Electronic Health Records System Based on Quorum Blockchain

BY

Muzna Khan

(Registration No: MS-SE-20 00000359412)

Supervisor

Dr. Farooque Azam

DEPARTMENT OF COMPUTER & SOFTWARE ENGINEERING,

COLLEGE OF ELECTRICAL & MECHANICAL ENGINEERING,

NATIONAL UNIVERSITY OF SCIENCES AND TECHNOLOGY,

ISLAMABAD

August 20, 2024

Annex A

THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS/MPhil thesis written by NS **Muzna Khan** Registration No. **00000359412**, of College of E&ME has been vetted by undersigned, found complete in all respects as per NUST Statutes/Regulations, is free of plagiarism, errors and mistakes and is accepted as partial fulfillment for award of MS/MPhil degree. It is further certified that necessary amendments as pointed out by GEC members of the scholar have also been incorporated in the thesis.

Signature : ______________________

Name of Supervisor: Dr Farooque Azam

Date: 20-08-2024

Signature of HOD:______________
(Dr Usman Qamar)
Date: 20 - 08 - 2024

Rashid

Signature of Dean:______________
(Brig Dr Nasir Rashid)
Date: 2 0 AUG 2024

Electronic Health Records System Based on Quorum Blockchain

BY

Muzna Khan

(Registration No:00000359412)

A thesis submitted to National University of Science and Technology Islamabad in partial fulfillment of the requirements for the degree of Master of Sciences in Software Engineering

Supervisor:

Dr. Farooque Azam

DEPARTMENT OF COMPUTER & SOFTWARE ENGINEERING,

COLLEGE OF ELECTRICAL & MECHANICAL ENGINEERING,

NATIONAL UNIVERSITY OF SCIENCES AND TECHNOLOGY,

ISLAMABAD

August 20, 2024

Dedicated to my beloved Parents, Sisters, Brothers & Little Yahya for their endless love, support and prayers.

ACKNOWLEDGEMENTS

First, I would like to praise and honor the Almighty Allah, the most beneficent and the most merciful, for granting me the ability, courage, knowledge, and skills required to undertake and accomplish this task successfully. No doubt, He has facilitated my journey, and I am unable to achieve anything without His blessings.

I would also like to appreciate the sincere efforts of my supervisor **Dr. Farooque Azam** for guiding me throughout the journey of my MS thesis. Furthermore, I am also grateful to him for teaching us the courses of Model Driven Software Engineering (MDSE) and Software Development and Architecture (SDA). He professionally taught us both subjects in depth and from that; I developed my interest in continuing my research in the field of model-driven software engineering.

I would also like to express my gratitude to my Guidance Committee Members **Dr. Wasi Haider Butt,** and **Dr. Mehwish Naseer** for providing guidance and assistance to further improve my work with their valuable recommendations. I would like to express my sincere gratitude to **Muhammad Waseem Anwar** for his assistance and cooperation throughout the journey of my thesis in achieving my research objectives. Without his unwavering support, the completion of this dissertation would not have been possible. I appreciate his patience and support throughout the whole thesis.

I am deeply grateful to my beloved parents for raising me and being available whenever I needed them and for their unwavering support throughout every aspect of my life.

ABSTRACT

This study explores the integration of Quorum blockchain, a permissioned blockchain developed by JPMorgan Chase, as an alternative to the critical challenges faced by the healthcare system in electricity. In the changing healthcare environment, technology innovations such as EHR systems are essential to improve patient experience, efficiency, and data management. However, electronic medical records have faced issues related to reliability, validity, data security, and interoperability, which have impacted their adoption and performance. The authors present a robust framework that ensures data integrity, privacy, and patient empowerment by leveraging Quorum’s decentralized, tamper-proof ledger and advanced encryption technology. Quorum’s decentralized architecture eliminates points of failure, increases reliability, and supports integration between different healthcare systems. Quorum's consensus and privacy features solve major problems with availability and security, ensuring secure and high-quality data management. This study shows that the Quorum blockchain can revolutionize the EHR system by providing a secure, interactive, and patient-focused approach to managing medical records, ultimately boosting patient outcomes and efficiency. By integrating this, healthcare organizations can overcome the inherent challenges of EHR systems and pave the way for a new era of clinical excellence through technology. The proposed system leverages Quorum's unique features, like distributed models, proof of concept, and advanced cryptography, to enhance the integrity, confidentiality, and patient-centricity of EHR systems. Addressing key issues such as reliability, usability, data security, interactivity, and patient empowerment, this research aims to transform the storage, validity, and use of health information to improve patient and operational efficiency in healthcare.

Keywords: Quorum Blockchain, Electronic Health Records (EHR), Data Security, Interoperability, Patient Empowerment

TABLE OF CONTENTS

ACKNOWLEDGEMENTS .... **II**

ABSTRACT .... **III**

TABLE OF CONTENTS .... **IV**

TABLE OF FIGURES .... **VI**

LIST OF TABLES .... **VII**

CHAPTER 1 .... **1**

INTRODUCTION **1**

1.1 BACKGROUND STUDY 1
1.1.1 The Promise of EHR Systems: *1*
1.1.2 Challenges Faced by EHR Systems: *2*
1.1.3 Operational and Technical Barriers: *3*
1.1.4 Regulatory and Data Exchange Issues: *3*
1.1.5 The Role of Advanced Data Analytics *4*
1.1.6 Addressing EHR Challenges *4*
1.1.7 Blockchain as Emerging Solution *5*
1.2 PROPOSED METHODOLOGY: 6
1.3 RESEARCH CONTRIBUTION: 7
1.4 THESIS ORGANIZATION: 7

CHAPTER 2 .... **9**

LITERATURE REVIEW **9**

2.1 EXISTING STUDIES 9
2.2 RESEARCH GAP: 12

CHAPTER 3 .... **13**

PROPOSED METHODOLOGY **13**

3.1 QUORUM BLOCKCHAIN TECHNOLOGY, ITS DEPENDENCIES AND PLATFORM OVERVIEW 14
3.1.1 Architecture *15*
3.1.2 Block *17*
3.1.3 CONSENSUS ALGORITHM *19*
3.2 FEATURES OF QUORUM BLOCKCHAIN 21
3.3 CHALLENGES FACED BY QUORUM BLOCKCHAIN 22

CHAPTER 4 .... **29**

IMPLEMENTATION **29**

CHAPTER 5 36

VALIDATION 36

CHAPTER 6 41

DISCUSSION 41

CHAPTER 7 43

CONCLUSION AND FUTURE WORK 43

REFERENCES

TABLE OF FIGURES

Figure 1 Transaction life cycle of a blockchain implementation 5
Figure 2 Flow of research 6
Figure 3 Thesis Organization 8
Figure 4 Forking of Ethereum 14
Figure 5 Architecture of Quorum Blockchain 17
Figure 6 The generic way of how the user-initiated transaction will be created into or will become part of the block creation 18
Figure 7 System Design of proposed framework 26
Figure 8 User Interaction with system 29
Figure 9 System Deployment on local server 36
Figure 10 Execution Time of Functions 37
Figure 11 1000 user 38
Figure 12 2000 user 38

LIST OF TABLES

Table 1Comparison of Quorum Fault Tolerance Methods 20
Table 2 . Comparison of Blockchain-based EHR Systems.. 42

CHAPTER 1

INTRODUCTION

This chapter presents an introduction to the research work. It emphasizes the background study, research technique, problem definition, research contribution, and thesis organization.

1.1 Background study

Technological advancement in the rapid development of healthcare landscape has led to major update that have the potential to provide unprecedented improvements in patient care, effectiveness, efficiency, and information management [1]. Among many innovations, the electronic health record (EHR) has developed as an important tool that revolutionizes the storage, access, and use of medical documents [2]. These systems have transformed the way doctors manage patient records, moving from traditional records to technology-based systems that facilitate data entry quickly and efficiently. Despite of the significant power of EHR systems to improve health and improve clinical outcomes, they face many challenges that impact their efficiency and effectiveness to inhibit adoption [3]. The process of getting the full potential of EHR systems is concerned with challenges such as reliability concerns, usability issues, and poor data security [4].

1.1.1 The Promise of EHR Systems:

Transition from Paper to Digital

Finally, EHR system offers an online archive of a particular patient's records that can be accessed in different health organizations; this knocks off traditional health records information systems [5]. These solutions are suggested for improving decisions made in the context of hospitals, improving the cooperation process between these facilities as well as organising the admistration procedures. Electronic health record enables the practitioner to have a foundation from which they are able to easily and safely record the patient details in order to promote appropriate treatment by the patient.

Benefits of EHR Systems

As they agree with many advantages with EHR (electronic health records), they most of the times do not fulfill the need and expectation due to many challenges and burdens. Naturally, the biggest issue with EHR systems is the consistency. These systems are utilized by physicians to attain real-time the quick access of patients record information. However, the developments occasioned by such trust can be derailed by things like electricity, malware and contradictory information, which hampers and causes unnecessary hardships to people in the societies affected. Lack of reliability of EHR systems is a special issue in the context of healthcare presenting particularly the hospitalized population in need of recovering data. Another area that has emerged as another responsibility is that of data and information alternatives as well as its consistencies in availability to justify why proper EHR systems are important, especially in healthcare facilities.

1.1.2 Challenges Faced by EHR Systems:

Reliability Issues

Electronic health records are seen by physicians and other healthcare givers as the source of up to date, timely and accurate information about patients. Nevertheless, events like explosion, software failures, and data discrepancies can disrupt these systems and result in negative consequences to the health of patients, poor patient management among others [6]. Inability to rely on EHR systems is a concern because time is of essence especially in a busy hospital where every moment is important. Sticking to data continuity and data integrity is a pressure point in facing the data demands of today’s providers and directs the need for EHR solutions on the more critical, reliable solutions.

Usability Concerns

Contrary to longitudinal medical records, EHR systems are the health care providers’ first choice for timely, accurate, and most recent status of the patient. These systems are essential for the right treatment of the patient and the competitiveness of their services. But they pose several issues, including blackouts, software glitches, and data discrepancies that make them not to function as expected. These outages can result in a stop of patient care and management errors [6]. In the health care organizations where time is critical and every second counts, the question of reliability in EHR systems becomes one of the major concerns. The healthcare staff needs these systems to run efficiently to be in a position to offer the best care to the patients. Any fault with the EHR systems is not only a threat to the instant patient care but also triggers a domino effect that ultimately affects all hospital activities.

Data Security Vulnerabilities

Although EHR systems contain risks of fraud and unauthorized access, integrity and confidentiality of data are important in healthcare sector [7]. Unfortunately, the conventional centralized EHR systems are susceptible to cyber threats, exposing the patients’ data. Furthermore, argument related to data ownership and patient consent may result to security and privacy problems in EHR systems [8]. Doctors should review the various legal necessities that should be fulfilled to guarantee conformity with proof and secure patients’ data against compromises.

1.1.3 Operational and Technical Barriers:

Patient Data Fragmentation

One of the common issues that healthcare facilities face in cases with EHRs is the fragmentation of patient records. This problem is worsened to the extent that patients' records are disorganized across various health facilities and health care systems resulting in poor information sharing which may lead to production of wrong or incomplete patient data [9]. Moreover, differences in the data entry method and the format create discrepancies in sharing data that can be used in interaction between systems in treatment and enable the easy passing of information [10]. Due to the absence of the interface between EHR systems, the effective exchange of patient information between the various healthcare workers becomes a challenge. It results to delayed maintenance of systems and passage of wrong information lists and prescriptions back to other parties.

Limited Patient Empowerment

Divine et al assert that another significant issue with inherent EHR systems is their failure to handle patients' records. Since healthcare organizations' control over large-scale organizational structures, patients are limited in their freedom when it comes to their health records, thus becoming less self-directed and losing their rights to freely make certain decisions regarding their thoughts [11]. Moreover, elaborate procedures regarding the access to, and documentation of patient records, influence motivation of patients and of care delivery, as well as improvement within e-SOH systems continually. Sharing decisions with patient self-management is extremely important to have team care where patients and the healthcare providers' goals are to have an excellent result.

1.1.4 Regulatory and Data Exchange Issues:

Regulatory Compliance Challenges

Also, the healthcare industry has many problems and barriers, including regulations and security, especially regarding EHR systems. The EHR systems fail to meet the strict regulatory requirements that are implemented to safeguard patient's privacy and data security health which leads to information disclosure and unauthorized access [12]. The incorporation of the sensitive patient information into EHR framework contribute to the creation of a weak link in that they become prone to cyber-attacks and disasters. Compliance management must be properly maintained and security systems reinforced in order to keep the patient's trust and safeguard their private health information.

Inefficient Data Exchange Practices

Health care providers too experience weak data-interchange since there are no data-interchange processes between EHR systems hence the doctors' ability to share patient information is cumbersome. This is inefficiency not only in terms of time taken to deliver care but also in the probability of error or miscommunication on the side of the patients and the care givers hence the significance of information exchange processes [13]. These difficulties are further magnified by various interchange in essence contradictory information between different medical facilities which take time to process and which involve likely human mistake prospects. Superior accuracy and efficiency of using Medical data exchange can heavily be improved by the constant observations on the process of data exchanged as well as uses of Data exchanged.

Interoperability Issues

Today health care industry is still facing the problem of how to solve interoperability problems of electronic medical records that try to exchange and transfer real data. This paper has identified that the concept of getting to a point of agreement on the patient medical information is constrained by absence of communication standards and inter-system relationship. Therefore, attempts to moderate it are undermined or adversely affect the quality of patient treatment (Wilson & Smith, 2018). Enhancing the quality of the health facilities has a primary focus on the factors that are cross-cutting. Current data sharing paradigms of information exchange enable interoperability and enhances the approaches that healthcare providers use to offer better and efficient patient care.

1.1.5 The Role of Advanced Data Analytics

Traditional EHR systems often require the ability to analyze high-level data, limiting healthcare providers' ability to obtain large amounts of pain information from individuals. The ability for self-monitoring and predictive testing is hampered by the inability to analyze and interpret data immediately, which can impact patient outcomes and monitoring [14]. EHR systems must improve their data evaluation capabilities if they want to enable physicians to use data to understand and optimize patient care strategies. By integrating advanced analytics tools, EHR systems can become a powerful platform to improve clinical decision-making and patient outcomes.

1.1.6 Addressing EHR Challenges

Enhancing Reliability and Usability

Ease of use solutions are essential to ensure the EHR works effectively without hindering clinical work and creating a vicious cycle. Consumers need to be rewired to help practitioners communicate emotionally without being hindered by innovation. Physicians should investigate regulatory requirements to comply with evidence requirements while protecting patient information from criminals.

Strengthening Data Security

The unified stockpiling of delicate patient information in EHR frameworks makes a weak link, making them defenseless to cyberattacks and breaks, featuring the earnestness for upgraded information safety efforts. It is essential to ensure regulatory compliance and robust security protocols for maintaining patient trust and protecting sensitive health information.

Improving Interoperability

Standardized forms of information exchange can allow for the integration to bring about streamlined continuity, thus ensuring care givers in the health care field bring forward comprehensive care. It is worth stating that enhancing the quality and amount of shared health care information ensures better efficacy when using standard and automatic exchange protocols.

1.1.7 Blockchain as Emerging Solution

Dispersed and decentralized Blockchain technology has attracted much attention for improving EHR system security as well as its contents. Blockchain is a peer to peer treasure consisting of blocks in which each transaction is recorded in a block and linked to other block. The given structure makes it possible to record data which cannot be manipulated in any way, including deletion, thus creating a transparent system of all the transactions. The application of cryptographic technologies and consensus algorithms also contributes to the improvement of the data acquired.

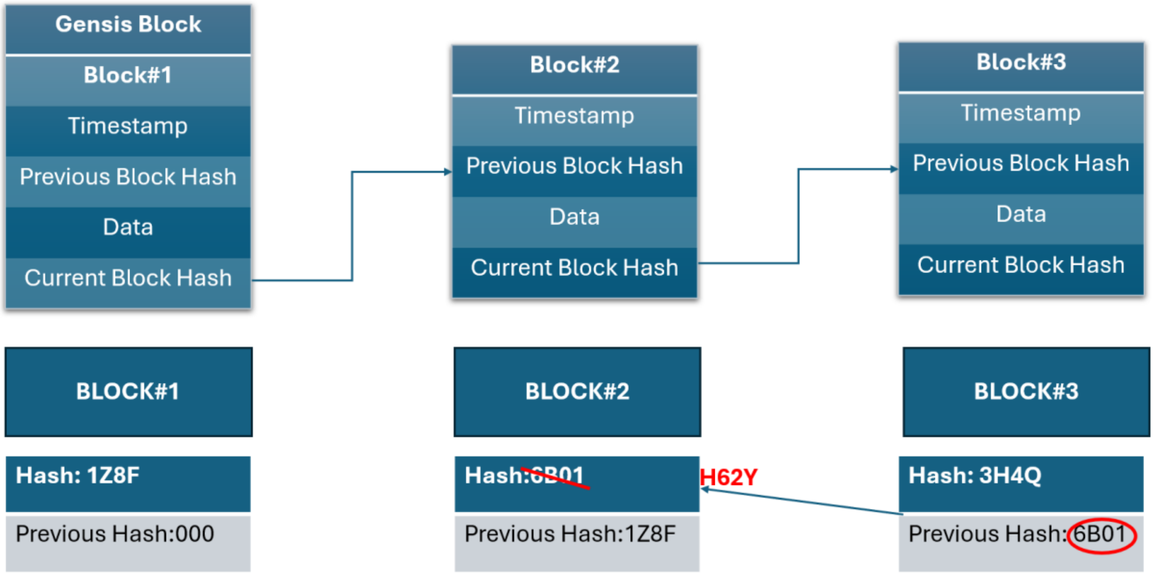


Figure 1 Transaction life cycle of a blockchain implementation

Blockchain for EHR Security and Integrity

Due to such challenges, blockchain technology has been proposed as a solution to enable the enhancement of the integrity and security of EHR systems [15]. Blockchain records a decentralized closed-book which is ready to safely store and manage clinical records while ensuring data integrity and confidentiality [16].Data security is achieved through ciphering techniques and consensus means; blockchain removes weak nodes and has a simple and unalterable record of transactions.

Empowering Patients with Blockchain

In addition, blockchain based EHR frameworks also involve patients into the system with a more prominent control over the health information they provide and the permission they grant and/or deny. This empowerment also increases patient confidence in the health care system and patients' self-ownership.

1.2 Proposed Methodology:

The research methodology of this study comprises of the following main stages. I start with the systematic literature review of similar researches of the integration of Quorum Blockchain with Electronic Health Record (EHR) systems, which offered ways of understanding the research gaps and the current state of the science about integration of the particular blockchain with the chosen EHR systems. Considering the findings of the literature study, we outline the shortcomings and weaknesses of conventional EHR systems, which comprise the following obstacles: reliability concerns, the problem of usability, data protection and security questions, integration problems, and the matter of patient engagement that form the basis of proposing the transformative EHR system. That is why, we suggest the implementation of Quorum Blockchain as a new perspective to reveal these common issues in EHR systems, describing in detail the main components and the process of using the Quorum Blockchain-based framework to improve the data quality, security, and focus on patients. The proposed solution is thus provided with a clear definition of the technical aspects needed, tools and structures that will be utilized together with the accountability of revealing a clear and stable working plan. Last, the efficacy of the proposed solution is supported by reference to several successful use cases and how Quorum Blockchain's implementation can transform EHR systems for the better, as well as increase patient satisfaction and organizational productivity.

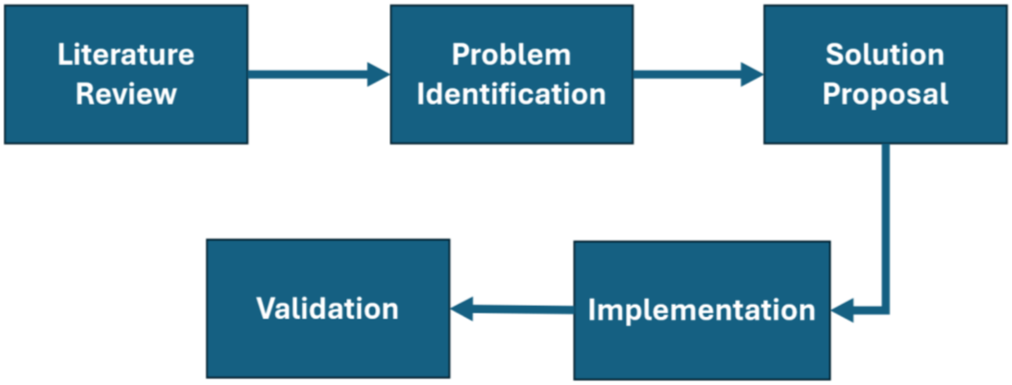


Figure 2 Flow of research

The study will thus employ the following broad research procedure, which is complemented by this literature review: By employing this research approach, the study will seek to offer a sound and novel framework to advance the use of Quorum Blockchain towards reshaping the healthcare system's data management systems and the quality of patients' care.

1.3 Research contribution:

The research contribution of this study is anchored on the envisaged integration of Quorum Blockchain which is a permissioned blockchain by JPMorgan Chase with EHR systems. This integration aims to address the significant challenges faced by traditional EHR systems, including:

- EHR systems are made more dependable by Quorum Blockchain Company because the architecture of this system does not have single points of failure.
- Due to the platform's simplicity and high level of cryptography; and can efficiently use EHR systems while offering healthcare services.
- Others, the Quorum Blockchain comes with a secure and immutably sealed data storage solution as well as utilizes sophisticated cryptography that shields patients' data form the deleterious effect of any unauthorized data breach.
- Quorum Blockchain system developed has a decentralized framework that allows the integration of various health care systems, in order to share the patient records with other systems.
- Through integration, the choice shifts more to patient's side where they have an authority to control the data by assigning permissions to whom and when, hence enhancing data control and data protection.

The study asserts that through the application of Quorum Blockchain , health systems get to implement a strong framework that guarantees the security of data and patients' rights, therefore promoting better patient experiences and highlighting high organizational performance in the healthcare sector. This concept also targets size, strength, and interaction issues, which are essential prerequisites for determining a superior quality, technologically advanced health care system.

1.4 Thesis Organization:

The dynamic field of health care has identified the inflection point that involves the application of technological advancements like EHR systems in improving the patient care delivery, system functionality, and information management. But EHR systems have several drawbacks concerning reliability, usability, security of the information, and the possibility of an exchange of data between systems that hamper extensive implementation and efficiency. This paper seeks to evaluate the use of Quorum Blockchain, a permissioned blockchain adopted by JPMorgan Chase, as a disruptive solution to these problems. Accordingly, engaging Quorum's decentralized, impenetrable blockchain and sophisticated cryptographic methodologies, the authors described an optimal framework for encryption, anonymisation and patient control. Chapter 1 gives the background of the research where the authors discuss the changes in the healthcare systems and the role of technologies. In the course of the literature review conducted in Chapter 2, the author presents a wide range of sources with focus to the integration of Quorum Blockchain with EHR systems, briefly elaborating on the identified gaps in the existing research with an overall aim of creating a strong background for the understanding of the current state of the research in the given field. Chapter 3 is the research methodology section that lists out the phases of the research, identifies the issues with the traditional EHR systems, and explains the proposed Quorum Blockchain-based solution. Chapter 4 is dedicated to the essential components of implementation at the technical level, tools, and the necessary framework for transparent and stable work. Chapter 5 describes case studies that prove the applicability of the proposed framework to extend Quorum Blockchain for EHR systems, where the integration may augment patients' lives and enhance operational effectiveness. As indicated in chapter one, chapter 6 of the study brings out the discussion and limitations met in the course of the study in detail. Last but not the least, Chapter 7 encompasses general conclusions derived from the augmentations to the thesis and recommendations for future research in the context.

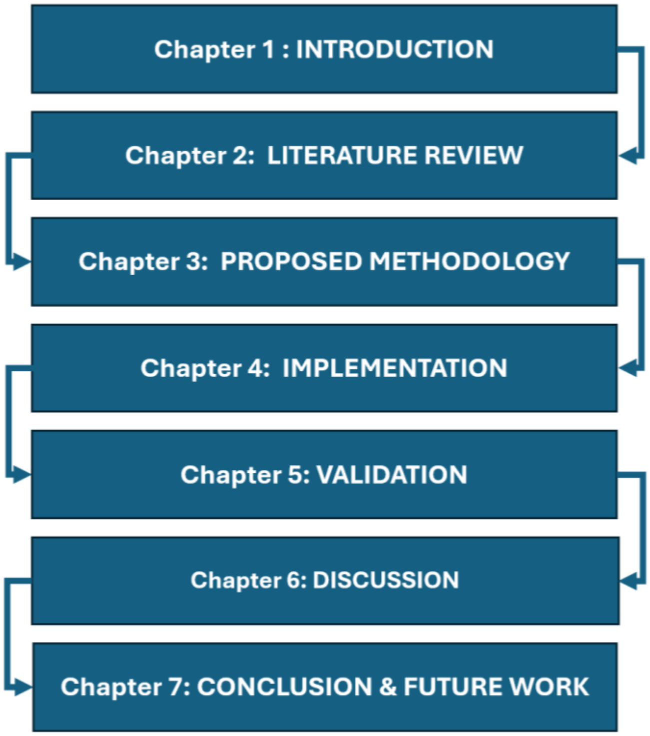

Chapter 1 : INTRODUCTION
Chapter 2: LITERATURE REVIEW
Chapter 3: PROPOSED METHODOLOGY
Chapter 4: IMPLEMENTATION
Chapter 5: VALIDATION
Chapter 6: DISCUSSION
Chapter 7: CONCLUSION & FUTURE WORK

Figure 3 Thesis Organization

CHAPTER 2

LITERATURE REVIEW

Chapter 2 of this research therefore consists of a major literature review and comprises of the following sections: In the first part, the authors present the state of the research concerning the implementation of Quorum Blockchain into EHR systems and elaborate on the critical issues the systems encountered: their reliability, usability, safety, and integration capabilities. This section also looks at the development of EHR systems and the main challenges experienced in the advancement of effective EHR systems. In the following sections, the results of various researches are discussed which includes the user acceptability of blockchain for EHR exchange, smart healthcare systems on blockchain, a hybrid blockchain-edge architecture for EHRs, and frameworks for interoperable EHRs. The literature review also discuss on the Large scale EHR management using two-channel Blockchain, Personalized Health Record System using Blockchain, Secure EHR exchange using Cryptographic Techniques and Healthcare Record Management System using Blockchain. Lastly, this chapter closes with a gap analysis, which in turn signifies that there is scope for implementing the proposed system, the need to optimise the proposed scalability at increasingly high utilisation rates, as well as integrating blockchain technology to materialise existing infrastructures of the healthcare domain. In this regard, the research sheds light to the following objectives in order to foster research advancement on integrating information management systems that would address the current challenges of interoperable and robust EHR systems in the current modern healthcare settings.

2.1 Existing Studies

Blockchain technology has proved oil as a plausible solution for improving security, compatibility justifiably and acceptability of the Electronic Health Record EHR systems in the healthcare industry. There are numerous publications that dissects on the possibilities and issues that are related to the integration of blockchain in managing health records. This literature review offer basic analysis of the findings and conclusion made from different published articles and conference proceeding that focuses on the blockchain based EHR systems.

Jaiman et al. (2023) [17] used the UTAUT to assess the user acceptability of blockchain technology with regard to the exchange of EHR. The research conducted by these authors pointed out several factors that can affect the extent to which blockchain solutions are adopted in the sphere of healthcare. Finally, performance expectancy, which can be defined as the subject’s attitude toward the idea that the use of blockchain will improve job performance, has been identified as a positive determinant. Another important factor was social influence, which corresponds to the extent to which individuals' peers and influential sources approve of blockchain usage. Another factor that has influenced acceptability of the service was perceived trust especially with reference to the security of the data that the user provides. For their part, the/find. / with regard to effort expectancy, which concerns the perceived simplicity of having faith in the chosen technology, in this case, Blockchain, and the facilitating conditions, which include the organisational and technical support systems for the implementation of Blockchain, did not also affect user acceptance. Thus, the results further imply that although users are confident in potential advantages of blockchain and its reliability, there may be factors such as usability and adequate backing they may face that have to be resolved to complement adoption.

Several papers have shown the benefits of applying Blockchain technology for improving the performance of EHR systems by using public and private chains, contracts, and access rights. These advancement have brought significant changes in handling, storing, and sharing of patients' heath information. For instance, due to the nature of blockchain's distributed ledger, one is well assured that medical records data cannot be changed without record of the change being produced, hence creating a secure audit trail. All the access control policies and procedures are automatically managed and enforced by the smart contracts, meaning that only authorized personnel will be allowed to access patients' data. Apart from this, it improves security and also alleviates some of the bureaucratic work that can be distressing to the healthcare providers. Moreover, the combination of the public and private ledgers also implies that the data access can be integrated freely, and some information can be stored secretly while achieving the functionality of the unreliable blockchain database.

Guo et al. (2023) [18] presented a solution of a dual blockchain-edge system combined with attribute-based cryptographic techniques for EHR sharing. Thus, this novel solution exploits the best of both worlds; in terms of security, it is a distributed blockchain network while the computational power is concentrated in edge-computing regions. In this architecture, blockchains nodes are placed closer to the edges of the network, closer to where data originates and where it is consumed, therefore have less latency. It is a type of encryption that allows access to data by only users with the required attributes, be it roles or permissions, thus supporting attribute-based access control. This approach will address some of the major issues of security and privacy in EHR systems because patients' information will be anonymous and access to data will be prohibited to unauthorized people and at the same time the solution will have acceptable response time for real-time applications in healthcare.

In Gulzar et al. (2023), [19] the authors proposed a blockchain framework for address decentralised and secure EHR sharing with effective user control. Current problems that revolve around the exchange and storage of health information are incorporated in the development of the framework using blockchain. It is important for the participants to share a version of the truth in order to inter-operate on this system and this is achieved by the use of a decentralized ledger. The framework also includes smart contracts that help enforce the rules of sharing data, as well as the rights and permissions relating to the patient's information. Theoretical and analytical assessment of the proposed framework shows that it is capable of breaking the existing barriers in terms of EHR interoperability including the issues of data silos and incompatible data structures hence leading to better healthcare delivery.

Diaz et al. (2023) [20] outlined a more general system of EHR management through a block chain using Hyperledger Fabric, a permissioned block chain. The issue of security, privacy and patients' information was highlighted as critical in the management of electronic health records according to the study. The design of layers in Hyperledger Fabric means that transaction processing can be split by different channels each with distinct participants with different read/write access. This dual-channel strategy also strengthens the extensibility sensitivity because it allows for the simultaneous processing of transactions and minimizes the burden on the primary blockchain network. It also has the benefit of flexibility as it concerns the issue of access and sharing and also it was also designed in a way that different authorised personnel in the healthcare institutions are able to share data without have direct access to each other's data. Due to the presented focus on such issues as scalability, more people will become aware of the fact that blockchain can be applied to the problem of large-scale EHR with equal efficiency as in small ones, without the question of the performance.

Kim, Cho, and Hong (2022) [21] proposed blockchain-based Personal Health Record (PHR) system, which deals with patient-controlled consent, the granularity of control, security, and privacy. This system combines blockchain application with advanced models in access control to improve the interaction and protect patient's information in healthcare. In this case, through enabling patients to exert full control over their information, the system guarantees that the affected individuals can dictate those ones, through whom their health record can be accessed and for what reasons. This not only emancipates the patients but also increases compliance with the data protection laws. From a security perspective the program implements complex encryption and access control procedures so that sensitive health related data is not accessed by unauthorized personnel this feature more so integrates the use of blockchain for the records of data access and changes are immutable.

Barman et al. (2022) [22] have suggested to solve the problem of effective EHR security using blockchain with the help of protected Elliptic Curve Cryptography (ECC) and fuzzy commitment schemes. In this case, it will facilitate the factors of scalability, integrity, confidentiality, and decentralization of healthcare data. ECC used to provide a good security level with comparably small key sizes and therefore can be effectively used in the zones with limited resources available. The fuzzy commitment scheme increases the data authenticity as the data items are linked with the cryptographic commitments that allow detection of changes. The paper confirmed the integrity of the EHR data through management via blockchain utilizing the Random Oracle model had the capability to neutralize the various forms of attack, but also necessary and feasible scalability to be implemented at large.

More recent work is a study by Marak et al. (2022) [23] where they presented an approach to the reliable storage and management of EHR through the use of blockchain technology. The system aims at solving the trade-off between security and privacy in the transaction of healthcare data through the implementation of a blockchain. In the system, there is permissioned blockchain that only allow specific people to be in the network and have access to the patient data. This improves privacy while achieving the advantages of a blockchain system being transparent and auditable. It also involves the use of other state-of-art cryptographic methods to enhance secure data transmission, so that patients' details cannot be accessed or modified by unauthorized individuals.

2.2 Research Gap:

In the literature review it is pointed out that there is an urgent demand to resolve the issues of EHR systems reliability, usability, security and data sharing along with patient engagement. Though there is various literature available on the enhancement of EHR systems, implementing a revolutionary strategy, here Quorum Blockchain is unexplored. This research therefore seeks to address this gap by profering a strong architectural framework that utilizes all the characteristics of Quorum Blockchain to address the issues of EHR system integrity, confidentiality and patient-centeredness with the view of increasing the quality of patient care and productivity of the healthcare industry.

The primary research question, therefore, resides in investigating the feasibility of using Quorum Blockchain as a permissioned Blockchain developed by JPMorgan Chase, as a solution to the challenges that affect conventional EHR systems. However, despite their possibilities, EHR systems have not reached the desired level of reliability, usability, data protection, compatibility, and patient engagement due to multiple limitations and inadequacies of conventional technologies mainly based on a centralized approach and prone to vulnerabilities and hacks. Therefore, this study will help to address this problem by introducing a framework that can effectively overcome the limitations of EHR systems based on the Quorum Blockchain platform, which ensure decentralized, immutable, system

CHAPTER 3

PROPOSED METHODOLOGY

The methodology foreviewed in this paper employs the Quorum Blockchain technology in enhancing EHR system's shortcomings such as data security and interoperability for patient's benefit. Here are the key components:Here are the key components:

Quorum Blockchain Integration: Applying Quorum's distributed ledger and cryptographic methodologies to improve EHR systems' trustworthiness and protection.

Decentralized Architecture: To reduce vulnerability of focusing on a single product or system, and to improve compatibility of the systems in healthcare facilities.

Consensus Mechanisms: Using the consensus algorithms from the Quorum platform to guarantee the organization safe and effective approaches in data management.

Patient Empowerment: This involved creating a guide that can be followed to enable the patient to manage his/her health information.

Performance Evaluation: Testing on the extent of time taken to execute each part of the framework, and how well it performs with different loads for scalability.

The methodology is expected to transform EHR systems into the improved systems by securing and making them interoperable in order to put the patient at the centre of health data.

However, getting ahead of solution it is important to mention that Quorum Blockchain and its platform.

3.1 QUORUM BLOCKCHAIN TECHNOLOGY, ITS DEPENDENCIES AND PLATFORM OVERVIEW

Quorum is permissioned blockchain platform that is actually built on top of Ethereum by JPMorgan Chase. It is forked from the Ethereum project. It is developed to suit applications in, for example, enterprises, which need to quickly and without compromising the speed of the process, achieve one or more private transactions among a certain number of known parties. The platform enlists features that serve the purpose of FIs and other industries where privacy and security are valued in blockchain activities. Quorum provides confidence to existing tools and frameworks that are built on the Ethereum infrastructure whilst providing the security and privacy that the business world demands more of.

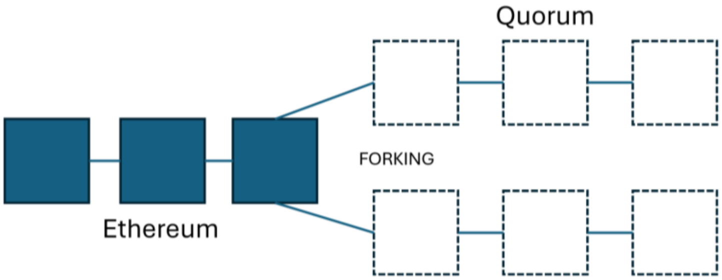


Figure 4 Forking of Ethereum

One of the most important features of Quorum is the use of a consensus mechanism, which is based on the majority vote and occupies a rather important position in ensuring the quality and reliability of the work. It allows for the fast execution of transactions and provides the certainty of the transaction completed and, as such, is optimal for the enterprise-level application. Quorum has also a consensus process that optimizes how participants of a network reach agreement on transactions, so they are sealed and recorded without affecting the security of the network.

Quorum has features which make it suitable for confidential transactions especially within a select network. This is made possible through the use of private smart data and smart deals where the information is only arrives to pre-defined parties or persons. Furthermore, Quorum offers effective security solutions; it is possible to encrypt both the network and data, as well as set up restrictions on the transactions that may be performed by users with various levels of access privileges. Such measures of security are useful in the protection of vital data and the compliance to rules in business. Quorum also provides a mechanism for fine grained access control and data encryption thus allowing any organization protect its data in the event of a breach.

The Quorum technology is efficient and secure when it comes to the performance of the enterprise applications that undertake many transactions with high levels of privacy. Its peculiarities make it truly beneficial to such segments as finance, healthcare, and supply chain management services. Due to the option of privacy and security and the capacity to manage transaction volumes, it is a good choice for enterprises that want to deploy blockchain in their operations.

Public and Private Contracts

Quorum employs basic Solidity for writing smart contracts as with Ethereum, for instance. When contracts are stated in lingo, they can be public which means that the contract will be visible and can be executed by any participants in a Quorum network or private where access to the contract is limited only to the network participants. For the creation of a public contract, a normal Ethereum style transaction is initiated into the network of Ethereum. In fact, for private contracts there is the Quorum-specific parameter privateFor which is specified in the transaction to define the list of participants that will have the ability to view the result of the contract and execute it. Private contracts can neither change the provisions of public contracts to mirror each participant's state across other participants. This double strategy lets the businesses adjust their contracts' implementations according to the degree of secrecy.

Contract Design Considerations

There also exists an interaction between a public contract and the privatization of the contract where once the contract has been made public it cannot be made privatized. By necessity, a public contract may have to be removed from the blockchain list, with the formation of a new private contract. Based on the points discussed above, Quorum's flexibility enables the customization of smart contracts and privacy and security of businesses. This flexibility is specifically advantageous to empowering such organization that may need to handle both a public and private ledger so as to maintain the privacy of the data and running block chain at the same time.

3.1.1 Architecture

Quorum is Ethereum's version used for business with high throughput and strengthened security for deal secrecy among the members of a specific list. Quorum Blockchain has been incorporated to suit the enterprises needs in terms of design, security, privacy, and scalability among others. The architecture process flow for Quorum Blockchain can be summarized as follows:The architecture process flow for Quorum Blockchain can be summarized as follows:

Transaction Initiation:Quorum Blockchain network –A new transaction starts when one of the users starts a new transaction. This user can be a physician, a hospital, a bank and any enterprise organization who wants to implement a secure transaction on this block chain. The transaction can be of any sort, including account transfers, record alteration or even the execution of a smart contract.

Private Transaction Manager: Quorum executes private transactions through a Private Transaction Manager securely. The Private Transaction Manager encrypts all the private info concerning the transaction and passes it to only a few other parties. This means that only the intended cass is able to access such information rather than all the people using the App. The Private Transaction Manager also lays down the record of the participants in the particular transaction to ensure safe communication.

Consensus Mechanism: Quorum implements consensus mechanism known as QuorumChain which is based on the majority vote. In the network, nodes have the privilege of making a consensus on the validity of the transactions to be carried out. This consensus mechanism helps in creating agreement amongst the nodes of the network maintaining the fairness of the blockchain network where no single entity can overpower the network. The majority voting approach also improves validity of transaction identification increasing its speed and effectiveness, which is beneficial in enterprise applications.

Privacy Features: It also provides an aspect of security and privacy including Private Smart Contracts and Private Transactions. Smart contracts for private transactions aim at performing specific transactions which can be not revealed to other parties. This feature is especially relevant for organizations and companies in the sphere of healthcare and, to some extent, finance since data confidentiality remains one of the most significant concerns. Private transactions also take the privacy of the transaction to another level since the details of the transaction will only be between the involved parties alone.

Permissioned Network: Quorum is for permissioned network where users involved in the network are identified and are of known identity. This permissioned approach also grants better security and manageability over the network since only those with the correct accreditation can register to and partake in the blockchain. That is why, the opportunity to invite only specific users to join Quorum also helps with met regulatory requirements since all participants are admitted either as representatives of certain organizations, or those who passed ID verification and meet certain requirements in terms of expertise and formal education.

Block Formation: The confirmed and authorized transactions are compressed and organized into small files known as block and are sent to all the nodes in the network. The various transactions and some additional information like the block number, the time stamp, and the hash of the previous block is stored in each block. This metadata is used for maintaining the chain unbroken and integrated. Every node holds his/her copy of the blockchain, and this makes the validation and consensus to be independent and decentralized.

Block Validation: In the network, the nodes employ known algorithms to confirm the legitimacy of blocks which have been formed by the transactions. In this process, it is checked and ensured that every transaction included in the block is accurate and properly organized. Once the inputs and outputs are verified, the block containing the details of the transactions is incorporated into the blockchain, thus making a record of the transactions which cannot be altered. Since only known algorithms can be used, the activities of validation can be easily checked by all parties.

Mining and Incentives: What we call mining is used for block validation in Quorum. The nodes that properly confirm the blocks are paid in the cryptocurrency to encourage individuals and organizations to be part of the process. This reward mechanism makes the nodes to be proactive in the validation process thus maintaining sound blockchain. Mining is also essential in preserving the decentralization of the network since this process is scattered across different nodes.

Transaction Finalization: After the validation then the transaction is successfully accomplished and the new blockchain is replicated throughout the network. This is a very important procedure, as it helps guarantee of all nodes have a current and agreeable copy of the blockchain for record-keeping. They are then added on the blockchains in a way that is permanent and very difficult to alter.

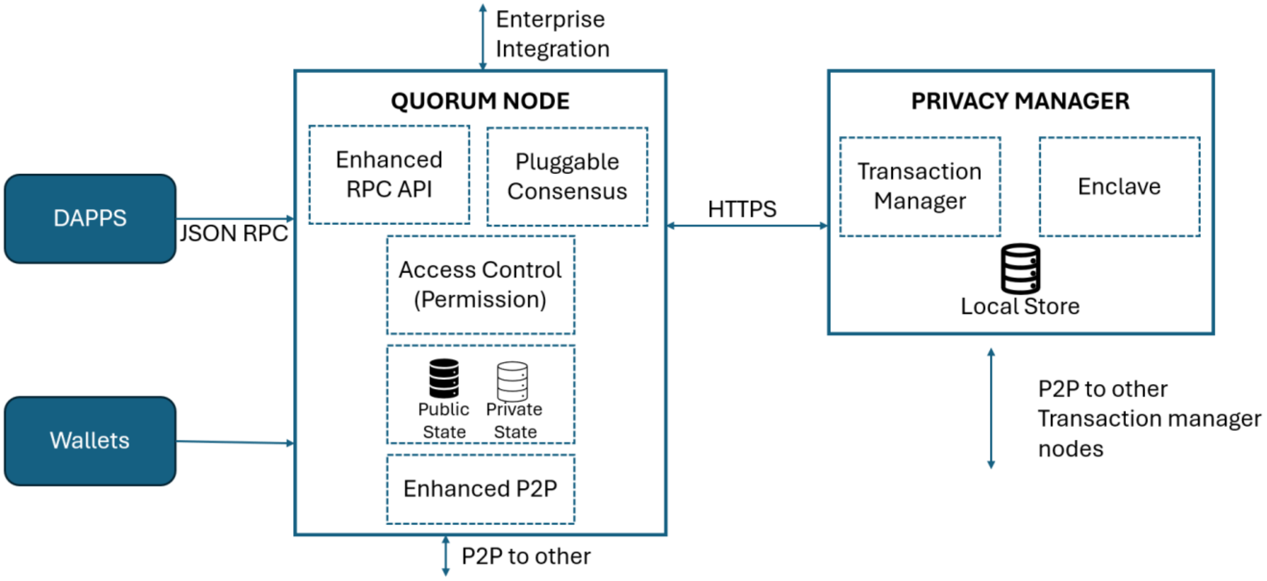


Figure 5 Architecture of Quorum Blockchain

The architecture of Quorum Blockchain is very much planned to provide solutions to the enterprise-scale problems in executing the transactions safely, effectively and with the scalability that is required. It is possible to state that all the mentioned factors – private transaction management, reliable consensus algorithms, and permissioned networks – allow for achieving a high level of working and maintaining confidentiality for Quorum users.

3.1.2 Block

The understanding of the Quorum block as one of the basic elements of the blockchain network and its significance is based on the analysis of the Quorum's anatomy. At the most basic level, a Quorum block is defined as a set of transactions that represent different operations performed on the blockchain including but not limited to, transfer of assets, execution of smart contracts, or update to data [1]. Another major component of a Quorum block is that the Meta data, which includes the block number, created timestamp, and the hash of the previous block are positioned at the block's header in order to maintain the chain records' integrity and continuity [2]. Also, the state root hash refers to the hash of the state of the blockchain after executing all the transactions in the block while the transaction root hash is the Merkle Tree hash of all the transactions to enhance on data security [3]. The consensus details included in the header include information concerning the consensus mechanism used, which will either be Raft or Istanbul BFT, instrumental in reaching consensus among validators as to the validity of transactions or the sequence of blocks [4].

As for the content of a Quorum block, the latter comprises actual transactions of grouped blocks, as well as private transactions which may be available only to certain participants ensuring that the flow of information in the network is kept discrete [5]. Such operations may include the move of simple assets, the performance of smart contracts and many others showing the versatility of Quorum Blockchain. Every operation performed during the forming of the block is saved and protected from forgery so that its integrity can be vouched for.

Contemplated activities included in the block sealing are mining or sealing where authorized nodes known as validators authenticate transaction, create new blocks, and append them to the blockchain [6]. At this step, validators vie for solving cryptographic problems that are computationally intensive hence preventing the addition of invalid transactions into the blockchain. The other processes such as Istanbul BFT or Raft help to achieve a consensus among the validators and also add to the protection of the network [7]. These consensus mechanisms must be designed to be fault-tolerant, which means the network must be able to operate as normally as possible despite having a problem with either a malicious group or a piece of hardware.

Transaction propagation occurs through the network from which validators pick potentials blocks and validate them in their nodes in the network, through the process of block and transaction validation, got to consensus level achieved by a successful validator with an assured sealing of the block for immutability of transactions [8]. In thiscase once a block is sealed it goes round the entire network so that any participant in the network has r the current block chain. It is necessary to say that the used distributed ledger approach is aimed at providing the necessary level of transparency and trust between the participants of the network.

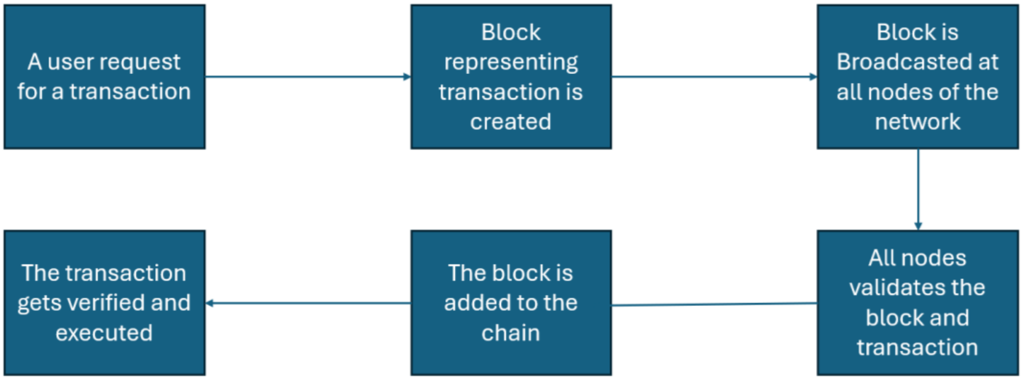

A user request for a transaction
Block representing transaction is created
Block is Broadcasted at all nodes of the network
All nodes validates the block and transaction
The block is added to the chain
The transaction gets verified and executed

Figure 6 The generic way of how the user-initiated transaction will be created into or will become part of the block creation

It is almost impossible to overstate the importance of blocks within the concept of Quorum network. Their non-alterability helps to preserve data’s purity and the order of these blocks builds a stable transaction flow list [24]. Each block forms a secure and a verified record of the transactions that there were within a given period in time and as such the activities in the system are easy to audit. Also, the consensus mechanism helps to ensure that only valid transactions get included into the blocks; thus, the security of the system is improved [25]. This validation process is quite thorough ensuring the efficacy of blockchain in minimizing fraudulent activities within the network.

Quorum has a highly distinct architecture that focuses solely on the needs of enterprises and their need for privacy, scalability, and performance [26]. Each block is tasked with the responsibility of increasing the robustness and reliability of the whole network with a view of being able to meet the needs of enterprise level applications. Thus, Quorum Blockchain’s mechanism of keeping secure transactions records ensures that the enterprise operations are carried out efficiently and safely.

3.1.3 CONSENSUS ALGORITHM

Quorum which is a blockchain platform specific for enterprise use employs various consensus algorithms to achieve consensus across the participants of the network. Of these consensus mechanisms it is intended to guarantee the reliability, safety and effectiveness of the transactions within the Quorum network. Let us delve into the examination of these consensus protocols. Let us delve into the examination of these consensus protocols:

1. Quorum-Chain (Voting-Based Consensus)

Quorum uses an algorithm of voting in arriving at a consensus. Within this framework, nodes which are selected as ‘‘validators’’ participate to perform voting to determine the authenticity and order of a transaction. This is a voting-based consensus mechanism and one of its aims is to be efficient and scalable so as to be able to validate especially the transaction. Only the authorized validators are permitted to vote, which makes it easier to validate transactions all over the system. This increases the level of security, reliability and sustainability of the blockchain by allowing only verified participants to be involved in the consensus.

2. Alternative Consensus Mechanisms

Quorum presents multiple consensus mechanisms that are apt for consortium chains, providing flexibility and adaptability to different enterprise needs:Quorum presents multiple consensus mechanisms that are apt for consortium chains, providing flexibility and adaptability to different enterprise needs:

QBFT (Quorum Byzantine Fault Tolerance): QBFT is a enhanced version of IBFT (Istanbul BFT) which assures a community with Hyperledger Besu. This consensus mechanism aims at reaching the end quickly within a very short time and also protecting the network against Byzantine failures. QBFT provides the much needed improvements to the Quorum network reliability and effectiveness to make it suitable for enterprise applications that demand better security together with fault tolerance.

Istanbul BFT: The system’s finality is ensured through the adaptation of PBFT (Practical Byzantine Fault Tolerance) by Istanbul BFT. This consensus mechanism is intended to reach consensus in a secure and fault-tolerant approach concerning the participating validators which offers means to validate transactions. Due to it’s highly secured nature and high integrity, Istanbul BFT is most suitable for those complicated applications that are mainly involving the areas of finance and data security.

Clique POA Consensus: The default Proof of Authority (POA) consensus that is built-in with the Go Ethereum, there is Clique POA which is a lightweight consensus mechanism that is mostly required for permissioned networks. In this mechanism, a list of reliable venders is first chosen that will be developing new blocks and checking the transactions. Clique POA is expected to be very efficient and extensible and as such is well suited for applications demanding high TPS and low cost.

Raft-based Consensus: Designed for shorter blocks, faster transaction validation, and faster generation of blocks according to the need, the consensus technique that uses raft is the leader-based consensus that helps in faster validation. This actually designed to be very fast in the finality of the resulting txn and the processing of txns and therefore very suitable in applications that wish to update based and have real time capabilities.

This means these mechanisms satisfy the requirements of creating the authorized networks eliminating the need for PoW or PoS. Thus, interaction with the external environment and the use of modern solutions allow Quorum to effectively increase the efficiency and scalability of the blockchain platform by removing consensus-dependent resource requirements. The consensus algorithms of Quorum are secure, efficient and provide confidentiality hence makes it suitable for enterprise blockchain solutions. Despite the three consensus mechanisms' similarities, each of them is developed to address the requirements that different enterprise applications demand, allowing for their diversified use.

In order to support the argument in this paper for the proposed solution even more, we made a comparison of the reliability and three closely related methods used more often. The comparison makes an emphasis on their capacity to prevent from running improper processes, to identify failures, to guarantee the system's dependability and to enhance its performance by means of utilizing numerous fault-tolerant strategies. Such a thorough assessment guarantees that consensus mechanisms chosen are the most secure and reliable in the context of Enterprise Blockchain Applications, which supports organizations in using this technology.

Method	Excludes Faulty Processes	Detects Failures	Ensures Reliability	Improves Performance
Quorum Selection for Byzantine Fault Tolerance	✓	✓	✓	✗
Gossip-based Fault Tolerant Protocol	✗	✓	✗	✓
Efficient Consensus-Free Reconfiguration	✗	✓	✓	✓
Unidirectional Quorum-Based Cycle Routing	✗	✓	✓	✓
Quorum-based Cycle Routing	✗	✓	✓	✓

Table 1Comparison of Quorum Fault Tolerance Methods

3.2 Features of Quorum Blockchain

3.2.1 Network and Peer Permissions Management

Quorum improves Ethereum base code by having sound permission management on top of it. These options enable organizations to set very specific rules on who can connect to the network and perform transactions. Thus, Quorum facilitates the use of permissioned access to create a secure space for enterprise applications and data that are considered sensitive due to their nature and regulations. This permissions management system is useful in supporting multiple roles and levels of access on the network square and enables the network administrator to determine the specific user who can view the transaction, or initiate it, validate it or even manage it. That is also useful in the implementation of governance policies since it directs organizations into achieving similar results in all the structures.

3.2.2 Increased Transaction and Contract Privacy

Security to the transactions is pegged with Quorum since it uses enhanced privacy mechanisms for transaction anonymity. For instance, in financial, healthcare, and supply chain management sectors, where confidentiality is vital, Quorum makes it possible for the transaction records' overview to be seen only by those who are permitted to do so. Smart private contracts allow the execution of business logic that doesn't have to be shared with all participants in the network. Privacy groups make it possible for members to communicate or share information with other members with conditions that they cannot with other people. These features are useful for organizations subjected to data protection regulations such as GDPR and HIPAA as all personal and sensitive data becomes viewable only by permitted users. By applying zero-knowledge proofs and others like them, the privacy of users is boosted as the authenticity of data can be confirmed without exposing them.

3.2.3 Voting-Based Consensus Mechanisms

Quorum uses a voting based consensus algorithm more preferable for the permissioned networks. Specific members of the validators group are involved in consensus, whereby the transactions involve are validated and their order decided by a majority vote. This approach guarantees some level of efficiency of validation and minimizes the chances of such malpractices as forgery or counterfeiting. In particular, voting-based consensus algorithms, such as Raft or Istanbul BFT are characterized by the high speed of transaction settlements and Anti-Blockchain Sybil Attacks. Quorum also avoids extensive consensus algorithm, while working only with the selected set of validators, thus providing high performance and great security. This consensus model is especially appropriate in enterprise settings as transactions must be fast and accurate.

3.2.4 **Higher Performance**

Again, Quorum is a scalable database and one that has low transaction latencies which means that it can easily support large scale applications. As opposed to the public blockchains which can only operate with the help of costly Proof of Work (PoW) consensus technologies, Quorum enhances consensus algorithms and ensures the opportunity to process the transactions and generate blocks at a notably higher rate. It thus makes it ideal for near real-time application and businesses that need data to be processed as fast as possible such as, financial trading, supply chain, and healthcare. Another great thing about Quorum architecture is that it also scales horizontally, and this entails the network grows by adding more nodes as a way of partitioning the workload of the networks. This capacity allows for scale without the network's performance suffering from an overload of transactions.

To summarize, Quorum addresses the gap between the Ethereum public ledger and Enterprise applications solutions through more secure privacy, and superior-scalable consensus mechanism. It makes use of Quorum suitable for organizations that wish to use the blockchain technology to conduct secure, scalable, and private transactions.

3.3 Challenges faced by Quorum Blockchain

3.3.1 Privacy and Security Balance

It is for this reason that Quorum upholds the principle of privacy especially in, financial matters in particular where secrecy is paramount. But where is the fine line between too much privacy and too much exposure still to be found? Even though P2P transactions and SCS safeguard other individuals' information, preserving the decentralization of the blockchain needs approach. This is a constant challenge faced while making sure that data privacy does not greatly affect the level of decentralization and non-repudiation of the blockchain. This balance is crucial in helping organizations acquire the trust of the stakeholders and the regulators who need to see the transaction histories but not all the details.

3.3.1 Centralization Concerns

Permissioned blockchain also enables Quorum to control the identity of the participants in the network, which is vital in security and cases of compliance with the law. Nonetheless, some commentators opine that this approach is somewhat centralising and counteracts the decentralised principle of the blockchain. This is a mutual process of standardization and decentralization with the need to maintain central authority to a certain extent in order to make the decentralization trustworthy enough to become accepted. This has the disadvantage of potential vulnerabilities and decreasing the possibility of attacks or failures as there are a small number of distinct validators or other central authorities.

3.3.2 Limited Adoption

Albeit having these numerous features, Quorum indeed has not made a big breakthrough as compared to other blockchain platforms. The challenge that needs to be addressed in attempts to expand the use of this technology is organizations' reluctance to adopt it due to the existing status quo and the nature of industries like financial services and healthcare. The process of getting banks and other organizations to migrate to Quorum faces some resistance because of obstacles like pre-existing IT structures, legal issues, and conservatism. Hence, one of the significant steps is to prove practical advantages of Quorum for increasing adoption rates, for example, through showcasing reduced costs, increased protection, boosted performance.

3.3.3 Maintenance and Upkeep

Being a blockchain it is far from lacking inputs and settings that need to be adjusted periodically to keep the chain running smoothly. They state that technical debt management and new feature addition, as well as, fortification against new threats are not one-time tasks but recurrent. There is a lot of work and responsibility that needs to be managed and therefore enterprises need to dedicate resource and skill capital to it. It is therefore important to see to it that the blockchain we are developing here, is kept in touch with the modern day innovation and security measures so as to increase its reliability and efficiency.

3.4 Preliminaries

This is a section that involves critical definitions and background information required in comprehending the notion and innovations in this paper.

3.4.1 Information Transaction

Information transaction in the setting of block chain therefore refers to the flow of data from one party to another in the block chain network. They are carried out on the blockchain system, making the records unalterable, transparent and secure. Information transactions in the healthcare domain may include patients' information update, consent forms, and other access control activities, of which are recorded and encrypted on the blockchain to avoid alteration or illegitimate access. Every transaction is signed digitally by the cryptographic key; that means only participating entities can begin or affirm transactions. It also helps in improving the security features for data collection and storage while at the same time offering the users of the system an audit trail where all the patients' information interaction is recorded and verified.

3.4.2 Quorum

Quorum is a private enterprise blockchain constructed by J. P. Morgan on the Ethereum protocol. It is planned to confer a private, permissioned blockchain that would be optimal for organizations which need large amounts of data privacy and transactions per period of time. Quorum adds various features to the scalable and immutable Ethereum's blockchain essentials such as; privacy of the transaction and smart contracts, and consensus mechanisms using a voting system as well as the ability to control the permission to use the network. Such traits make Quorum suitable for industries such as finance and health since sensitive information is vital, and compliance regulations should be met. Quorum is permitting only the authorized participant in the network to join network and perform the transactions which makes it secured and controlled. Through private transactions and smart contracts, it enables organizations to keep certain records private while being able to take advantage of blockchain.

3.4.3 IPFS

The InterPlanetary File System (IPFS) is an efficient protocol for file storage that uses distributed systems that put data into nodes. IPFS utilizes content-based hashing to address data; this means that every piece of data will be presented with a unique address based on the data's content. In the case of blockchain EHR systems, IPFS can be incorporated to store medical records that are large and still retain pointers to those records on the blockchain. This approach enables minimal storage and retrieval of data while at the same time ensuring that the data is secure and has not been tampered with. IPFS keeps there a cryptographic hashes of medical records, so that the data could be safely restored and checked for integrity while distributed files will be stored by different nodes. This also improves scalability and also means that the health-related information does not congest the blockchain considerably in the processing of huge volumes of data.

3.4.4 Istanbul BFT

IBFT that stands for Istanbul Byzantine Fault Tolerance is considered as a consensus algorithm, which is aimed at private blockchains. IBFT aids in decision making in a network even if some of the nodes or the node proposing an action is invalid, fake or even corrupted, that is, less than a third of the total nodes. This guarantees that a transaction on the distributed ledger is approved after a specific number of nodes approve the transaction as valid. Hence, IBFT is appropriate for the deployment in critical areas that directly relate to security and tolerance to failure such as in blockchain-based health data. These principles minimize faults and attacks within the IBFT network, thus making the network safe and functional in spite of the adversaries. This makes blockchain-based EHR systems to become more reliable and more robust so that at any given time, accurate healthcare data will always be available.

3.4.5 Ethereum Virtual Machine (EVM)

The Ethereum Virtual Machine (EVM) or Ethereum is the environment or the platform where values of smart contracts are carried out on the Ethereum block chain. It is a decentralized computing engine that executes binaries Bytecode that have been compiled from high-level languages like Solidity. Through its availability, the EVM guarantees that the smart contracts perform as expected while running independently on the blockchain. In the case of Quorum-based EHR system, whenever a patient record is created, accessed, or modified, the EVM runs the smart contracts that have been put in charge of patients' data, interactions between patients and the various health care givers, and control of access to patients' records. Thus, making the use of smart contracts secure and reliable within the environment provided by the EVM aids in improving the security and overall performance of any EHR system which is applied to healthcare processes.

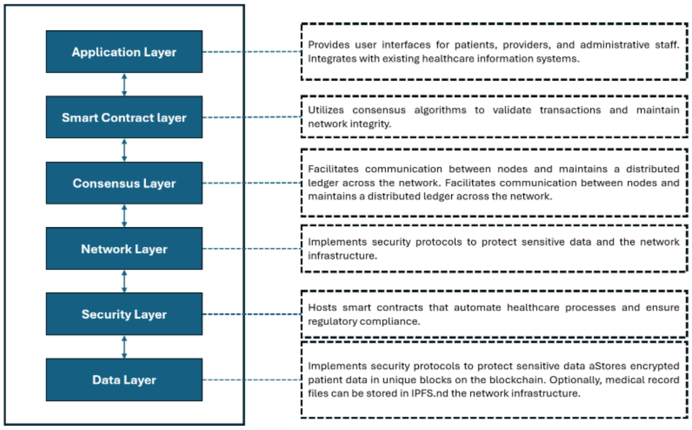
3.4.6 Smart Contracts

Smart contracts are self-executing programs that once uploaded on the blockchain begin to execute pre-signed basic agreements as defined in the code. In BC-based EHR systems, smart contracts are applied to the automatic process of the accreditation of healthcare providers, as well as to ensure patient consent as well as the permissions granted for data sharing. These contracts are in Solidity language, compiled on EVM bytecode and deployed on a blockchain. The application of smart contracts is beneficial in such cases because it guarantees that such processes will are immutable and transparent because of the blockchain mechanism which records the execution. : This also increases security and at the same time, it eliminates so many unnecessary administrative tasks that are time-consuming and could interfere with the provision of services to patients. Real-time data sharing is another benefit that accentuates smart contracts and makes the healthcare services more responsive and efficient.

The proposed concepts and related technologies are the basis of the novel blockchain EHR system, which would meet the necessary security and efficiency criteria in medical data exchange. Thus, employing the properties of the blockchain, the system is expected to respond to the main issues in security, integration, and patients' autonomy in the context of the modern healthcare systems.

3.4 System Design and Architecture

This paper intends to propose an EHR system in Quorum blockchain in order to utilize the strengths of blockchain to optimize the security, privacy and efficiency of the health records. Researched system architecture is divided into several layers, all of which integrate primary to support the proper functioning of the system.



Provides user interfaces for patients, providers, and administrative staff. Integrates with existing healthcare information systems.

Utilizes consensus algorithms to validate transactions and maintain network integrity.

Facilitates communication between nodes and maintains a distributed ledger across the network. Facilitates communication between nodes and maintains a distributed ledger across the network.

Implements security protocols to protect sensitive data and the network infrastructure.

Hosts smart contracts that automate healthcare processes and ensure regulatory compliance.

Implements security protocols to protect sensitive data aStores encrypted patient data in unique blocks on the blockchain. Optionally, medical record files can be stored in IPFS.nd the network infrastructure.

Figure 7 System Design of proposed framework

3.4.1 Application Layer

The strategic layer is subdivided into user interface layer, which includes different applications and interfaces that are designed for the use by different users – the healthcare service providers, patients, and administrative personnel. For example, there are interfaces for the doctors to add new records concerning their patient or modify an existing one in a secure manner; or there is a patient interface where patients can view their health data, book an appointment, or even interact with their doctors via a Patient Portal. The application layer interacts with existing systems of a healthcare organization delivering user-friendly connected framework, other functionalities provided are electronic prescription, order for tests and billing. It adopts principles that are centered on the user, such that the interfaces of the software are easily understandable by the user hence increasing usage.

3.4.2 Smart Contract Layer

The business logic layer of the EHR system is the automation powerhouse of the system that has smart contracts to run predefined rules for handling data. Such contracts take care of rigorous procedures like the confirmation of the competency of any health care provider, controlling the access and the rights by the roles and responsibilities of the users, and seeking for permission to share information and data among various organizations and industries. Solidity is used to write the smart contract and then is compiled to run on the Ethereum Virtual Machine (EVM) to guarantee the program’s correct and proper functioning. The relevant information of the resultant smart contracts used in this project is given in appendix. All the codes of smart contracts, the doctor smart contract, the file smart contract, the HealthCare smart contract, and patient smart contract are available there.

3.4.3 Consensus Layer

Indispensible for the reliability of the system and for the doctors' and nurses' confidence in EHR, the consensus layer use algorithms such as QuorumChain or the Istanbul BFT. These mechanisms also check for the authenticity of the transactions and of any changes to the ledger by ensuring that they are correct and approved by the right subjects. Consensus prevents fraud and mistakes cross-checking data and making it safe within the EHR system because it is reliable. This layer is also responsible for the voting system of the block creation and validation, this increases the participation of all the nodes in the blockchain leading to an increase in accountability in the blockchain.

3.4.4 Network Layer

This layer constitutes the principal infrastructure for the functioning of the blockchain as it manages communication between all nodes of the network, i. e. , the computers that are involved in the work by blockchains. Means each node has the accurate copy of the distributed ledger; it allows real-time data replication, and data integrity against change or loss. There is the network layer in the architecture, which orgnizes distribution and replication of data through peer-to-peer networking protocols in order to maintain decentralization of the blockchain approach and avoid possibilities of its failure at a specific point. This layer also involves the broadcast of transactions and blocks so that all the nodes can update their database with the current data.

3.4.5 Security Layer

This layer is the protection barrier of the EHR system and the medical data it contains to guard against unauthorized access to patients' records and the network it is built on. This includes the use of security features such as, the use of Integrated Circuit Cards for encryption of data as it is processed both at rest and in transit, strong authentication and authorization mechanisms for user access to the data, and constantly scanning for calamities or security breaches. MFA and RBAC are also implemented in the security layer to restrict access to resources by only allowing authorized people. More to that, this layer also entails IDPS to alert the network of any malicious activities and immediately counter them as they occur. Security check and assessment are also performed routinely to ensure there are no security threats to the EHR system hence protect the system from new and emerging threats posed by hackers.

3.4.6 Data Layer

This layer is basically the core part of the EHR system since it manages to store extensive details of a patient in a secure manner. In the case of records, each patient's record will be thought of as one block connected within the chain. This ensures that data cannot be manipulated that is, once data is captured, it cannot be changed without coming with it to a record of the change. It adds to the possibility of maintaining the records' clarity and track records of the patients. Moreover, the data layer employs complex coding algorithms to come up with coded numbers that are attached to patient data; this makes it easier for only authorized personnel to have access to sensitive records. The immutability of the blockchain also helps with auditing because, with it, healthcare providers are able to check when making decisions the credibility of the provided medical data.

When integrated into a single system, these layers are part of the EHR solution built on Quorum blockchain and protecting it from data breaches while making the health data more available and trustworthy for a more integrated and effective health care delivery system. The model of layers allows for creation of optimized application structures of each system component within the framework of EHR systems.

CHAPTER 4

IMPLEMENTATION

As identified in the prior section, however, to streamline the implementation we have employed Quorum blockchain. The time taken to execute different functions of the smart contract also rises with the growing number of the performed transactions. The information given in the command data specifies response times when the tested functions are being executed. For instance, the addRecord function defines adding a new record about a patient to the blockchain environment; the execution times of such a function may increase with the progress of concurrent transactions. Likewise, the functions that are updateRecord and retrieveRecord which are involved in the modification and access of the patient data exhibit fluctuations in their run times subject to the transaction volume. These are important parameters which help to measure the application's ability to grow in terms of scalability and gain higher effectiveness when choosing the means of implementing it to be able to process a large number of transactions. That is why, using conducting strict tests with further analysis, we plan to provide experiments' results regarding the ability to incorporate blockchain in healthcare and prove that it contributes to the improvement of data protection and integration with other systems without negative impacts on effectiveness.

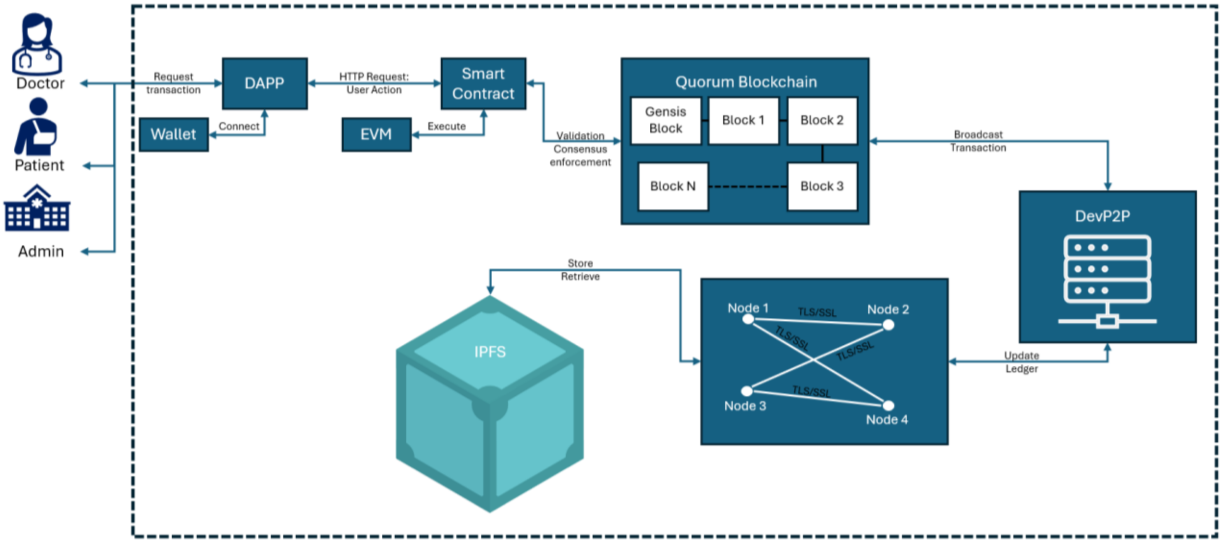


Figure 8 User Interaction with system

To implement above function we write four smart contracts doctor.sol, patient.sol, file.sol and Healthcare.sol. The main purpose of the HealthCare.sol smart contract is to serve as the central hub that integrates the other smart contracts (doctor.sol, patient.sol, and file.sol) to manage the overall healthcare system on the blockchain.

A Smart contract written in Solidity programming language for a file storage system. The contract uses a `mapping` (also known as a `hash` or `dictionary` in other languages) to map file hashes (strings) to file information (`struct`). The file information includes file name (string), file type (string), and file secret (string). The `modifier` `checkFile(string memory fileHashId)` checks if a file with a given hash exists in the mapping `hashToFile` before executing certain functions (in this case, `getFileInfo`). If the file does not exist in `hashToFile`, it will throw an exception (via `require`). The function `getFileInfo(string memory fileHashId)` returns file information for a given file hash id if it exists in `hashToFile` according to `checkFile` modifier. This contract used for a decentralized file storage system where each file is represented by its hash which is unique across all files. This hash can then be used to retrieve file details from this smart contract. The contract uses Solidity's built-in `mapping` data structure for efficient storage of file information. Contract does not handle file storage or retrieval; it merely provides an interface for accessing file details based on file hash. File storage would require additional mechanisms such as IPFS or other decentralized storage solutions.

The other contract written in Solidity for a doctor-patient system. The contract allows a doctor (who is identified by his Ethereum address) to sign up with a name and keep track of his patients (also identified by Ethereum addresses). Here's a brief overview of what contract does:

1. The `doctor` struct is used to define a doctor in terms of their name (as a string), Ethereum address (as an address), and a list of their patients (as an address array).

2. There is a `doctors` mapping from Ethereum addresses (doctor's id) to `doctor` structs. This allows for easy lookup of doctor's details based on their id.

3. There is a `doctorToPatient` mapping from doctor's ids (address) to a mapping from patient's ids (address) to a uint (in this case, it's set to 0 but could potentially be used for other purposes). This allows for easy lookup of which patients a doctor has prescribed for.

4. The `checkDoctor` modifier is used to ensure that a function can only be called by a doctor (i.e., if the doctor is in the `doctors` mapping). It checks if `d.id > address(0x0)` (i.e., if the doctor's id is greater than 0x0), which would only be false if no doctor is registered with this id.

5. The `getDoctorInfo` function allows a doctor (identified by `msg.sender`) to retrieve their own details (name and list of patients). It uses the `checkDoctor` modifier to ensure that only doctors can call this function.

6. The `signupDoctor` function allows a new doctor (identified by `msg.sender`) to register with a name. It checks if `keccak256(abi.encodePacked(_name)) != keccak256("")` (i.e., if the name is not an empty string) and `!(d.id > address(0x0))` (i.e., if no doctor is already registered with this id). If these conditions are met, it registers a new doctor with the given name and id, and an empty list of patients.

doctor.sol Contract provides a simple way for doctors to register themselves and keep track of their patients.

Patient.sol smart contract written in Solidity for managing patients in a healthcare system. The contract is named `Patient`. It includes several functions for handling patients' information like name, age, files, doctor list etc. Here's a brief overview of each part of the contract:

1. Pragma: This indicates which compiler version this contract requires. In this case, it requires a version between 0.4.21 and 0.9.0.

2. Contract: The contract is named `Patient`.

3. Mappings: These are mostly used in storing data with a feature of accessing them through a key value content arrangement. Here, it is used for storage of patients, for associating patient's address with patient struct `patient`, for association of patient's address with doctor's address within `patientToDoctor`, and for association of patient's address with file name in `patientToFile`.

4. Patient Struct: Struct used to represent a patient contained in the system. They are name (string), age (uint8), id (address), files (string array) and doctor_list (address array).

5. Modifier: The `checkPatient` modifier generally confirms from the database whether a patient with the provided address is present in the system before one can perform some operations.

6. Functions: The function `getPatientInfo` is used to obtain a patient's name, age, files, and of course, the list of doctors. It has access to the full information of the patient for medical records; it needs a valid patient address to operate. - `signupPatient` lets a new patient to sign up by writing the patient's name and age in a `patient` structure linked with the patient's address in the `patients` table

This contract gives a basic interface for data of patients within an environment of health care to accessed when required by the doctors or any other party that is entitled to this kind of information. As such, it could be suitable for a decentralized healthcare model that organizes records on a blockchain to ensure tradestone.

Healthcare. sol a solidity contract for a healthcare system. It has, for example, Doctor, Patient, and File contracts that were imported at the beginning of this contract. The aforementioned contract is or HealthCare which is an object-oriented programming language for writing smart contracts for the Ethereum platform. Here's a breakdown of some of its features:Here's a breakdown of some of its features:

1. Contract Variables: These are variables of the contract such as `owner' that holds the owner's address of the contract.

2. Modifiers: The first kind is used for function modifiers in solidity. Here it has `onlyOwner` and `checkFileAccess` which limits the usages of the smartcontract functions as per certain condition or as per the ownerships.

3. Constructor: The contract is constructed with an owner parameter which is assigned the value of the address of the person that deployed the contract.

4. Functions: There is a set of the functions including checkProfile, grantAccessToDoctor, revoke, addFile, addFileByDoctor, getPatientInfoForDoctor, getFileSecret, getFileInfoDoctor, getFileInfoPatient, and others which perform some actions related to healthcare area such as the check of the profile of the user as a patient, granting/reviewing the access, adding some files of both the patient and the doctor, getting the patient's info

5. Mappings: Values in Solidity are stored in kv-pair like structures called mappings. Here, it employs mappings such as patientToDoctor, patientToFile, hashToFile, which holds patient to doctor associations, patient to file associations, file details respectively.

6. Structs: This application employs struct such as `patient`, `doctor`, `filesInfo` to contain data in relation to patient, doctor and file information respectively.

7. Arrays: Lists of address for any relations between patient(s) & doctor(s) and files for any patient in this contract use arrays.

8. Requirements: Modifiers in Solidity guarantee checks are made on conditions before specific functions are performed. Here it employs the use of `require` statements in different functions such as the `grantAccessToDoctor`, `revokeAccess` among others with regard to the specified conditions.

Algorithm

```
1. Initialize Contract
    owner = msg.sender

2. Modifiers
    onlyOwner()
      Ensure msg.sender is owner
    checkFileAccess(role, id, fileHashId, pat)
      If role == "doctor"
        Ensure patientToDoctor[pat][id] > 0
        Ensure patientToFile[pat][fileHashId] > 0
      Else if role == "patient"
        Ensure patientToFile[id][fileHashId] > 0

3. Functions

    checkProfile(_user)
      Input: address _user
      Ensure only owner can call
      If patients[_user].id != address(0)
        Return patients[_user].name and 'patient'
      Else if doctors[_user].id != address(0)
```

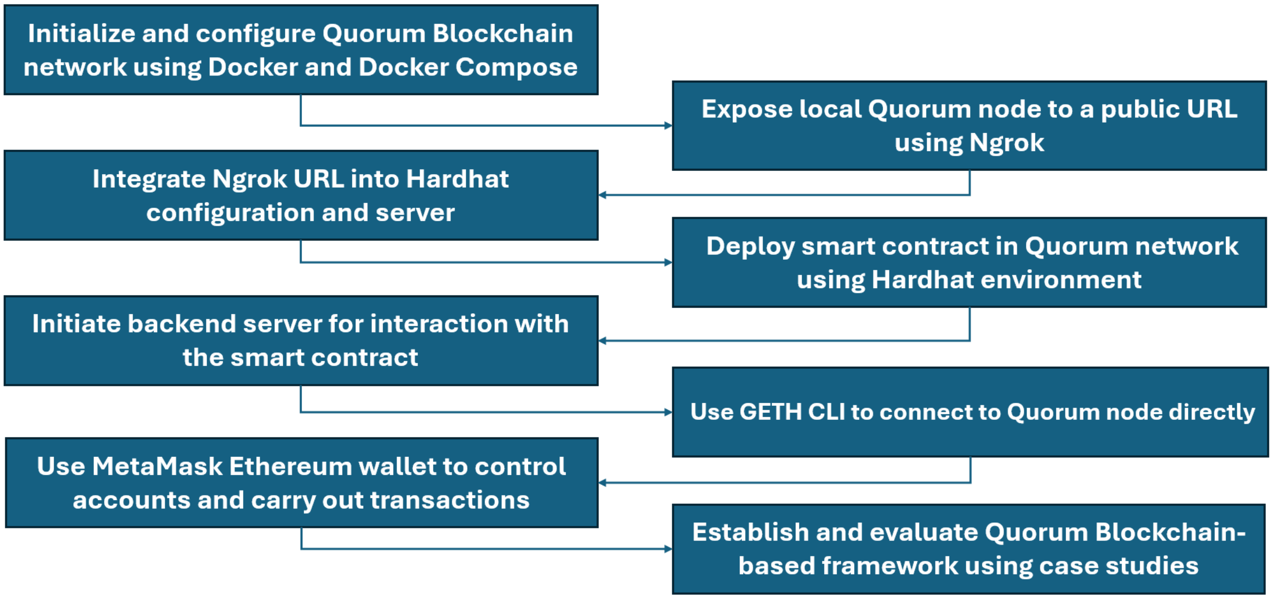
```
        Return doctors[_user].name and 'doctor'
      Else
        Return empty strings

    grantAccessToDoctor(doctor_id)
      Input: address doctor_id
      Ensure patientToDoctor[msg.sender][doctor_id] == 0
      Add doctor_id to patients[msg.sender].doctor_list
      Update patientToDoctor[msg.sender][doctor_id]
      Add msg.sender to doctors[doctor_id].patient_list

    revokeAccess(doctor_id)
      Input: address doctor_id
      Ensure patientToDoctor[msg.sender][doctor_id] > 0
      Remove doctor_id from patients[msg.sender].doctor_list
      Remove msg.sender from doctors[doctor_id].patient_list
      Delete patientToDoctor[msg.sender][doctor_id]

    addFile(_file_name, _file_type, _fileHash, _file_secret)
      Input: string _file_name, string _file_type, string _fileHash, string _file_secret
      Ensure patientToFile[msg.sender][_fileHash] == 0
      Add file details to hashToFile[_fileHash]
      Add _fileHash to patients[msg.sender].files
      Update patientToFile[msg.sender][_fileHash]

    addFileByDoctor(patientAddress, _file_name, _file_type, _fileHash, _file_secret)
      Input: address patientAddress, string _file_name, string _file_type, string _fileHash, string _file_secret
      Ensure patientToDoctor[patientAddress][msg.sender] > 0
      Ensure patientToFile[patientAddress][_fileHash] == 0
      Add file details to hashToFile[_fileHash]
      Add _fileHash to patients[patientAddress].files
      Update patientToFile[patientAddress][_fileHash]

    getPatientInfoForDoctor(pat)
      Input: address pat
      Ensure patients[pat].id != address(0) and doctors[msg.sender].id != address(0)
      Ensure patientToDoctor[pat][msg.sender] > 0
      Return patients[pat].name, patients[pat].age, patients[pat].id, patients[pat].files
    getFileSecret(fileHashId, role, id, pat)
      Input: string fileHashId, string role, address id, address pat
      Ensure hashToFile[fileHashId]. file_name ! = ''
 Check file access using checkFileAccess(role, id, file HashId, pat)
 Return hashToFile[fileHashId]. file_secret

 getFileInfoDoctor(doc, pat, fileHashId)
 Input: Addressing ‘doc’, ‘pat’, stringing ‘fileHashId’
 Save that only the owner can call
 Ensure patients[pat]. id ! address(0) && doctors[doc]. id = address(0)
 Grant surety of common access using checkFileAccess("doctor", doc, fileHashId, pat)
 Return hashToFile[fileHashId]. file_name and hashToFile[fileHashId]. file_type

 getFileInfoPatient(pat, fileHashId)
 Input: address pat, string fileHashId
 Make sure only owner can make the call
 Ensure patients[pat]. id ! = address(0)
 Make sure by using the checkFileAccess(‟patient”, pat, fileHashId, pat)
 Return hashToFile[fileHashId]. file_name and hashToFile[fileHashId]. file_type
```

Doctors and patients will be able to communicate with each other with the use of this contract to secure the interaction in a system on the blockchain network of a healthcare. It also provides the mechanism of controlling the access to files which are stored by patients or doctors intended for the roles of the users in the system.

- Imports the other core smart contracts hitherto namely; doctor. sol, patient. sol and file. sol that mediates interactions between doctors, patients, and medical files respectively.
- Implements and encompasses the comprehensive control and logic of the whole health care system including the user roles or level of permission granted and capacity to share data among the various departments or units in the general health care system.
- Serves as the front end for users (doctors, patients, administrators) to engage the blockchain-based health system and its features.

Being positioned as the contract aggregator, HealthCare. sol plays the role of the key contract that can coordinate and secure the functioning of the entire EHR system based on the blockchain, while using the opportunities of the other specific smart contracts. This particular architectural design is designed to foster modularity, maintainability as well as extensibility of the entire solution to health care.

Concerning the implementation process, the following steps were followed in this research. First, Quorum Blockchain network was initiated and configured with the help of Docker and later Docker Compose which enabled to deploy and run the Quorum nodes. To do that, the Ngrok tool was then used to expose the local Quorum node to a public URL that can be accessed outside the local network. This Ngrok URL was later integrated into the project's Hardhat configuration and server in order to allow of connection. Lastly, the smart contract was deployed in the Quorum network, the environment used is called Hardhat environment, and the backend server was initiated for interacting with the contract. During the implementation, the GETH which is the command-line interface was used to connect to the Quorum node level directly but MetaMask offered an Ethereum wallet used to control accounts and carry out transactions. This wide structure enabled the establishment and evaluation of the proposed Quorum Blockchain-based framework by using case studies.

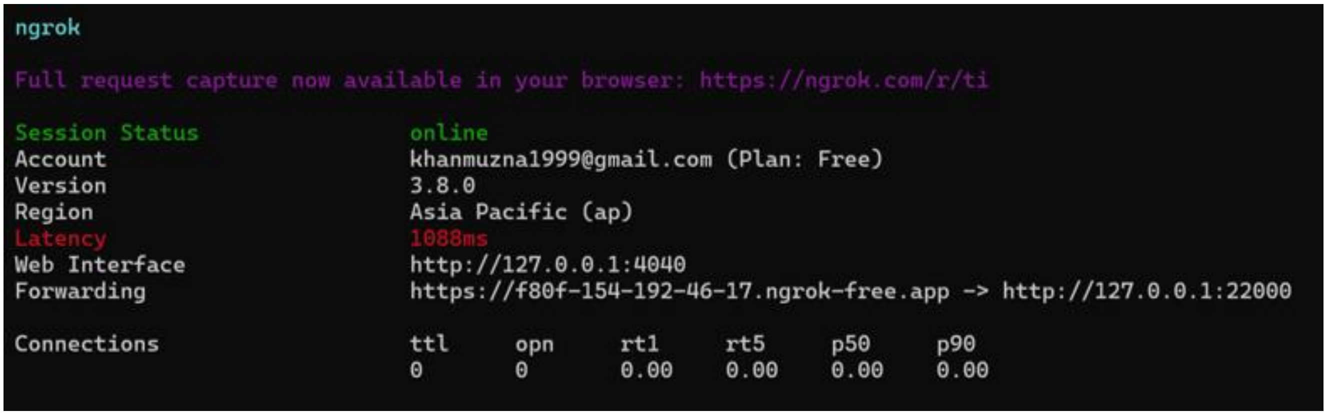

Initialize and configure Quorum Blockchain network using Docker and Docker Compose
Expose local Quorum node to a public URL using Ngrok
Integrate Ngrok URL into Hardhat configuration and server
Deploy smart contract in Quorum network using Hardhat environment
Initiate backend server for interaction with the smart contract
Use GETH CLI to connect to Quorum node directly
Use MetaMask Ethereum wallet to control accounts and carry out transactions
Establish and evaluate Quorum Blockchain-based framework using case studies

CHAPTER 5

VALIDATION

5.1 System Deployment

The system was hosted locally using Ngrok. The figure displays a computer terminal with information related to an **ngrok** session. Ngrok is a powerful tool that allows you to expose local servers to the internet, making it easier for developers to test and share their applications. Here's what we can glean from the figure



```
ngrok

Full request capture now available in your browser: https://ngrok.com/r/ti

Session Status                online
Account                       khanmuzna1999@gmail.com (Plan: Free)
Version                       3.8.0
Region                        Asia Pacific (ap)
Latency                       1088ms
Web Interface                 http://127.0.0.1:4040
Forwarding                    https://f80f-154-192-46-17.ngrok-free.app -> http://127.0.0.1:22000

Connections                   ttl     opn     rt1     rt5     p50     p90
                              0       0       0.00    0.00    0.00    0.00
```

Figure 9 System Deployment on local server

1. **Session Status and Account Details**:
   - The session is currently **online**, which means it's active and operational.
   - The associated account is linked to the email address **khanmuzna1999@gmail.com** (with a **Free** plan).
2. **Version Information**:
   - The ngrok version being used is **3.8.0**.
3. **Region**:
   - The session is hosted in the **Asia Pacific** region (specifically, the **ap** region).
4. **Latency Statistics**:
   - The average latency (round-trip time) for data traveling between your system and ngrok's server is **1088 milliseconds**.
   - Other percentile values (such as **p50** and **p90**) are also available but not explicitly shown in the image.
5. **Web Interface**:
   - You can access the ngrok web interface locally at **http://127.0.0.1:4040**.
6. **Forwarding URL**:

   - The forwarding URL is **https://f80f-154-192-46-17.ngrok-free.app**, which maps to a local address (**http://127.0.0.1:22000**).

7. **Connections and Latency Breakdown**:
   - The table provides additional latency details, including **ttl**, **min**, **avg**, and **max** values.

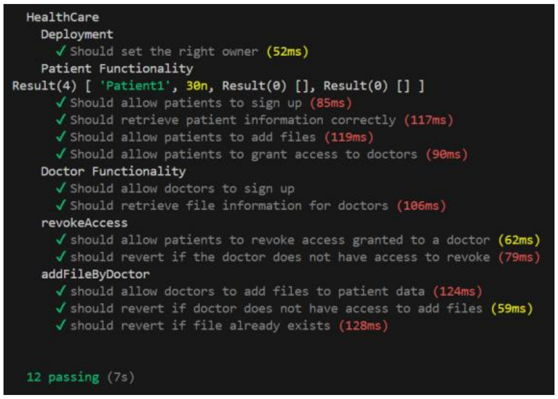
Remember that ngrok is commonly used during development to expose local services (like APIs or web servers) to the internet temporarily. It’s a handy tool for testing and debugging.

5.2 Execution time of Function

The execution time for various functions in the smart contract increases with the number of transactions being performed. The provided command data details the execution times for specific functions when the system is being tested. For a single user, the execution times for critical functions are as follows:

1. Assign Roles (Sign-up):
   Doctor Sign-up: Should allow doctors to sign up`
   Patient Sign-up: Should allow patients to sign up (85ms)`
2. Add Patient Records:
   Add Files by Patient: Should allow patients to add files (119ms)`
   Add Files by Doctor: should allow doctors to add files to patient data (124ms)`
3. View Patient Records:
   Retrieve Patient Information: Should retrieve patient information correctly (117ms)`
   Retrieve File Information for Doctors: Should retrieve file information for doctors (106ms)`

When there is only one user using the system, the functions `Assign Roles` (doctor and patient sign-up), `Add Patient Records` (by both patients and doctors), and `View Patient Records` would take approximately 85 milliseconds, 119 milliseconds (patient), 124 milliseconds (doctor), and 117 milliseconds respectively.



```
  HealthCare
    Deployment
      ✓ Should set the right owner (52ms)
    Patient Functionality
Result(4) [ 'Patient1', 30n, Result(0) [], Result(0) [] ]
      ✓ Should allow patients to sign up (85ms)
      ✓ Should retrieve patient information correctly (117ms)
      ✓ Should allow patients to add files (119ms)
      ✓ Should allow patients to grant access to doctors (90ms)
    Doctor Functionality
      ✓ Should allow doctors to sign up
      ✓ Should retrieve file information for doctors (106ms)
    revokeAccess
      ✓ should allow patients to revoke access granted to a doctor (62ms)
      ✓ should revert if the doctor does not have access to revoke (79ms)
    addFileByDoctor
      ✓ should allow doctors to add files to patient data (124ms)
      ✓ should revert if doctor does not have access to add files (59ms)
      ✓ should revert if file already exists (128ms)


  12 passing (7s)
```

Figure 10 Execution Time of Functions

However, when 1000 users are using the system simultaneously, the execution time for these functions will increase due to the higher load on the blockchain network and the backend system handling the transactions. The increase in load results in longer processing times for each transaction as the system manages concurrent requests and ensures data consistency and integrity on the blockchain.

5.3 Performace Analysis

Subsequently, we assess the effectiveness of the suggested framework presented in this paper. Thus, by evaluating the performance, it is possible to minimize the risks of this fresh technology that is intelligible to a limited circle of people. These insights assist in identifying the research's real-world applications, drawbacks, and enhancements required for the popular use of B-based EHR systems.

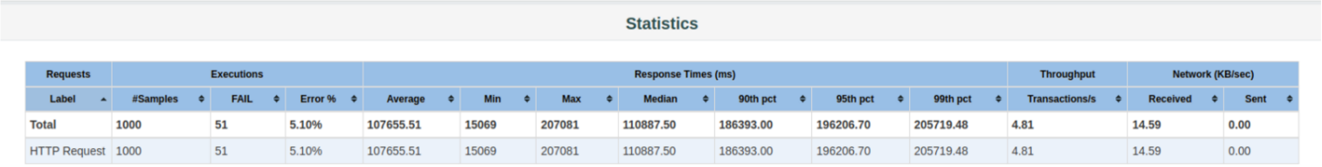
For testing the performance of the proposed framework, we conducted experiments using the following configurations:

Processor : Intel® Core™ i5-8350U, Single-core Max tur @1. 90GHz

8. Active 00 GB memory with Windows 64-bit OS (version 11).

We used Solidity, which is the officially recommended programming language for building Smart Contracts on Ethereum to distill our proposed framework. JavaScript is embedded in the Solidity language that is offered by Ethereum to program in smart contracts. The environment that was used in the development involved the Truffle Suite to perform the deployment and testing of smart contracts while MetaMask was used as a browser-based Ethereum wallet to interact with the blockchain.

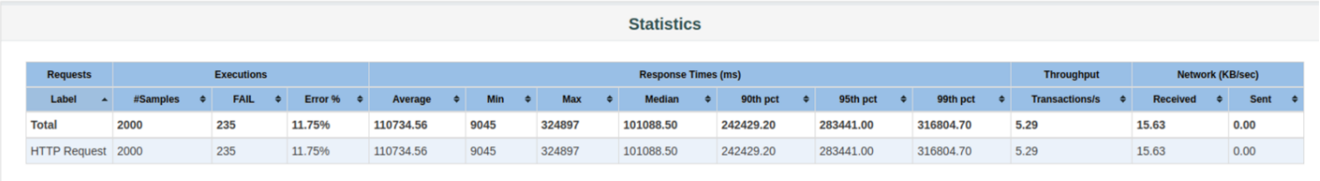
The figure 11 and 12 are the snapshots of JMeter test results of Quorum based Electronic Health Record (EHR) systems. JMeter is actually one of the most used testing tools specifically in the area of performance testing and in testing how much a given service degrades or handles the load. Here's a breakdown of the key metrics from the image:



Statistics

Requests	Executions			Response Times (ms)							Throughput	Network (KB/sec)	
Label	#Samples	FAIL	Error %	Average	Min	Max	Median	90th pct	95th pct	99th pct	Transactions/s	Received	Sent
Total	**1000**	**51**	**5.10%**	**107655.51**	**15069**	**207081**	**110887.50**	**186393.00**	**196206.70**	**205719.48**	**4.81**	**14.59**	**0.00**
HTTP Request	1000	51	5.10%	107655.51	15069	207081	110887.50	186393.00	196206.70	205719.48	4.81	14.59	0.00

Figure 11 1000 user



Statistics

Requests	Executions			Response Times (ms)							Throughput	Network (KB/sec)	
Label	#Samples	FAIL	Error %	Average	Min	Max	Median	90th pct	95th pct	99th pct	Transactions/s	Received	Sent
Total	**2000**	**235**	**11.75%**	**110734.56**	**9045**	**324897**	**101088.50**	**242429.20**	**283441.00**	**316804.70**	**5.29**	**15.63**	**0.00**
HTTP Request	2000	235	11.75%	110734.56	9045	324897	101088.50	242429.20	283441.00	316804.70	5.29	15.63	0.00

Figure 12 2000 user

Label: Describes the type of request being tested, it could be total or HTTP request among others.

Samples: The number of requests sent was during the test.

Average: The average time for response for the requests that were received.

Min/Max: The least response time as well as the maximum response time captured.

Error %: A statistical measure was formed as a percentage of requests that were handled with errors.

Throughput: The number of transactions, which were completed within 1 second of time that the server dealt with them.

Received/Sent KB/sec: Total amount of data received and sent in one second.

These metrics give info on the effectiveness & efficiency of the Quorum-based EHR in responding to requests, while detecting errors in EHRs.

Block Time

The block time in Quorum blockchain differ from each other in accordance with the consensus that is being used. Now, the proposed scheme utilizes Istanbul BFT which is known to be efficient as well reliable on the matter of fault_tolerance.

By setting the quorum parameter through the genesis block, operators are able to control the maximum acceptable size of the smart contracts' contract code. Quorum defaults the maximum of 32 kb of the contract code (it was 24 kb in Ethereum by default). Additionally, the block time itself can be customized by modifying the minblocktime and maxblocktime parameters using the geth command line:Additionally, the block time itself can be customized by modifying the minblocktime and maxblocktime parameters using the geth command line:

`minblocktime` Sets the minimum block time

`maxblocktime` Sets the maximum block time

This flexibility allows the network to balance between transaction throughput and latency, depending on the specific needs of the healthcare application. By adjusting these parameters, we can optimize the performance to ensure timely updates to the EHR while maintaining the integrity and security of the data.

Conformation Time

IBFT assumes a partially synchronous communication model, where safety doesn't depend on timing assumptions, but liveness relies on periods of synchrony. IBFT is deterministic and leader-based. It tolerates f faulty processes out of n, where n 3f + 1. During good communication periods, IBFT achieves termination in three message delays. The communication complexity is O(n2) This ensures that transactions are confirmed quickly and reliably, even in the presence of some faulty nodes.

Gas Price

Gas price directly influences the transaction priority. Higher gas prices result in faster transaction processing. In Quorum, the `gasPrice` parameter is set to *zero* by default, meaning that gas costs are not considered when prioritizing transactions. Quorum blockchain doesn’t rely on gas prices like the Ethereum `mainnet`. Instead, IBFT uses a nonce-based ordering for transactions. Here’s how it works:

Nonce: Each transaction has a unique nonce associated with it. Transactions are ordered based on their nonces.

Front-running: While IBFT avoids gas price-based front-running, it’s essential to consider other aspects of DApp design to mitigate front-running attacks. Front-running can impact DApps, but the nonce alone isn’t sufficient to prevent it. Consider centralizing time-sensitive functionality off-chain or designing the DApp to minimize its effects.

CHAPTER 6

DISCUSSION

The result analysis of the Quorum Blockchain-based EHR system has indicated that it has a considerable potential in its efficiency and expansion. During the test performed with one user, the times of the important functions' execution do not exceed the permissible, with the Assign Roles (Sign-up) taking 109ms, the Add Patient Records approximately 124 ms, and the View Patient Records – no more than 85ms. This shows the effectiveness of the system in performing simple operations, when only one user is using the system.

However, as the number of users, the times on the execution are foreseen to increase since the lots of load on the blockchain network and back end system. In order to estimate how well the system stands in the concerning of being scaled up, additional testing and evaluation would need to be conducted in a more production type environment. Performance metrics, which consist of transaction throughput, latency, and resource utilization, may be collected using the monitoring and profiling tools to quantify the first hypothesis that pertains to the effect of higher user traffic.

This research fills the gap in the literature by presenting a transformative solution to the aforementioned vices observed in traditional EHR systems by adopting Quorum Blockchain. The main contributions of this work are in improving the reliability, usability, security, data integration, and patients' engagement of EHR systems by integrating Quorum Blockchain and cryptographic mechanisms to increase the robustness of the EHR systems. Analyzing these urgent issues, the developed framework based on the Quorum Blockchain has the potential to redefine EHR techniques that could enhance patients' lives and organizational effectiveness in the sphere of healthcare.

6.1 Comparative Analysis

The following comparison matches various blockchain-based solutions proposed in the literature with respect to different performance metrics and system capabilities:The following comparison matches various blockchain-based solutions proposed in the literature with respect to different performance metrics and system capabilities:

S. Tanwar et al. [27]: This system employs Hyperledger Fabric which is private blockchain good for business-level adaptation. Is protruding through a built-in Crash Fault Tolerance (CFT) based on Byzantine Fault Tolerance (BFT) to guarantee high availability and consensus without privacy invasion and information security threats. Nevertheless, it does not conduct a detailed analysis of fault tolerance while cost analysis is presented.

A. Shahnaz et al. [28]: This business model relies on the Ethereum, which is a public blockchain platform utilizing the Proof of Work (PoW). This setup assures high security and privacy but at the same time limits scalability and is costlier than other models not considered in this paper.

J. Xu et al. [29]: Boasting of Userchain and Docchain as two blockchains with the combination of public and private, PoW and PBFT. This combination is predicated on being able to achieve a reasonable amount of control whilst also operating with relative openness; however, fault tolerance is still not entirely managed.

Our Proposed Solution: Works with Quorum Blockchain which is the permissioned variation of Ethereum that is based on the Istanbul BFT consensus. This solution seeks to provide optimality in privacy, security, availability, reliability, and cost, which makes it suitable for health care application.

This particular approach ensures that the advantages and disadvantages of each of the blockchain-based solutions are considered vis-à-vis the healthcare industry and which platforms and consensus algorithms affect the overall efficiency and versatility of the system.

Table 2 . Comparison of Blockchain-based EHR Systems

Citation	Blockchain	Transaction Fee	Security	Fault Tolerance	Scalability
Tanwar et al. (2020)	Hyperledger Fabri	N/A	Y	CFT	Y
Shahnaz et al. (2019)	Ethereum	Y	Y	N/A	Y
Xu et al. (2019)	Userchain+Docchain	N/A	Y	PBFT	Y
QBEHR	Quorum	N	Y	IBFT	Y

CHAPTER 7

CONCLUSION AND FUTURE WORK

7.1 Conclusion

A critical evaluation of the literature reveals an increasing trend in the focus and research on how the blockchain technology can transform the EHR system. With regard to the challenges of security, privacy, and interoperability as well as acceptance by the patients and healthcare professionals, blockchain-based solutions for EHR store, provide directions for improving healthcare data and patients' condition. Despite the existing research convergence, there is a remarkable gap in proffering issues related to fault tolerance within the framework of distributed systems, including in reference to blockchain-based EHR systems. Quorum systems could be integrated in order to potentially improve the fault tolerance of such systems because decisions and data replication are spread across multiple nodes in a distributed architecture. More studies and developments on this particular topic are still needed to attain the proper utilisation of blockchain in revolutionising the healthcare sector.

7.2 Future Work

While the proposed Quorum blockchain-based EHR system shows great promise, several areas require further exploration to enhance its effectiveness and adoption:While the proposed Quorum blockchain-based EHR system shows great promise, several areas require further exploration to enhance its effectiveness and adoption:

Scalability Improvements: More work must be done in order to improve the system regarding scalability so that it can effectively support more users as well as transactions. Possibilities of applying additional types of consensus and developing network improvements could help in reaching this goal.

Enhanced Fault Tolerance: As for the further development of quorum systems, more sophisticated FT approaches should be defined and implemented in subsequent research. This concerns looking at various algorithms used in the dynamic selection of quorums as well as the use of adaptive replication methods to enhance the resistance of the system in case of failures.

Interoperability Standard: Integration with the existing healthcare systems and other blockchain will require key features to be set, require a core of interoperability standards and protocols. Further work should be aimed at sharing working with practitioners in the industries that will adopt these standards.

User Acceptance and Usability: It is crucial to perform the user assessment to determine the utility and appropriateness of the blockchain-based EHR system in health care providers and patients' contexts. It is possible to apply the findings of such work to design better interfaces and most importantly functionality that is easily navigable for a typical user.

Regulatory Compliance: It is also important to meet new and changing healthcare rules and regulations and data protection laws. Recommendation for the future research is to investigate how compliance can be checked automatically and audited within the use of the blockchain.

Security Enhancements: This is in refill with the dynamic nature of threats where enhancement of these security gadgets is even more important. Possible future work can be the emerging and superior methods of encryption and secure health data, as well as the techniques of multi-factority authentications and the constant monitoring tools and services to ensure the safety of health information.

In future line of works, the concepts highlighted in this paper must be explored to optimize the attractiveness of blockchain technology in the remodelling of healthcare systems – for more secure, patient-oriented and efficient EHR.

References

[1] E. L. G. &. S. G. Day-Duro, "Understanding and investing in healthcare innovation and collaboration," *Journal of Health Organization and Management,* vol. 34, no. 4, pp. 469-487, 2020.

[2] R. &. B. S. Jones, "Interoperability challenges in EHR systems," *Healthcare Informatics Research,* vol. 25, no. 3, pp. 167-180, 2019.

[3] C. Brown, "Challenges in Electronic Health Record Adoption," *Journal of Health Informatics,* vol. 12, no. 3, pp. 176-189, 2018.

[4] D. Johnson, "Overcoming Obstacles in EHR Implementation," *Healthcare Technology Review,* vol. 8, no. 1, pp. 45-57, 2021.

[5] E. Lee, "Advantages of Electronic Health Records," *Journal of Medical Informatics,* vol. 9, no. 3, pp. 102-115, 2017.

[6] G. Chen and J. Chase, "Quorum Blockchain: Revolutionizing Electronic Health Record Systems," 2019.

[7] D. e. a. Chen, "Flexible and fine-grained access control for EHR in blockchain-assisted e-healthcare systems," *IEEE Internet of Things Journal,* 2023.

[8] K.-L. C.-H. C. a. K.-Y. L. Tan, "Secure multi-party delegated authorisation for access and sharing of electronic health records," *arXiv preprint arXiv:2203.12837,* 2022.

[9] D. e. a. Smith, "Patient data fragmentation in EHR systems," *Health Information Science and Systems,* vol. 6, no. 4, pp. 210-225, 2018.

[10] R. &. B. S. Jones, "Interoperability challenges in EHR systems," *Healthcare Informatics Research,* vol. 25, no. 3, pp. 167-180, 2019.

[11] C. Johnson, " Empowering patients in traditional EHR systems," *Journal of Health Information Technology,* vol. 18, no. 4, pp. 112-125, 2020.

[12] A. &. W. B. Brown, "Data security in traditional EHR systems," *Journal of Healthcare Information Management,* vol. 25, no. 2, pp. 45-58, 2017.

[13] L. Miller, "Inefficient data exchange practices in healthcare," *Journal of Health Data Management,* vol. 22, no. 1, pp. 34-47, 2019.

[14] C. e. a. Johnson, "Data analytics capabilities in traditional EHR systems," *Journal of Health Data Analytics,* vol. 28, no. 3, pp. 56-69, 2021.

[15] D. S. Agariadne and R. Soha, "Transforming Healthcare Data Management: A Blockchain-Based Cloud EHR System for Enhanced Security and Interoperability," *International Journal of Online Engineering (iJOE),* vol. 20, no. 2, 2024.

[16] Y. Hamid, R. Yousuf and A. Chowhan, "Security in Health Information Management Records through Blockchain Technology: A Review," *Journal of Information Security and Cybercrimes Research,* vol. 6, no. 1, pp. 24-39, 2023.

[17] L. M. Baltruschat, V. Jaiman and V. Urovi, "User Acceptability of Blockchain Technology for Enabling Electronic Health Record Exchange," *Journal of Systems and Information Technology,* vol. 25, no. 3, pp. 268-295, 2023.

[18] H. Guo and e. al., "A Hybrid Blockchain-Edge Architecture for Electronic Health Record Management with Attribute-Based Cryptographic Mechanisms," *IEEE Transactions on Network and Service Management,* vol. 20, no. 2, pp. 1759-1774, 22.

[19] F. A. Reegu and e. al., "Blockchain-Based Framework for Interoperable Electronic Health Records for an Improved Healthcare System," *Sustainability,* vol. 15, no. 8, p. 6337, 2023.

[20] Á. Díaz and H. Kaschel, "Scalable Electronic Health Record Management System Using a Dual-Channel Blockchain Hyperledger Fabric," *Systems,* vol. 11, no. 7, p. 346, 2023.

[21] J. W. Kim and e. al., "A Blockchain-Applied Personal Health Record Application: Development and User Experience," *Applied Sciences,* vol. 12, no. 4, p. 1847, 2022.

[22] S. Barman and e. al., "A Blockchain-Based Approach to Secure Electronic Health Records Using Fuzzy Commitment Scheme," *Security and Privacy,* vol. 5, no. 4, p. e231, 2022.

[23] L. S. U. D. Trealindora Marak, "Blockchain-Based Healthcare Record Management System," *International Journal of Engineering Applied Sciences and Technology,* vol. 6, no. 9, pp. 288-295, 2022.

[24] C. Cachin, G. Losa and L. Zanolini, "Quorum Systems in Permissionless Network," *arXiv preprint,* 2022.

[25] G. A. F. Rebello and e. al., "Security and Performance Analysis of Quorum-Based Blockchain Consensus Protocols," *2022 6th Cyber Security in Networking Conference (CSNet),* 2022.

[26] A. Baliga and e. al., "Performance Evaluation of the Quorum Blockchain Platform," *arXiv preprint*, 2018.

[27] K. P. R. E. Sudeep Tanwar, "Blockchain-Based Electronic Healthcare Record System for Healthcare 4.0 Applications," *Journal of Information Security and Applications,* vol. 50, 2020.

[28] U. Q. a. A. K. Shahnaz, "Using Blockchain for Electronic Health Records," *IEEE Access*, pp. 147782-147795 , 2019.

[29] J. X. K. L. S. T. H. H. J. H. P. &. Y. N. Xu, "Healthchain: A Blockchain-Based Privacy Preserving Scheme for Large-Scale Health Data," *IEEE Internet Things J.* , vol. 6, no. 5, pp. 8770-8781, 2019.