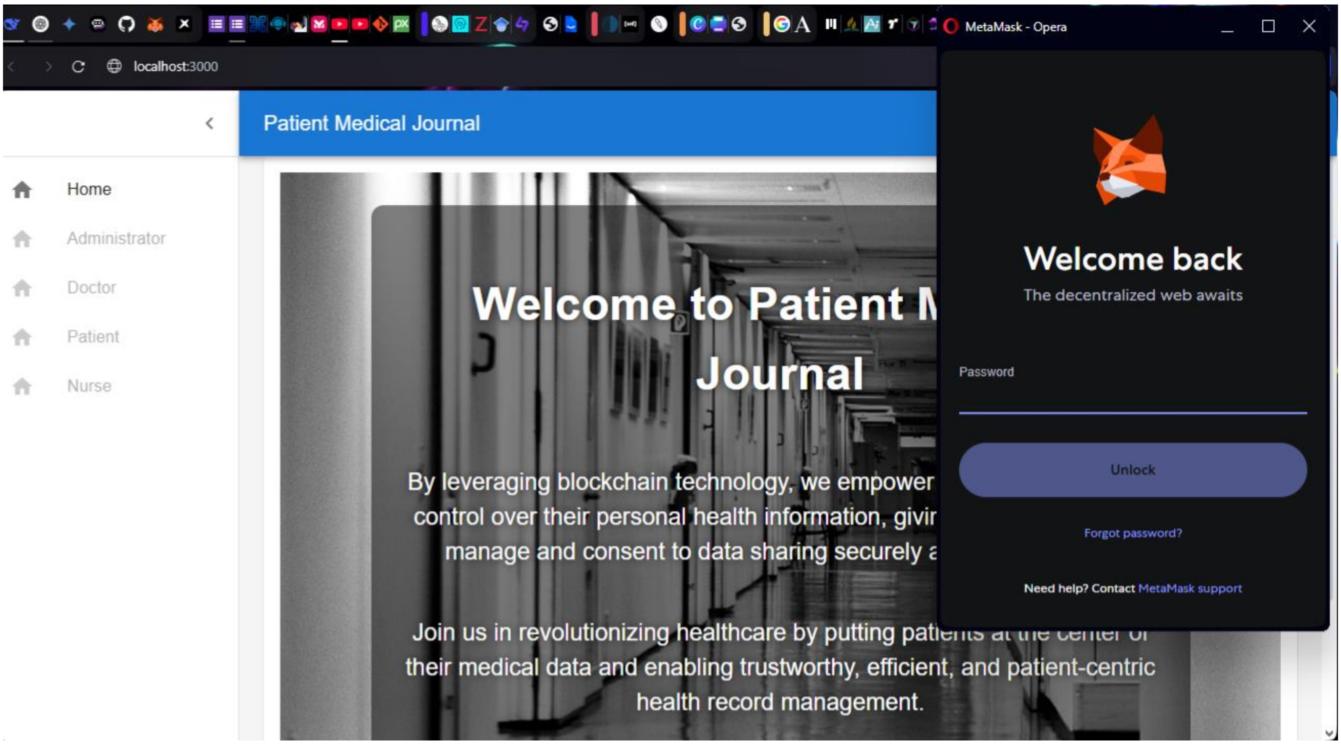
Patient Name:
Age:
Gender:
Height:
Weight:
Address:
Phone:
Email:
Date:

**Attendant Details**

Attendant Name:
Relation:

Figure 10: Doctor Dashboard

The frontend displays medical data to patients/doctors, enable patients to grant or revoke access to doctors, connect to the blockchain using Metamask or another Web3 wallet and send/receive data from smart contracts using ethers.js or web3.js.



Welcome to Patient M
Journal

By leveraging blockchain technology, we empower
control over their personal health information, givir
manage and consent to data sharing securely a

Join us in revolutionizing healthcare by putting patients at the center of their medical data and enabling trustworthy, efficient, and patient-centric health record management.

Figure 11: Connection to Blockchain Using Metamask

The blockchain provides a secure and decentralized platform to store and verify medical data without relying on a centralized database. Blockchain ensures data immutability and integrity. Handles authentication via Ethereum (Metamask) and Maintains trust among users (patient, doctor, hospital).

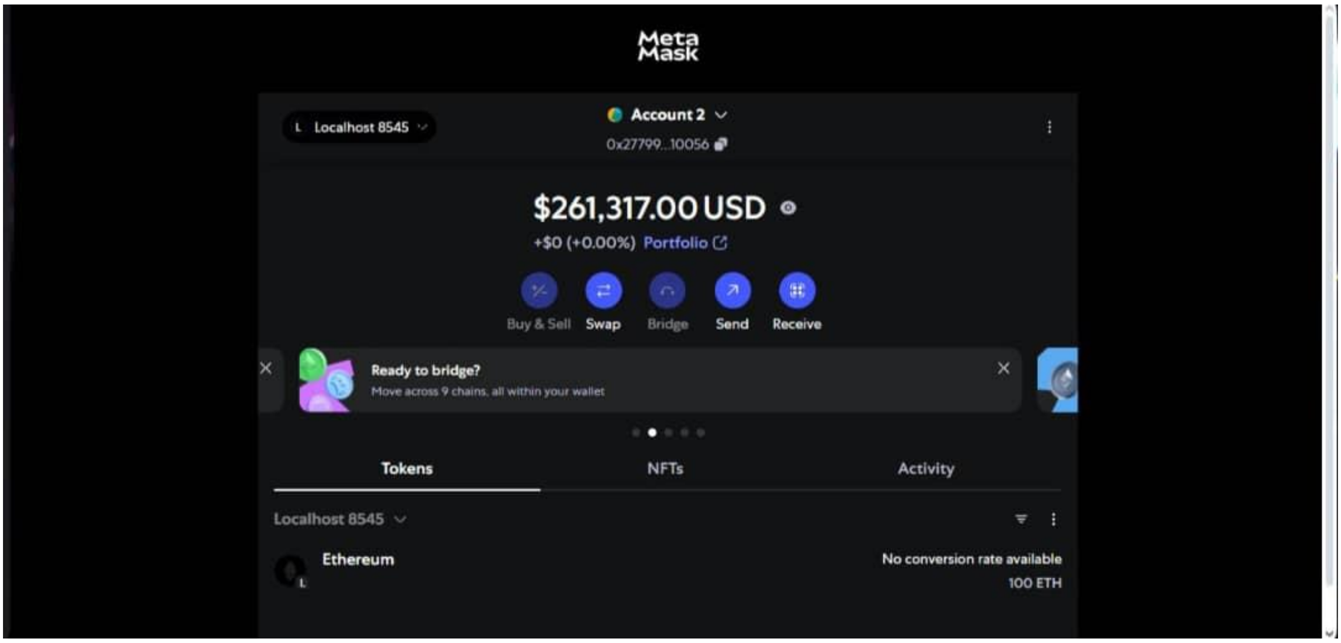
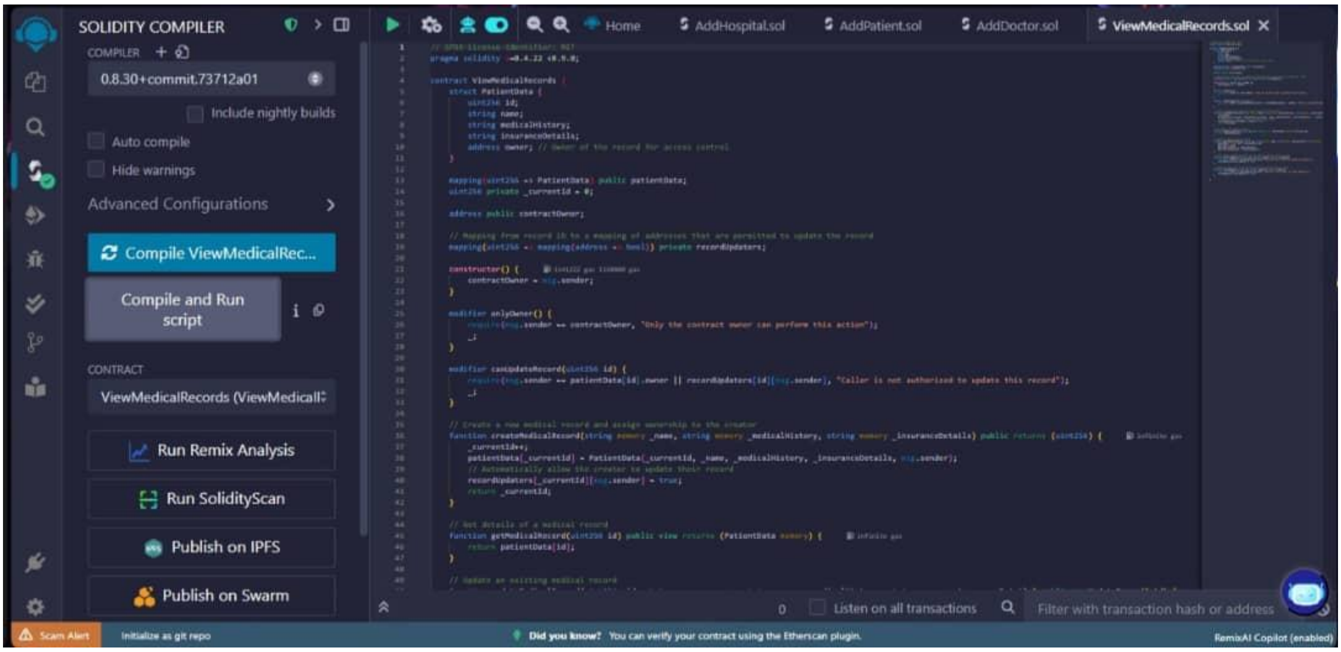


Figure 12: Metamask Account

Smart contracts specify the logic for creating, storing, sharing and controlling access to medical records.

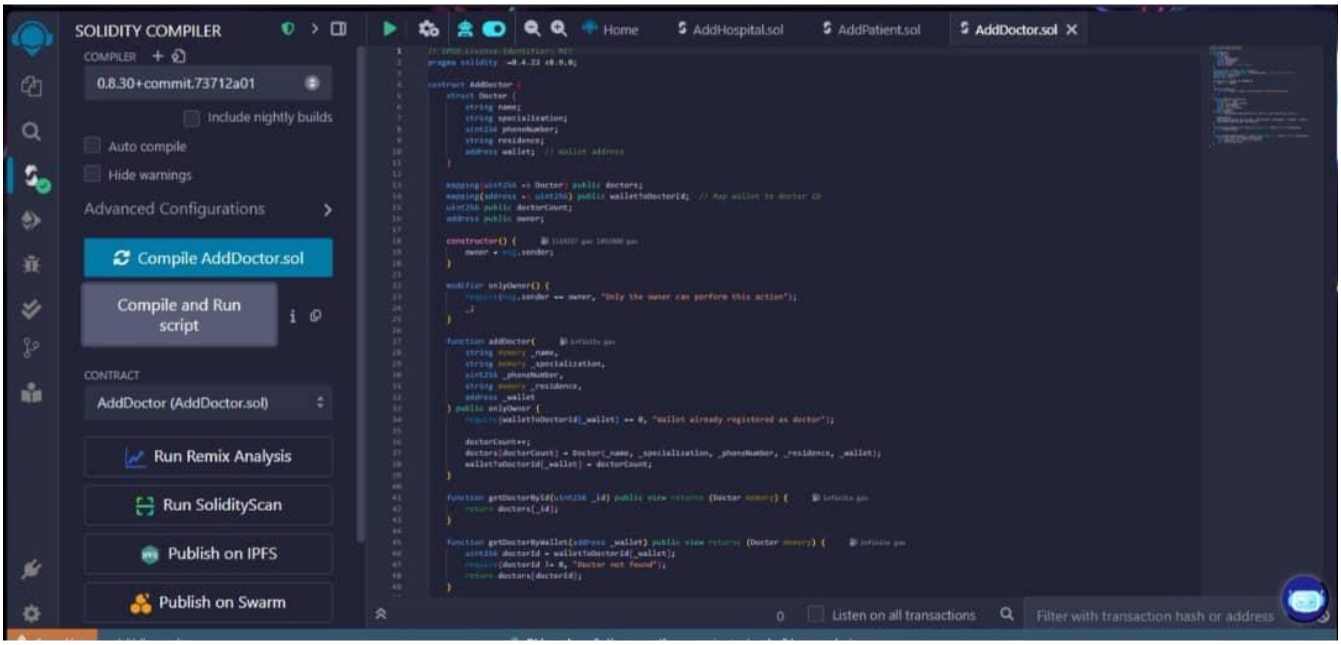
ViewMedicalRecords: Regulates creation and viewing of patient medical records.



```
// SPDX-License-Identifier: MIT
pragma solidity >=0.4.22 <0.9.0;

contract ViewMedicalRecords {
    struct PatientData {
        uint256 id;
        string name;
        string medicalHistory;
        string insuranceDetails;
        address owner; // Owner of the record for access control
    }

    mapping(uint256 => PatientData) public patientData;
    uint256 private _currentId = 0;

    address public contractOwner;

    // Mapping from record ID to a mapping of addresses that are permitted to update the record
    mapping(uint256 => mapping(address => bool)) private recordUpdaters;

    constructor() {
        contractOwner = msg.sender;
    }

    modifier onlyOwner() {
        require(msg.sender == contractOwner, "Only the contract owner can perform this action");
        _;
    }

    modifier canUpdateRecord(uint256 id) {
        require(msg.sender == patientData[id].owner || recordUpdaters[id][msg.sender], "Caller is not authorized to update this record");
        _;
    }

    // Create a new medical record and assign ownership to the creator
    function createMedicalRecord(string memory _name, string memory _medicalHistory, string memory _insuranceDetails) public returns (uint256) {
        _currentId++;
        patientData[_currentId] = PatientData(_currentId, _name, _medicalHistory, _insuranceDetails, msg.sender);
        // Automatically allow the creator to update their record
        recordUpdaters[_currentId][msg.sender] = true;
        return _currentId;
    }

    // Get details of a medical record
    function getMedicalRecord(uint256 id) public view returns (PatientData memory) {
        return patientData[id];
    }

    // Update an existing medical record
```

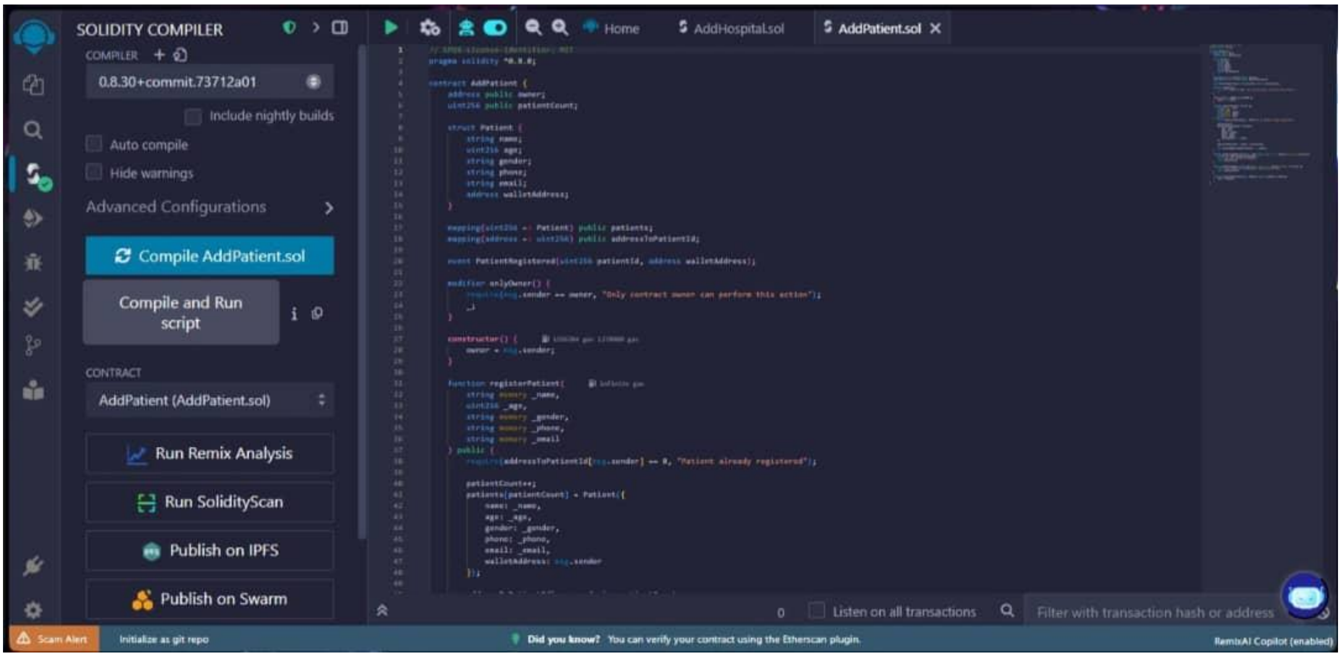
Figure 13: ViewMedicalRecords Smart Contract

AddDoctor, AddHospital, AddNurse, AddPatient: Regulates identity and roles.



```
// SPDX-License-Identifier: MIT
pragma solidity >=0.4.22 <0.9.0;

contract AddDoctor {
    struct Doctor {
        string name;
        string specialization;
        uint256 phoneNumber;
        string residence;
        address wallet;  // wallet address
    }

    mapping(uint256 => Doctor) public doctors;
    mapping(address => uint256) public walletToDoctorId;  // Map wallet to doctor ID
    uint256 public doctorCount;
    address public owner;

    constructor() {
        owner = msg.sender;
    }

    modifier onlyOwner() {
        require(msg.sender == owner, "Only the owner can perform this action");
        _;
    }

    function addDoctor(
        string memory _name,
        string memory _specialization,
        uint256 _phoneNumber,
        string memory _residence,
        address _wallet
    ) public onlyOwner {
        require(walletToDoctorId[_wallet] == 0, "Wallet already registered as doctor");

        doctorCount++;
        doctors[doctorCount] = Doctor(_name, _specialization, _phoneNumber, _residence, _wallet);
        walletToDoctorId[_wallet] = doctorCount;
    }

    function getDoctorById(uint256 _id) public view returns (Doctor memory) {
        return doctors[_id];
    }

    function getDoctorByWallet(address _wallet) public view returns (Doctor memory) {
        uint256 doctorId = walletToDoctorId[_wallet];
        require(doctorId != 0, "Doctor not found");
        return doctors[doctorId];
    }
```

Figure 14: AddDoctor Smart Contract



COMPILER
0.8.30+commit.73712a01

CONTRACT
AddPatient (AddPatient.sol)

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract AddPatient {
    address public owner;
    uint256 public patientCount;

    struct Patient {
        string name;
        uint256 age;
        string gender;
        string phone;
        string email;
        address walletAddress;
    }

    mapping(uint256 => Patient) public patients;
    mapping(address => uint256) public addressToPatientId;

    event PatientRegistered(uint256 patientId, address walletAddress);

    modifier onlyOwner() {
        require(msg.sender == owner, "Only contract owner can perform this action");
        _;
    }

    constructor() {
        owner = msg.sender;
    }

    function registerPatient(
        string memory _name,
        uint256 _age,
        string memory _gender,
        string memory _phone,
        string memory _email
    ) public {
        require(addressToPatientId[msg.sender] == 0, "Patient already registered");

        patientCount++;
        patients[patientCount] = Patient({
            name: _name,
            age: _age,
            gender: _gender,
            phone: _phone,
            email: _email,
            walletAddress: msg.sender
        });
```

Did you know? You can verify your contract using the Etherscan plugin.

Figure 15: AddPatient Smart Contract

Access control functions allow patient to control who sees or edit their data.

Smart contracts provide transparency and automatic log logic, cannot be changed or modified after deployment and Removes reliance on a central authority.

### 4.3 Software Testing

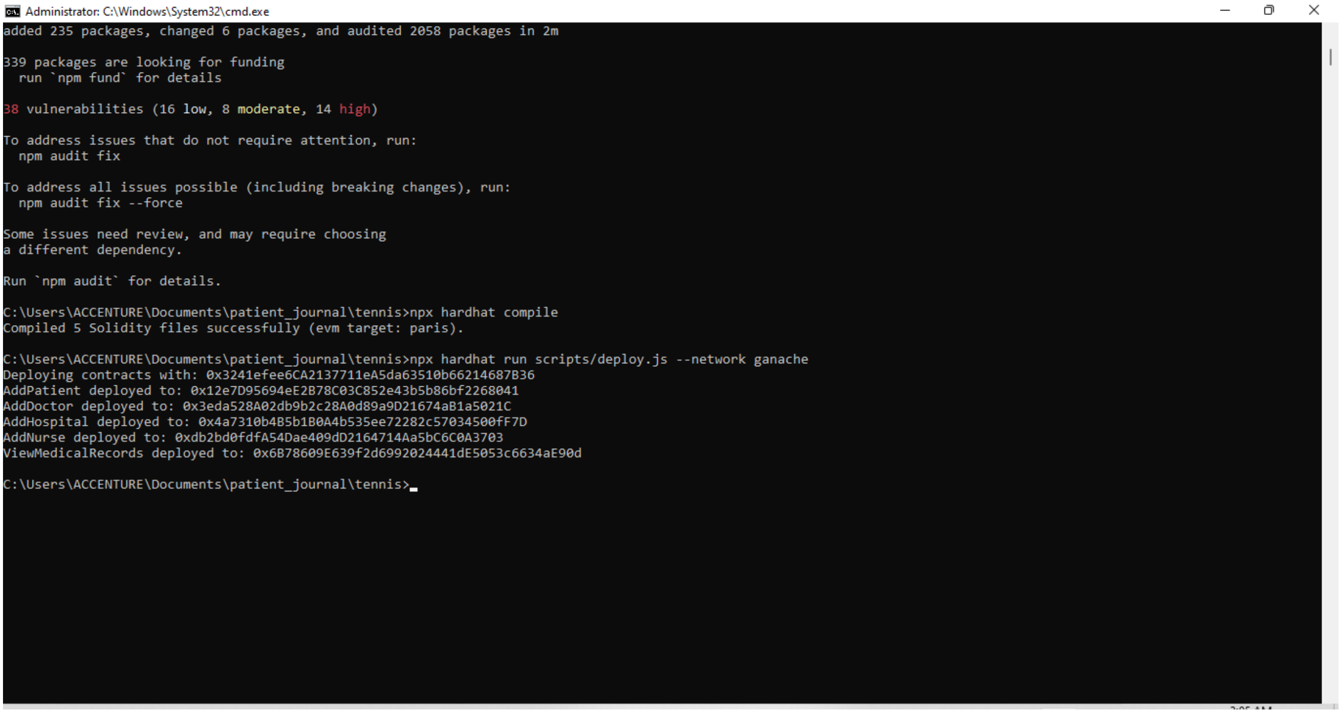
Software testing is a critical stage in the life cycle of development that validates the system developed against agreed-upon requirements and behaves as expected under projected conditions. Software testing involves executing the software with the intention to identify any defects or lack of conformance to expected outcomes (Sommerville, 2015). Software testing not only verifies that a system works as required but also as needed by the stakeholders (Sommerville, 2015). In the Blockchain-Based Health Journal for Sharing Medical Records Between Different Health Providers, software testing was employed to assess the system's functionality, security and usability. Since health data is sensitive and requires interoperability between different health providers, exhaustive testing was needed to guarantee data integrity, privacy and role- based access control was implemented correctly.

Testing was aimed at both functional requirements (e.g., login, medical record upload, grant/revoke access) and non-functional requirements such as performance, reliability, and security. Testing involved unit testing of smart contracts, integration testing of the blockchain with the frontend, and system testing to ensure the system overall (Myers, et al., 2011). Effective software testing increases system reliability and increases user confidence, particularly in systems handling sensitive data such as medical records. Additionally, due to the decentralized and immutable nature of blockchain, there was a need to ensure smart contracts behaved as expected, as errors once deployed could not be altered easily (Dinh, et al., 2018). Finally, usability testing with a few targeted users (patients, doctors, and administrators) was conducted to trial the interface and ensure the system was easy to use and addressed their requirements. This type of testing is especially important in health informatics systems where end-users' interaction affects adoption and efficacy (Zhou, et al., 2019).

### 4.3.1 White Box Testing

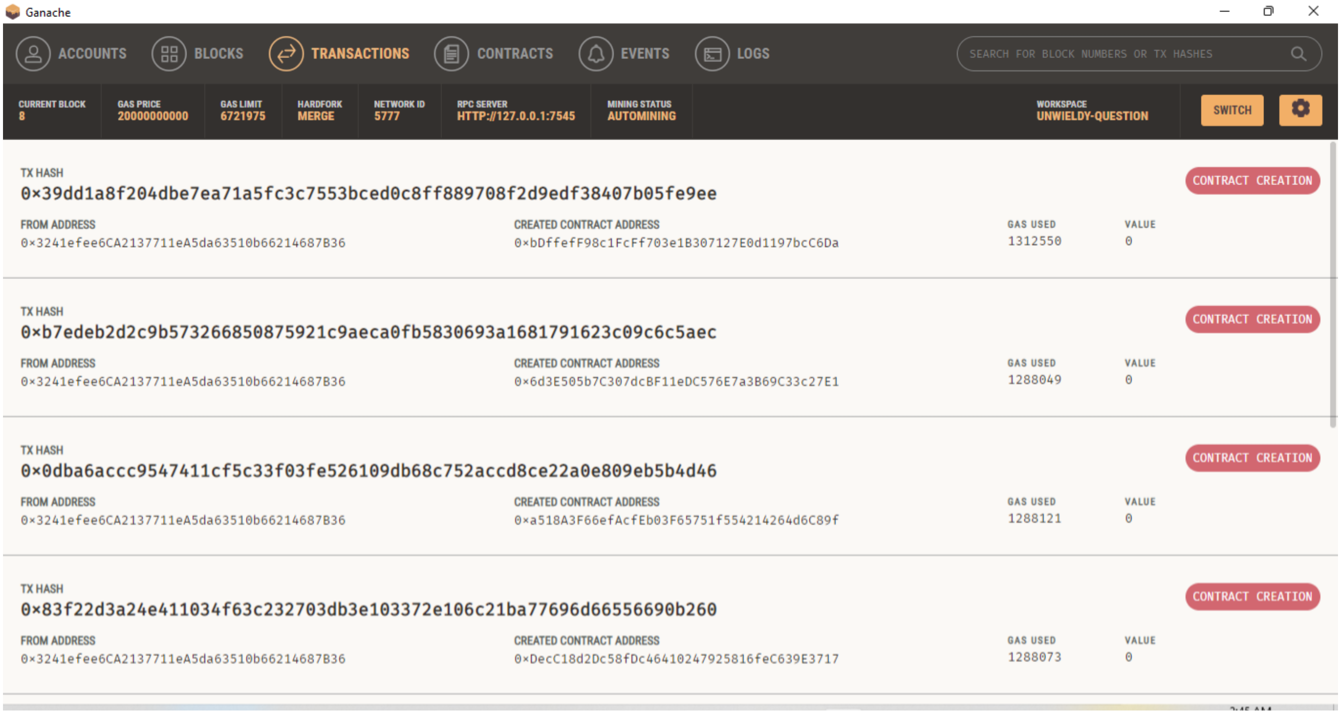
White-box testing, alternately referred to as structural or glass-box testing, involves verifying the internal structure, logic, and code of the software application. This technique allows testers to verify paths within the code, conditions, loops, and internal data structures (Myers, et al., 2011). In this study, white box testing was particularly utilized in the smart contracts on the Ethereum blockchain. These contracts responsible for automating access control and patient consent were interested in ensuring all conditional logic was executed correctly and unauthorized data access was always rejected.

Unit testing tools like Truffle and Hardhat were used to execute purposeful functions in the smart contracts and observe results based on different role-based inputs.



```
added 235 packages, changed 6 packages, and audited 2058 packages in 2m

339 packages are looking for funding
  run `npm fund` for details

38 vulnerabilities (16 low, 8 moderate, 14 high)

To address issues that do not require attention, run:
  npm audit fix

To address all issues possible (including breaking changes), run:
  npm audit fix --force

Some issues need review, and may require choosing
a different dependency.

Run `npm audit` for details.

C:\Users\ACCENTURE\Documents\patient_journal\tennis>npx hardhat compile
Compiled 5 Solidity files successfully (evm target: paris).

C:\Users\ACCENTURE\Documents\patient_journal\tennis>npx hardhat run scripts/deploy.js --network ganache
Deploying contracts with: 0x3241efee6CA2137711eA5da63510b66214687B36
AddPatient deployed to: 0x12e7D95694eE2B78C03C852e43b5b86bf2268041
AddDoctor deployed to: 0x3eda528A02db9b2c28A0d89a9D21674aB1a5021C
AddHospital deployed to: 0x4a7310b4B5b1B0A4b535ee72282c57034500fF7D
AddNurse deployed to: 0xdb2bd0fdfA54Dae409dD2164714Aa5bC6C0A3703
ViewMedicalRecords deployed to: 0x6B78609E639f2d6992024441dE5053c6634aE90d

C:\Users\ACCENTURE\Documents\patient_journal\tennis>
```

Figure 16: Smart Contracts deployed using Hardhat



CURRENT BLOCK 8 | GAS PRICE 20000000000 | GAS LIMIT 6721975 | HARDFORK MERGE | NETWORK ID 5777 | RPC SERVER HTTP://127.0.0.1:7545 | MINING STATUS AUTOMINING | WORKSPACE UNWIELDY-QUESTION

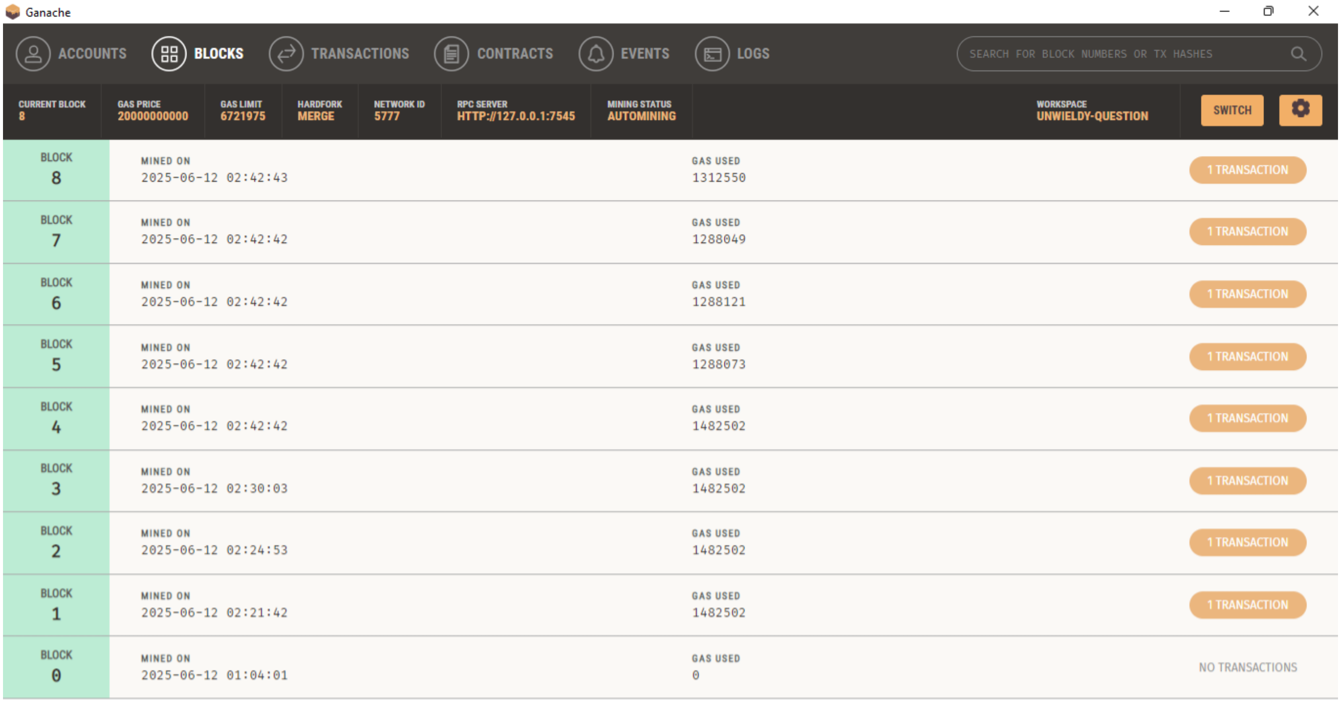
TX HASH
0×39dd1a8f204dbe7ea71a5fc3c7553bced0c8ff889708f2d9edf38407b05fe9ee
CONTRACT CREATION
FROM ADDRESS 0×3241efee6CA2137711eA5da63510b66214687B36
CREATED CONTRACT ADDRESS 0×bDffefF98c1FcFf703e1B307127E0d1197bcC6Da
GAS USED 1312550
VALUE 0

TX HASH
0×b7edeb2d2c9b573266850875921c9aeca0fb5830693a1681791623c09c6c5aec
CONTRACT CREATION
FROM ADDRESS 0×3241efee6CA2137711eA5da63510b66214687B36
CREATED CONTRACT ADDRESS 0×6d3E505b7C307dcBF11eDC576E7a3B69C33c27E1
GAS USED 1288049
VALUE 0

TX HASH
0×0dba6accc9547411cf5c33f03fe526109db68c752accd8ce22a0e809eb5b4d46
CONTRACT CREATION
FROM ADDRESS 0×3241efee6CA2137711eA5da63510b66214687B36
CREATED CONTRACT ADDRESS 0×a518A3F66efAcfEb03F65751f554214264d6C89f
GAS USED 1288121
VALUE 0

TX HASH
0×83f22d3a24e411034f63c232703db3e103372e106c21ba77696d66556690b260
CONTRACT CREATION
FROM ADDRESS 0×3241efee6CA2137711eA5da63510b66214687B36
CREATED CONTRACT ADDRESS 0×DecC18d2Dc58fDc46410247925816feC639E3717
GAS USED 1288073
VALUE 0

Figure 17: Transactions Log showing gas used



| CURRENT BLOCK | GAS PRICE | GAS LIMIT | HARDFORK | NETWORK ID | RPC SERVER | MINING STATUS | WORKSPACE |
|---|---|---|---|---|---|---|---|
| 8 | 20000000000 | 6721975 | MERGE | 5777 | HTTP://127.0.0.1:7545 | AUTOMINING | UNWIELDY-QUESTION |

| | | | |
|---|---|---|---|
| BLOCK<br>8 | MINED ON<br>2025-06-12 02:42:43 | GAS USED<br>1312550 | 1 TRANSACTION |
| BLOCK<br>7 | MINED ON<br>2025-06-12 02:42:42 | GAS USED<br>1288049 | 1 TRANSACTION |
| BLOCK<br>6 | MINED ON<br>2025-06-12 02:42:42 | GAS USED<br>1288121 | 1 TRANSACTION |
| BLOCK<br>5 | MINED ON<br>2025-06-12 02:42:42 | GAS USED<br>1288073 | 1 TRANSACTION |
| BLOCK<br>4 | MINED ON<br>2025-06-12 02:42:42 | GAS USED<br>1482502 | 1 TRANSACTION |
| BLOCK<br>3 | MINED ON<br>2025-06-12 02:30:03 | GAS USED<br>1482502 | 1 TRANSACTION |
| BLOCK<br>2 | MINED ON<br>2025-06-12 02:24:53 | GAS USED<br>1482502 | 1 TRANSACTION |
| BLOCK<br>1 | MINED ON<br>2025-06-12 02:21:42 | GAS USED<br>1482502 | 1 TRANSACTION |
| BLOCK<br>0 | MINED ON<br>2025-06-12 01:04:01 | GAS USED<br>0 | NO TRANSACTIONS |

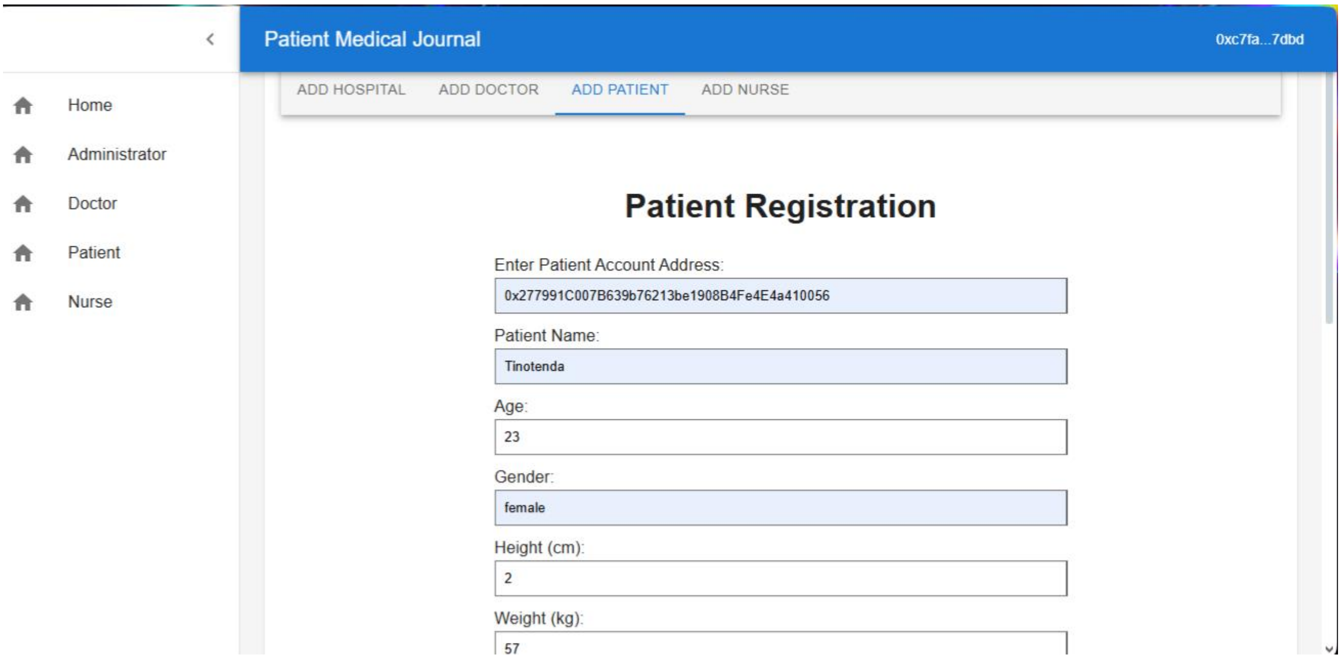
Figure 18: Blocks to store the contracts or data

### 4.3.2 Black Box Testing

Black-box testing entails testing the system from the user's perspective, without any regard to the internal operations of the application. The aim is to determine if the software conducts itself as expected when subjected to various inputs and conditions (Sommerville, 2015). In this research, black-box testing was utilized to test the user interface, system workflows and interactions between patients, doctors and administrators.

Test cases were derived from the system’s functional requirements, including:

Admin adds a new hospital or user role



Patient Registration

Enter Patient Account Address: 0x277991C007B639b76213be1908B4Fe4E4a410056

Patient Name: Tinotenda

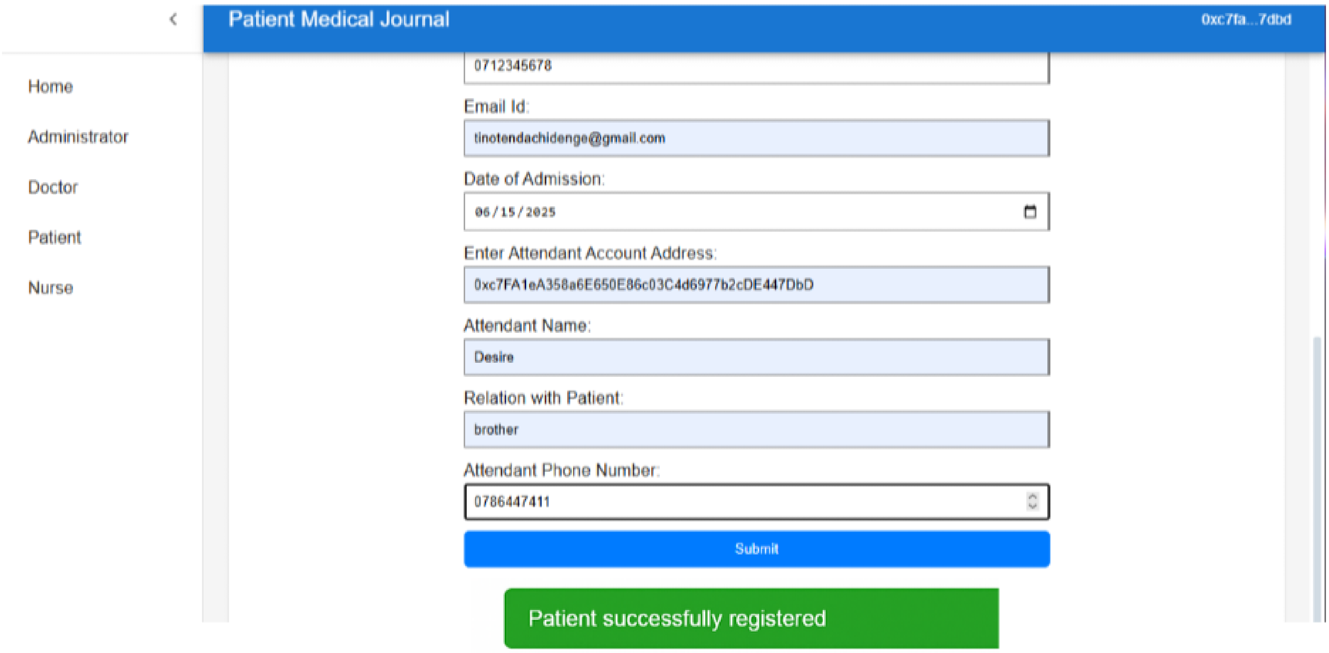
Age: 23

Gender: female

Height (cm): 2

Weight (kg): 57

Figure 19: Patient Registration



0712345678

Email Id: tinotendachidenge@gmail.com

Date of Admission: 06/15/2025

Enter Attendant Account Address: 0xc7FA1eA358a6E650E86c03C4d6977b2cDE447DbD

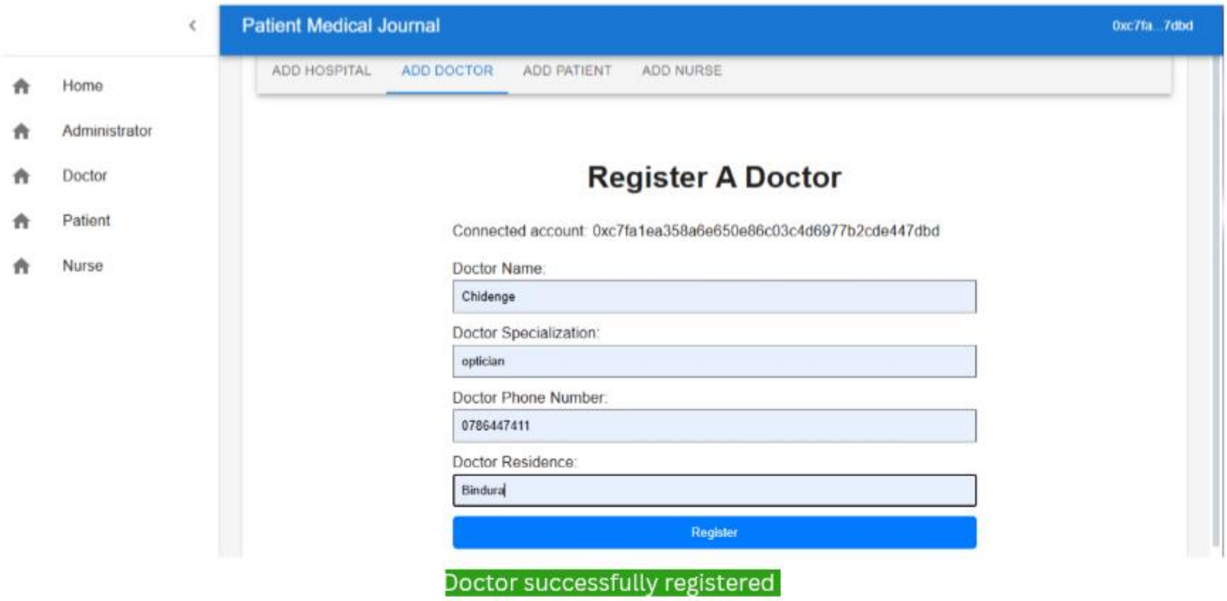
Attendant Name: Desire

Relation with Patient: brother

Attendant Phone Number: 0786447411

Patient successfully registered

Figure 20: Patient Registration



Register A Doctor

Connected account: 0xc7fa1ea358a6e650e86c03c4d6977b2cde447dbd

Doctor Name: Chidenge

Doctor Specialization: optician

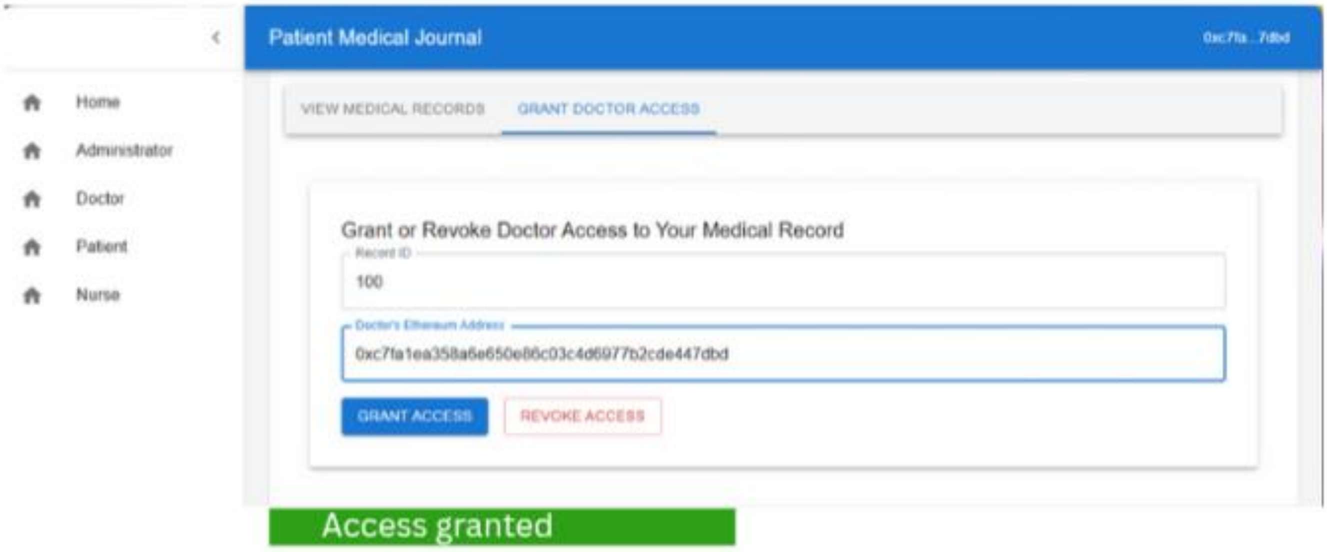
Doctor Phone Number: 0786447411

Doctor Residence: Bindura

Doctor successfully registered

Figure 21: Doctor Registration

Patient grants and revokes access



Grant or Revoke Doctor Access to Your Medical Record

Record ID: 100

Doctor's Ethereum Address: 0xc7fa1ea358a6e650e86c03c4d6977b2cde447dbd

Access granted

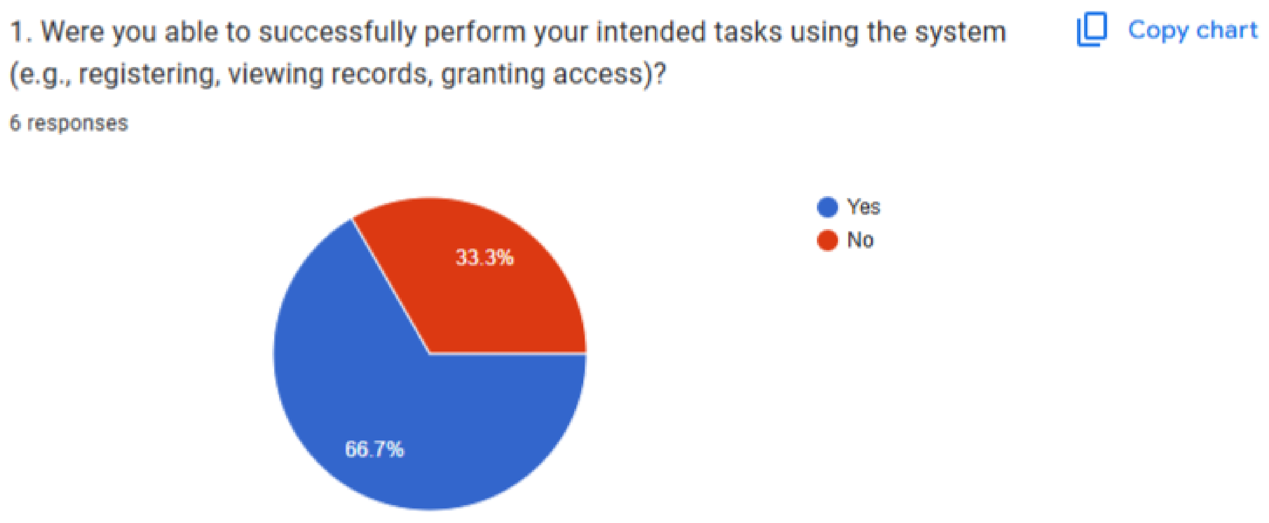
Figure 22: Patient Grant Doctor Access

Each test scenario was executed to ensure the system produced the correct outputs for valid inputs and handled invalid or unauthorized inputs appropriately. This type of testing helped identify usability issues, validation errors and unexpected behaviors, especially from a non-technical end-user perspective.

### 4.3.2 Evaluation Metrics

1. System Usability

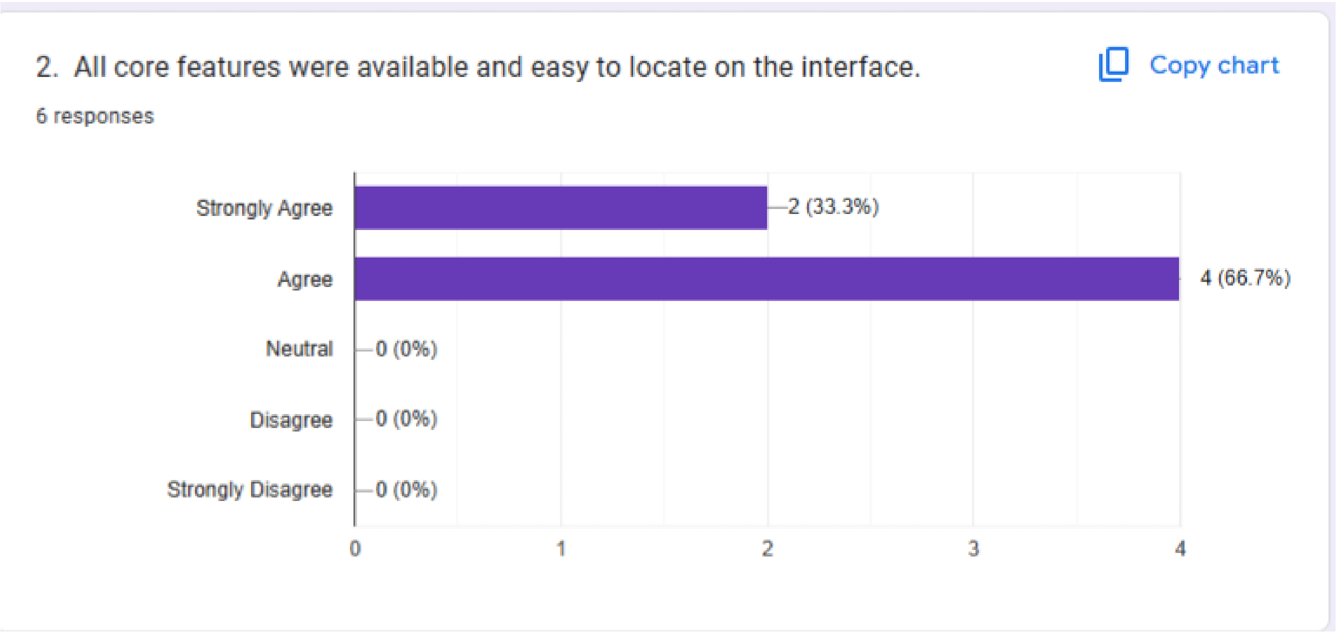
User feedback via surveys. Users found the UI intuitive, with 66.7% completing their tasks without external help.



1. Were you able to successfully perform your intended tasks using the system (e.g., registering, viewing records, granting access)?

6 responses

Figure 23: System Usability



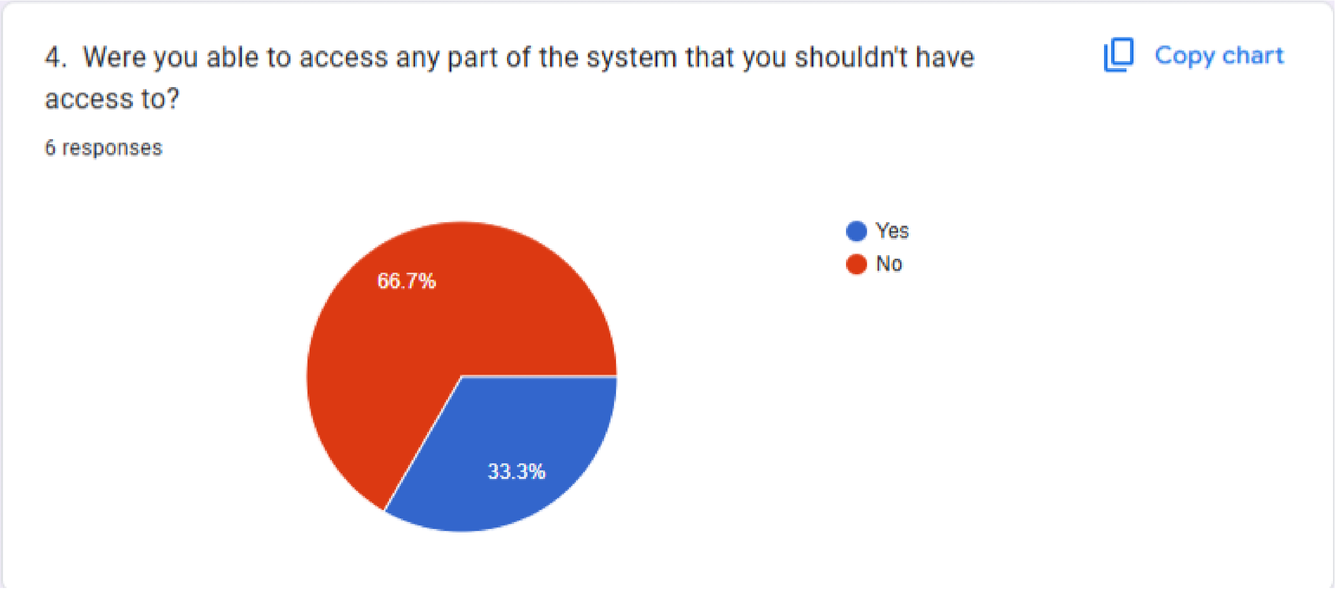
2. All core features were available and easy to locate on the interface.

6 responses

Figure 24: System Usability

Access Control Accuracy

Number of unauthorized accesses. Validates the effectiveness of role-based and patient-controlled access.

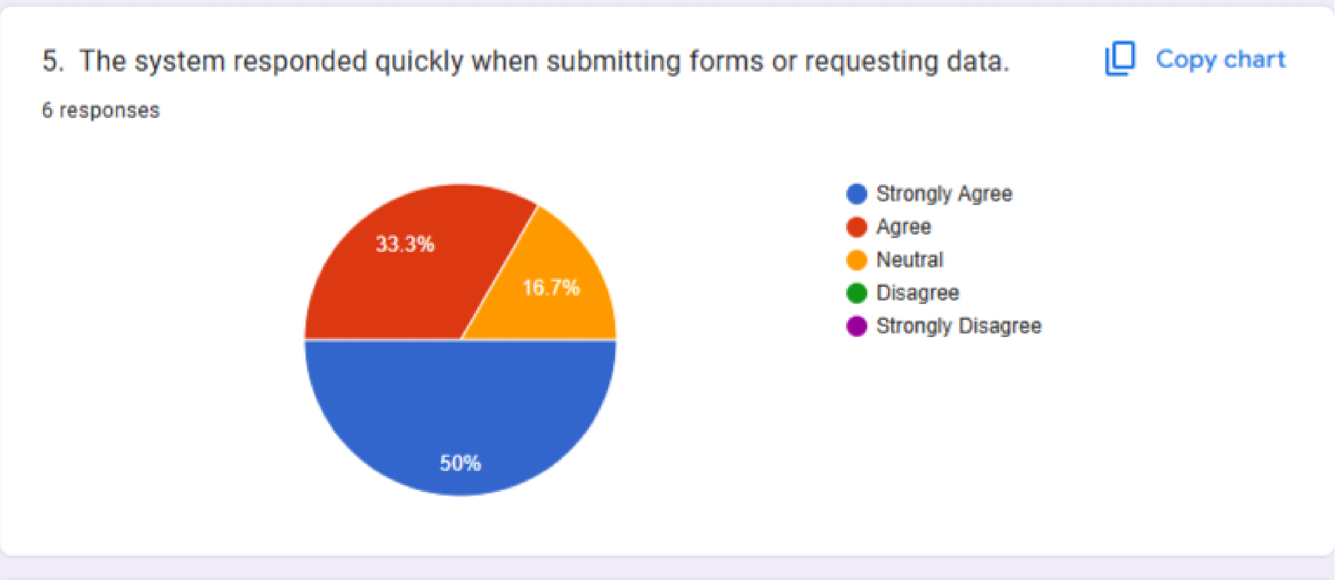


4. Were you able to access any part of the system that you shouldn't have access to?

6 responses

Figure 25: Access Control Accuracy

Response Time

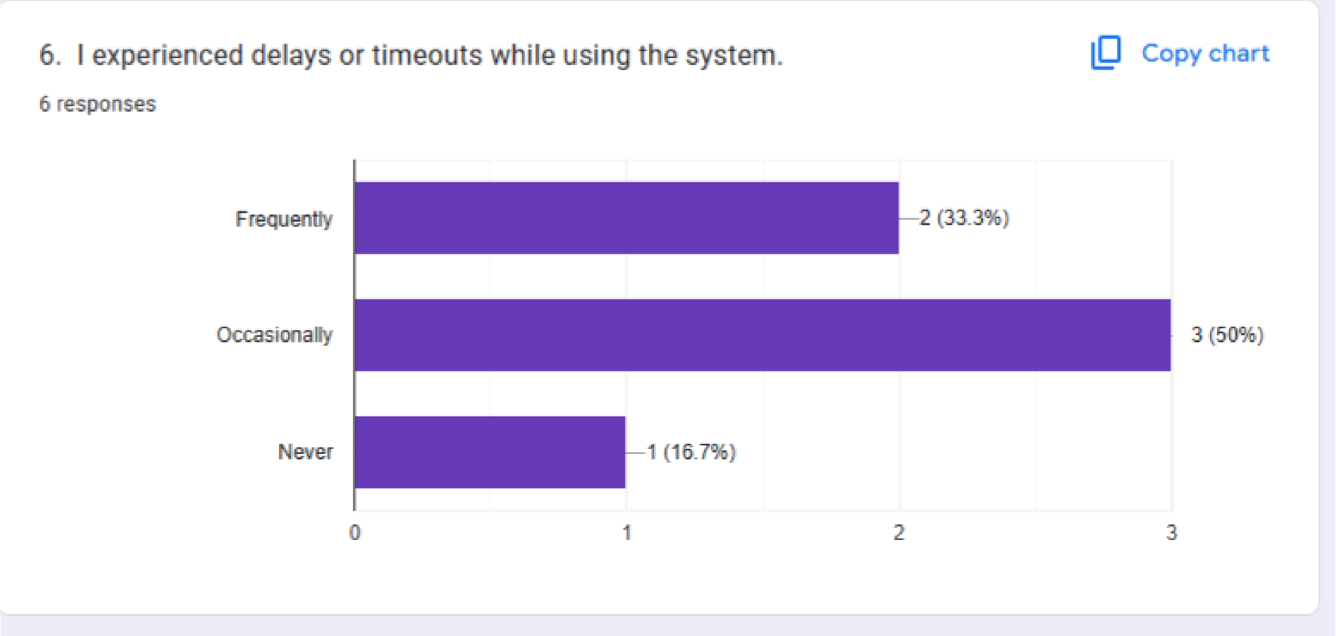


5. The system responded quickly when submitting forms or requesting data.

6 responses

Figure 26: Response time

Delay Time

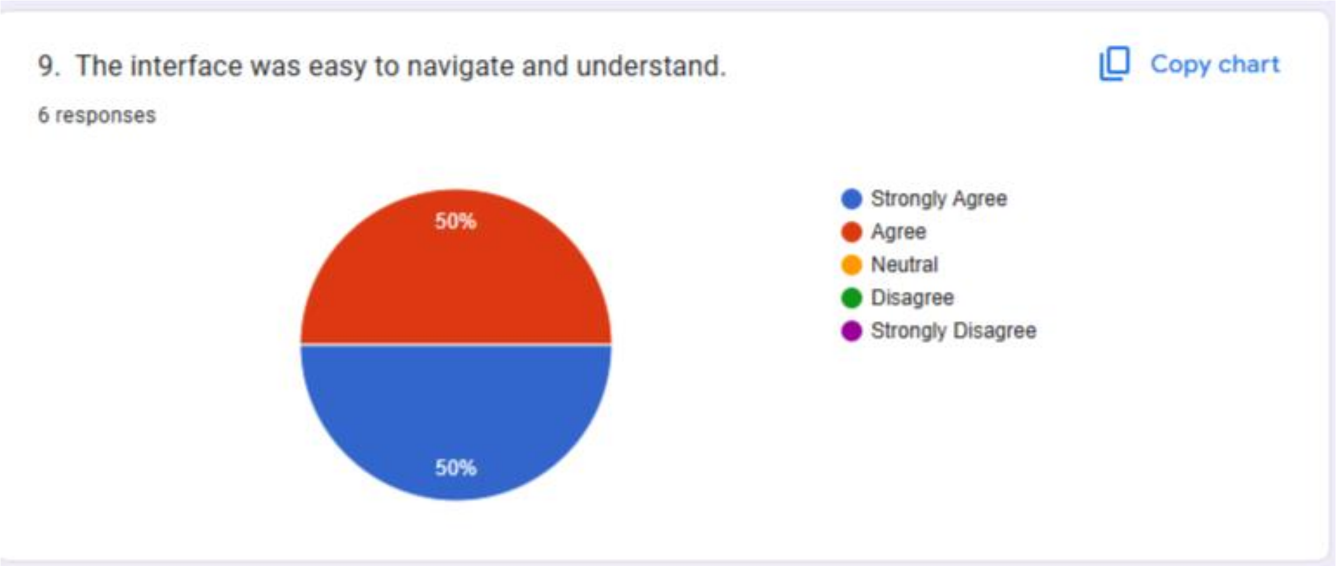


6. I experienced delays or timeouts while using the system.

6 responses

Figure 27: Delay Time

User Experience



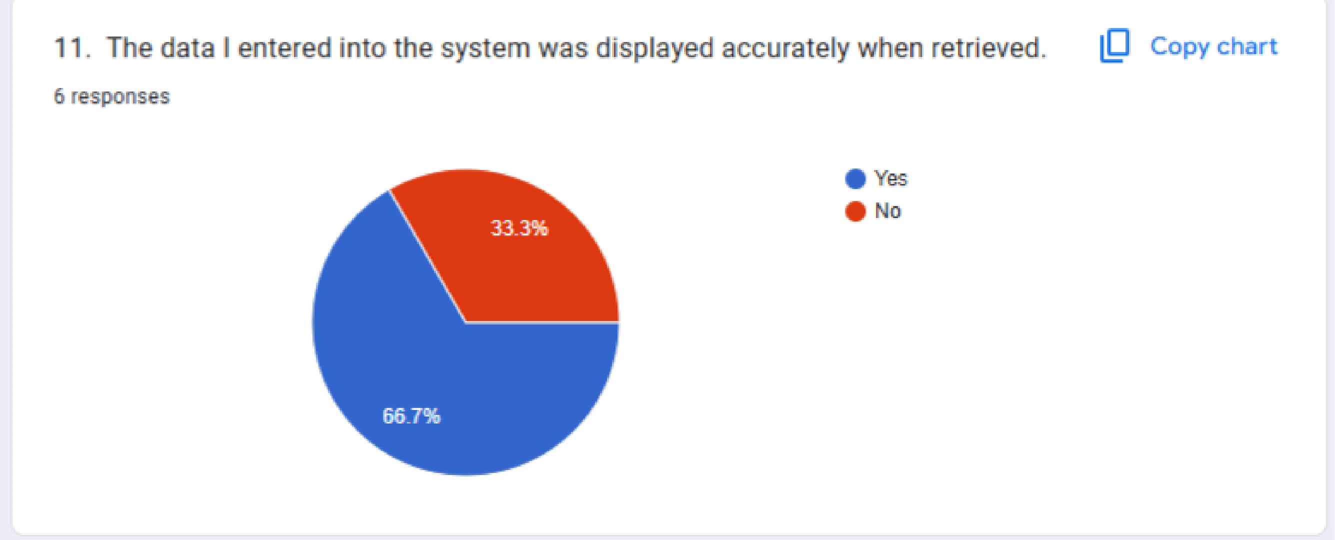
9. The interface was easy to navigate and understand.

6 responses

Figure 28: User Experience

Data Integrity

Ensures that data submitted matches data retrieved. Patient details retrieved from blockchain matched input data 66.7% of the time."

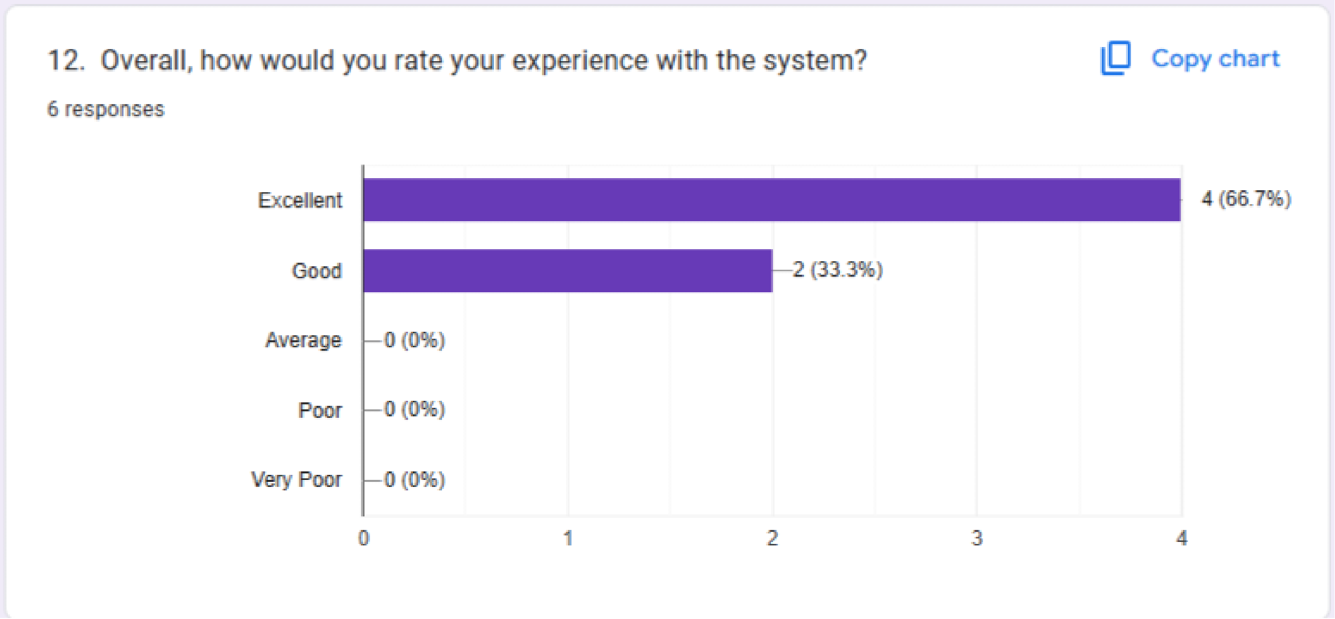


11. The data I entered into the system was displayed accurately when retrieved.

6 responses

Figure 29: Data Integrity

Overall System Performance



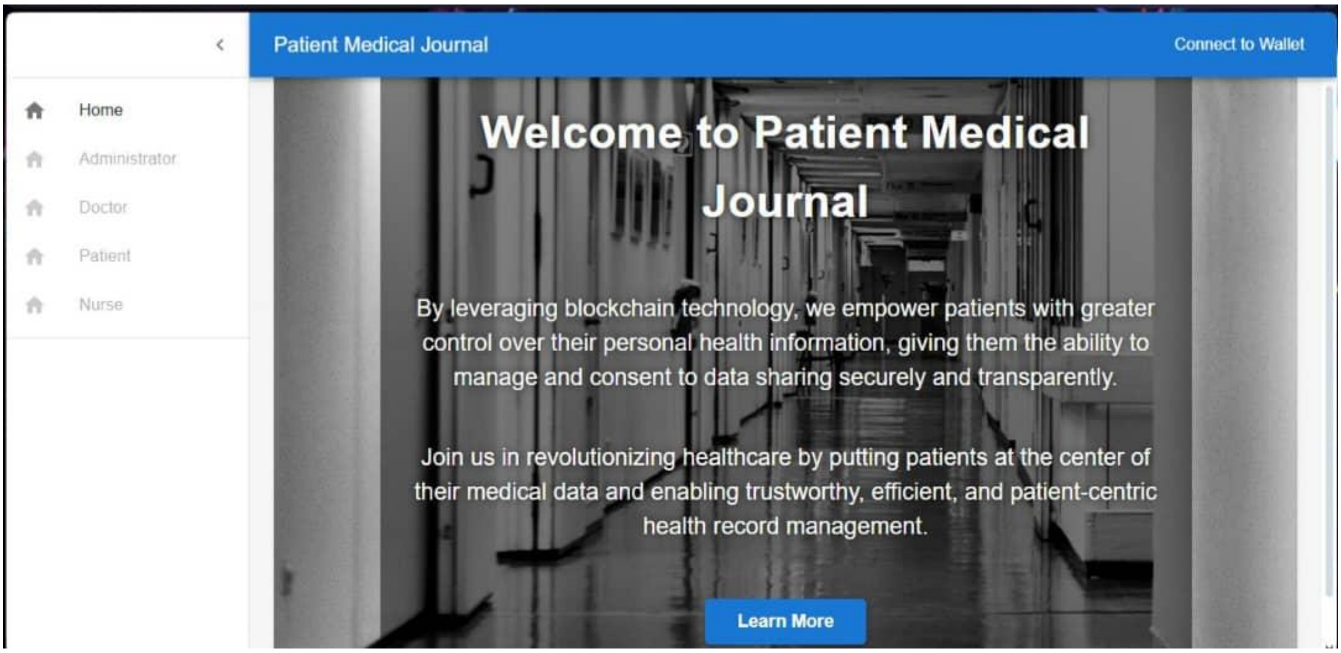
12. Overall, how would you rate your experience with the system?

6 responses

Figure 30: Overall Performance

### 4.4 System Overview

1. Landing page



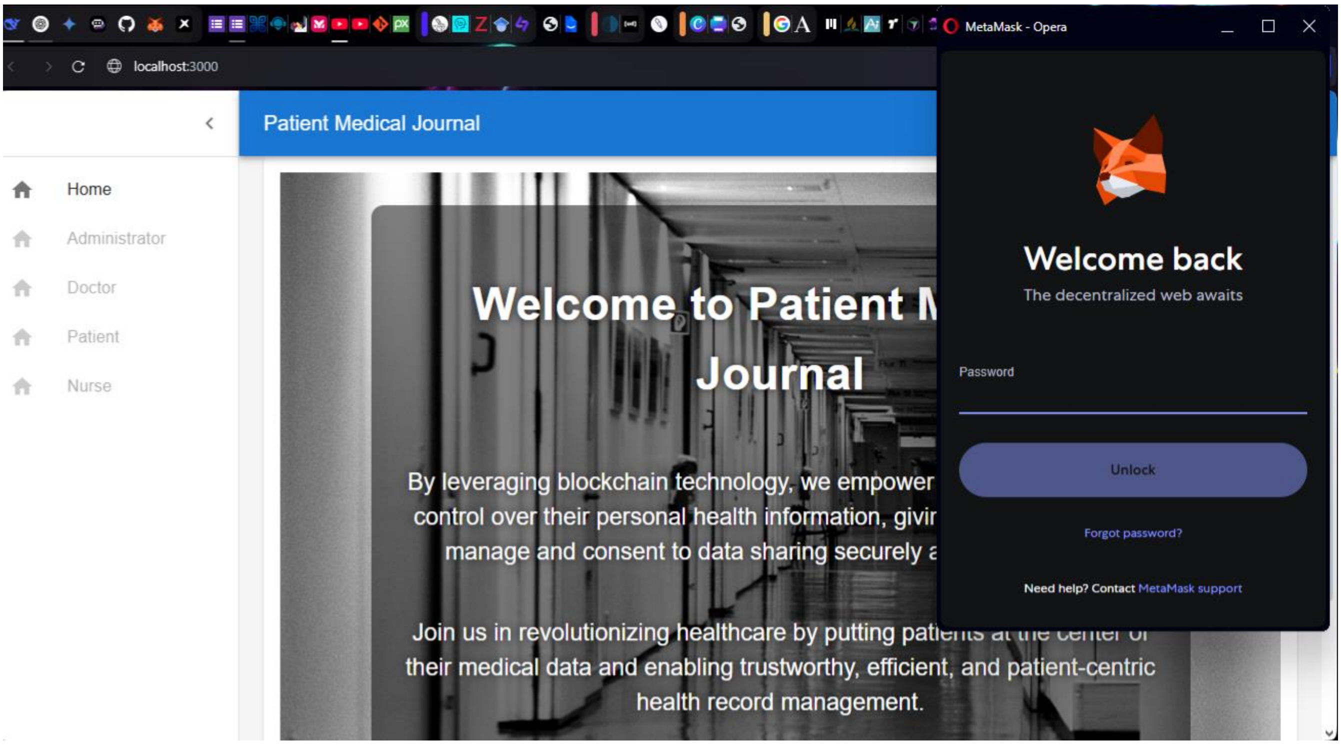
Welcome to Patient Medical Journal

By leveraging blockchain technology, we empower patients with greater control over their personal health information, giving them the ability to manage and consent to data sharing securely and transparently.

Join us in revolutionizing healthcare by putting patients at the center of their medical data and enabling trustworthy, efficient, and patient-centric health record management.

2. User Connects with MetaMask.

The user is prompted to connect with MetaMask and Metamask authenticates the user’s Ethereum address and determines their role.



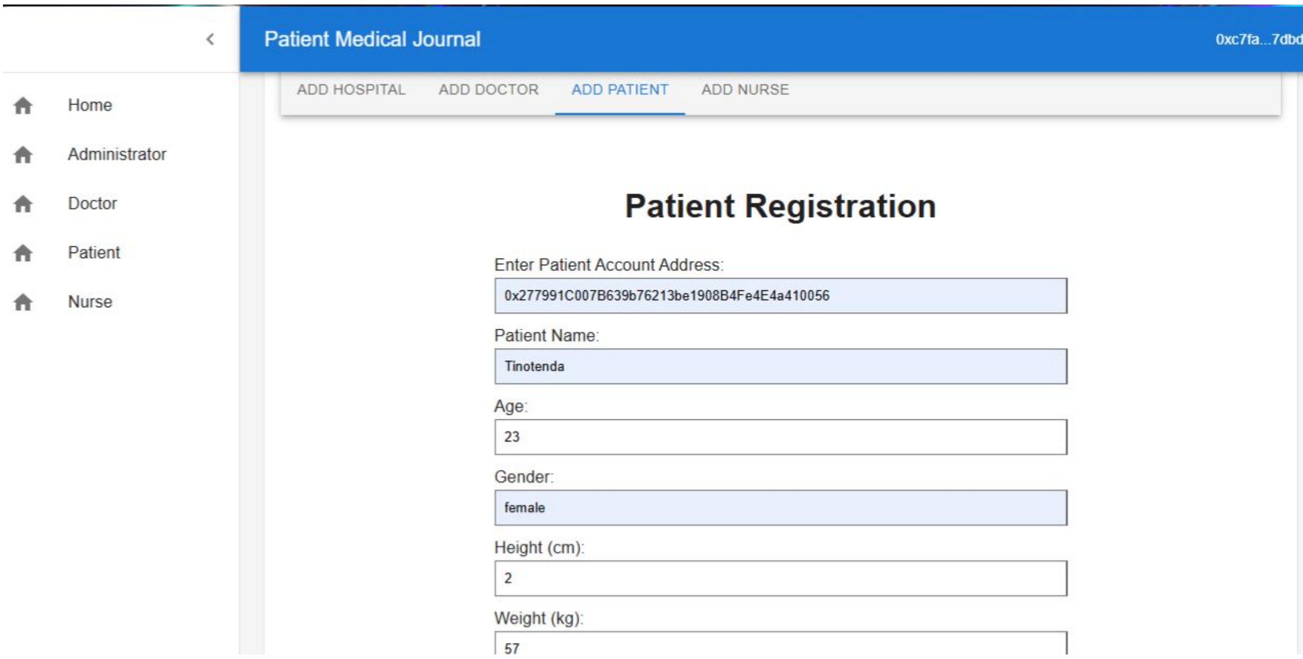
Welcome to Patient M
Journal

By leveraging blockchain technology, we empower
control over their personal health information, givir
manage and consent to data sharing securely a

Join us in revolutionizing healthcare by putting patients at the center of their medical data and enabling trustworthy, efficient, and patient-centric health record management.

4. Admin Dashboard

Admin can register hospitals, doctors, nurse and patients via respective forms. Each action triggers a Web3 transaction to smart contract.



Patient Registration

Enter Patient Account Address: 0x277991C007B639b76213be1908B4Fe4E4a410056

Patient Name: Tinotenda

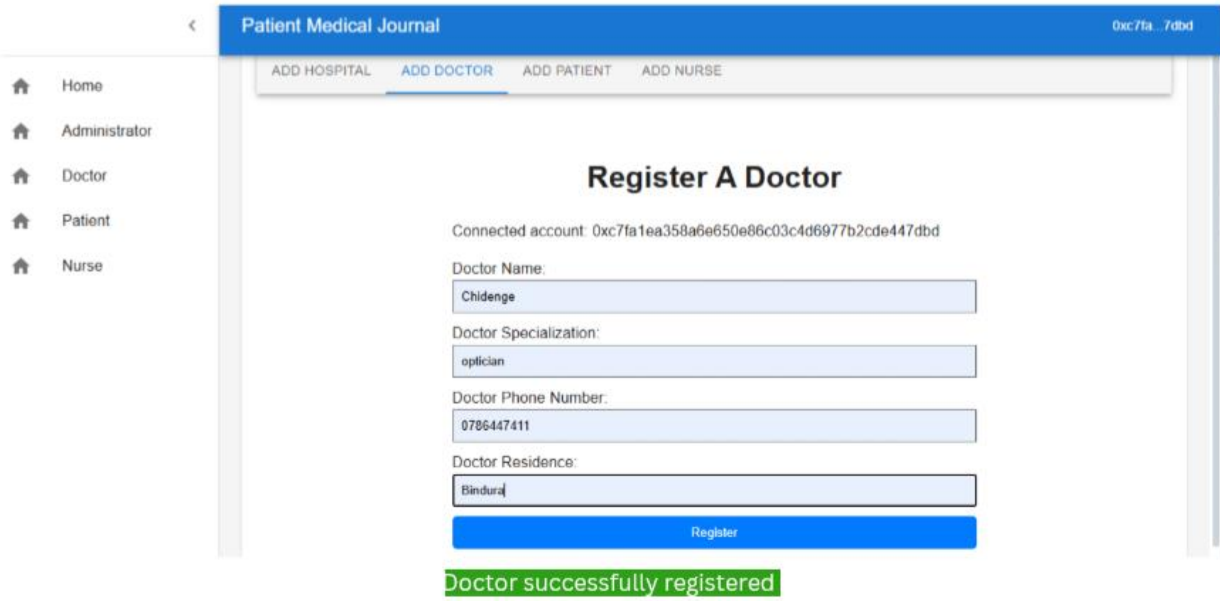
Age: 23

Gender: female

Height (cm): 2

Weight (kg): 57

*Figure 31: Adminr registering patient*



Register A Doctor

Connected account: 0xc7fa1ea358a6e650e86c03c4d6977b2cde447dbd

Doctor Name: Chidenge

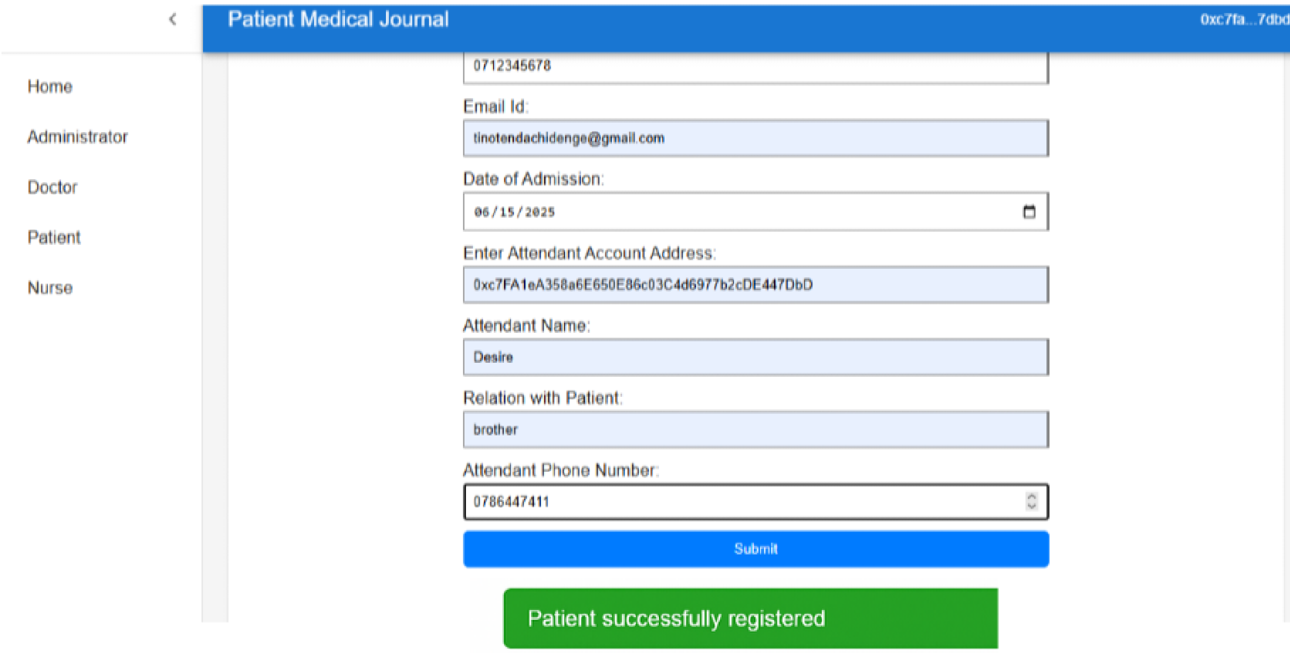
Doctor Specialization: optician

Doctor Phone Number: 0786447411

Doctor Residence: Bindura

Doctor successfully registered

*Figure 32: Doctort Registration*



0712345678

Email Id: tinotendachidenge@gmail.com

Date of Admission: 06/15/2025

Enter Attendant Account Address: 0xc7FA1eA358a6E650E86c03C4d6977b2cDE447DbD

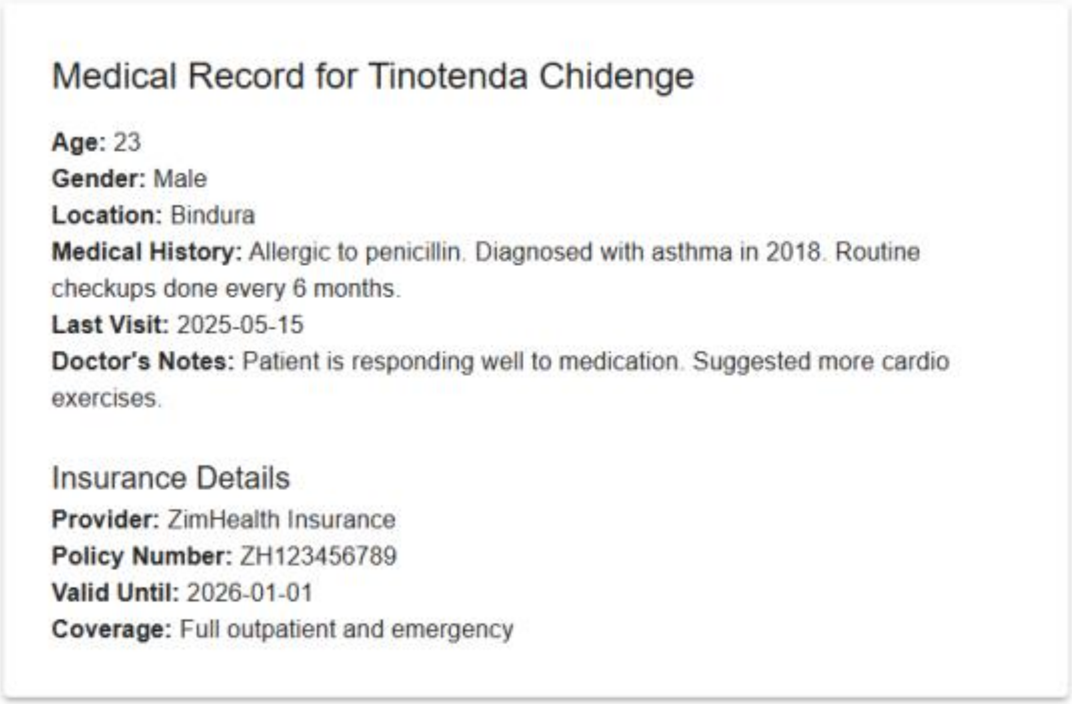
Attendant Name: Desire

Relation with Patient: brother

Attendant Phone Number: 0786447411

Patient successfully registered

5. Doctor and Patient View medical records



Medical Record for Tinotenda Chidenge

**Age:** 23
**Gender:** Male
**Location:** Bindura
**Medical History:** Allergic to penicillin. Diagnosed with asthma in 2018. Routine checkups done every 6 months.
**Last Visit:** 2025-05-15
**Doctor's Notes:** Patient is responding well to medication. Suggested more cardio exercises.

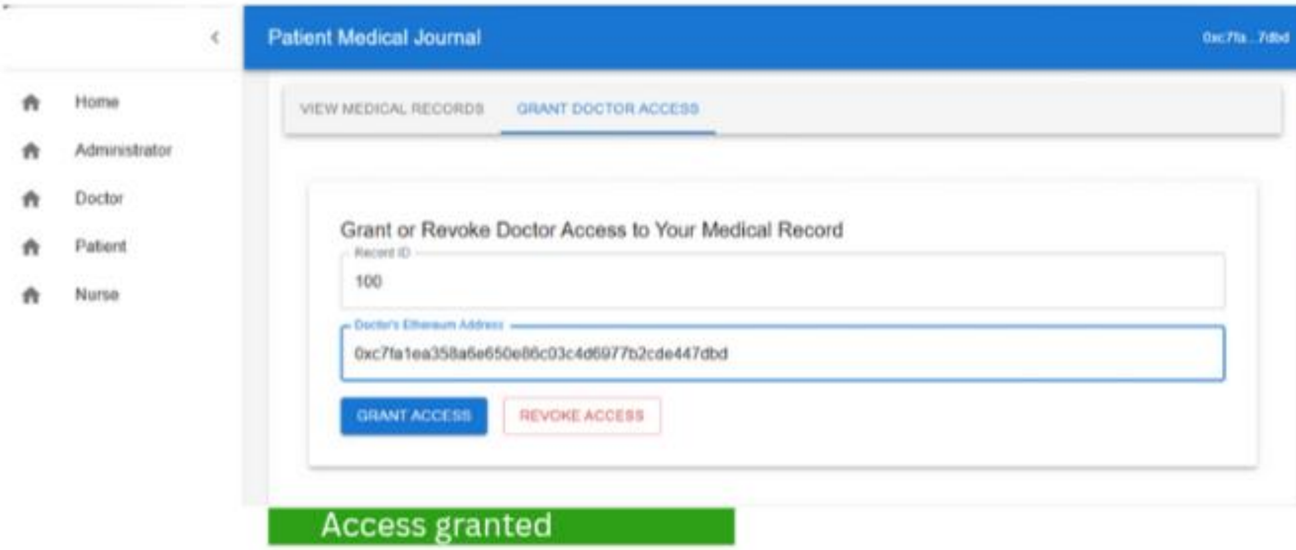
Insurance Details

**Provider:** ZimHealth Insurance
**Policy Number:** ZH123456789
**Valid Until:** 2026-01-01
**Coverage:** Full outpatient and emergency

*Figure 33: View Medical Records*

The patient can view their own medical records and also the Doctor ca view the patient's medical records after being given access by the patient.

6. Patients Grant and Revoke Access to Doctors to view their medical records



Grant or Revoke Doctor Access to Your Medical Record

Record ID: 100

Doctor's Ethereum Address: 0xc7fa1ea358a6e650e86c03c4d6977b2cde447dbd

Access granted

## 4.5 Research Findings

This section critically analyzes the findings presented in this chapter, interpreting their significance in light of studies. It aims to explain how the developed blockchain-based health journal system confirms, contradicts, or extends previous research in health information management. Furthermore, this discussion addresses any unexpected results and acknowledges the inherent limitations of the study, providing a comprehensive interpretation of the research outcomes.

### 4.5.1 Secure and Decentralized Medical Record Sharing

The primary objective of this research was to develop and deploy a blockchain-based journal that enables safe, decentralized, and interoperable sharing of medical records. The findings validate the successful deployment of a decentralized framework to store and exchange medical records in an immutable, open, and transparent format, leveraging immutability, distributed access to data, and storage processes based on encryption. The blockchain architecture inherently eliminates the requirement for centralized databases and hence reduces the risk of data breaches. The findings firmly substantiate the theoretical underpinnings of blockchain technology, which presumes an immutable, distributed digital ledger that securely holds transactions, ensuring immutability and transparency. This follows up on Nakamoto's initial concept of a trustless system (Nakamoto, no date)and Tapscott et al.'s emphasis on data authenticity and integrity(Tapscott *et al.*, 2016). The realization of security and decentralization via immutability, distributed access to data, and encryption-based storages is a paradigm shift in data administration. Decentralization, as Pilkington et al. defines it, removes the single points of failure to which traditional centralized Electronic Health Record (EHR) systems are prone(Pilkington et al., 2016). Immutability, a core tenet of blockchain theory, prevents a record from ever being changed once entered, thereby preserving its integrity. The combination of these two traits directly contributes to the heightened degree of trustworthiness in medical records to ensure that patients and providers can rely on the authenticity and temporal truth of the data, a factor paramount in clinical decision-making and litigation.

The truth that the system reduces dependency upon central databases and lessens the risk of data breaches has far-reaching implications for system stability as well as for patient trust. Traditional centralized architecture is a tempting threat to cyberattacks, and its breach can lead to significant data losses, undermining patient confidence. By dispersing the ledger and protecting information off-chain, the system significantly minimizes the attack surface and eliminates a point of vulnerability. That design choice directly equates to a more resilient and secure system with less potential for catastrophic data loss or unauthorized access. For patients, this increased security inspires them to share their personal health information more confidently, a critical foundation for successful adoption of any digital health solution, particularly in environments like Zimbabwe where data security is a pressing issue. Real-world experience from Azaria et al. (MedRec), Kuo et al., Zhang et al. (FHIRChain), and Wang et al. (MedShare) consistently demonstrates the feasibility and benefits of applying blockchain for secure and decentralized sharing of information(Azaria *et al.*, 2016; Kuo *et al.*, 2017; Zhang *et al.*, 2018; Wang *et al.*, 2021). This study's successful utilization of a decentralized architecture, coupled with off-chain encrypted storage (InterPlanetary File System - IPFS), takes these findings forward by providing an applied model purpose-built to address data fragmentation and security threats prevalent in contexts like Zimbabwe.

### 4.5.2 Patient Autonomy and Control Enhanced by Patient-Centered Design

One of the core objectives of this study was to examine how a blockchain health journal can provide patients greater autonomy over their health records and facilitate informed consent for data sharing. The findings indicate that the system successfully embraced a patient-centric approach, giving users complete autonomy over their health information. Patients are able to view their information, share it with specific providers, and revoke access at any time. High satisfaction with control mechanisms and with usability was demonstrated through user feedback and black-box testing. This consent-based access model ensures medical records are only shared when personally authorized by the patient, promoting informed consent and increased trust.

This outcome directly confirms the postulates of Patient-Centered Care (PCC) Theory, emphasizing the approach to the patient as an active participant, honoring his/her preferences, being open to communication, and making decisions together. Direct application of these theory postulates by the structure of the system, in the sense of providing patients with control over access, is raised by(Makubalo *et al.*, 2020). The success of providing patients with full control over their medical data and permitting them to authorize or deny access to personal providers is a direct application of PCC Theory. PCC supports patients as proactive individuals in their own care, respecting autonomy and collaboration in decision-making. Within classical models, patient information tends to be stored by institutions, which deprives patients of direct control. Utilizing blockchain's decentralized system, this model transfers data custodianship, effectively back to the patient. This is a radical re-alignment with PCC philosophy, demonstrating how technology can facilitate a more moral and patient-facilitated healthcare model directly.

The high levels of satisfaction with control mechanisms and overall usability reported in user feedback suggest that the patients value this greater control. If the patients are assured that their confidential medical information is secure and they are in control of it being shared, they are more likely to be active within the healthcare system and have a role in their treatment decisions. In accordance with Chisi and Nyoni, limited patient access to records has the potential to lead to inferior health outcomes and lower satisfaction (Chisi & Nyoni, 2022). Patient-centered design of this system therefore has the potential to improve not only patient satisfaction but care plan compliance and overall health outcomes by fostering a more active and trusting relationship between patients and providers.

The outcomes of this study are consistent with empirical data from MedRec(Azaria *et al.*, 2016), OmniPHR(Roehrs *et al.*, 2019), ACTION-EHR(Dubovitskaya *et al.*, 2020), PCEHRM(Haddad *et al.*, 2023), and MedShare(Wang *et al.*, 2021), each of which emphasizes the capacity of blockchain to provide control to and enable patients in the possession of their data. This study extends this work by demonstrating user acceptability and real-world applicability of such control systems in a prototype specific to the Zimbabwean healthcare setting.

### 4.5.3. Autonomous Access Management and Consent Control using Smart Contracts

The third research objective entailed integrating smart contracts into the blockchain-based health journal to automate patient consent and access control for medical records. The findings confirm that the smart contracts were effectively tested and deployed as an effective tool to implement access control logic in terms of patient permissions. The contracts implemented rules correctly, including granting access to legitimate users, automatically canceling expired permissions, and denying access to unauthorized users. White-box testing validated the correctness of the smart contract logic, and live simulations validated the reliability of automated access determination. The automation significantly reduced the need for manual monitoring. This outcome illustrates the theoretical potential of smart contracts within blockchain, as outlined in Blockchain Theory, to enable "trustless systems" in which transactions are "secure and verifiable without parties trusting each other". The automation provided by smart contracts is consistent with the assumptions of Data Governance Theory, particularly Information Governance (IG) and Data Stewardship, in guaranteeing compliance and responsibility through rules encoded. Automating access control with smart contracts addresses one of the primary challenges in traditional healthcare data management: the manual, often cumbersome, process of obtaining and managing patient consent. This manual mechanism is prone to human intervention and can engender administrative overhead. With the codification of consent clauses into self-executing smart contracts, the process circumvents such manual mechanisms. This automation brings about a reduction in the amount of effort and cost involved in handling consent, along with a reduction in the risk of errors or inconsistencies in access rights. This improves an optimal and reliable environment for healthcare data exchange.

Smart contract logic's accuracy and dependability, as validated through white-box testing, are important implications for data trust and ethical governance. The Data Trust and Ethics Framework points out such values as consent, transparency, privacy, and responsibility. Smart contracts, through the immutability of all access decisions and the automated enforcement of patient-defined rules, provide a degree of transparency and accountability hitherto unknown, backed by code rather than by human judgment. This programmatic, inherent imposition of ethical data management does directly support the trusted data sharing environment, positioning the system in compliance with main ethical and regulatory requirements (e.g., GDPR, HIPAA1). Studies like MedRec(Azaria *et al.*, 2016), ACTION-EHR(Dubovitskaya *et al.*, 2020), OmniPHR(Roehrs *et al.*, 2019), PCEHRM(Haddad *et al.*, 2023), MedShare(Wang *et al.*, 2021), have all examined the use of smart contracts in consent and access control. This work extends their contribution by providing tangible evidence of the correctness and integrity of the smart contracts through rigorous white-box testing within a proof-of-concept environment, demonstrating their practical application in real-time automated consent management for healthcare.

### 4.5.4 Interoperability in Health Information Exchange

The study aimed to create a blockchain-based journal for enabling interoperable sharing of medical records across different health providers. The findings demonstrate that the solution achieved interoperability by enabling healthcare providers (doctors and hospitals) to retrieve medical records that had been shared by patients across institutions via a common blockchain infrastructure. The findings legitimize the core aim of Health Information Exchange (HIE) Theory to promote secure, seamless, and efficient sharing of medical records between different health providers. The system's approach aligns with the decentralized framework promoted by HIE theory, allowing interaction without needing a central authority. The effective demonstration of interoperability through a common blockchain infrastructure is a significant background trend in health informatics. Historically, interoperability between disparate healthcare systems has been addressed by complex, bespoke point-to-point integrations, which yield fragmented data and narrow interoperability. This blockchain solution presents a paradigm shift: instead of trying to get heterogeneous systems to directly talk to each other, all of them communicate with a single common, shared, and immutable blockchain layer. This provides a shared platform for trading medical records that is designed to offer a trustless coordination space for data exchange, making coordination easier and reducing the inefficiencies of present systems.

While previous efforts have identified interoperability as a substantial challenge to be standardized in works like(Kuo *et al.*, 2017), this work, similarly to Zhang et al.'s FHIRChain(Zhang *et al.*, 2018) and Dubovitskaya et al.'s ACTION-EHR(Dubovitskaya *et al.*, 2020) using HL7 FHIR, demonstrates one feasible method of achieving it by using a common blockchain layer. This study follows on these efforts by illustrating how an integrated blockchain infrastructure can facilitate data sharing, even in a setting like Zimbabwe where disconnected electronic systems and data fragmentation are pronounced. It offers one potential solution to the disjointed referral system by establishing a shared, tamper-proof record.

### 4.5.5 System Usability, User Acceptance, and Reliability

System testing included identifying its proper usability, user acceptance, and reliability through various testing methods. Black-box testing and feedback from users indicated that users were highly satisfied with the control mechanisms and overall ease of use. System testing, comprised of black-box and white-box testing, indicated that the solution was reliable under expected conditions. The interface was found to be user-friendly and accessible by patients, doctors, and administrators.

The user-friendly interface and high satisfaction levels of users overall confirm the principles of the Technology Acceptance Model (TAM), which asserts that perceived usefulness and perceived ease of use are likely to be good predictors of technology adoption. The system's design appears to enhance these factors, reflecting a positive predisposition to adoption on the behalf of intended users. The usability and reliability results are aligned with what most empirical studies' expectations are of feasible, effective blockchain solutions.

However, the 66.7% data integrity match is in direct contradiction of blockchain's very promise of immutability and data integrity. For a system that handles sensitive medical records, 100% data integrity is non-negotiable. The very result here indicates an expected deficiency or flaw in the data handling process, which is most likely a result of the off-chain storage or retrieval because the blockchain only stores hashes. This unexpected result warrants critical attention and a follow-up investigation.

The research findings provide a localized perspective in terms of usability and acceptance, extending from the broader theories (TAM, Diffusion of Innovations (DOI)) to the Zimbabwean situation. However, the existing challenges in Zimbabwe, that is poor ICT infrastructure, lack of skilled personnel, data security and privacy issues, potential resistance to change, and usability issues, identified by, show that while the prototype is encouraging, real-life actual large-scale application will have significant challenges not fully captured by the performance indicators of the prototype. Though the prototype was found to exhibit high levels of satisfaction with the control mechanisms and overall ease of use and to perform reliably under expected conditions, the problems in the Zimbabwean healthcare setting that were revealed that is poor internet connectivity, high costs and resistance to change and lack of skilled personnel will causally influence the actual user acceptance and diffusion rates of the system. Technology Acceptance Model (TAM) and Diffusion of Innovations (DOI) theories stress that facilitating conditions, ease of use, and perceived usefulness are crucial for adoption. If the ICT infrastructure on which it is based is weak, or if there is significant resistance to change, then the perceived ease of use and usefulness of the system in an actual scenario will be low, regardless of whatever its prototype performance. This implies that effective implementation requires not only an effective technical solution but also a significant investment in the creation of infrastructure, training, and change management programs, especially in resource-constrained environments.

### 4.5.6 Study Limitations

The study identifies several constraints and challenges that will influence the interpretation and generalizability of its finding as per the limitations/challenges chapter in chapter 1 and the research gaps in chapter 2.

1. Technical Limitations and Scalability:

   This study also acknowledges that Blockchain is still evolving and there may be technical limitations that affect scalability, security and usability of the proposed system".1 While the prototype performed well in the laboratory environment, whether the system would be able to handle large volumes of data and heavy transaction loads for a national-scale implementation remains a question, as noted by(Kuo *et al.*, 2017; Dubovitskaya *et al.*, 2020) The use of a local test network for Ethereum (Ganache) rather than a public blockchain also limits the scalability and performance metrics observed to real-world, high-volume scenarios to some degree.
2. Interoperability and Standardization Issues:

   While demonstrating interoperability through a common blockchain layer, the research notes that medical records are usually in different formats and systems, which can make it challenging to standardize and transfer data between various health providers. This is in accordance with the general interoperability issue pointed out by HIE theory and empirical evidence. Though HL7 FHIR was adopted, full semantic interoperability with all legacy systems remains an interrelated issue yet to be fully addressed by the prototype.
3. Compatibility with Existing Infrastructure:

   The primary limitation is the potential lack of compatibility with existing healthcare systems and infrastructure which can limit its adoption and effectiveness. This applies particularly in Zimbabwe, where a significant portion of healthcare facilities relies on paper-based systems or disconnected electronic systems, and poor internet connectivity is an issue recorded. Presuming that basic internet connectivity will be available at most healthcare facilities may not be true across all rural areas, influencing the feasibility of the system.

4. Regulatory Compliance Difficulty:

   The study acknowledges that compliance with rules such as GDPR and HIPAA is made more difficult by the immutable and distributed nature of blockchain, requiring specific design choices to reconcile legal requirements. Despite the system aiming for compliance through tracking consent and role-based access control, the full legal implications of immutable records and rights to delete data in a blockchain environment require closer analysis and policy study.
5. Adoption Obstacles and Resistance on the Part of the Users:

   The study automatically identifies adoption obstacles such as entrenched legacy systems, high implementation costs and limited technical expertise among stakeholders. Besides, the possible resistance to change and usability issues identified in the Zimbabwean context by (Chilunjika & Uwizeyimana, 2024) pose major challenges to widespread user acceptability despite the prototype's positive reception on usability under controlled conditions. The presumption that healthcare providers and other stakeholders will be willing to adopt is too optimistic without taking these socio-technical factors into account.
6. Scope of Testing:

   Testing was conducted with deidentified patient data and synthesized to simulate real-world conditions. While for ethical reasons, this limits the ability to completely ascertain the system's performance and robustness with the complexity and volume of real patient data and dynamic clinical processes. The research also did not launch the system on a public blockchain, which would have been more realistic testing of network speed and transactional fees.

### 4.6 Chapter Summary

The research demonstrated that a blockchain based health journal can address key challenges in medical record management, particularly those related to interoperability,patient autonomy , and secure data sharing. By leveraging decentralization and smart contract automation, the system provides a promising approach to improving health information exchange while safeguarding patient rights.

## CHAPTER 5: CONCLUSIONS AND RECOMMENDATIONS

### 5.1 Introduction

This chapter gives a summary of the principal findings, conclusions of the study, and suggestions stemming from the findings of the blockchain-based health journal system. The study aimed at solving significant difficulties in the sharing and management of medical records among multiple health providers through proposing a safe, decentralized, and patient-centered solution based on blockchain technology. The chapter begins by revisiting the research objectives and summarizing how each was completed in the design, implementation, and evaluation stages. It next tabulates the major conclusions derived from the findings discussed in Chapter 4. These conclusions provide insights into the effectiveness, practicality, and impact of using blockchain and smart contracts for health information exchange. Finally, the chapter outlines specific recommendations for further research, system improvement, and possible real-world adoption in healthcare environments. Based on both technology and user-centered evaluations, the chapter combines the research contributions and gives direction to future work in digital health innovation.

## 5.2 Major Conclusions Drawn

### 5.2.1 Blockchain Enables Secure and Decentralized Medical Record Sharing

The study demonstrated that blockchain technology can be effectively used to create a decentralized system that ensure the secure sharing of medical records between different healthcare providers. The immutability, transparency, and distributed nature of blockchain enhanced the integrity and trustworthiness of health data exchange, while minimizing risks associated with centralized systems, such as single points of failure or data manipulation.

### 5.2.2 Patient-Centered Design Enhances Data Ownership and Consent

By integrating user-controlled access mechanisms, the system allowed patients to grant and revoke access to their medical records, thereby promoting greater autonomy and control over personal health information. This design empowered patients to participate more actively in their healthcare decisions and facilitated informed consent, which is a key ethical and legal requirements in modern medical practice.

### 5.2.3. Smart Contracts Provide Automated and Reliable Access Control

The incorporation of smart contracts into the system enabled automated enforcement of consent and access permissions. These smart contracts ensured that only authorized users such as approved doctors or health institutions could access a patient’s records, and only under the conditions specified by the patient. This automation reduced administrative overhead, minimized human error and ensured compliance with user-defined policies in real-time.

### 5.2.4. Interoperability is Achievable Through a Unified Blockchain Layer

The system showcased that different healthcare providers can interact and share data effectively through a common blockchain infrastructure. By standardizing data access through blockchain and APIs, the system achieved a level of interoperability, which is crucial for coordinated care , referrals, and long-term patient record continuity across institutions.

### 5.2.5. Usability and System Reliability Were Confirmed Through Testing

System testing including black-box and white-box testing, revealed that the solution performed reliably under expected conditions. The user interface was found to be intuitive and accessible for patients, doctors, and administrators. The system responded appropriately to different user roles and actions, further confirming its practical viability for deployment in real-world healthcare settings.

## 5.3 Recommendations

Based on the research findings and conclusions drawn from the implementation and evaluation of the blockchain-based health journal, the following recommendations are proposed:

### 5.3.1 Recommendations to Society

Promote Digital Health Literacy

Governments and health advocacy groups should invest in digital health literacy programs to ensure that patients are educated on how to securely manage their own medical data. Empowering patients with knowledge about their rights and the use of digital tools will improve trust and adoption of decentralized health technologies.

Encourage Public Trust in Blockchain for Health

Public awareness campaigns should be launched to demystify blockchain and its role in securing personal health information. Society must understand that decentralized technologies can enhance privacy, not threaten it, when designed ethically and transparently.

### 5.3.2 Recommendations to Healthcare Organizations

Adopt Patient-Centered Data Sharing Models

Healthcare providers should consider implementing blockchain-based systems that prioritize patient consent and control. Such systems reduce data silos, streamline collaboration across institutions and improve the continuity of care.

Integrate Blockchain with Existing Health Information Systems

Organizations should explore hybrid solutions where blockchain acts as a secure access layer, while existing hospital databases remain in use for storage. This ensures a smoother transition and cost-effective adoption of decentralized data sharing models.

Collaborate on Standardization and Interoperability

There is a need for collaboration among healthcare institutions, software vendors, and policymakers to establish interoperability standards that support blockchain integration. Common protocols will facilitate scalable and secure health data exchange.

### 5.4 Suggestions for Further Research Work

Scalability and Performance Studies

Future researchers should investigate how blockchain networks perform under heavy transaction loads and large dataset. Exploring layer -2 solutions or private blockchain configurations may enhance performance and scalability for national-level deployments.

Legal and Ethical Frameworks for Blockchain Health Systems

Further studies are needed to explore how blockchain-based health systems align with existing data protection laws (e.g., GDPR, HIPAA) and to develop clear ethical guidelines for consent, data ownership, and emergency access.

Integration of Artificial Intelligence (AI) and Analytics

Future research could focus on combining blockchain with AI to create intelligent health systems capable of personalized care, predictive analytics, and fraud detection while maintaining data privacy through secure multiparty computation or homomorphic encryption.

User Experience Research

Additional usability studies with larger and more diverse populations are recommended to enhance system design and ensure that blockchain-based health solutions are accessible to patients  of all ages and literacy levels.

### 5.5 Summary

This research set out to design and implement a blockchain- based health journal that enables secure, decentralized, and interoperable sharing of medical records across different healthcare providers. The study successfully achieved its objectives by developing a functional prototype that integrates blockchain technology and smart contracts to ensure patient-centered control, privacy, and automation in medical data sharing. Through the implementation of a decentralized architecture, the system addressed key challenges in traditional electronic health records systems, including data fragmentation, lack of interoperability, and limited patient control. Patients were empowered to manage access to their health data through smart contracts, which enforced consent rules automatically and transparently. The findings demonstrated that blockchain can serve as a reliable foundation for secure health data exchange, with potential to transform how healthcare institutions collaborate and how patients engage with their health information. Additionally, testing confirmed the usability, reliability, and functional correctness of the system, validating its feasibility in real-world healthcare environments. In conclusion, this research contributes both a technological solution and theoretical insights into the application of blockchain in digital health. It laid a foundation for further exploration and adoption of decentralized systems that promote trust, security and patient empowerment in medical record management.

## References

Anon., n.d. s.l.:s.n.

Anon., n.d. s.l.:s.n.

Antonio, B. A. & Nhapi, L. B., 2022. Interoperability and integration of e-health systems with blockchain. *International Journal of Engineering Research & Technology,* 11(2).

Azizi, N., Mousavi, S. H. & Khosravi, A., 2019. *Blockchain technology in healthcare: A systematic review.* s.l.:Medical Systems.

Baguma, R., Mutungi, F. & Janowski, T., 2019. Digital health technologies for anti corruption in Zimbabwe. *International Journal of Education and Research In Learning and Administration Sciences.*

Chen, H., Yu, H. & Wang, F., 2018. Blockchain technology and its applications in healthcare: A systematic review. *Journal of Medical Systems,* 42(9), pp. 1-10.

Chibanda, E., Muponda, M. & Mhloyi, M., 2020. Challenges and opportunities for electronic health records implementation in Zimbabwe: A scoping review. *BMC Health Services Research,* 20(1).

Chigora, P. & Mutisi, T., 2018. Challenges of electronic health record systems in Zimbabwe: A case study of public hospitals. *Journal of Health Informatics in Africa,* 6(1), pp. 1-10.

Chikanda, A. & Matiza, T., 2019. Health informations systems in Zimbabwe: challenges and opportunites. *Health Informatics Journal,* 25(1), pp. 123-134.

Chikanda, A. & Mhlanga, D., n.d. s.l.:s.n.

Chilunjika, A., 2024. Blockchain technology for health information management: A case of Zimbabwe. *Insights into Regional Development,* 6(1), pp. 65-78.

Chilunjika, A. & Uwizeyimana, D. E., 2024. `Blockchain technology for health information management: A case of Zimbabwe. *Insights Into Regional Development,* 6(1), pp. 59-73.

Chisi, J. & Nyoni, T., 2022. Patient engangement in the Zimbabwean healthcare system: Current practices and future directions. *Journal of Health Communication,* 27(3), pp. 245-256.

Chitungo, I., Dzinamarira, T. & Musuka, G., 2021. Public health challenges and responses in Zimbabwe during COVID-19: A critical analysis. *The Pan African Medical Journal,* Volume 38, p. 185.

Daraghmi, Y.-A., Yuan, S.-M. & Yang, M.-M., 2019. Blockchain technology for medical record access and permissions management. *Journal of Medical Systems,* 43(5), pp. 1-12.

Gomba, C., Mudzamiri, R. & Mashizha, T., 2020. The impact of health information systems on healthcare delivery in rural Zimbabwe: A case of Manicaland Province. *International Journal of Health Sciences and Research,* 10(8), pp. 93-101.

Iyer, A., Gupta, A. & Kumar, R., 2021. Blockchain technology in healthcare: A systematic review. *International Journal of Medical Informatics,* Volume 150, p. 104453.

Kuo, T.-T., Kim, H.-E. & Ohno-Machado, L., 2017. Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association,* 24(6), pp. 1211-1220.

Mhere, J. & Mapuranga, R., 2021. The role of digital technologies in Zimbabwean healthcare: Opportunities and challenges for electronic health records. *African Journal of Health Systems,* 3(2), pp. 45-55.

Mhlanga, D. & Chikanda, A., 2020. The impact of fragmented health information systems on patient care in Zimbabwe. *African Journal of Primary Health Care & Family Medicine,* 12(1), pp. 1-6.

Mhlanga, D. & Chikanda, A., 2020. *The impact of fragmented health information systems on patient care in Zimbabwe..* s.l.:African Journal of Primary Health care & Family Medicine.

Moyo, S. & Zinyemba, A., 2022. Assessment of referral system effectiveness in Zimbabwean public health institutions. *African Health Monitor,* 26(1), pp. 21-28.

Munyoro, M., Mavhunga, M. & Nyoni, T., 2021. Cybersecurity challenges in Zimbabwe's healthcare system: A critical analysis. *Journal of Cybersecurity and Privacy,* 1(4), pp. 489-502.

Munyoro, M., Mavhunga, M. & Nyoni, T., 2021. Cybersecurity challenges in Zimbabwe's healthcare system: A critical analysis. *Journal of Cybersecurity and Privacy,* 1(4), pp. 489-502.

Sommerville, I., 2015. *Software engineering. 10th.* s.l.:Addison-Wesley.

Alaa Haddad *et al.* (2023) 'Generic Patient-Centered Blockchain-Based EHR Management System', *Applied Sciences*, 13(3), pp. 1761–1761. Available at: https://doi.org/10.3390/app13031761.

Alan R. Hevner *et al.* (2004) 'Design science in information systems research', *Management Information Systems Quarterly*, 28(1), pp. 75–105. Available at: https://doi.org/10.2307/25148625.

Alevtina Dubovitskaya *et al.* (2020) 'ACTION-EHR: Patient-Centric Blockchain-Based Electronic Health Record Data Management for Cancer Care.', *Journal of Medical Internet Research*, 22(8). Available at: https://doi.org/10.2196/13598.

Alex Roehrs *et al.* (2019) 'OmniPHR : a Blockchain based interoperable architecture for personal health records'.

Asaph Azaria *et al.* (2016) 'MedRec: Using Blockchain for Medical Data Access and Permission Management', *International Conference on Open and Big Data*, pp. 25–30. Available at: https://doi.org/10.1109/obd.2016.11.

Chris Hart *et al.* (1999) 'Doing a literature review'.

Clemens Scott Kruse *et al.* (2018) 'The use of Electronic Health Records to Support Population Health: A Systematic Review of the Literature', *Journal of Medical Systems*, 42(11), pp. 214–214. Available at: https://doi.org/10.1007/s10916-018-1075-6.

David Gefen, Ofir Ben-Assuli, and Yaron Denekamp (2023) 'Adaptive Structuration Theory: A Health Information Exchange (HIE) Diffusion Study', *Information systems management*, pp. 1–18. Available at: https://doi.org/10.1080/10580530.2023.2174278.

David Yermack and Yermack, D. (2017) 'Corporate Governance and Blockchains', *Review of Finance*, 21(1), pp. 7–31. Available at: https://doi.org/10.1093/rof/rfw074.

Dominik Lis *et al.* (2021) 'Towards a Taxonomy of Ecosystem Data Governance', *Hawaii International Conference on System Sciences*, p. 6067. Available at: https://doi.org/10.24251/hicss.2021.733.

Don Tapscott *et al.* (2016) 'Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World'.

Faiza Hashim *et al.* (2021) 'MedShard: Electronic Health Record Sharing Using Blockchain Sharding', *Sustainability*, 13(11), p. 5889. Available at: https://doi.org/10.3390/su13115889.

Farahnaz Sadoughi *et al.* (2019) ‘The used theories for the adoption of electronic health record: a systematic literature review’, *Health technology*, 9(4), pp. 383–400. Available at: https://doi.org/10.1007/s12553-018-0277-8.

Huqa Arbale and African Journal Of Empirical Research (2024) ‘Book Review: “Research Methods for Business Students” (Eighth Edition) by Mark N. K. Saunders, Philip Lewis, and Adrian Thornhill (Pearson Education, 2019)’, *African Quarterly Social Science Review* [Preprint]. Available at: https://doi.org/10.51867/aqssr.1.2.2.

Ibrahim Alhassan *et al.* (2019) ‘Critical Success Factors for Data Governance: A Theory Building Approach’, *Information Systems Management*, 36(2), pp. 98–110. Available at: https://doi.org/10.1080/10580530.2019.1589670.

Kai R. Larsen *et al.* (2025) ‘Validity in Design Science’, *Social Science Research Network* [Preprint]. Available at: https://doi.org/10.2139/ssrn.5176095.

Ken Peffers *et al.* (2007) ‘A Design Science Research Methodology for Information Systems Research’, *Journal of Management Information Systems*, 24(3), pp. 45–77. Available at: https://doi.org/10.2753/mis0742-1222240302.

Luciano Floridi *et al.* (2016) ‘What is data ethics’, *Philosophical Transactions of the Royal Society A*, 374(2083), p. 20160360. Available at: https://doi.org/10.1098/rsta.2016.0360.

M. Snyder *et al.* (2024) ‘Clinicians’ use of Health Information Exchange technologies for medication reconciliation in the U.S. Department of Veterans Affairs: a qualitative analysis’, *BMC Health Services Research* [Preprint]. Available at: https://doi.org/10.1186/s12913-024-11690-w.

Marc Pilkington, Pilkington, M. and Marc, P. (2016) ‘Blockchain Technology: Principles and Applications’. Available at: https://doi.org/10.4337/9781784717766.00019.

Martin Glinz and Glinz, M. (2007) ‘On Non-Functional Requirements’, pp. 21–26. Available at: https://doi.org/10.1109/re.2007.45.

Melanie Swan and Swan, M. (2015) ‘Blockchain: Blueprint for a New Economy’.

Mingyue Wang *et al.* (2021) ‘MedShare: A Privacy-Preserving Medical Data Sharing System by Using Blockchain’, *IEEE Transactions on Services Computing*, pp. 1–1. Available at: https://doi.org/10.1109/tsc.2021.3114719.

Nakamoto, S. (no date) ‘Bitcoin: A Peer-to-Peer Electronic Cash System’.

‘[No title found]’ (no date) *Insights into Regional Development*, 6(1).

P. Chinnasamy *et al.* (2023) ‘Smart Contract-Enabled Secure Sharing of Health Data for a Mobile Cloud-Based E-Health System’, *Applied Sciences*, 13(6), pp. 3970–3970. Available at: https://doi.org/10.3390/app13063970.

P. Delport, Rossouw Von Solms, and Mariana Gerber (2024) ‘Methodological Guidelines for Design Science Research’, *Procedia Computer Science* [Preprint]. Available at: https://doi.org/10.1016/j.procs.2024.05.096.

Panashe Jhamba *et al.* (2024) ‘Blockchain-based Patient Portal for Mental Health Management’, *Proceedings of the International Conference on Industrial Engineering and Operations Management* [Preprint]. Available at: https://doi.org/10.46254/af05.20240251.

Peng Zhang *et al.* (2018) ‘FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data.’, *Computational and structural biotechnology journal*, 16, pp. 267–278. Available at: https://doi.org/10.1016/j.csbj.2018.07.004.

Peng Zhang and zhang, peng (2017) ‘An Empirical Study of Health Information Exchange Success Factors’. Available at: https://doi.org/10.25148/etd.fidc004029.

Ray Hylock *et al.* (2019) ‘A Blockchain Framework for Patient-Centered Health Records and Exchange (HealthChain): Evaluation and Proof-of-Concept Study’, *Journal of Medical Internet Research*, 21(8). Available at: https://doi.org/10.2196/13592.

Rene Abraham, Johannes Schneider, and Jan vom Brocke (2023) ‘A taxonomy of data governance decision domains in data marketplaces’, *Electronic Markets*, 33(1). Available at: https://doi.org/10.1007/s12525-023-00631-w.

Robert F. Smallwood and Smallwood, R.F. (2014) ‘Information Governance: Concepts, Strategies, and Best Practices’. Available at: https://doi.org/10.1002/9781119491422.

Roger S. Pressman *et al.* (2016) ‘Software Engineering: A Practitioner’s Approach, 8/E International Edition’.

Seyma Cihan *et al.* (2025) ‘A systematic review of the blockchain application in healthcare research domain: toward a unified conceptual model’, *Medical and Biological Engineering and Computing* [Preprint]. Available at: https://doi.org/10.1007/s11517-024-03274-x.

Sylvana Kroop (2025) ‘Artifact Validity in Design Science Research (DSR): A Comparative Analysis of Three Influential Frameworks’, *arXiv.org* [Preprint]. Available at: https://doi.org/10.48550/arxiv.2502.11199.

T. Kemp *et al.* (2024) ‘Using socio-technical systems theory to study the health information management workforce in Australian acute hospitals’, *Social Theory &amp; Health* [Preprint]. Available at: https://doi.org/10.1057/s41285-024-00214-5.

Themba Makubalo *et al.* (2020) ‘Blockchain Technology for Empowering Patient-Centred Healthcare: A Pilot Study’, *IFIP International Conference on e-Business, e-Services, and e-Society*, pp. 15–26. Available at: https://doi.org/10.1007/978-3-030-44999-5_2.

Tsung-Ting Kuo *et al.* (2017) ‘Blockchain distributed ledger technologies for biomedical and health care applications’, *Journal of the American Medical Informatics Association*, 24(6), pp. 1211–1220. Available at: https://doi.org/10.1093/jamia/ocx068.

Vijay Khatri *et al.* (2010) ‘Designing data governance’, *Communications of The ACM*, 53(1), pp. 148–152. Available at: https://doi.org/10.1145/1629175.1629210.

Watkinson, F., Dharmayat, K.I. and Mastellos, N. (2021) ‘A mixed-method service evaluation of health information exchange in England: technology acceptance and barriers and facilitators to adoption’, *BMC Health Services Research*, 21(1), p. 737. Available at: https://doi.org/10.1186/s12913-021-06771-z.