USABILITY OF BLOCKCHAIN TECHNOLOGY IN HEALTHCARE

A Thesis Submitted

In Partial Fulfillment of the Requirements

for the Degree of

DOCTOR OF PHILOSOPHY

by

Neetu Sharma

(2K19/PHD/EC/25)

Under the Supervision of

PROF. RAJESH ROHILLA

Department of Electronics and Communication Engineering

Delhi Technological University

Department of Electronics and Communication Engineering

Delhi Technological University

(Formerly Delhi College of Engineering)

Shahbad Daulatpur, Main Bawana Road, Delhi-110042, India.

December- 2024

ACKNOWLEDGMENTS

I would like to express my deepest gratitude to my supervisor, **Prof. Rajesh Rohilla**; without him, the completion of this PhD thesis would not have been possible. Their guidance, expertise, and unwavering support have been instrumental in shaping my research and nurturing my intellectual growth. I am thankful to **Prof. Prateek Sharma**, Vice Chancellor, Delhi Technological University, for providing an enriching academic environment and the resources necessary for my research. I would like to acknowledge the invaluable support of **Prof. O.P. Verma**, HoD, ECE, **Prof. Rajeshwari Pandey** and **Prof. Neeta Pandey**, who helped me access resources.

I want to thank my family for their unconditional love, encouragement, and understanding throughout this challenging journey. Your unwavering belief in me has been my greatest motivation. I am grateful to my friends and colleagues who have provided valuable insights, engaging discussions, and emotional support during the ups and downs of my research. I extend my appreciation to all the individuals who participated in my research, as their contributions were essential to the success of my work.

(NEETU SHARMA)

Delhi Technological University

(Formerly Delhi College of Engineering)
Shahbad Daulatpur, Main Bawana Road, Delhi-42

CANDIDATE'S DECLARATION

I, **Neetu Sharma**, roll no**. 2K19/PHD/EC/25**, hereby certify that the work which is being presented in the thesis entitled **"Usability of Blockchain Technology in Healthcare"** in partial fulfillment of the requirement for the award of the Degree of Doctor of Philosophy, submitted in the **Department of Electronics and Communication Engineering**, Delhi Technological University, Delhi, is an authentic record of my own work carried out during the period from **August 2019** to **December 2024** under the supervision of **Prof. Rajesh Rohilla**.

The matter presented in the thesis has not been submitted by me for the award of any other degree of this or any other institute.

Candidate's Signature

This is to certify that the student has incorporated all the corrections suggested by the examiners in the thesis and that the statements made by the candidate are correct to the best of our knowledge.

Signature of Supervisor(s) **Signature of External Examiner(s)**

Delhi Technological University

(Formerly Delhi College of Engineering)

Shahbad Daulatpur, Main Bawana Road, Delhi-42

CERTIFICATE BY THE SUPERVISOR(S)

Certified that **Neetu Sharma**, roll no. **2K19/PHD/EC/25,** has carried out their research work presented in this thesis entitled **"Usability of Blockchain Technology in Healthcare"** for the award of **Doctor of Philosophy**, from Department of Electronics and Communication Engineering, Delhi Technological University, Delhi, under my supervision. The thesis embodies results of original work and studies are carried out by the student herself and the contents of the thesis do not form the basis for the award of any other degree to the candidate or to anybody else from this or any other University/Institution.

(**Prof. Rajesh Rohilla**)

Professor at Department of Electronics and Communication Engineering

Delhi Technological University, Delhi-42

Date:

ABSTRACT

In this research, we explore how blockchain technology can improve the accuracy and security of critical healthcare data, such as electronic health records (EHRs), medical practitioner records (MPRs), telecare medical records (TMRs), Vaccination records, drug discovery and drug supply chain records.

Ensuring data integrity in these records is vital for preventing harm to patients and protecting public health. Blockchain features show great potential for enabling patients to verify that records created by various healthcare organizations are reliable and trustworthy.

We introduce blockchain-based systems for managing these records, providing benefits like accurate patient diagnosis, secure sharing of EHRs, and safeguarding against imposters in medical practice registration.

Additionally, we propose a system for real-time fitness monitoring and medication management through blockchain and smart devices, enhancing telehealth during pandemics. Each record in our systems is secured using the SHA-256 hash algorithm and has been successfully executed, demonstrating their suitability for managing EHRs, MPRs, and TMRs.

Another study focuses on creating a cost-effective blockchain solution for lifelong vaccination record management based on patient preference. It includes QR code-based validation and off-chain storage for scalability, offering an efficient and secure way to handle vaccination records. The smart contract has been successfully deployed and tested in the Remix IDE environment. Performance has been evaluated by analysing execution costs at different transaction sizes.

In drug discovery, collaboration and data integrity are crucial. We present a Hyperledger-based blockchain application that allows organizations to securely upload, verify, and manage contributions, aided by machine learning. This system promises a more secure and efficient drug development process. In this work, we have successfully built an end-to-end decentralised drug discovery application with a front-end interface and demonstrated chaincode algorithms. The end-to-end application is not available in any previous work.

Medicine counterfeiting is a global issue, and our proposal tackles it through a blockchain-based supply chain solution. Multiple organizations collaborate in a distributed network, enhancing transparency, security, and traceability. QR code watermarking adds an extra layer of security, ensuring only legitimate buyers can access products. The Caliper tool has been used to investigate throughput, latency, and resource statistics.

Our simulations and performance measurements show the effectiveness of these blockchain solutions in terms of scalability, validation, throughput, latency, and resource usage, offering promising benefits in the healthcare and pharmaceutical industries.

LIST OF PUBLICATIONS

Journal Publications

- Sharma N, Rohilla R. "A novel Hyperledger blockchain-enabled decentralized application for drug discovery chain management." Computers & Industrial Engineering 183 (2023): 109501. (**SCI indexed, Impact factor- 7.9**, **Elsevier)** https://doi.org/10.1016/j.cie.2023.109501

- Sharma N, Rohilla R. "A multilevel authentication-based blockchain powered medicine anti-counterfeiting for reliable IoT supply chain management." The Journal of Supercomputing 80.4 (2024): 4870-4913. (**SCI/SCIE indexed, Impact factor- 3.3**, **Springer)** https://doi.org/10.1007/s11227-023-05654-w

- Sharma N, Rohilla R. "A novel scalable and cost efficient blockchain solution for managing lifetime vaccination records based on patient preference" under publication in Int. J. of Electronic Security and Digital Forensics Inderscience (2023). (**Scopus indexed**, **Inderscience)** DOI: 10.1504/IJESDF.2025.10063362

- Sharma N, Rohilla R. "Scalable and cost-efficient PoA consensus-based blockchain solution for vaccination record management." Wireless Personal Communications (2024):1-31. (**SCIE indexed, Impact factor-2.2, Springer**) https://doi.org/10.1007/s11277-024-11115-1

Conference Publications

- Sharma N, Rohilla R. "Blockchain based secured telecare medical record management: A system design," Fifth International Joint Colloquiums on Computer Electronics Electrical Mechanical and Civil - CEMC 2020, Grenze International Journal of Engineering & Technology (GIJET) 7.1 (2021). (**Scopus indexed)**
- Sharma N, Rohilla R. "Blockchain based approach for managing medical practitioner record: A secured design." Advanced Computing: 10th International Conference, IACC 2020, Panaji, Goa, India, December 5–6, 2020, Revised Selected Papers, Part II 10. Springer Singapore, 2021. https://doi.org/10.1007/978-981-16-0404-1_6.
- Sharma N, Rohilla R. "Blockchain based electronic health record management system for data integrity." Proceedings of International Conference on Computational Intelligence: ICCI 2020. Springer Singapore, 2022. (**Scopus indexed)** https://doi.org/10.1007/978-981-16-3802-2_24.

TABLE OF CONTENTS

ACKNOWLEDGMENTS ……..……..……i
CANDIDATE'S DECLARATION…… ii
CERTIFICATE ……..……..iii
ABSTRACT ……..……...iv
LIST OF PUBLICATIONS....……vi
TABLE OF CONTENTS……..viii
LIST OF TABLES……...……xi
LIST OF FIGURES ……...……xii
LIST OF ABBREVIATIONS……...……xv
CHAPTER 1: INTRODUCTION ……...…...……1
1.1 Blockchain Technology……..……...7
1.1.1 Types of Blockchain……..……9
1.1.2 Consensus in Blockchain ……..……9
1.2 Scope of Blockchain in Healthcare……..... ……10
1.2.1 Scope of Blockchain in Drug Discovery Chain Management…….. ……..10
1.2.2 Scope of Blockchain Technology in Supply Chain Management ……...…11
1.3 Thesis Outline ……..…12
CHAPTER 2: LITERATURE SURVEY…...……...13
2.1 Literature Survey Related to EHR-Based Schemes…… ……13
2.2 Literature Survey Related to Vaccination-Based Schemes……..15
2.3 Literature Survey Related to Drug Discovery Chain-Based Schemes……..…17
2.4 Literature Survey Related to Supply Chain-Based Schemes……...19
2.4.1 Literature Survey Related to Blockchain Watermarking ……..22
2.5 Research Gaps ……..24
2.6 Motivation ……...……26
2.7 Problem Addressed…… ……..26
2.8 Research Objectives ……..……27
CHAPTER 3: METHODOLOGY……29

3.1 Ethereum Blockchain……29
3.2 Blockchain Scalability……30
3.3 Interplanetary File System ……31
3.4 Fundamentals Of Hyperledger-Fabric Blockchain……32
3.4.1 Consensus Mechanism ……33
CHAPTER 4: BLOCKCHAIN-BASED EHR, MPR, AND TMR MANAGEMENT SCHEMES……..34
4.1 Overview ……34
4.2 Proposed EHR Management System ……36
4.2.1 Architecture of EHR Management……36
4.2.2 Implementation and Simulation Results ……38
4.3 Proposed MPR Management System……42
4.3.1 System Structure of Developed MPR Management Model ……43
4.3.2 Implementation and Simulation Results ……44
4.3.3 Comparative Analysis ……45
4.4 Proposed TMR Management System……48
4.4.1 Architecture of TMR Management System ……49
4.4.2 Implementation and Simulation Results……52
4.5 Discussion.. ……55
CHAPTER 5: SCALABLE AND COST-EFFECTIVE BLOCKCHAIN SOLUTION FOR MANAGING VACCINATION RECORDS……56
5.1 Overview ……56
5.2 Proposed Work……57
5.2.1 System Architecture ……58
5.2.2 Workflow……60
5.2.3 Patient Preferences of Data Availability ……67
5.3 Simulation Results ……68
5.3.1 Computation of IPFS-Network Parameters……69
5.3.2 Computation of Probability of Data Availability ……70
5.3.3 Data Availability Analysis……71
5.3.4 Execution Cost Analysis ……74
5.3.5 Energy Efficiency Analysis……76
5.3.6 Comparative analysis ……77
5.4 Discussion.. ……80
CHAPTER 6: BLOCKCHAIN-BASED SCALABLE DRUG DISCOVERY CHAIN MANAGEMENT SCHEME……81
6.1 Overview ……81
6.2 Proposed Drug Discovery Chain Management Design……82
6.2.1 Use-case of Hyperledger-based Drug Discovery Chain……83
6.2.2 Layered Architecture……85

6.3 Design Implementation ……87
6.3.1 Development Environment ……87
6.3.2 Proposed System Assets ……88
6.3.3 Proposed Chaincode Modules……88
6.3.4 Architecture of Drug Discovery Scheme in the Hyperledger Environment ……..90
6.4 Results and Analysis ……...92
6.4.1 Simulation Results……...92
6.4.2 Performance Analysis….. ……100
6.4.3 Findings and Comparison……..103
6.5 Discussion…. ……104
CHAPTER 7: BLOCKCHAIN-ENABLED TRACEABILITY AND VALIDATION SYSTEM FOR MEDICINE ANTI-COUNTERFEITING.. ……106
7.1 Overview ……106
7.2 Proposed Medicine Anti-Counterfeiting Design……107
7.2.1 Proposed Use case ……107
7.2.2 Anti-counterfeited Supply Chain Components ……109
7.3 Design Implementation ……..112
7.3.1 Workflow ……...112
7.3.2 Development Environment……118
7.3.3 Hyperledger-based Supply Chain Architecture……119
7.3.4 Blockchain-based Watermarking (BCW) ……122
7.3..4.1 Embedding with BCW ……122
7.3.4.2 SHA 256 based Encryption ……..124
7.4 Simulation Results……..125
7.4.1 Simulation Results of the Implemented Chaincodes ……125
7.4.2 Result of BCW ……130
7.4.3 Performance Analysis of Fabric-based Framework ……..132
7.4.4 Performance Evaluation of BCW……..135
7.4.5 Comparative Analysis ...……137
7.5 Discussion…. ……139
CHAPTER 8: CONCLUSION, FUTURE SCOPE AND SOCIAL IMPACT…..……144
REFERENCES ……....148
LIST OF PUBLICATIONS AND THEIR PROOFS
PLAGIARISM REPORT
CURRICULUM VITAE/BRIEF PROFILE

LIST OF TABLES

Table 2.1: Details of existing electronic health record-based works……14

Table 2.2: Details of existing vaccination process-based works.……..15

Table 2.3: Details of existing drug discovery management works……..17

Table 2.4: Details of existing supply chains and drug counterfeiting works. ……..19

Table 4.1: Comparitive analysis of EHR work with prior works.……42

Table 4.2: Comparison between MPR work and prior works… ……..47

Table 5.1: Summary of notations……... ……..68

Table 5.2: Probability of data availability at 10% down nodes……72

Table 5.3: Probability of data availability at 20% down nodes…….……...72

Table 5.4: Probability of data availability at 30% down nodes…….……...73

Table 5.5: Execution costs of the smart contract functions…… ……..75

Table 5.6: Comparison of the vaccination scheme with prior works……. ……..77

Table 6.1: Specifications of the development environment. ……87

Table 6.2: Resource statistics of the drug discovery design. ……103

Table 6.3: Comparison of the proposed scheme with existing schemes…….. ……..104

Table 7.1: Specifications of the development environment……. ……..119

Table 7.2: Access rights of organizations in supply chain design……..……121

Table 7.3: Resource statistics of the supply chain design…….. 135

Table 7.4: Comparison of NC for QR Code Watermarking……. ……..136

Table 7.5: Comparison of PSNR, NC and SSIM under various attacks…….. ……..137

Table 7.6: Comparison of supply chain scheme with existing schemes…… 138

LIST OF FIGURES

Figure 1.1: Healthcare data breaches by year [2].....2

Figure 1.2: Blockchain applications in healthcare…….3

Figure 1.3: Illustrates a blockchain transaction…….8

Figure 3.1: Illustrates the benefits of Ethereum blockchain……..……..……29

Figure 4.1: Architecture of the EHR management system……...37

Figure 4.2: EHR modules of the designed system……... ……39

Figure 4.3: Simulation result of the EHR addition module……..40

Figure 4.4: Simulation result of the EHR retrieval module……. ……41

Figure 4.5: Use-case scenario of the MPR design……... 43

Figure 4.6: Architecture of the MPR management design…….……..44

Figure: 4.7. Simulation result of the MPR addition module…… 46

Figure 4.8: Simulation result of MPR retrieval module……...47

Figure 4.9: Use case scenario of the proposed TMR management system……..48

Figure 4.10: Architecture of TMR management system……..50

Figure 4.11: Illustrates the workflow of developed TMR management system….. ……51

Figure 4.12: Simulation result of TMR1 addition module…….. 53

Figure 4.13: Simulation result of TMR1 retrieval module……...……54

Figure 4.14: Simulation result of the TMR2 addition module…….54

Figure 4.15: Execution result of the TMR2 retrieval module…… ……..55

Figure 5.1: Traditional and proposed use-case scenarios……... ……..58

Figure 5.2: Architecture of the vaccination system……...……...59

Figure 5.3: Workflow diagram of the proposed syst…….. ……..61

Figure 5.4: QR code and information on the vaccination certificate……...62

Figure 5.5: Probability of data availability at 10% down nodes……..72

Figure 5.6: Probability of data availability at 20% down nodes……

……..73
Figure 5.7 Probability of data availability at 30% down nodes……. ……..74
Figure 5.8: Remix IDE interface representing the smart contract functions……...……75
Figure 5.9: Execution costs vs. transaction sizes……. 76
Figure 5.10: Block sealing process at node 1 and node 2…….. ……..77
Figure 6.1: Use-case scenario of the fabric-based drug discovery chain system... ……..84
Figure 6.2: Layered architecture of the drug discovery chain design…… ……..85
Figure 6.3: ML-based quality score analysis of searched targets……..……...86
Figure 6.4: Workflow of drug discovery management design…… …….90
Figure 6.5: Architecture of the proposed Fabric-based drug discovery design.……...91
Figure 6.6: Generation of digital certificates and channel artifacts……... ……..93
Figure 6.7: Docker containers of the drug discovery design……....94
Figure 6.8: Installation of the proposed chaincode…… ……..94
Figure 6.9: Web-interface to sign-in to the proposed Dapp……... ……..95
Figure 6.10: User interface to upload a new contribution……96
Figure 6.11: Back-end of Dapp to create a contribution asset……. ……97
Figure 6.12: User interface to issue a contribution certificate…… …….98
Figure 6.13: Back-end to creates the contribution certificate asset……..98
Figure 6.14: User interface to verify contribution assets……. 99
Figure 6.15: Back-end to validate the drug discovery contribution……... 100
Figure 6.16: Simulation result to measure performance using the caliper tool…….101
Figure 6.17: Performance analysis at different block sizes……102
Figure 6.18: Performance analysis at different numbers of endorsers……... 102
Figure 7.1: Traditional vs. proposed supply chain designs…….. ..108
Figure. 7.2: Architecture of the medicine supply chain…… ...……...110

Figure. 7.3: Illustrates the workings of various chaincode modules……... ……...114

Figure 7.4: Validation module to validate medicine consignment.
……..……..116

Figure 7.5: Validation module to validate the medicine strip and view module……117

Figure. 7.6: Architecture of the fabric-based drug anti-counterfeiting design……..120

Figure 7.7: Docker containers of the drug anti-counterfeiting design……. ...……...120

Figure 7.8: QR code watermarking using Blockchain……. ……..123

Figure 7.9: Simulation result to register a new company……
……...126

Figure 7.10: Backend to register a new company……..126

Figure 7.11: Simulation result to register a new drug……127

Figure 7.12: Backend to create a new drug asset……. ……..127

Figure 7.13: Simulation result to create a new purchase order…….. ……128

Figure 7.14: Backend to create a new shipment……129

Figure 7.15: Simulation result to retail medicine……...129

Figure 7.16: Backend to view medicine history.……130

Figure 7.17: Results of the QR code BCW validation process. ……...……..131

Figure 7.18: Histograms of crypto weight for the BCW operation.……...132

Figure 7.19: Extractions of watermark under various attacks.……...132

Figure 7.20: Simulation result of add drug API…….133

Figure 7.21: Performance evaluation based on numbers of transactions
……...133

Figure 7.22: Performance evaluation based on the number of peers……...……..134

LIST OF ABBREVIATIONS

EHR	Electronic Health Record
TMR	Telecare Medical Record
MPR	Medical Practitioner Record
DDoS	Distributed Denial of Service
TTP	Trusted third Party
ML	Machine Learning
PoW	Proof of work
PoA	Proof of Authority
PoS	Proof of Stake
IoT	Internet of Things
PHI	Personal Health Information
IPFS	Interplanetary File System
MCDM	Multi-Criteria Decision Making
HFS	Hesitant Fuzzy Set

PUF	Physical Unclonable Function
RFID	Radio Frequency Identification
DWT	Discrete Wavelet Transform
DRM	Digital Rights Management
RSA	Rivest Shamir Adleman
SVD	Singular Value Decomposition
EVM	Ethereum Virtual Machine
MSP	Membership Service Provider
CA	Certificate Authority
CC	Chaincode
UUID	Universally Unique Identifier
SHA	Secure Hash Algorithm
UI	User Interface
DAPP	Decentralized Application
CCP	Common Connection Profile
WHO	World Health Organization
TPS	Transaction Per Second
EQR	Encrypted QR
BCW	Blockchain-based Watermarking
PSNR	Peak Signal to Noise Ratio

CHAPTER 1

INTRODUCTION

One of the key aspects of healthcare is medical data [1], and healthcare data breaches are the major problem facing the healthcare sector. To request information, healthcare services use mobile apps and email. A minor flaw in the app or email can result in a security breach. Hackers steal healthcare data and trade stolen healthcare data for fraud activities. Through ransomware attacks, hackers are increasingly locking healthcare organizations data and demanding huge amounts of money to give the data decryption key. Even third-party stakeholders that offer services can create a security risk.

To control the data shared with stakeholders, a suitable information security policy that incorporates information security obligations into contracts is required. There have been more than 5,150 healthcare data breaches between 2009 and 2023. Figure 1.1 shows the healthcare data breaches by year. These breaches have caused the theft or loss of 382,262,109 healthcare records [2]. There are lots of issues in existing healthcare systems, like data integrity, security, privacy, availability, transparency, authentication, authorization, data breaches, backup, interoperability, access controls, audit trails and data duplicity.

To ensure that patients receive the right medication and treatment and to prevent harm from inaccurate past treatment records, the electronic health record (EHR) must be kept accurate. Healthcare organizations typically handle this kind of data through centralized systems that are vulnerable to ransomware and denial-of-service attacks, among other cybercrimes [3].

Confinement of various types of health records is a major concern [4]. Distributed ledger technology has attracted business owners from a variety of industries, including medicine [5].

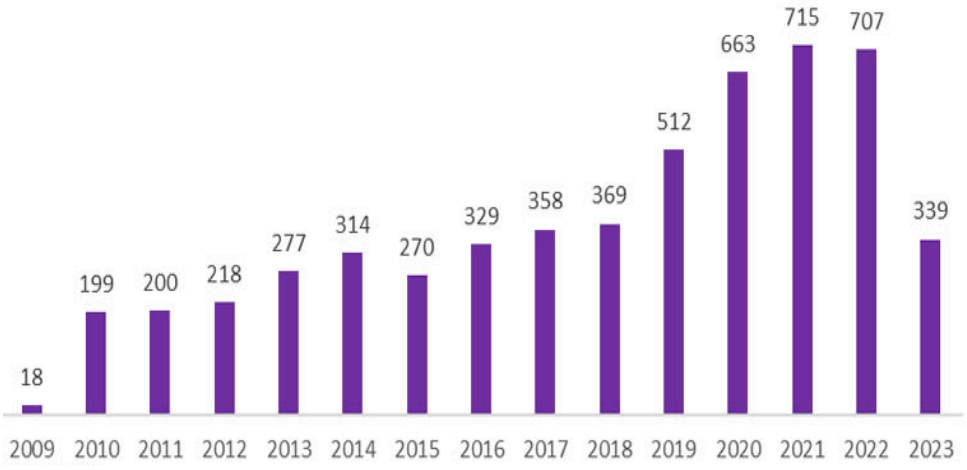


Figure 1.1: Healthcare data breaches by year [2].

Blockchain offers safe health data sharing in addition to enhancing digital data security, transparency, and reliability [6, 7]. Distributed ledger technology can be used to create a safe, cybercrime-free design for the exchange of health data [8]. Blockchain technology can be used to improve the healthcare record management system's complex nature [9]. Genomic data is just one type of health data that blockchain can handle effectively [10]. Blockchain gets rid of the need for a middleman in situations where cybercrimes are suspected to be involved [11]. Illegal access to health records is nearly impossible when they are stored in a distributed format [12]. Blockchain technology ensures that data cannot be tampered with during the exchange or sharing process [13].

Blockchain can prove to be the solution to issues in existing healthcare systems. It can be applicable in healthcare for various purposes, such as electronic health records (EHR), medical practitioner records (MPR), telecare medical records (TMR), vaccination records, drug discovery chains, and drug supply chain management. Figure 1.2 represents the blockchain applications in healthcare. The management of electronic health records (EHRs) is critical for improving patient care by providing easy access to medical information and increasing healthcare efficiency by reducing administrative burdens.

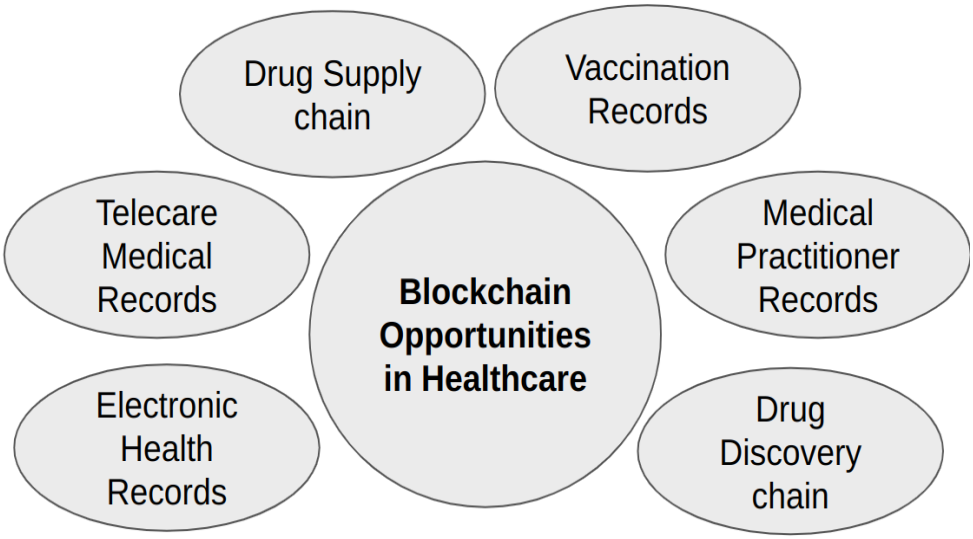


Figure 1.2: Blockchain applications in healthcare.

TMRs management is required to ensure remote access to patient data, allowing for timely and accurate diagnoses and treatment decisions, as well as improving healthcare accessibility and continuity. MPR management is critical for preventing fraudulent medical practitioners from affecting public health.

Vaccinations play a crucial role in protecting public health against infectious diseases. Vaccination needs to be a mandatory requirement imposed by the government on the public [14]. As governments seek to ensure widespread vaccination coverage, it is essential to explore mandatory vaccination requirements to protect communities from transferable diseases [15]. In the context of pandemics, vaccines not only save lives but also contribute to economic resilience [16]. Vaccines develop antibodies to protect the body against spreadable diseases [17]. The immunised public can contribute to a bigger umbrella of group invulnerability by preventing the spread of disease to individuals who aren't fully vaccinated.

Digitization has provided a practical solution for patients to access and manage their vaccination records efficiently. It has also facilitated the concept of immunity passports, serving as essential documentation for medical consultations, migration, education, and employment [18]. Digitization of vaccination records has alleviated the practical challenge of managing hardcopy records from various sources, enabling seamless record-keeping. However, this digital transformation has introduced new challenges related to data privacy and healthcare system integration.

Despite these advancements, improper management of vaccination data can lead to delayed or incorrect treatment, ultimately affecting public health. The exchange of digital information has increased significantly over the past ten years [19]. Resolving the issues with sharing personal information is significant [20]. A mechanism is required for maintaining data validity in a trustworthy and secured manner [21]. The lack of synchronization among different healthcare sector members working independently poses a significant challenge in integrating digital copies of individual records into a united repository [4].

Moreover, traditional healthcare systems rely on centralized databases to store vaccination records, which can be susceptible to single-point failures and vulnerable to various cyberattacks like Distributed Denial of Service (DDoS) attacks and ransomware incidents.

Blockchain is primarily for building trust, improving accessibility, security, integrity, confidentiality, and transparency [3]. These security weaknesses and lack of data integrity and interoperability in centralized systems may lead to record blocking and breaches, eroding public trust in healthcare providers [22]. To restore and enhance this trust, it is essential to leverage technology and implement innovative strategies for tracking and validating vaccination records by authorized entities.

COVID-19 has shown the importance of reliable systems [23] and [24]. It has brought distributed technologies, such as blockchain, for the handling of data on multiple nodes [25]. The applications of blockchain in cryptocurrency and the token marketplace are flourishing in the business community [26]. Blockchain is also well suited for healthcare applications such as drug supply chain and drug discovery chain management systems [27]. Moreover, the integration of blockchain with artificial intelligence presents an innovative business environment for healthcare management [28].

In cybercrime-prone environments, blockchain removes the need for a third-party trusted party (TTP) [29]. Centralised systems have no distributed controlling power [30], but blockchain guarantees distributed control so no one can alter data [3]. The optimization of storage pressure is required to utilise blockchain benefits in securing sensitive vaccination records and data obtained from smart devices [31]. Moreover, To fully realize the potential of blockchain for vaccination record management, governance policies are critical [32]. By leveraging blockchain technology and fostering collaborative efforts, healthcare organizations can establish a reliable, secure, and interoperable framework for vaccination record management.

Drug discovery is a multi-phase process that looks for novel ways to treat and cure illnesses. The finished drug must be safe, effective for the intended use, and compliant with the law. Drug discovery requires the placement of a wide range of national and international structures that are funded by health institutes [33]. In the pharmaceutical industry, finding and developing a new drug is an expensive and time-consuming process. A new drug's development typically costs about $985 million [34]. It takes 12–15 years to develop the approved medication [35].

The integrity of the contributions made by multiple organizations can occasionally be compromised by their involvement in the drug discovery process. A new drug's ability to reach the market and produce research value from patents can both be hampered by privacy and security concerns in the drug discovery chain [36]. Technical solutions for transparently sharing discovery chain data among multiple organizations must be investigated [37].

Pharma 4.0 is changing the conventional method of drug discovery through cooperation [38]. The pharmaceutical industry faces many obstacles when it comes to adopting new technologies [39] and setting up a safe, shared workspace where all parties can work together. Blockchain technology creates a multifunctional decentralized ecosystem. Instead of being held by a single entity, data in a blockchain is encrypted by a distinct hash value and accessible across several locations [40]. The European Commission claims that $20 billion is squandered annually trying to find innovations that have already been developed. The pharmaceutical industry is less threatened by the sharing of research failures because the company that owns them is doomed.

A blockchain-based framework can also be used to share research failures through the use of smart contracts. Machine learning (ML) has several applications in drug development, including molecular generation and drug screening [41]. Blockchain technology and machine learning (ML) can be combined to expedite the drug discovery process. Current drug development methodologies encounter various obstacles, such as the following:

- There is no atmosphere that encourages cooperation between the different drug discovery institutes.
- Concerns about the contribution and ownership of knowledge [42].
- Centralized systems maintain genetic data at one location only, making them prone to single-point failures like technical outages, cyberattacks, or natural disasters. A data

breach can lead to misuse due to the confidentiality of genetic information. These possibilities show the need of robust security techniques and distributed storage alternatives.

- Clinical trial phases are lengthy and expensive [43].
- During clinical trials, ensuring public protection and privacy is necessary to protect individuals from potential harm. Strict roules are followed to reduce risks, protect sensitive data, and avoid misuse of sensitive data. Identity of participants and personal details are anonymized to maintain confidentiality.

The serious effects of medicine counterfeiting on people's health and lives result in a significant number of deaths each year [44]. The Hyperledger-Fabric framework can be used to address drug counterfeiting problems that the pharmaceutical industry has long faced [45]. Blockchain encryption and QR verification together can improve the dependability of anti-counterfeiting measures.

Since supply chain middlemen can attack centralized solutions, a decentralized strategy is better for preventing counterfeiting. Additionally, it increases fault tolerance and reliability. The pharmaceutical industry can enhance drug safety, transparency, and traceability by utilizing blockchain technology [46]. It is essential to put in place a system to monitor the authenticity of products from production to consumption [47].

Supply chain sustainability is supported by blockchain's ability to automate verification, which creates built-in trust [15, 48, 49]. Blockchain systems assure customers of the quality of their products by enabling trust programmatically [50]. Studies validate the possible advantages of implementing blockchain technology in supply chain operations for manufacturers and consumers [51]. Prominent tech firms like IBM and Cisco are presently investigating blockchain-based remedies for healthcare, encompassing the prevention of counterfeit medications [52]. Blockchain-based solutions for tracking medications in the supply chain have already been introduced by startups [42].

However, practical implementation faces significant challenges [53]. Fast transactions, privacy, security, and scalability are necessary for enterprise solutions. It is crucial to examine how various obstacles to blockchain adoption in international trade interact [54].

1.1 Blockchain Technology

A blockchain is a decentralised computer network based on cryptography [55]. Blockchain nodes are computers that keep copies of the transactions and maintain the blockchain network. Blockchain is primarily used for recording or securely sharing transactions across multiple nodes [56] and for building trust. Satoshi Nakamoto founded the blockchain technology [57], and the bitcoin blockchain is the first application of the blockchain technology that evolved in 2008 for cryptocurrency transactions [58].

In a blockchain network, transactions are recorded inside the blocks. Every block is added after the consensus process. Blockchain databases are always online and transparent. So all permitted members with internet facilities can access transactions. Moreover, blockchain eliminates mediators, making systems cheaper and more streamlined. Since it is unchangeable, once recorded data cannot be changed and is always accessible. Additionally, users of blockchain-based systems can develop trust thanks to its transaction visibility features. The basic features of this technology are security, integrity, immutability, transparency, and transaction availability [59]. The detailed features are listed below:

- Free from intermediaries: The blockchain enables verification without the need for any third-party [60].
- Decentralised: The data is shared across each node in the blockchain network.
- Immutable: It is immutable. So, the data cannot be altered or deleted [61].
- Secure: It uses asymmetric cryptography to secure the data blocks [62]. Also, the current block is dependent on its previous block to complete the encryption process.
- Integrity and trustworthiness: All the transactions attach to the block after the process of trust verification through broadcasting, consensus, and auditing.
- Timestamp: All the blocks in the blockchain ledger are time stamped. It enables precise tracking of transactions or data changes.
- Data Availability: It is decentralized and allows lifetime data availability.
- Transparency and Transaction Visibility: The transactions that take place are visible to all authorized participants. It is transparent and preserves integrity and trust.

- Provenance: The records can be traced back to their origin.
- Consensus: Consensus mechanisms are needed to verify the transaction data, which avoids the hazard of a duplicate record.
- Smart Contract: Automatic transactions can be triggered with smart contracts using pre-set conditions.

Figure 1.3 illustrates a blockchain transaction. Whenever any user places a digitally signed transaction request, the requested transaction is flooded to all the nodes of the network through the gossip protocol [63].

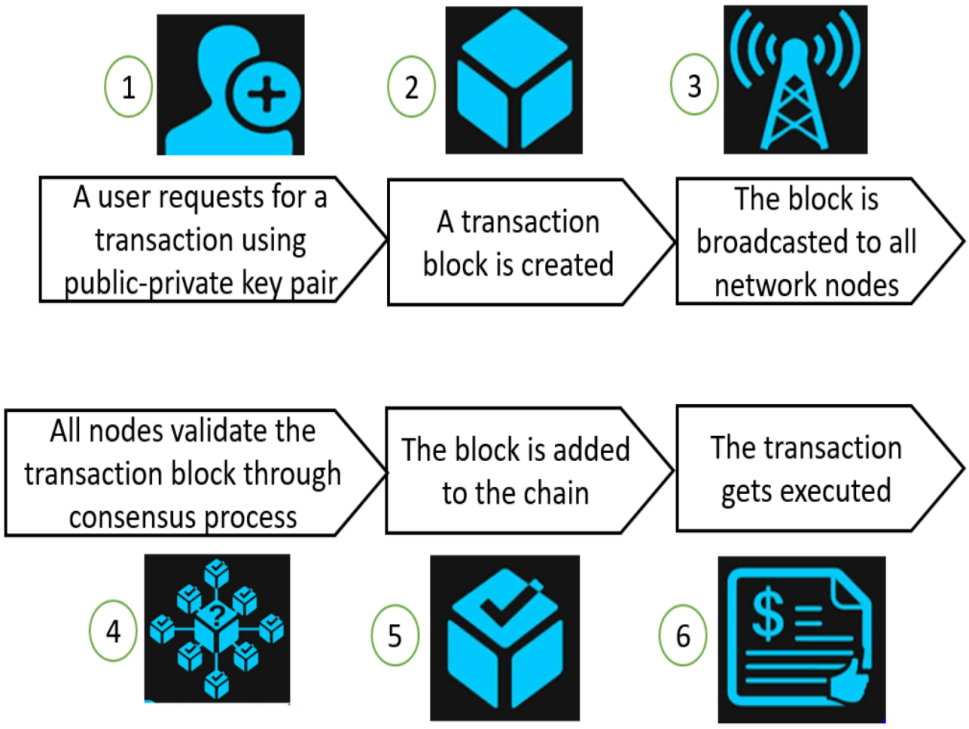


Figure 1.3: Illustrates a blockchain transaction.

Blockchain uses a pair of public-private keys to digitally sign transactions [64]. A transaction encrypted by a private key can be accessed by a corresponding public key. The private key is owned by the individual mmember only,and the public key is shared among all members across the blockchain network. The blocks are encrypted by hashes and each block hash can be calculated using the current block data, nonce, and the previous block hash [3]. The method of generating a valid hash for new block creation is known as mining. Mining involves complex math for finding a good nonce, satisfying difficulty and obtaining an acceptable hash. The difficulty level needs to be met to add blocks to the chain. Then a new

transaction block is created by the consensus process and broadcast to all other validator nodes. When all validator nodes come to a consensus, a new block is appended to the existing chain, and the transaction is executed. Any change in block data in the ledger requires re-mining all of the blocks that come after.

1.1.1 Types of Blockchain

There are three kinds of blockchain: public, private, and consortium [65] [66]. The public blockchain is non-restrictive in that anyone can join as an authorised node to perform, verify, and record transactions. E.g., Bitcoin is a public blockchain because anyone in the entire world can join as a node. Bitcoin is the first and most popular cryptocurrency (digital asset) [67]. The private blockchain is a restrictive one that only authorised users can join. The advantage of a private blockchain is that it has high transaction speeds. The weakness is that it is less secure and transparent. A consortium blockchain is a permissioned blockchain in which multiple organisations run a blockchain platform.

1.1.2 Consensus in Blockchain

In the blockchain network, mathematical algorithms are used to validate transactions and transaction blocks. These algorithms are called consensus mechanisms. The three most elementary consensus engines are PoW, PoA, and Proof of Stake (PoS) [55]. Every consensus mechanism has its uses, benefits, costs, and trade-offs. The consensus mechanism that involves complex mathematical algorithms and enormous computing power to confirm transaction blocks is known as PoW. The benefits of the PoW consensus engine are the high degree of decentralisation and security. Its limitation is that it consumes a lot of energy [68, 69].

The PoS resolves the issue of energy consumption existing in the PoW [70]. The benefits of the PoS are low block creation time and energy consumption. But, PoS is less secure and requires a monetary stake to validate the new block [71]. PoA is an improved version of the PoS consensus protocol for reaching consensus through authorised validators. In this consensus mechanism, a limited number of nodes have block sealing power, and the validator's identity is at stake, so any faulty behavior can damage the sealer's reputation. PoA is a viable alternative to PoW and PoS because of its cost-effectiveness, throughput, fault

tolerance capability and scalability features [72]. It is well-suited for applications that require users to trust validators.

1.2 Scope of Blockchain in Healthcare

This section describes the scope of blockchain in the healthcare sector, with emphasis on drug discovery and drug supply chain management.

1.2.1 Scope of Blockchain in Drug Discovery Chain Management

The advancement of drugs has a big influence on medical results. The entire process of development is exceedingly intricate, and the way it is handled will greatly influence the result. Better health outcomes can be attained sooner the faster a drug is developed [73]. Machine learning and blockchain technology have made this possible. A subset of artificial intelligence known as machine learning (ML) enables software tools to analyze and display data. Blockchain technology and machine learning (ML) can be used to pre-process drug development data, facilitate decision-making, and accelerate the drug development process. Blockchain regulates the verifiable and permanent recording of transactions across a network of entities as a distributed, immutable ledger [22]. Blockchain applications are being investigated in a variety of industries, including life sciences and pharmaceuticals. In addition to being the most widely used cryptocurrency application, blockchain can be utilized for health record management [74], digital forensic evidence management [75], code copyright [76], transparent voting systems [77], transparent voting systems [77], and smart home security [78, 79]. Because only authorized users have access rights, the advantages of blockchain can also be used for fair exchange [80], password recovery [81], and preventing hacker manipulation [82].

Furthermore, this emerging field can be effectively utilised for supply chain monitoring [83]. The pharmaceutical industry stands to greatly benefit from blockchain features such as integrity, confidentiality, safety, and decentralisation [46]. This technology has the inherent ability to overcome issues with record security [84]. The advantages of incorporating blockchain technology into the proposed drug discovery process are as follows:

- Removes the concern about the accuracy and ownership of drug discovery contributions.
- Provides verifiable and unchangeable databases for drug lead development, clinical testing, and analysis.
- Speeding up the drug development journey through the collaboration of all parties involved with secure data access.
- Provides a safe ecosystem for confidential patient data during clinical testings.
- A transparent, decentralized ecosystem lends credibility to the human engagement process.

1.2.2 Scope of Blockchain Technology in Supply Chain Management

Numerous industries, including the life sciences and pharmaceuticals, are investigating the use of blockchain technology for managing health records [22], practitioner data [3], medication supply chains, and other related issues. Supply chain traceability may be effectively addressed by blockchain technology. Pharma companies are able to track the journey of a product from manufacturing to delivery by digitizing assets and keeping a decentralized, immutable ledger of transactions [27].

The drug supply chain can be strengthened against pharmaceutical counterfeiting by combining blockchain technology with the Internet of Things (IoT). Using QR codes and barcodes, medicine units are tracked and authenticated by mobile apps with integrated security platforms. IoT assigns distinct identities to physical objects by connecting them to the internet through physical identifiers. Blockchain is useful in many different fields because of its characteristics, which include provenance, privacy, security, immutability, traceability, accountability, and transparency.The past five years have seen a tenfold increase in blockchain investments [42], with an emphasis on confidentiality and accountability [85]. Authorization, audibility, and privacy present difficulties for real-world applications [86].

1.3 Thesis Outline

In this thesis, while addressing problems in the healthcare sector, novel contributions based on blockchain technology in the field of healthcare are made. An introduction to the proposed research work and blockchain technology is presented in Chapter 1. A detailed literature survey for EHR, drug discovery and drug supply chain related works is covered in Chapter 2. Research gaps are identified, and the objectives of the thesis are formulated on the basis of the literature survey. The methodology of the research work, including the fundamentals of Ethereum and Hyperledger blockchains, is presented in Chapter 3. Blockchain-based EHR, MPR, and TMR systems are designed, implemented and tested in Chapter 4. A scalable Ethereum-based blockchain solution for managing vaccination records is proposed in Chapter 5. Hyperledger blockchain-enabled drug discovery and drug supply chain management solutions are proposed, and their performances are measured in Chapters 6 and 7. The summary of the results of the proposed schemes is presented in Chapter 8. The conclusions of the proposed work on blockchain-based healthcare applications and their future scope are drawn in Chapter 9.

CHAPTER 2

LITERATURE SURVEY

This chapter covers the prior work related to electronic health records, vaccination records, drug supply chains, and drug discovery chain management systems.

2.1 Literature Survey Related to EHR-Based Schemes

In [8], a blockchain-based, cyber-free approach to EHR sharing was introduced. Scalability and design testing are absent from this work. The author described a blockchain-based cloud-based medical information monitoring system in [87]. In [88], the author suggested securely exchanging cancer patients' genomic data. [89] provided an example of the difficulty in transferring the treatment case to a different healthcare facility due to latency.

In [90], a distributed technology-based electronic health record validation strategy was created. Blockchain-based secure EHR exchange was created in [91]. In [92], the system for certificate-free cloud-based medical data was investigated. In [93], a participant-oriented EHR structure was created. Research was done on the application of blockchain to electronic health records in the healthcare industry in [94, 95]. Table 2.1 shows a summary of existing electronic health records-based schemes.

Table 2.1: Detail of existing electronic health record-based works.

Existing Scheme	Objective	Drawbacks
[8]	Created a blockchain-powered EHR interchange platform.	Design testing is lacking, and scalability is not addressed
[96]	Created a blockchain-based platform to manage personal health information (PHI).	Lack of design architecture availability
[97]	Proposed an EHR model with cloud assistance	There is no discussion of scalability
[98]	Suggested utilizing blockchain technology to create a scalable e-health management system.	There is no scalability testing conducted for numerous clinical trials.

A blockchain-based system for professional fitness monitoring data sharing was created in [96]. For this work, the architectural design was not available. In [97], a secure electronic health record system with cloud support was created. Scalability is not discussed in this work. A blockchain-based scalable electronic healthcare system for medical records was created in [98]. This work does not perform the scalability testing for multiple clinical trials. Options for sharing medical records were assessed in [99].

An efficient and personalized blockchain-based telemedicine system was proposed in [100]. A distributed ledger technology-based cloud-assisted medical information sharing model is created in [101]. A blockchain-based defensive health data sharing mechanism was investigated in [102]. In [103], a prototype for access control based health record management was recommended. In [104], a design for an integrated medical record handling solution was presented. According to an evaluation published in [105], blockchain-based systems are more complex than conventional sharing systems. Options for exchanging health information were assessed in [106]. A review of the literature demonstrates that blockchain's many benefits, including security, immutability, transparency, and provenance of the stored data, make it suitable for EHR management.

2.2 Literature Survey Related to Vaccination-Based Schemes

To fully leverage the potential of blockchain technology, addressing scalability is a critical area that requires further research [107]. A summary of the existing vaccination process-based schemes is presented in Table 2.2.

Table 2.2: Details of existing vaccination process-based works.

Existing Scheme	Objective	Limitation
[14]	Created a blockchain-based prototype of vaccination system	Restricts certificate validation rights
[15]	Proposed an intelligent system for vaccine supply using blockchain	Restricts certificate validation rights
[16]	Presented the methodology for storing vaccination records using blockchain	Not cost efficient
[17]	Described the usability of blockchain in supporting vaccination process	Scalability is not addressed, is not cost efficient, lacks cost analysis
[18]	Proposed an app for covid 19 vaccination certification	Scalability is not addressed, lacks cost analysis
[108]	Presented digital health passport using blockchain	Privacy issues due to use of public IPFS network
[109]	Proposed digital vaccine passport system using blockchain	Scalability is not addressed
Proposed	Proposed Cost-efficient and scalable blockchain-based vaccination record management system using private-IPFS network	Addressed scalability, cost efficiency and data availability

In [14], a prototype of a blockchain-based system aimed at securing the vaccination process has been developed, and a blockchain-based approach for vaccine supply monitoring is proposed in [15]. However, the performance of these

works has not been analyzed. Moreover, both of these systems utilize a private blockchain, which restricts the right to validate vaccination certificates to authorized individuals only. Another design, presented in [16], attempts to manage vaccination records, but it is not a cost-efficient approach. Similarly, the role of distributed technology to improve the vaccination process is explored in [17], and in [18], a decentralized application is developed to support the record-keeping of COVID-19 test reports and vaccination certificates. However, these designs lack in terms of scalability, lack of cost analysis, and limited functionality; thus, they are not entirely cost-efficient. Digital passport systems using blockchain are proposed in [108] and [109]. The first system raises concerns about privacy issues due to its reliance on the public interplanetary file system (IPFS) network, and the second system faces challenges related to scalability.

In the review of applications of blockchain in healthcare information management [110], this system is found to focus on theoretical contributions, lacking practical implementation. Additionally, a cloud-supported electronic health (eHealth) system proposed in [111] fails to address scalability concerns. In [112], a blockchain-based system for health data management is designed and validated, but it lacks performance analysis. Moreover, in [113], a healthcare data securing and exchanging system is suggested, but the use of a private blockchain restricts validation rights. The proposal in [114] introduces a cost-efficient healthcare data security system using on-chain and off-chain storage, but it lacks performance analysis. Similarly, the architecture for deploying blockchain technology in the healthcare domain presented in [104] lacks both cost analysis and validation mechanisms.

In contrast, the proposed work in this study adopts a PoA Consensus-based blockchain for managing patients' lifetime vaccination records. It boasts more smart contract functionalities, providing coverage of the entire vaccination process at a lower execution fee. Moreover, to enhance scalability, availability, and storage cost reduction, the complete data is stored off-chain based on patient preference, and only the hash of the vaccination record is recorded on the Ethereum blockchain. We have also presented the performance evaluation. Additionally, the study investigates data availability on the private IPFS network

based on patient preference. Network parameters are examined to achieve optimal data availability at a low storage cost.

Thus, this section emphasizes that blockchain design plays a crucial role in ensuring the immutability, transparency, integrity and accessibility of recorded data. The studies suggest that blockchain can prove to be the most effective tool for vaccination record management. By addressing existing limitations and incorporating advanced functionalities, blockchain technology can significantly improve various aspects of healthcare data management and ultimately enhance the vaccination process and public health outcomes.

2.3 Literature Survey Related to Drug Discovery Chain-Based Schemes

This section discusses existing drug discovery schemes as well as blockchain-based schemes. Target molecule identification, fusion, verification, optimization, and other processes are all involved in drug discovery. In [35], the author gave a summary of the drug development procedure. There is no practical application of this work. The Hyperledger framework was used in the construction of the drug discovery model in [36]. This work lacks design architecture, algorithms, and validation mechanisms. Table 2.3 depicts a summary of existing schemes.

Table 2.3: Details of existing drug discovery management works.

Existing Scheme	Objective	Drawbacks
[36]	Developed a Hyperledger-based collaborative drug discovery model.	lacks algorithms, validation procedures, design architecture, and demonstration
[37]	A proposed database for collective drug development services	centralised
[38]	Centered on the drug discovery process's clinical testing stage	Conclusions drawn from scholarly journals

[73]	Discussed how blockchain technology can be used to manage drug cycles.	Only ideas in theory
[116]	Offered a cloud-based platform for drug discovery researchers to work together.	less secured
[120]	Proposed use of blockchain technology to transform failed research projects into a value-creation model	Only the design concept is being developed, not the solution.
Proposed	Proposed scalable Hyperledger blockchain-based drug discovery chain management scheme	Created and tested end-to-end design and addressed scalability

In [37], the author proposed a database-based collective drug development service. This was a centralized (single-custody) database, making it less reliable. The authors of [38] concentrated on the clinical testing stage of drug discovery. The conclusions of this study have not been empirically proven. The authors of [39] discussed the challenges of using emerging technologies to validate smart pharmacovigilance devices. The authors of [41] focused on the use of cloud computing for ML modeling in drug discovery. [73] describes the use of blockchain for complete drug cycle management. In the drug development process, chemical identifiers that are used to identify the chemical structure of substances are represented as strings, also known as InCHI [115]. The authors of [116] presented a cloud-based solution for collaborating drug discovery researchers to share databases. The goal of this work was to improve the drug development process. This scheme is devoid of integrity and security. The author raised the issue of information security in cloud computing in [87].

The authors used the Caliper tool to measure the performance of the Hyperledger network under test in [117] and [118]. Both types of performance analysis are carried out on a smaller number of organizations. The author emphasized Hyperledger Fabric's accountability feature in [119]. The authors of [120] stress the application of blockchain technology to transform research failures into models for value creation. This survey provided a design concept and not solution implementation. This sub-section demonstrates the value of adopting blockchain for managing drug discovery contributions.

2.4 Literature Survey Related to Supply Chain-Based Schemes

The details of existing supply chains and drug counterfeiting work is presented in Table 2.4. A literature review on the use of blockchain in medicine is presented in [42]. This study included only theoretical concepts and not design implementation. A new medicine supply chain management system that uses blockchain technology on the Hyperledger Fabric platform to safely share medical supply chain records was presented in one of the studies [44]. There are no drug tracking or validation systems in this study.

Table 2.4: Details of existing supply chains and drug counterfeiting works.

Existing Scheme	Objective	Drawbacks
[42]	To utilise blockchain in medicine	Only theoretical concepts
[44]	To suggest a new model for the supply chain of medicines for a smart hospital	Absence of drug monitoring and verification systems
[46]	To create a medication supply chain that is Hyperledger enabled	Absence of a drug validation system
[83]	To create a textile industry supply chain that is enabled by Hyperledger	lacks mechanisms for product validation, scalability, and design algorithms
[121]	Introducing the Gcoin blockchain to facilitate easy medical transactions	Just the design concept; do not develop a solution
[122]	To investigate the application of blockchain to supply chain multicriteria decision making	There is no implementation available.
[123]	To examine how new technologies are being used to combat phony medical claims	Only ideas in theory

[125]	Utilizing blockchain technology to track supply chain transactions	inadequate application of design
[9]	To assess how well the blockchain-based healthcare system is performing	Scalability issue
[113]	To suggest a healthcare system powered by Hyperledger	Not scalable,
[126]	To suggest an anti-counterfeit supply chain based on blockchain	less maintaining privacy and less scalable
[127]	To suggest a method for integrating blockchain technology with IoT data collection modules by utilizing a fuzzy logic model	less private-preserving and less scalable
[128]	To suggest a method for user authentication	limited assessment of performance
Proposed	Multi-tier authentication and blockchain-based anti-counterfeiting methodology for medicines	enhanced performance, design implementation, scalability, product validation, authentication, and access control

It reveals that a large number of earlier works had inadequate design development and lacked validation, scalability, and traceability mechanisms. A supply chain design using blockchain technology and traceability features was shown in [46]. Additionally, this study lacks validation procedures. It was suggested in [83] to use GPS location traceability for supply chain verification; however, the suggested design is devoid of validation mechanisms.

In order to stop the sale of fake medications, a different study [121] presented the Gcoin blockchain for transparent transactions in the medical field. This study presents design concepts only, not solution implementation. [122] covered the significance of blockchain technology in a number of industries, including food and medicine. Additionally, rather than implementing a solution, this study presented theoretical contributions.

The medical supply chain is highlighted as a promising area for research in [123], which also identifies the challenges associated with the current healthcare

blockchains. Blockchain technology was found to be the most promising approach in [124], which compared several established and cutting-edge technologies for combating drug counterfeiting. Without making any new discoveries, this study reviewed the body of work that has already been written in the area. In [125], a blockchain-based framework for enhanced supply chain management is suggested. There is no design implementation in this work. With transaction rates of up to 250 and 10,000, respectively, performance assessments of blockchain-based healthcare systems utilizing the Hyperledger Fabric framework are carried out in [9] and [113]. Scalability issues plague these works. It was discovered that the computationally costly testing in [9] was restricted to a maximum of 250 transaction rates. With respect to [26], their system was unable to accommodate more than 4 users within the 10,000 transaction limit for their performance evaluation.

On the other hand, we have effectively tested our suggested system up to 100,000 TPS, proving its increased performance and scalability. Access control, tracking, privacy, scalability, and multi-level authentication features are critical for guaranteeing security in the supply chain management of medications. The proposed work provides a mechanism for validating products in addition to these features. A blockchain-based counterfeit-proof supply chain strategy that makes use of Ethereum blockchain technology and radio frequency identification (RFID) was put forth by the authors in [126]. This work's use of the public blockchain makes it less scalable and privacy-preserving. There can only be 600 transactions in the performance evaluation, and the maximum throughput and latency are 60 TPS and 1600 ms, respectively. Additionally, the range of product traceability is lowered by the use of RFID. By using the Hyperledger framework and IoT technology, the suggested work enhances privacy, scalability, and real-time monitoring over extended distances. Furthermore, the suggested work's performance is assessed up to one million transactions, with a maximum throughput of 417.5 TPS and a latency of 0.15 s. In addition, we assessed performance metrics based on the number of peers, including execution time, throughput, and latency.

Using a fuzzy logic model, the authors of [127] integrated the Ethereum blockchain with IoT data collection modules. This work's use of the public

blockchain makes it less scalable and privacy-preserving as well. The authors of [128] described a method of user authentication that combined access control, blockchain technology, and a physical unclonable function (PUF). The focus of this work is not on product traceability. Furthermore, there is a 1000 transaction cap on the performance evaluation. The proposed Hyperledger-based design offers better performance and more scalability than these Ethereum-based works.

A product certification program for automotive supply chains was put forth in [129]. The Hyperledger Besu blockchain, an Ethereum client created under the Hyperledger brand, is utilized in this work. Nevertheless, the study found that there were delays and significant transaction costs in the implemented blockchain network. A deep learning-based supply chain management attack prediction mechanism was presented in [130]. This study was not concerned with creating a defense but rather with identifying attacks.

In [131], a decentralized storage strategy for data protection based on blockchain technology is examined, with a focus on the system's security and privacy features. A blockchain-based supply chain model for personal protective equipment is proposed in [132] as a response to the COVID-19 pandemic, with the goal of improving traceability and efficiency in the distribution of necessary supplies.

Overall, previous research suggests that new digital technologies like blockchain and the Internet of Things could improve supply chain systems' reliability, transparency, and efficiency.

2.4.1 Literature Survey Related to Blockchain Watermarking

To improve the precision and security of QR code anti-counterfeiting methods, a large amount of research has been done. The use of anti-counterfeiting watermarking techniques as a substitute to stop the duplication or fabrication of QR barcodes was covered by the authors in [133]. They emphasized key algorithms that make it possible to create digital QR barcodes. For labeled QR codes, a multi-channel-robust watermarking system using the discrete wavelet transform (DWT) was presented for QR code validation in [134]. The goal of this

technique was to increase printed QR code security. An anti-counterfeiting technique based on statistical analysis of a single related feature differential sequence of a critical region was introduced in [135]. The procedure used a bone width transformation algorithm, supervised and assisted segmentation techniques, and inks to generate random, delicate texture patterns. It also identified important areas of sample photos. A QR code-based watermarking technique for protecting digital photos was investigated in [136]. The QR code framework's high information capacity and error correction capabilities made it a good choice for watermarking. The security and resilience of the QR code watermarking system against frequent digital photo attacks were the main topics of the study.

A demonstration of QR code-based image watermarking using the DWT transform domain within the framework of digital rights management (DRM) was presented in [137]. By using watermarks, this method was meant to safeguard digital photos. In [138], a dual anti-counterfeiting approach for QR codes that combined digital watermarking and encryption frameworks was presented. The process included using RSA-based encryption to encrypt authorization data, creating an image watermark from the encrypted data, and applying DWT and singular value decomposition (SVD)-oriented methods for embedding image watermarking and anti-print extraction. In [139], it was covered how to use QR codes to speed up data transfer in medical settings. The study used cutting-edge encryption standards to secure the data contained in QR codes and concentrated on creating a platform for medical data in health files.

In [140], DWT-based watermarking methods for color image security were introduced. These methods made use of bit plane complexity (Blockchain) and edge detection. The watermark embedding process made use of the HH element of the DWT transform domain. The method's effectiveness was assessed in a range of watermark attacks. In an effort to improve the security of digital images, effective watermarking methods for digital color images were presented in [141] that combined encryption with blockchain technology and DWT edge coefficients. Comparably, edge detection-based watermarking methods were put forth in [142], highlighting how crucial it is to include edge data when watermark embedding.

Overall, by investigating different approaches and assessing their security, resilience, and performance under various circumstances and attacks, these studies have advanced the field of QR code anti-counterfeiting and watermarking.

2.5 Research Gaps

- After reviewing the literature, we identified that there is a need to explore the patient centric requirements of healthcare sector. Lack of security and trust in centralized healthcare system causes information and innovation to be blocked. This results in delayed availability or sometimes unavailability of past treatment records to provide better treatment and discovery of new insights for improvement in public health. Also, such systems are not patient oriented so the privacy of sensitive health information is not ensured.

- Traditional healthcare systems are prone to various attacks like DDoS, ransomware, etc. Even hackers use student data (especially medical student data) to create fake identities. There have been several incidents of physical injury and the possible death of patients due to medication errors caused by fake practitioners. The healthcare sector is missing a system to validate medical practitioner’s identities.

- Remote healthcare is needed in pandemics for real time fitness monitoring and medication. Telemedicine overcomes the practical difficulty of visiting clinic and provides virtual consulting between doctor and patient. But such system needs to be safe. There is lack of management to synchronize functioning of different members in existing healthcare system.

- Medicine counterfeiting is one of the biggest problems occurring due to various loopholes in existing supply chain management. Innovative strategies to track and validate all medicinal products at each stage are required to avoid harm due to fake medicines. The existing supply chain approaches only provided the framework and theoretical solutions and did not include the implementation. The supply chain's transportation and logistics are essential components, and blockchain technology can

improve their efficiency. Even though blockchain technology is still in its infancy, efforts are being made to overcome throughput, scalability, and speed issues. Restrictions on access would be extremely beneficial for use cases like the supply chain for medications. The majority of previous studies assessed the functionality of their 1000 transaction limit designed systems. In order to effectively combat counterfeiting and save lives, we made the decision to develop a transparent and reliable blockchain-based solution for managing the medicine supply chain. We used a multi-level authenticity mechanism and conducted more transactions to gauge performance.

- Confidentiality and providing ownership to contributors are major concerns when handling drug discovery chain data. We could locate only one previous blockchain-based drug discovery study. A design architecture, chaincode algorithms, validation procedures, ideal scalability, and end-to-end development were absent from this work. We made the decision to use blockchain and machine learning to develop a novel framework for tracking contributions in a drug discovery process. The safe, efficient, and quick development of new drugs can be aided by this framework. It can guarantee ownership of research contributions, confidentiality, integrity, and openness. All authorized participants in the drug discovery process can have access to validated information on the blockchain. This may eventually result in a faster time to market by lowering the overhead associated with data transfer processing.

- Scalability issues need attention when handling huge amounts of data, such as public vaccination data, and global recognition is also required. The existing blockchain-based vaccination works have limited smart contract functionality, scalability, high execution costs, and storehouse cost issues. Also, the existing systems use PoW consensus engines that are very energy-consuming. In order to control the data shared with stakeholders, an appropriate information security policy is required. It can be done by adding access controls as security provisions as part of the contract. We decided to create novel smart contract algorithms that will cover the entire vaccination process for a low execution fee. For improved

security, privacy, scalability, availability, and decreasing storehouse costs, we only store the hash of the vaccination record in the blockchain. The actual data is stored in the IPFS (Interplanetary File System).

2.6 Motivation

The digitization of the medical record has created a new challenge for securing sensitive health information. Lack of security, integrity and proper management of healthcare data causes delayed or incorrect treatment, which consequently affects public health. It is difficult to synchronize functioning of different members of the healthcare sector that work independently. So integrating them together is a big issue. Traditional Healthcare systems maintain records in centralized systems, which may suffer from single point failure and are also prone to various attacks like DDoS, ransomware, etc. Lack of security, integrity and interoperability in centralized systems causes record blocking and breaches. As a consequence, public is losing trust in healthcare providers, which needs to be created by means of technology. Innovative strategies to track and validate medical records by all authorized members and secure the sharing of data to deal with pandemics and threats are required.

Blockchain can prove to be the smart solution to problems in existing healthcare systems by preventing unauthorized access, but the use of blockchain in healthcare is in an immature stage. So the necessity of blockchain-based, secured and distributed storage systems for improving healthcare performance and building trust has motivated me to work in this area.

2.7 Problem Addressed

This thesis work is focused on the development of robust blockchain-based healthcare solutions. Potential issues in existing blockchain-based systems are identified, and untouched work is also identified. How systems for managing healthcare records such as EHR, MPR, TMR, vaccination records, drug discovery and drug supply chain records can be made more reliable using blockchain and

how the scalability issue in blockchain can be tackled to ensure the sustainability of blockchain-based solutions. Proper design, implementation and performance testing of blockchain solutions need to be addressed.

2.8 Research Objectives

This work is focused on exploring the requirements of healthcare sector and designing blockchain-based systems to address those requirements. The objectives of this work, based on requirements of different healthcare applications, are listed below:

- To design blockchain-based, secured medical practitioner record management system

This is to be designed to validate medical practitioner's identity before consulting practice and onboarding in any health organization. This keeps fraudulent medical professionals from jeopardizing the health of the general public. This also enhances the trust factor to ensure health improvement.

- To develop blockchain based secured telecare medical record management system

This is to be designed for secured uploading and retrieval of real time fitness monitoring and medication data using blockchain technology and smart healthcare 'devices. This system permits healthcare providers to gain fast access to the fitness tracking data of patients in order to prescribe suitable medication over a blockchain network. This system can prove to be a very beneficial mechanism to secure telehealth in pandemics by sharing without violating privacy.

- To design medicine traceability and validation system to combat medicine counterfeiting.

This helps in detecting and preventing medicine counterfeiting in order to protect the health of the public. This requires blockchain technology in integration with IOT for tracking and validating medicinal products. The security features are

medical product validation, access controls, user authentication, collusion resistance, tamper-proof storage and data encryption keys.

- To develop a blockchain-based, scalable drug discovery chain management system.

This helps in maintaining the confidentiality of drug discovery data throughout the drug development process in a secure manner. The security features are access controls, data integrity validation, confidentiality, availability and authorization mechanisms.

- To develop a blockchain-based, scalable and optimal vaccination record management system.

This helps in handling the huge amount of public vaccination data by improving scalability.

CHAPTER 3

METHODOLOGY

This chapter contains the fundamentals of Ethereum and Hyperledger Fabric Blockchain.

3.1 Ethereum Blockchain

Ethereum is a platform for building blockchain-based distributed applications. Ethereum was founded by Vitalik Buterin in 2013 and is popular for executing smart contracts. Smart contracts have increased blockchain applications tremendously [70]. Smart contracts are computer programs stored on a distributed ledger that execute transactions automatically when certain criteria are satisfied. Other than smart contracts, it offers various benefits, such as immutability, transparency, security and decentralisation.

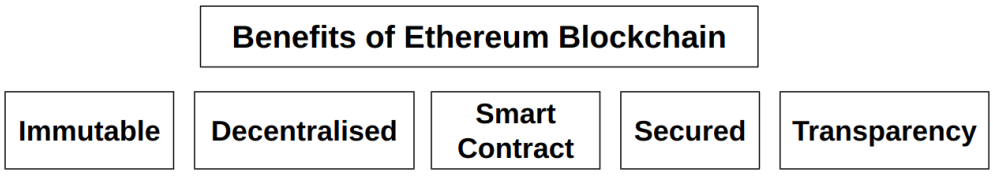


Figure 3.1: Illustrates the benefits of Ethereum blockchain.

Machines can execute smart contracts that are compiled into the Ethereum Virtual Machine (EVM) bytecode. The Ethereum transaction includes the following components:

- From: The transaction sender's 20-byte address.
- To: The transaction recipient's 20-byte address.
- Value: The sum of money (wei) sent from the sender to the recipient.
- Data: It contains transaction inputs.
- Gas: The amount needed to complete a transaction is measured in gas.
- Gas Price: The amount of ether the sender is willing to pay to run the transaction for each unit of gas.
- Gas Limit: Maximum gas set by the sender for the transaction.

3.2 Blockchain Scalability

Currently, the blockchain has a scalability issue that limits its usability in various applications [143]. Scalability means the limited capability of a highly distributed network to handle a huge number of transactions and update ledgers in a short amount of time. The transaction per second can be calculated using the following mathematical formula:

$$\text{Transactions per second} = \text{Transactions per block} / \text{Block generation time} \quad (3.1)$$

The above equation shows that to increase transaction speed, transactions per block should be high and block generation time should be low. But block generation time is generally fixed by the blockchain platforms to maintain the network. The transaction per block can be calculated using a mathematical formula:

$$\text{Transactions per block} = \text{Block size} / \text{Average transaction size} \quad (3.2)$$

The above equation shows that transactions per block can be increased either by increasing block size or by decreasing the average transaction size. An increase in block size can destroy harmony in the blockchain network by splitting the community. The PoW, which is a traditional cryptocurrency-based system, is an

energy-inefficient consensus engine [144, 145]. So the throughput can be improved by switching from PoW to PoA. PoA increases transaction speed, reduces the wastage of energy by all validators, and also prevents the 51% attack. On-chain scaling increases the block size, and optimising consensus mechanisms degrades decentralisation and security. Hence, the storage efficiency of smart contracts needs to be improved to increase the overall throughput [146]. This can be done by creating a lightweight blockchain using off-chain storage.

3.3 Interplanetary File System

The IPFS is a peer-to-peer file-sharing system for off-chain storage of large amounts of data [55]. Off-chain scaling can be done through IPFS without the involvement of a blockchain network. It is a protocol for peer-to-peer secure data storage, as all the data files kept on IPFS are encrypted by a cryptographically generated hash value. It reduces the computational overhead of mining large data files. IPFS allows users to store and share data files in the network by their content address instead of their location address. Everyone can access the data on the public IPFS network. Patients need complete control over their information, so making it publicly accessible is not an option. Private IPFS permits only connecting to other peers who have a shared secret key. With private IPFS networks, privacy can be achieved. The key features of the IPFS are as follows:

- Content Addressing: IPFS uses content addressing rather than addressing files according to their location or particular server. Files are identifiable by their content hash, which is derived from the information contained in the file. This guarantees that the material is verifiable and unchangeable.

- Decentralisation: IPFS works as a peer-to-peer network, which means that files are dispersed throughout a network of nodes (computers) as opposed to being kept on a single server. This decentralised architecture improves fault tolerance and reduces reliance on single points of failure.

3.4 Fundamentals Of Hyperledger-Fabric Blockchain

The proposed work utilizes a private Hyperledger blockchain, recognized for its superior efficiency and energy-saving attributes compared to public blockchains. Hyperledger Fabric, a notable enterprise-ready solution within the Hyperledger open-source project hosted by the Linux Foundation, offers a range of features including network security, privacy preservation, real-time tracking, reliability, fault tolerance, scalability, privacy, and access restrictions.

Within the Hyperledger network, key components play pivotal roles:

- Channel: Facilitates data compartmentalization among network stakeholders.
- Assets: Represents the tracked and stored data on the network.
- Transaction: Enables the alteration of asset states within the network.
- Ledger: Maintains a list of transactions and corresponding asset states.
- World state: Represents the current state of all assets and associated transactions.
- Smart contract (Chain code): Contains logic for executing transactions and modifying asset states.
- Peer: A computing resource participating in the network.
- Ordering service: Receives transactions from peers, sequences them into blocks, and writes them onto ledgers.
- MSP (Membership Service Provider): Offers credentials or IDs required by applications to interact with the network in this permissioned environment.
- Certificate authority (CA): Issues certificates to distinguish elements within the network.
- Anchor peer: Designated by each organization, responsible for maintaining communication with Anchor peers from other organizations.

- Committer: Writes or commits blocks published by the ordering service onto the ledger. Any channel-affiliated peer can act as a committer for a transaction.
- Endorser: Simulates incoming transactions, forwards them to the ordering service. A peer becomes an endorser if it has a deployed chain code.

3.4.1 Consensus Mechanism

To secure and promptly validate transactions while minimizing resource consumption, Hyperledger blockchains leverage efficient and time-effective consensus algorithms. Hyperledger Fabric adopts a pluggable consensus architecture, allowing users to select from various consensus mechanisms tailored to their network requirements. This adaptability proves especially valuable in enterprise scenarios where diverse networks may adhere to different trust models and performance criteria.

Hyperledger Fabric supports several consensus mechanisms, including Solo, Raft, and Kafka, each outlined below:

- Solo Consensus: Hyperledger Fabric features Solo, a straightforward, single-node consensus mechanism suitable for development and testing purposes.
- Raft Consensus: Raft, a fault-tolerant, replicated consensus algorithm, enables users to configure a group of nodes as orderers, collectively ordering transactions and generating consistent blocks.
- Kafka Consensus: Utilizing the Kafka messaging system, this consensus mechanism orders and distributes transactions to peers, offering high throughput and scalability.

CHAPTER 4

BLOCKCHAIN-BASED EHR, MPR, AND TMR MANAGEMENT SCHEMES

This chapter presents the blockchain based EHR, MPR and TMR management system designs and implementation

4.1 Overview

In order to protect patients from harm caused by inaccurate past medical histories and to guarantee that they will get the right medication and care, electronic health records (EHR) must be accurate. Protecting the public's health also depends on accurate medical practitioner records (MPR) management. Medication mistakes can result in a variety of physical injuries and even patient deaths. Additionally, telehealth is crucial during pandemics, and accurate treatment depends on the accuracy of telecare medical records (TMR).

Healthcare organizations typically manage this data in self custody systems that are vulnerable to variety of cybercrimes, such as ransomware, Distributed denial of service, etc. The unique properties of blockchain technology, such as collusion resistance, transaction visibility, tamperproofness, and security, have the potential to maintain the integrity of EHRs, MPRs, and TMRs. The purpose of this work is to create EHR, MPR, and TMR management systems using distributed ledger technology for data integrity and trust building.

The envisioned EHR management system has the potential to serve as an invaluable tool in maintaining accurate Electronic Health Records (EHRs) for various applications, such as enhanced patient diagnosis, streamlined insurance claims, and expedited drug discovery processes. This innovative system empowers healthcare organizations to seamlessly transmit electronic health records through the blockchain network to patients.

Furthermore, it facilitates EHR requesters in accessing these records with the explicit permission of the patients.

The proposed MPRs management system can be a very helpful mechanism to ensure that the correct records are available at the time that medical practitioners are registered to practice in any health organization, thereby preventing imposters from endangering the public's health. With the help of the proposed model, medical institutions can share MPR content across the blockchain network, and hospitals, patients, and medical colleges can request access to it to confirm a doctor's record.

Using blockchain technology and smart medical devices, the proposed TMR management system can be useful for uploading and retrieving real-time fitness monitoring and medication data. The system created enables medical professionals to quickly access patient fitness tracking data so they can recommend the right medication over a blockchain network.

Additionally, the system preserves all previous TMR records, which patients may access at any time in the future. This system may prove to be a very useful tool for protecting telehealth during a pandemic.

In designed systems, each EHR, MPR, and TMR block is hashed using the secure hash algorithm (SHA)-256, and individual IDs are calculated for each EHR, MPR, and TMR using UUIDs. The developed prototypes' modules are all successfully executed, and the result section includes a few examples of execution results. The results of the execution demonstrate that the developed systems are suitable for managing EHRs, MPRs, and TMRs.

4.2 Proposed EHR Management System

The primary challenge encountered by traditional healthcare systems in EHR management is the risk of system failure when handled by a single centralized unit. Without access to past health records, the need for fresh diagnoses and lab tests arises, escalating treatment costs and time.

Additionally, these systems lack interoperability for securely sharing EHRs, potentially leading to improper patient treatment. There are instances where patients pay for unused services and medicines due to a lack of EHR visibility. Leveraging blockchain technology holds promise in fortifying the integrity of the EHR management system, thwarting potential attackers from tampering with EHRs. This technology also fosters collaborative efforts among multiple users to enhance public health outcomes.

4.2.1 Architecture of EHR Management

Efficient EHR management is pivotal for enhancing public health. The proposed model adeptly addresses challenges inherent in traditional healthcare systems by comprehensively addressing facets like privacy, security, transparency, and meticulous record management. This ensures seamless communication among various participants, including doctors, patients, healthcare providers, pharmaceutical companies, and insurance companies.

Endorsement policies, such as patient consent, are integral for preserving the confidentiality of sensitive data, restricting EHR access to only genuine entities like healthcare providers, medical researchers, or insurance companies.

Illustrated in Figure 4.1, the architecture of the proposed EHR management system comprises a three-layer structure: the user layer, application layer, and blockchain layer. The user layer facilitates health organizations (hospitals) in transmitting EHRs to patients via the blockchain network and empowers EHR requesters (doctors, medical researchers, pharmaceutical companies, and insurance companies) to access transferred data on the blockchain ledger with

patient consent. The application layer manages the EHR uploading and retrieval process between the user and the blockchain layer.

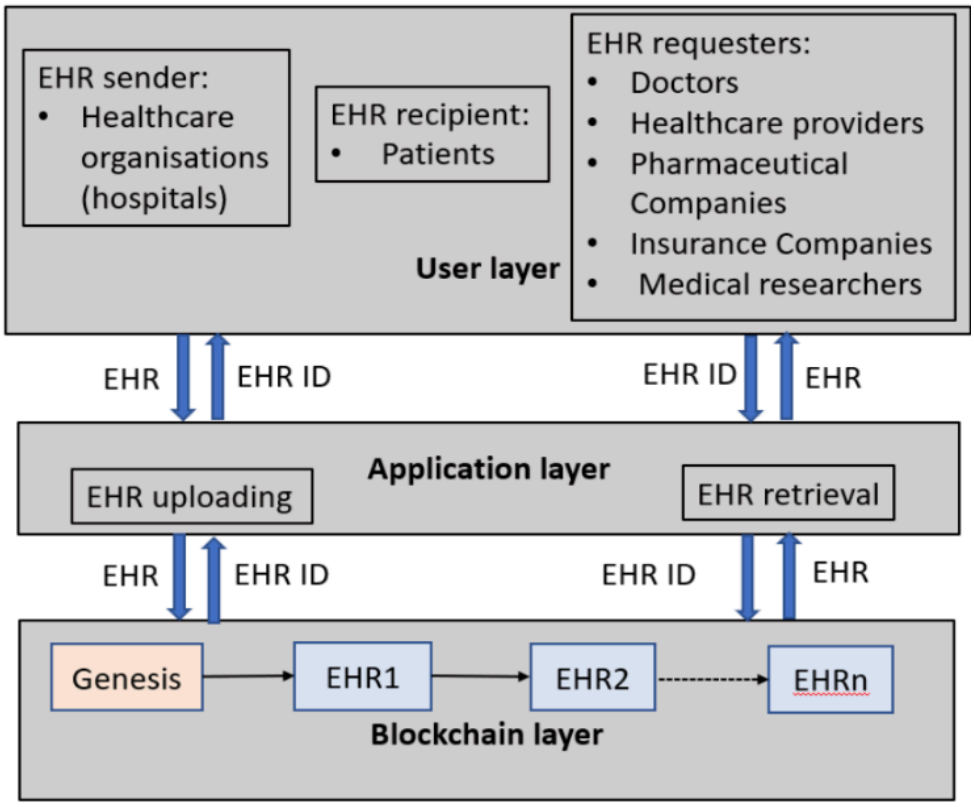


Figure 4.1: Architecture of the EHR management system.

Within the blockchain layer, specific roles contribute to the seamless operation of the system:

- Broadcasting: Disseminating the uploaded EHR to all nodes within the blockchain network.
- Block Creation: Generating a new EHR block.
- Mining: Executing the mining process for the new EHR block.
- Validation: Confirming the legitimacy of the new EHR block by all network nodes for its integration into the blockchain ledger.

In this layer, the initial block serves as the genesis block, while subsequent blocks denote the transferred EHRs (EHR1, EHR2, … EHRn). In the proposed system, hospitals update and add each patient's EHR on the blockchain network.

Requesters, with patient consent, access EHRs for diverse purposes such as treatment improvement, drug development, and insurance claims.

The process unfolds with health organizations initiating transaction requests, transferring drug EHR data to patients through the application layer. Upon data transfer, the blockchain layer generates a unique EHR ID, communicated back to the sender, and disseminates the transferred data to all blockchain layer nodes. A new block, signifying the uploaded EHR, undergoes mining to calculate its hash value using the SHA-256 algorithm. The block hash, contingent on the previous block hash, current block data, and nonce, provides proof of work for new block verification. Hash encryption secures information within the blocks. Post-mining, unanimous approval from all nodes occurs, and the EHR-containing block becomes a permanent part of the blockchain network.

Following EHR transfer, recipients (patients) can retrieve it using the block hash or EHR ID. All EHR requesters necessitate patient consent for access. Only upon the patient's acceptance, confirmed with the EHR ID, can the requester gain access to this confidential data.

4.2.2 Implementation and Simulation Results

This design study proposes a blockchain-centric approach for EHR management, harnessing distributed technology to uphold the integrity of EHRs in a secure and decentralized manner. In this refined system, healthcare organizations dispatch EHRs to patients and enable EHR requesters to retrieve them with patient consent. The EHRs in the proposed model are structured in JSON format, with Visual Studio Code employed for blockchain development, utilizing the Node.js programming language for source coding. The implemented design incorporates four core building modules: EHR uploading, EHR mining, EHR addition, and EHR retrieval.

Figure 4.2 visually outlines the EHR modules within the developed system. The EHR uploading module empowers healthcare organizations to seamlessly transfer the EHRs (EHR1, EHR2, EHR3... EHRn) of their patients across the blockchain network. Each EHR encompasses comprehensive patient information, including

name, age, weight, blood pressure, diet chart, diagnosis, treatment, medication, lab test and radiology results, vaccinations, allergies, and the sender's name.

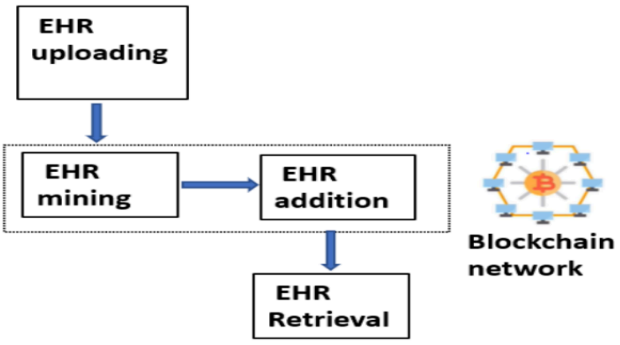


Figure 4.2: EHR modules of the designed system.

After sending a request response to the EHR sender, the uploaded EHR is broadcasted as a pending transaction to all network nodes on the blockchain ledger. Each uploaded EHR is assigned a unique EHR ID generated through the uuid (universally unique identifier) function. In the EHR mining module, the miner node further validates the uploaded EHR by executing proof of work.

A dedicated miner, known as the validator node, employs the SHA-256 algorithm to create new blocks for EHR. These blocks encapsulate the current EHR, block index, timestamp, nonce, current block hash, and the hash of the previous block. Following the mining of the current block, the EHR addition module secures unanimous approval from all blockchain nodes. Upon approval by all nodes, the EHR block is appended to the blockchain ledger. The execution result of the EHR addition module is illustrated in Figure 4.3.

In the EHR retrieval module, EHR requesters can access the EHR of any patient with their consent using the designated EHR ID. The execution result of the EHR retrieval module is depicted in Figure 4.4.

Figure 4.3: Simulation result of the EHR addition module.

Table 4.1 provides a comparative analysis of the proposed scheme and prior works based on various performance parameters. Notably, the proposed system, like existing ones, is blockchain-based and designed for managing electronic health records. This study encompasses the development of the architecture and presents the design test of the developed blockchain system, a feature unavailable in existing works.

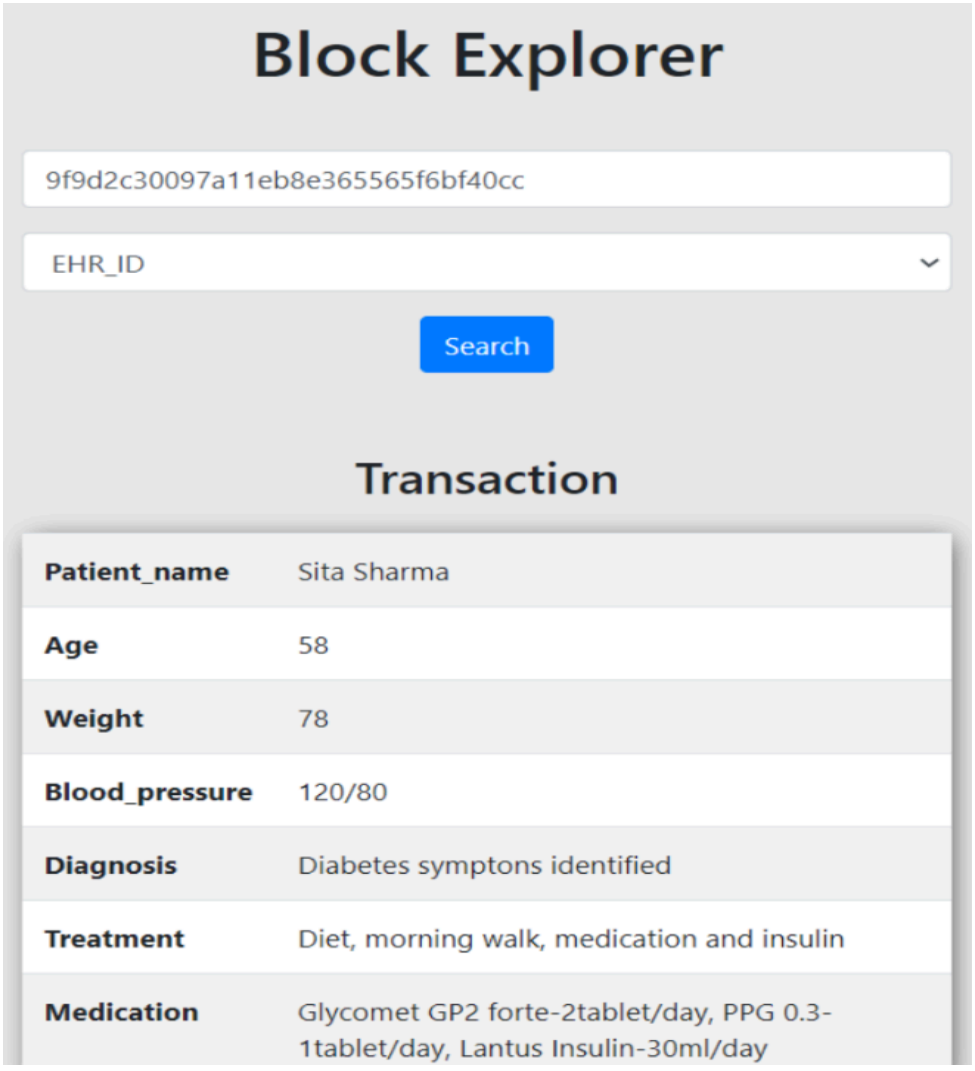


Figure 4.4: Simulation result of the EHR retrieval module.

Table 4.1: Comparitive analysis of EHR work with prior works.

Qualitative metrics	[8]	[89]	[96]	Proposed
Blockchain-based	✔	✔	✔	✔
Electronic health record	✔	✔	✔	✔
Architecture design	✔	×	×	✔
Simulation results	×	×	✔	✔

✔: Available, ×: Unavailable

4.3 Proposed MPR Management System

Health professionals play a pivotal role in preventing diseases and delivering essential medical services to enhance public health. Unfortunately, in today's world, there exists a subset of individuals operating as doctors without legitimate medical degrees, posing a risk of medication errors leading to physical injuries and potential patient fatalities. Compounding this issue, many medical institutes and organizations maintain records in a centralized manner, vulnerable to compromise or theft by hackers for creating fraudulent identities. In response to these challenges, there arises a critical need for a framework that can securely maintain accurate records of medical practitioners. Such a system should be easily retrievable by entities such as patients and hospitals to validate the credentials of medical professionals. Figure 4.5 depicts a use case scenario for the MPR model.

An MPR system is not only beneficial for medical professionals but can also serve patients, medical colleges, hospitals, and various stakeholders over an individual's lifetime. Illustrating two contrasting cases, the first mirrors the existing system, while the second exemplifies the proposed one. In the initial scenario, Doctor A prescribes treatment for Patient A. However, Patient A lacks the capability to validate Doctor A's MPR, rendering them susceptible to seeking treatment from a fraudulent practitioner, potentially worsening their health. In the proposed scenario, Doctor B prescribes treatment for Patient B. Here, Patient B can verify the authenticity of Doctor B's MPR through the blockchain network, ensuring that

they only accept treatment from a genuine professional. This is feasible because Doctor B's medical institute meticulously maintains every MPR within the secure blockchain network. By scrutinizing Doctor B's MPR, Patient B can confidently ascertain the correctness of the prescribed treatment.

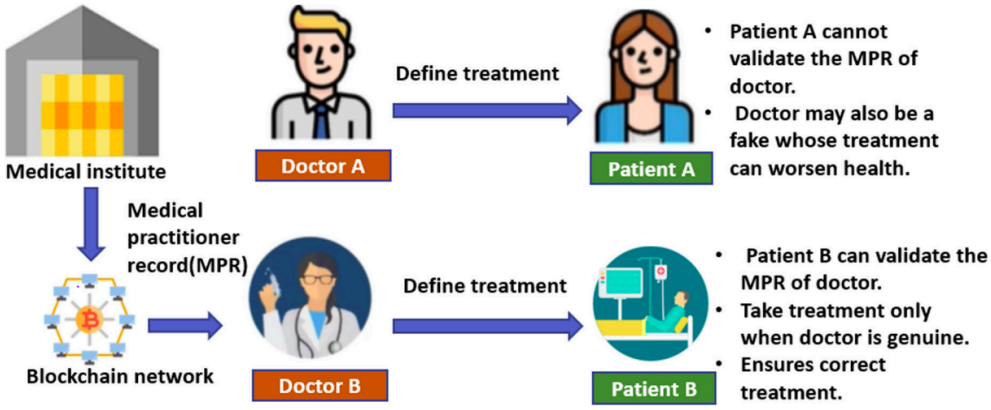


Figure 4.5: Use-case scenario of the MPR design.

4.3.1 System Structure of Developed MPR Management Model

In our proposed blockchain-based digital MPR system, we have crafted a prototype of a public blockchain, offering seamless retrieval of MPR by demanding entities at any given moment. The primary goal is to ensure consistent access to accurate records, enabling the verification of medical practitioners. Patients, hospitals, and medical colleges are among those who can participate in this public blockchain. Comprising two integral components, the model includes a user interface (UI) and a blockchain decentralized application (Dapp). The UI is developed to empower users, allowing them to submit MPR and view the transferred records on the blockchain ledger. On the other hand, the blockchain Dapp is designed to execute essential functions such as broadcasting the transferred MPR to all nodes in the blockchain network, generating new MPR blocks, mining MPR blocks, and validating these blocks universally before incorporating them into the chain. The architecture of this MPR management model is depicted in Figure 4.6.

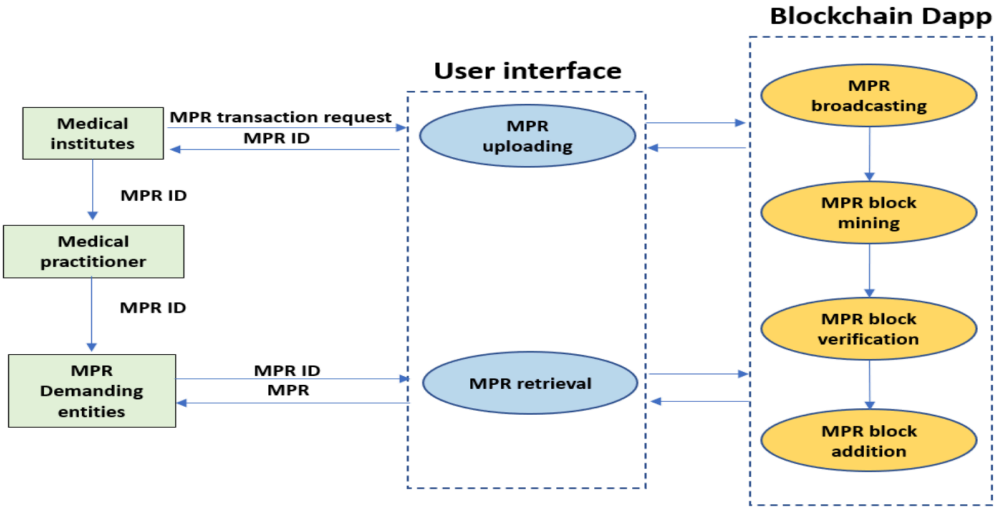


Figure 4.6: Architecture of the MPR management design.

Initially, medical institutions (comprising medical colleges and hospitals) initiated transaction requests by transferring MPR to the blockchain ledger through the UI. Following MPR transfer, a distinctive MPR ID was generated and returned by the blockchain Dapp. The medical institution could then share this MPR ID with the respective medical practitioner. The transferred MPR information was disseminated to all nodes within the blockchain Dapp. Subsequently, a new block, detailing the MPR information, underwent mining to calculate its hash value using the SHA-256 algorithm. The hash of each block relied on the previous block hash, current block information, and nonce, providing proof of work for new block verification. Hash encryption was employed to secure the stored MPR information within the blocks. Following the mining process, unanimous approval from all nodes was obtained, and the block containing MPR was seamlessly added to the blockchain network. Post MPR transfer, retrieval was facilitated using a block hash or the assigned MPR ID.

4.3.2 Implementation and Simulation Results

This study presents a blockchain-based model for managing MPR information, ensuring the accuracy of records within a secure and decentralized database. This MPR data remains accessible to entities seeking it, providing flexibility and transparency. In the proposed model, the UI serves as a communication interface

with the blockchain Dapp. This user-friendly dashboard facilitates MPR retrieval through a search option, employing a block hash or MPR ID accessed via the uniform resource locator (URL). MPR information is structured in JSON format, and the comprehensive source coding is executed in Node.js on Visual Studio Code.

The developed model comprises four essential modules: MPR transferring, MPR mining, MPR addition, and MPR retrieval. In the MPR transferring module, medical institutes seamlessly transfer MPR over the blockchain network via the UI, encompassing vital data such as the medical practitioner's name, undergraduate and postgraduate degree details, clinical experience, sender name, and recipient (medical practitioner) name. Acknowledgments are sent to the sender, and the transferred MPR is communicated as a pending transaction to all nodes of the blockchain Dapp via API. Each transferred MPR is assigned a unique MPR ID generated using the uuid function.

The MPR mining module further processes MPR through the miner node, creating a new block that includes the block index, timestamp, MPR information, nonce, hash of the new block, and hash of the previous block. Post new block mining, the MPR addition module verifies the MPR block across all nodes. Upon successful verification, the MPR block is seamlessly added to the blockchain Dapp. Figure 4.7 illustrates the test result for the MPR addition module, validating the efficacy of the proposed system.

In the MPR retrieval module, entities seeking information can view the MPR block details by utilizing a block hash. Additionally, they have the option to access MPR information on Blockchain Explorer by inputting their MPR ID. Figure 4.8 succinctly presents the test result of the MPR retrieval module, showcasing its effectiveness in providing accessible and verifiable MPR data.

4.3.3 Comparative Analysis

Table 1 provides a qualitative comparison between our proposed scheme and prior works, utilizing diverse metrics. The innovative blockchain-based approach we introduce for managing medical practitioner records is a unique concept not explored in any existing work. Although existing schemes are also

blockchain-based, they were specifically designed for the management and sharing of Electronic Health Records (EHRs). Furthermore, our presentation encompasses the architecture and test results of the developed blockchain system, a crucial inclusion that was absent in several existing works.

Figure: 4.7. Simulation result of the MPR addition module.

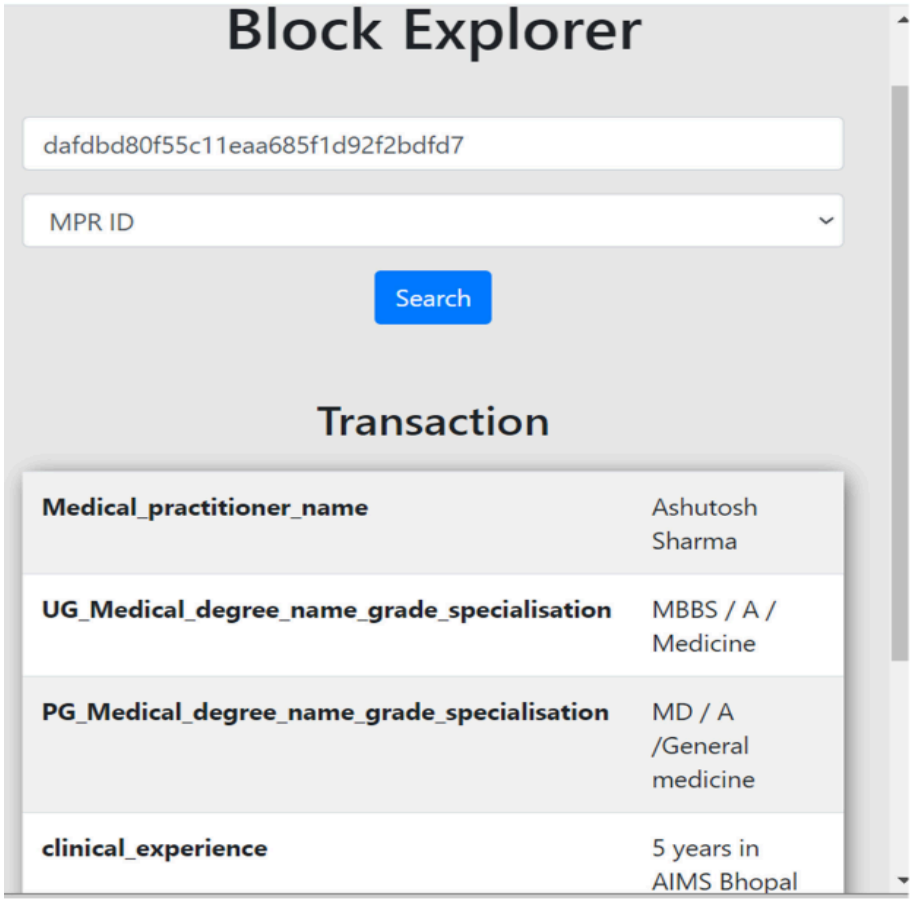


Figure 4.8: Simulation result of MPR retrieval module.

Table 4.2: Comparison between MPR work and prior works.

Qualitative metrics	**[8]**	**[89]**	**[96]**	**Proposed work**
Blockchain-based system	True	True	True	True
Developed system	EHR	EHR	EHR	MPR
Architecture available	True	False	False	True
Design tested	False	False	True	True

4.4 Proposed TMR Management System

The proposed telecare medical record (TMR) management system is developed for the uploading and retrieval of real time fitness monitoring and medication data using blockchain technology and smart devices.

The developed system permits healthcare providers to gain fast access to the fitness tracking data of patients in order to prescribe suitable medication over the blockchain network and also allows patients to access this data.

Figure 4.9 represents the use-case scenario of a blockchain-based TMR management system. This use case scenario shows the transaction of patient's fitness monitoring parameters generated by smart healthcare devices to the healthcare provider and also the transaction of suitable medication prescribed by the healthcare provider to the patient in real time.

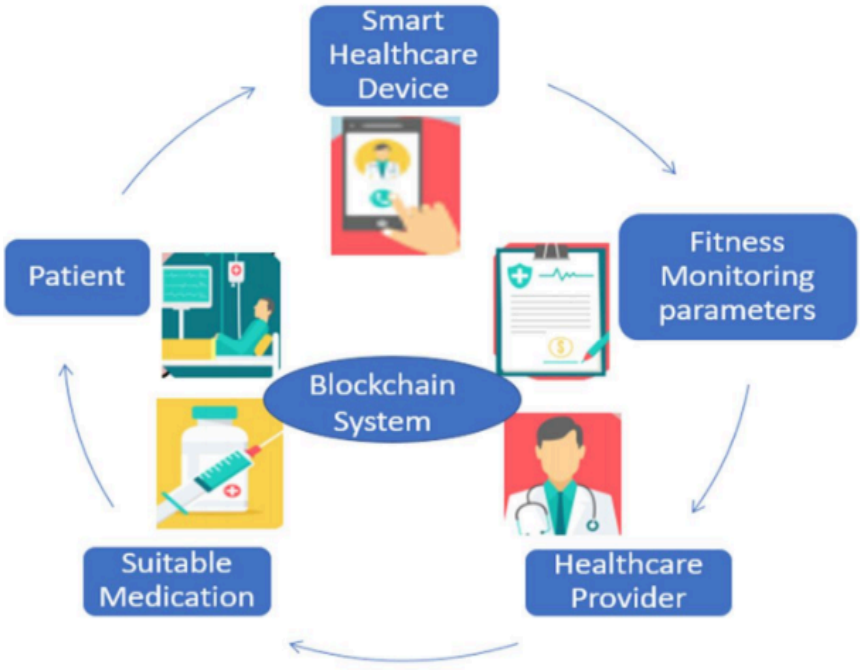


Figure 4.9: Use case scenario of the proposed TMR management system.

This system can prove to be a very beneficial mechanism, especially in the context of pandemics such as COVID-19. The benefits of proposed system are listed as follows:

- Tracking: This allows care providers to track patients in real time and eventually leads to better health outcomes.
- Cybersecurity: Privacy and security of confidential patient data due to blockchain mechanisms, preventing attackers from blocking TMRs for forgery purposes.
- Cost reduction: Cost-effective for patients due to the elimination of conveyance costs involved in visiting clinics and for healthcare providers due to the reduced need for infrastructure and staff.
- Freedom from single-point failure: Free from the harm of losing past records due to single-point failure, which is suffered by most of the current telecare systems.
- Interoperability: Quick sharing of TMR with multiple experts for better treatment delivery to the patient in a secure manner.

4.4.1 Architecture of TMR Management System

The proposed TMR management system plays a crucial role in enhancing public health, especially during the pandemic period. It successfully addresses challenges inherent in traditional telecare systems by addressing various aspects of the healthcare domain, including privacy, security, transparency, and meticulous record management. These features contribute to seamless communication between patients and healthcare providers. Endorsement policies, such as patient consent, are integral to preserving the confidentiality of sensitive data and ensuring that TMR access rights are granted exclusively to genuine healthcare providers. Figure 4.10 visually outlines the architecture of the proposed TMR management system, providing a clear representation of its design and functionality.

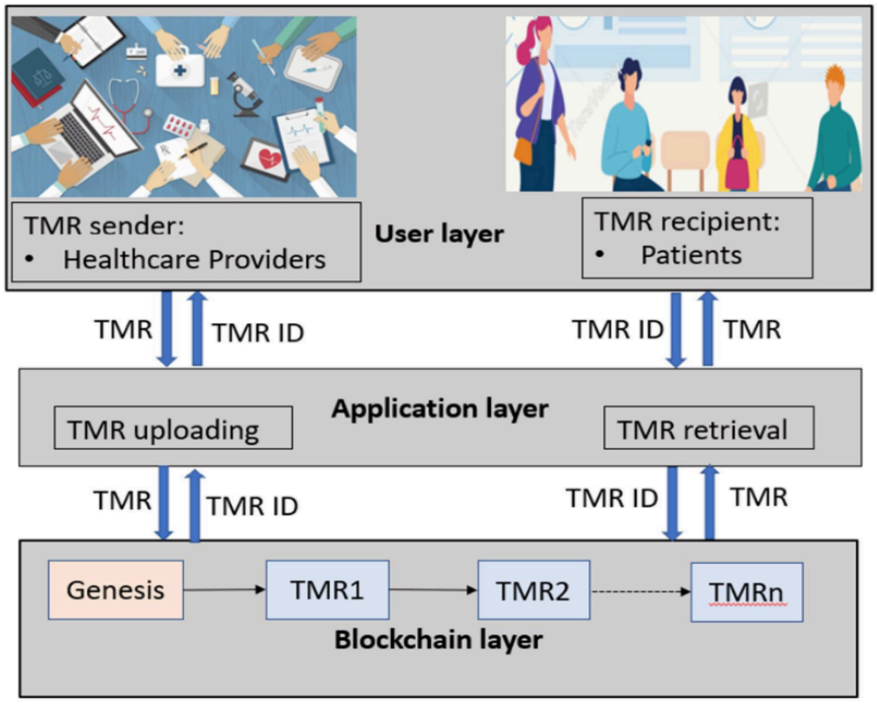


Figure 4.10: Architecture of the TMR management system.

The system that has been developed comprises three layers: the blockchain layer, the application layer, and the user layer. The user layer enables the transaction of health parameters of patients generated by smart healthcare devices to healthcare providers over the blockchain network. This layer also facilitates healthcare providers sending medications based on patient health parameters to patients over the blockchain network. Smart healthcare devices like fitness trackers, blood pressure monitors, ECG monitors, sugar level monitors, etc. can be used to monitor the physical condition of patients in real time. Health parameters representing fitness data and medication data will be stored in the form of TMR in the blockchain ledger of the developed system. Healthcare providers and patients can view transferred TMR on the blockchain ledger through the user layer.

Healthcare providers gain access to TMRs only with the explicit consent of patients. The application layer serves as the intermediary between the user layer and blockchain layer, managing the TMR uploading and retrieval processes. The blockchain layer, with distinct functions, encompasses:

1. Broadcasting: Distributing the uploaded TMR to all nodes in the blockchain network.
2. Block Creation: Generating a new TMR block.
3. Mining: Executing the mining process for the new TMR block.
4. Validation: Confirming the legitimacy of the new TMR block by all network nodes before appending it to the blockchain ledger.

Within the blockchain layer, the initial block signifies the genesis block, while subsequent blocks represent the transferred TMRs (TMR1, TMR2...TMRn). Figure 4.11 visually depicts the workflow of the developed TMR management system, offering insight into its operational processes. Initially, smart healthcare devices used by patients generated and transferred TMR1, containing the patient's health parameters, to the healthcare provider over the blockchain ledger. The blockchain layer generates a distinct TMR1 ID upon transferring TMR1 and sends it to the patient. The patient can share their TMR ID with the healthcare provider for medication.

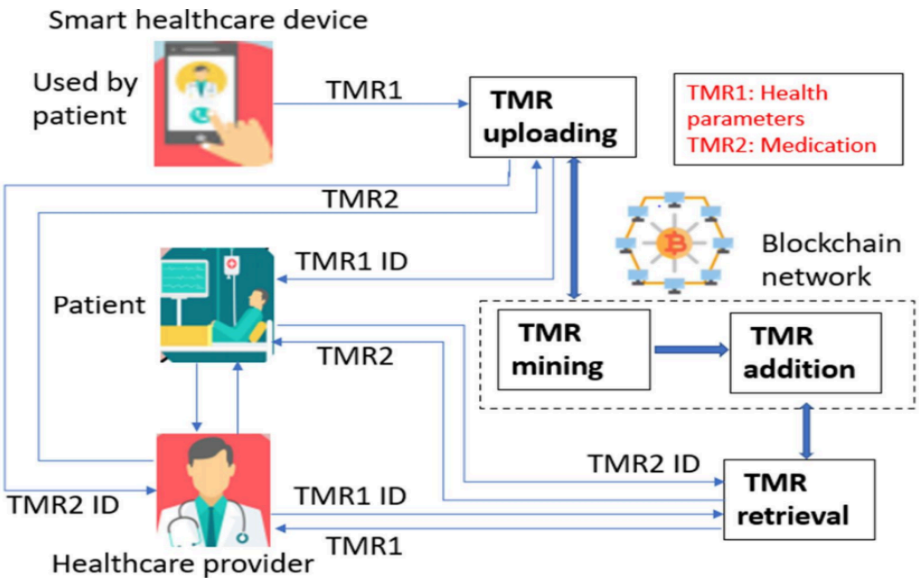


Figure 4.11: Illustrates the workflow of the developed TMR management system.

Every blockchain layer node receives transferred TMR via broadcast. A new block representing the uploaded TMR1 is generated and undergoes mining to compute its hash value through the SHA-256 algorithm. The block hash is contingent on the previous block hash, current block information, and nonce. The

mining process serves as proof of work for the verification of the new block. Hash encryption is applied to secure the information encapsulated within the blocks. Following the mining procedure, unanimous approval from all nodes is obtained, and the block containing TMR is ultimately incorporated into the blockchain network.

With the patient's permission, the healthcare provider can retrieve TMR1 by using its TMR ID after it has been transferred. The next TMR2 containing the medication is then uploaded by the healthcare provider and sent to the patient via the blockchain layer. The blockchain layer creates and sends a distinct TMR2 ID to the healthcare provider upon TMR2 transfer. When writing a prescription, the medical professional can give the patient access to their TMR2 ID. A new block signifying the creation, mining, and addition of TMR2 to the blockchain network. Finally, patients can retrieve the medication prescribed by their healthcare provider using the TMR ID of TMR2. In a similar fashion, uploading and retrieval of various TMRs can be done.

4.4.2 Implementation and Simulation Results

In developed system, TMRs are sent to healthcare providers and patients by smart healthcare devices and by healthcare providers themselves and can be retrieved by healthcare providers and patients. In proposed model, TMRs have been created in JSON format using Postman software (for simulation purposes). We have developed our own blockchain using Visual Studio Code software and source coded NodeJS. The four building modules of the implemented design are TMR uploading, TMR mining, TMR addition, and TMR retrieval. In proposed design, Both TMR uploading and retrieval modules have two phases to complete one cycle of fitness tracking and medication. In first phase of TMR uploading, smart healthcare devices transfer TMR1 containing health parameters of patients over blockchain network. Health parameters included walking distance, body temperature, blood pressure, and blood sugar level. Subsequently, a unique TMR ID is dispatched to the patient, while the uploaded TMR is disseminated as a pending transaction to all network nodes on the blockchain ledger. The generation of a unique TMR ID for the uploaded TMR is facilitated through the uuid

function. In the TMR mining module, additional proof of work for the uploaded TMR is orchestrated by the miner node, referred to as the validator node. This node crafts a new block for each TMR utilizing the SHA-256 algorithm. The newly obtained block comprises the current TMR, block index, timestamp, nonce, current block hash, and hash of the previous block. Post mining of the current block, the TMR addition module secures approval across all blockchain nodes. Once the TMR block attains unanimous approval from all nodes, it seamlessly integrates into the blockchain ledger. Figure 4.12 provides a visual representation of the execution result of the TMR1 addition module.


```
"chain": [
  {
    "index": 1,
    "timestamp": 1602593033044,
    "transactions": [],
    "nonce": 1435345300,
    "hash": "asdasdasdas0",
    "previousBlockHash": "dasdadsasdasd"
  },
  {
    "index": 2,
    "timestamp": 1602593061923,
    "transactions": [
      {
        "Patient_name": "Suresh Kumar Sharma",
        "Walking_distance": "3 KM",
        "Body_temperature": "98 degree celsius",
        "Blood_pressure": "120/80",
        "Blood_sugar_level": "100",
        "TMR_ID": "c2fd3be00d5111eb8d5e99929abc2b96"
      }
    ],
    "nonce": 876309,
    "hash": "0000020f3f5a9520b1103f755c0426a75cbed400a189bb0c93dd4c4f19b659a2",
    "previousBlockHash": "asdasdasdas0"
```


Figure 4.12: Simulation result of TMR1 addition module.

In the initial phase of the TMR retrieval module, healthcare providers can safely access the TMR1 of patients with their consent using the designated TMR ID. Figure 4.13 illustrates the execution result of the TMR1 retrieval module, offering insights into its functionality.

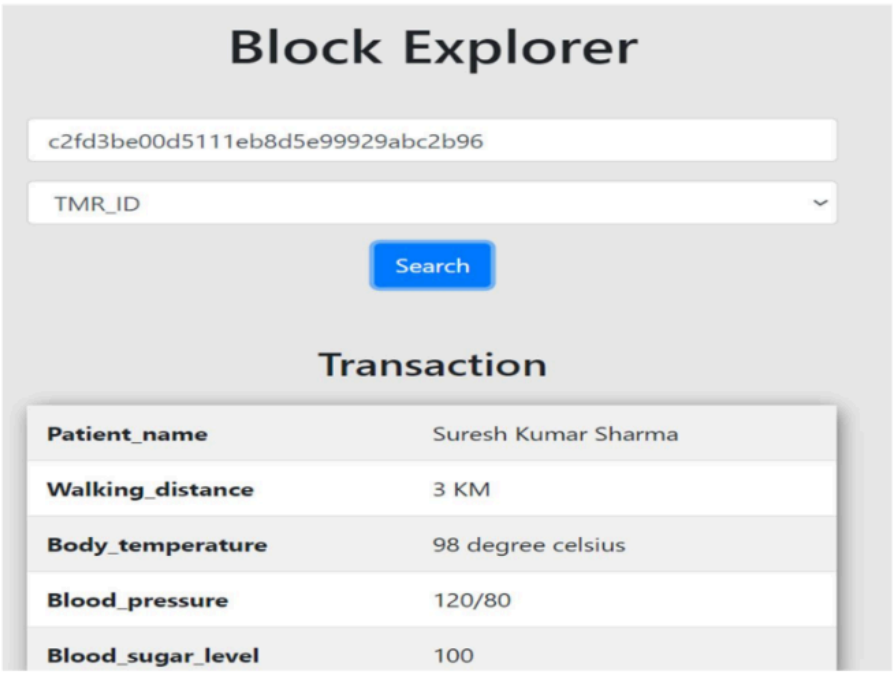


Figure 4.13: Simulation result of TMR1 retrieval module.

In the second phase of the TMR uploading module, the healthcare provider uploads TMR2 containing medication information and sends it to the patient over blockchain. The patient can retrieve it using the TMR ID shared by healthcare providers. The TMR2 addition module's execution result is displayed in Figure 4.14, and the TMR2 retrieval module's execution result is displayed in Figure 4.15. These results show that blockchain has the potential to maintain telecare medical records.


```
"index": 3,
"timestamp": 1602596761112,
"transactions": [
    {
        "Patient_name": "Suresh Kumar Sharma",
        "Medication": "Ecosprin 75mg-2 tablets/day, Cardace 2mg-
        1tablet/day",
        "Sender": "Dr. Jagat",
        "TMR_ID": "39bbd1800d5a11eb814307e60b24ea55"
    }
],
"nonce": 323648,
"hash": "000009cd552cbf3e216ea5fb78b7592fa820799ad639c4028f19daf6cdcc4b79"
```


Figure 4.14: Simulation result of the TMR2 addition module.

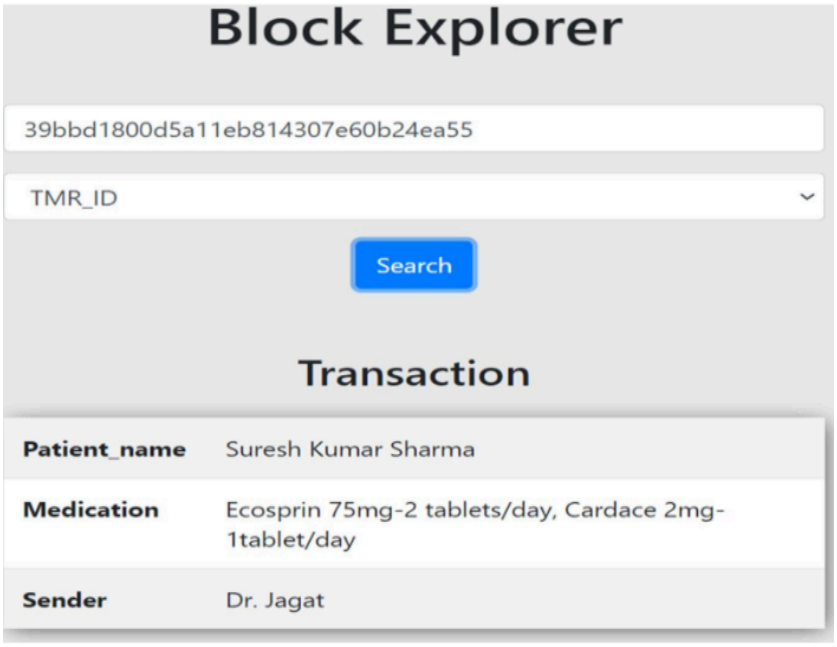


Figure 4.15: Simulation result of the TMR2 retrieval module.

4.5 Discussion

Blockchain technology plays an important role in cybersecurity and can be used to provide integrity to the EHR, MPR and TMR management systems. This technology has the capability of preventing attackers from blocking data. We proposed blockchain-based approaches for EHR, MPR and TMR management that permit healthcare organizations to upload records over a blockchain network and also empower requesters to retrieve the confidential records with the consent of individuals. The developed system can be highly suitable to ensure availability of genuine EHR data during future treatment, MPR records during practitioner validation, and TMR records for prescribing medicines. The designed models of proposed systems consist of four modules, which are uploading, mining, addition and retrieval. The execution results indicate that the created blockchain-based models can maintain the integrity of records. We have also successfully created and tested these proposed blockchain-based management systems.

CHAPTER 5

SCALABLE AND COST-EFFECTIVE BLOCKCHAIN SOLUTION FOR MANAGING VACCINATION RECORDS

This chapter contains a scalable and cost-efficient solution for managing vaccination records based on patient preference.

5.1 Overview

This chapter aims to design a novel, cost-efficient blockchain-based solution for managing lifetime vaccination records based on patient preference. The proposed design reduces fraud in vaccination certification by providing QR code-based validation. The proposed system stores the cryptographic hash of vaccination certificates on the blockchain for security and integrity validation.

For scalability, availability, and store-house cost reduction, vaccination records have been stored off-chain through a private interplanetary file system (IPFS) based on patient preference. The smart contract has been successfully deployed and tested in the Remix IDE environment. Performance has been evaluated by analysing execution costs at different transaction sizes. Moreover, we have evaluated the probability of data availability for a private IPFS network, which was not done in any previous work. Furthermore, we have analysed the network parameters to get optimal data availability at a low storage cost. The comparative analysis of features proves that this scheme is better than existing schemes.

5.2 Proposed Work

In today's world, people move a lot from one place to another frequently, and it is almost inevitable that one or more vaccinations are missed, either due to a lost physical copy or a poorly managed online record. In cases of unavailability at times of need like scheduled vaccinations, illness, migration, education, or employment purposes, the patient attempts to contact the concerned health organisation for those records to present them to the requesting entity.

But current health organisations maintain data in a centralised manner that can be altered or lost by cyberattacks. The process of transferring the vaccination data from the hospital often requires multiple hospital-to-patient communications, leading to delays, that can be unbearable in the case of an illness.

Moreover, patients visit many hospitals to take various kinds of vaccines in their lifetime. Some of which are Hepatitis A and B, Haemophilus, Rotavirus, Influenzae type b, Poliovirus, Diphtheria, Tetanus, Pertussis, Pneumococcal, Meningo coccal, Influenza, Measles, Mumps, Rubella, Varicella, Human Papillomavirus, Covaxin, Covishield, etc. The scattering of vaccination records makes it difficult to manage and retrieve them. Bringing together different hospitals on a centralised system cannot be a solution, as the database will remain in the custody of one administrator and can be tampered with or lost.

So in this situation, it is a necessity that the health ministry initiate a decentralised system to maintain immutable and trustworthy vaccination records that can be easily accessible by any requesting entity throughout their life. Figure 5.1 shows the traditional and proposed use-case scenarios.

In this scenario, a person moves out of town or country and has been asked for a past vaccination record urgently due to one of the following reasons: person is sick, the person has a scheduled vaccination date, or the person has applied for education or employment. In the traditional scenario, the person, in the absence of a few records, contacts the old health organisation that provided vaccination earlier. The organisation takes time to provide a duplicate copy of the vaccination certificate to the person. The integrity of this certificate has no guarantee.

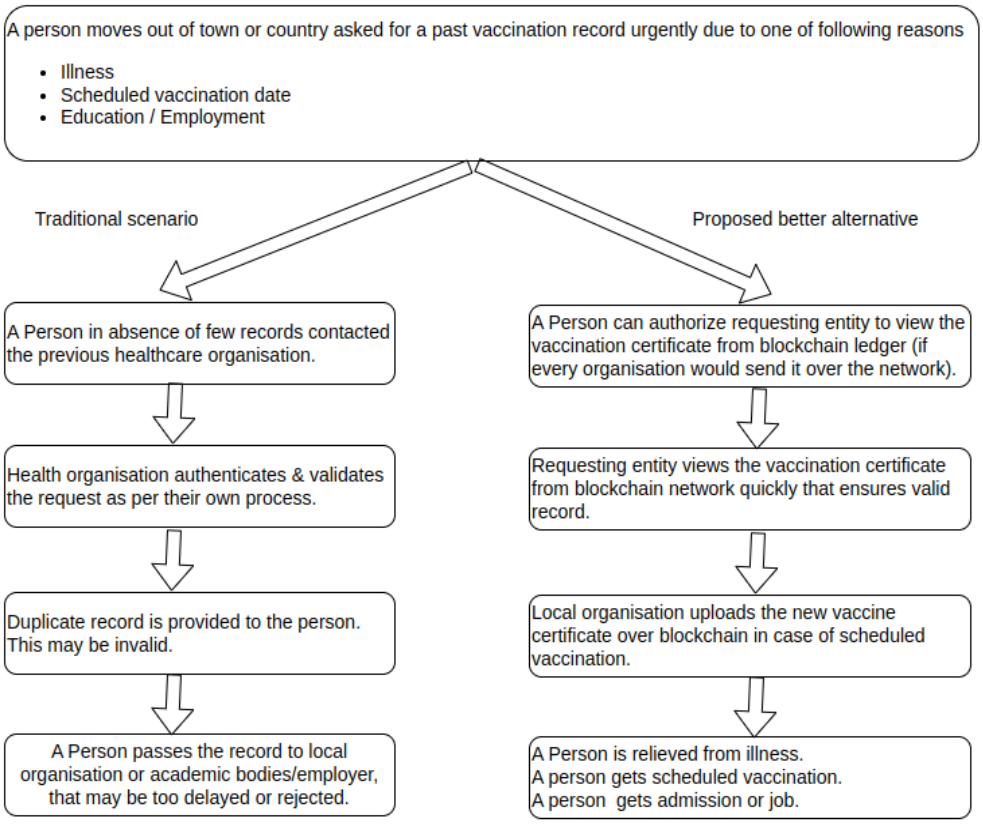


Figure 5.1: Traditional and proposed use-case scenarios.

The person might not be able to submit vaccination certificates on time. In the proposed scenario, the person gives authorization to view the vaccination record over the blockchain network to the requesting entities. That could be possible if the health ministry makes the uploading of vaccination records over the blockchain network mandatory for all health organisations. The requesting entity quickly views the authentic vaccination records on the blockchain network.

5.2.1 System Architecture

A blockchain-based vaccination system allows users to update and retrieve vaccination records from anywhere and at any time. In order to shield the patient from infections, the goal is to ensure accurate record accessibility for planned vaccinations or illnesses. The suggested blockchain-based approach to managing vaccination record functions is decentralized. At the same time, it ensures record accessibility for all requesting entities. The architecture of this system, shown in Figure 5.2, has the following layers:

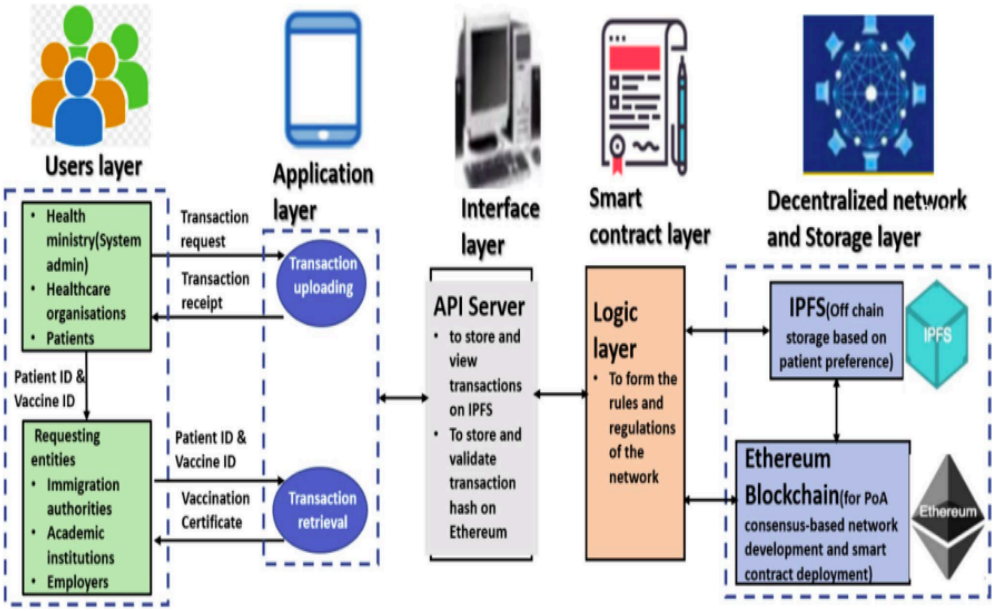


Figure 5.2: Architecture of the vaccination system.

- The user layer consists of the Health Ministry, health organisations, patients, and requesting entities that invoke transactions on the blockchain network. The health ministry acts as an admin to govern the entire network. A patient can authorise requesting entities to view the vaccination certificate using the patient ID and vaccination ID.

- The application layer forms the front end of the application. In the proposed model, this user interface is to create an environment for interacting with the blockchain-IPFS network. It allows users to upload and retrieve transactions. After transaction completion, a transaction receipt containing transaction details is received by the sender through this interface.

- The collection of APIs used to interact with the blockchain and obtain the desired outcome, such as adding or retrieving data, is known as the interface layer.

- The blockchain network's logic is formed by the Smart Contract layer, which also makes sure the network complies with all laws and regulations pertaining to the intended use.

- The private IPFS and public Ethereum blockchain are the decentralized network and storage layer, respectively. The Ethereum platform has been used to form the base of the blockchain network and ledger for holding transaction data. The PoA consensus mechanism has been utilised for mining purposes. The transactions are kept off-chain, but the hash of each transaction is kept on the blockchain. Every transaction sender uses an API (application program interface) server as middleware to run both an IPFS node and a blockchain node. This middleware stores the original data in IPFS before creating a blockchain transaction with the hash of the data when publishing off-chain. After obtaining the hash from the blockchain, the middleware uses it to retrieve all of the content from IPFS. To make sure it has not been altered, the local IPFS node automatically compares the retrieved content to the hash. Scalability and lower storehouse costs have been achieved by combining IPFS with the blockchain's patient preference feature.

5.2.2 Workflow

The workflow diagram for all parties involved in the vaccination system is depicted in Figure 5.3. Initially, the health ministry adds the health organisations that have vaccination facilities. The patient invokes registration requests on the network. Health organisations register new patients in response to registration requests. Now patients can view all health organisation details to check the address, available vaccines, and date-time slots.

After viewing the organisation details, the patient places a vaccination request with any suitable health organisation to get an appointment for vaccination. The health organisation then accepts the vaccination request by including an approved status. After that, the patient views the transaction request status and visits the health organisation physically.

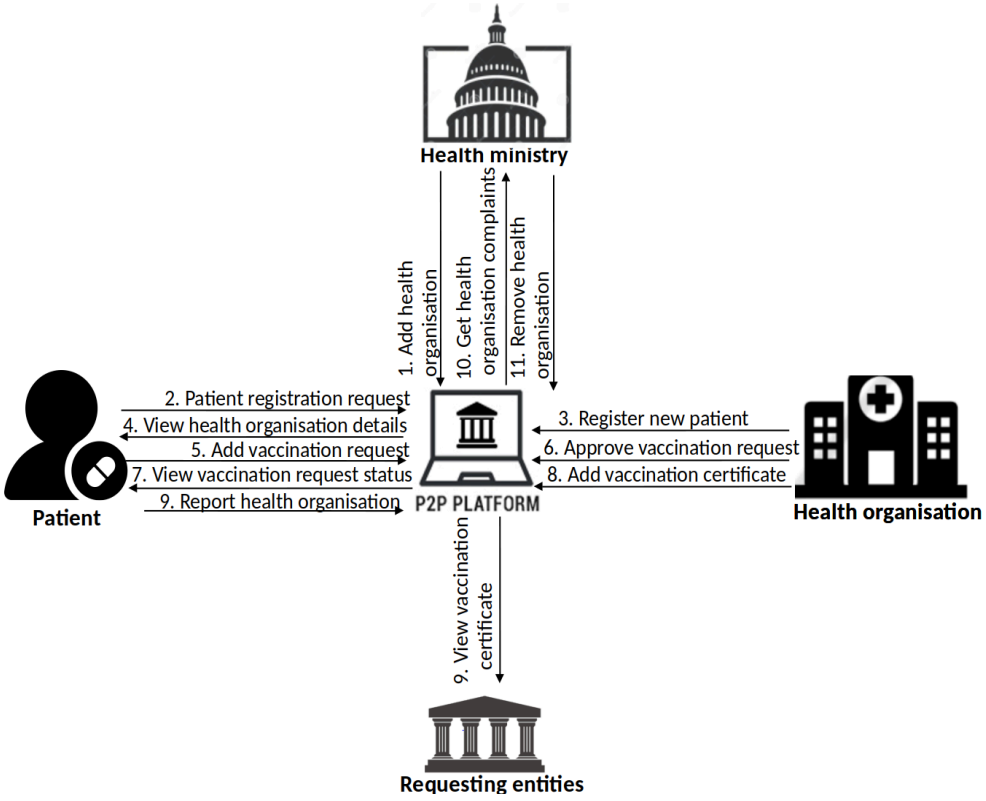


Figure 5.3: Workflow diagram of the proposed system.

After the vaccination process, the health organisation uploads the vaccination certificate, which any authorised requesting entity can access. Patients can report a complaint against health organisations in cases of issues faced during the vaccination process. The health ministry can retrieve the complaints reported against any organisation. The health ministry can remove health organisations against which reported complaints exceed the predefined value.

After vaccination, the patient's vaccination certificate is generated with a QR code. The actual data is kept on the private IPFs network, while the hash of the vaccination certificate is added to the blockchain. The user gets the vaccination certificate with a QR code that can also be used as vaccination proof. This helps with requesting authorities to permit cross-border travel, the next vaccination, and recruiting individuals. The requesting entities can view the vaccination certificate and scan the QR code to verify it on the blockchain.

Figure 5.4 represents the QR code and information on the vaccination certificate The vaccination certificate contains the following information: patient ID,

Aadhaar number, date of birth, organisation ID, vaccination ID, and date of vaccination. In response to the QR code scanning, requesting entities will get the hash of the vaccination certificate if it matches the stored hash on the blockchain. The proposed design reduces fraud in vaccination certification by providing QR code-based validation on the blockchain.

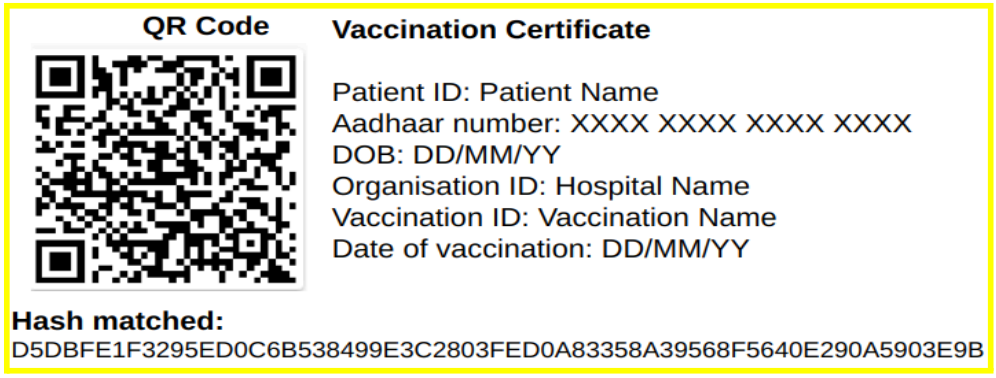


Figure 5.4: QR code and information on the vaccination certificate.

The functionalities of the involved parties with access controls are defined inside the smart contracts. Algorithm 1 shows the smart contract functionality of the health ministry. The health ministry can invoke the following functions:

- addHealthOrganisation(): This function has been defined to add health organisations. It contains the organisation ID, address, registration number, and list of available vaccines with the date and time slots.
- getHealthOrganisationComplaints(): This function has been defined to get complaints reported against health organisations. It contains the organisation ID.
- removeHealthOrganisation(): This function has been defined to remove health organisations in the event that complaints are reported by more than one-third of the vaccinated patients. It contains the field of organisation ID.

Algorithm 1: Smart contract functionality of the health ministry.

```
1.  function addHealthOrganisation (Organisation ID, Address,
    Registration number, Available Vaccine slots)
2.      if msg.sender == Health ministry then
3.          if Organisation ID does not exist then
4.              Add health organisation to the Health organisation asset
5.          else
6.              Invalid transaction
7.          end if
8.      end if
9.  end function
10. function getHealthOrganisationComplaints (Organisation ID)
11.     if Organisation ID exist then
12.         return Complaints reported against health organisation
13.     else
14.         Invalid Organisation ID
15.     end if
16. end function
17. function removeHealthOrganisation (Organisation ID)
18.     if Organisation ID exist then
19.         if Complaint reported > 1/3(Vaccination count of organisation)
    then
20.             remove health organisation
21.         else
22.             Invalid Organisation ID
23.         end if
24.     end if
25. end function
```

Algorithm 2 shows the smart contract functionality of a health organisation. The health organisations can invoke the following functions:

- RegisterNewPatient(): This function has been defined to register new patients. Any health organisation can register a new patient. It contains patient ID, Aadhaar number, age, and data availability choices.
- approveVaccinationRequest(): This function has been defined to accept vaccination requests and include the "approved status". It contains patient ID, date and time, requested vaccination, and status.
- addVaccinationCertificate(): This function has been defined to upload vaccination certificates and increment the vaccination count. It contains organisation ID, vaccination ID, patient ID, vaccination certificate.

Algorithm 2: Smart contract functionality of health organisation.

```
1.  function registerNewPatient (Patient Name, Aadhaar Number, Age, Data Availability choice)
2.      if Patient ID does not exist then
3.          Add patient to the Registered patient asset
4.      else
5.          Invalid transaction
6.      end if
7.  end function
8.  function ApproveVaccinationRequest (patient name, Date, Time, Requested vaccination, status)
9.      if Patient ID exist then
10.         Approve vaccination request by adding "approved" status
11.     else
12.         Invalid transaction
13.     end if
14. end function
15. function AddVaccinationCertificate (Organisation ID, Vaccination ID, patient ID, Vaccination certificate)
16.     if patient ID and vaccination ID exist then
17.         add vaccination certificate and increment vaccination count of organisation
```

```
18.     else
19.         Invalid transaction
20.     end if
21. end function
```

Algorithm 3 shows the smart contract functionality for patients. The patients only have access control to invoke the following functions (in the case of a child patient, this function can be invoked by a parent):

- patientRegistrationRequest(): This function has been defined for placing registration requests. It contains the fields of patient ID, Aadhaar number, age, and data availability choice.
- viewHealthOrganisationDetails(): This function has been defined to view health organisation details. It contains the field for organisation ID.
- addVaccinationRequest(): This function has been defined to place vaccination requests. It contains the fields of patient ID, date and time, requested vaccination, and organization ID.
- ViewHealthorganisationStatus(): This function has been defined to view the status of vaccination requests. It contains the field for the organisation ID.
- reportHealthOrganisation(): This function has been defined to report complaints against health organisations by incrementing the reported complaints. It contains the field of organisation ID.

Algorithm 3: Smart contract functionality for patients.

```
1.  function patientRegistrationRequest (Patient ID, Aadhaar Number, Age,
    Data Availability choice)
2.      if Patient ID does not exist then
3.          Add patient to the registration request asset
4.      else
5.          Invalid transaction
```

```
6.        end if
7.    end function
8.    function Viewhealthorganisation (Organisation ID)
9.        if Organisation ID exist then
10.           return Health organisation details
11.       else
12.           Invalid Organisation ID
13.       end if
14.   end function
15.   function addVaccinationRequest (patient ID, Date Time, Requested
      vaccination, Organisation ID)
16.       if patient ID exist then
17.           add vaccination request to the vaccination request asset
18.       else
19.           Invalid transaction
20.       end if
21.   end function
22.   function viewVaccinationRequestStatus (Patient ID)
23.       if Patient ID exist then
24.           return Vaccination request status
25.       else
26.           Invalid Patient ID
27.       end if
28.   end function
29.   function ReportHealthOrganisation (Organisation ID)
30.       if Organisation ID exist then
31.           Increment complaint reported
32.       else
33.           Invalid transaction
34.       end if
35.   end function
```

Algorithm 4 shows the smart contract functionality of the requesting entity. Any requesting entity with a valid patient ID and vaccination ID can invoke the below functions:

- View Vaccination certificate(): This function has been defined to view the vaccination certificate. It contains the fields of patient ID and vaccination ID.

Algorithm 4: Smart contract functionality of requesting entity.

```
1. function viewVaccinationCertificate (Patient ID, vaccination ID)
2.     if Patient ID and vaccination ID exist then
3.         return Vaccination certificate
4.     else
5.         Invalid Patient ID and vaccination ID
6.     end if
7. end function
```

5.2.3 Patient Preferences of Data Availability

In the proposed system, the patients specify their vaccination data availability choices as high, moderate, or low in the transaction request. Based on given preferences, the system stores the data at the desired number of nodes in off-chain storage. Table 5.1 provides a list of the notations used in this work along with an explanation of each. We have first calculated the possible ways to get inactive data nodes from total inactive nodes, active data nodes from total active nodes, and total data nodes from total nodes. This gives the probability of data unavailability as:

$$ {}^{T\,IAN}C_{IADN} * {}^{T\,N-T\,IAN}C_{TDN-IADN} \,/\, {}^{T\,N}C_{TDN} \tag{5.1} $$

So the probability of data availability can be calculated as

$$ P = 1-[\,({}^{TIAN}C_{IADN} * {}^{T\,N-T\,IAN}C_{TDN-IADN}) \,/\, {}^{T\,N}C_{TDN}] \tag{5.2} $$

Suppose that TN = 100, TDN = 90, IAN = 10, and IADN = 0, which gives the probability of data availability P equal to 1.

Table 5.1: Summary of notations.

Symbol	**Description**
TN	Total number of network nodes
TDN	The total percentage of data nodes
TIAN	The total percentage of inactive nodes
IADN	Inactive data node count in percentage
TDN	Total number of data nodes
TIAN	Total number of inactive nodes
IADN	Number of inactive data nodes
(TN,TDN,TIAN,IADN)	Set of private IPFS-network parameters
Q	Options to determine the number of inactive-data nodes from the total number of inactive nodes
R	Options to determine the number of active-data nodes from the total number of active nodes
S	Possible ways to get total number of data nodes from all nodes
P	Probability of data availability

5.3 Simulation Results

To analyse the performance of the vaccination framework, we have conducted experiments using the Intel Core i5, an 8th generation CPU, on an Ubuntu 64-bit

operating system with 12.00 GB of RAM. We have used the Ethereum Geth environment to create the blockchain network. Using the Solidity programming language, we have constructed a smart contract. The smart contract of the proposed design has been deployed and tested in the remix IDE. The set of APIs to communicate with the blockchain has been written in Node.js. The algorithms to compute the IPFS network parameters and probability of data availability have been written in JavaScript.

5.3.1 Computation of IPFS-Network Parameters

In this section, the private IPFS-network parameters have been calculated and are shown in Algorithm 5.

Algorithm 5: Computation of private IPFS-network parameters.

```
1.  INPUT: PPDA, TN, TIAN%, IADN%.
2.  OUTPUT: TDN, TIAN, IADN
3.  function getTotalDataNodes (PPDA, TN)
4.      if PPDA == "HIGH" then
5.          TDN% = 90
6.          TDN= TDN%*TN/100
7.          return TDN
8.      else if PPDA == "MODERATE" then
9.              TDN% = 75
10.             TDN= TDN%*TN/100
11.             return TDN
12.    else if PPDA == "LOW" then
13.            TDN% = 50
14.            TDN= TDN%*TN/100
15.            return TDN
16.    else
17.        TDN% = 50
18.         TDN= TDN%*TN/100
19.         return TDN
```

```
20.     end if
21.  end function
22.  function getTotalInactiveNodes(TN,TIAN%)
23.       TIAN= TIAN%*TN/100
24.       return TIAN
25.  end function
26.  function getInactiveDataNodes(TN,IADN%)
27.      IADN= IADN%*TN/100
28.      return IADN
29.  end function
```

Initially, the preferences for data availability for patients have been fetched from the ledger. This algorithm performs the following functions:

- getTotalDataNodes(): This function takes the patient preference for data availability and a total number of network nodes as inputs and returns the total number of data nodes as an output.
- getTotalInactiveNodes(): This function takes the total number of network nodes and inactive nodes in % of all nodes as an input, and returns the total number of inactive nodes as an output.
- getInactiveDataNodes(): function takes the total number of network nodes and in active data nodes in % of all nodes as input and returns the total number of inactive nodes as an output.

5.3.2 Computation of Probability of Data Availability

In this section, the probabilities of data availability have been calculated and are shown in Algorithm 6. This algorithm performs the following functions:

- getProbabilityofDataAvailability() This function takes the set of IPFS network parameters (TN, TDN, IAN, and IADN) as an input and returns the probability of data availability as an output. This function performs the following operations: it determines the total data nodes, total number of

inactive nodes, number of inactive data nodes, possible ways to get inactive data nodes from total inactive nodes, active data nodes from total active nodes, and total data nodes from total nodes, and finally it determines the probability of data availability.

Algorithm 6 Computation of the probability of data availability.

```
1. INPUT: Set of IPFS-network parameters (TN, TDN, TIAN, IADN)
2. OUTPUT: Probability of data availability P
3. function getProbabilityofDataAvailability (TN, TDN, TIAN, IADN)
4.         Q= combination (TIAN,IADN)
5.         R= combination ((TN-TIAN), (TDN-IADN))
6.         S = combination (TN, TDN)
7.         P = (Q*R)/S
8.         return P
9. end function
```

5.3.3 Data Availability Analysis

The patients can specify the data availability preference as high, moderate, or low. Based on preference, the system stores the data at the desired number of network nodes. If the preference is high, data is shared with 90% of the total number of network nodes. If the preference is moderate, data is maintained at 75% of the total number of network nodes. Data is kept at 50% of the total number of network nodes if the preference is low. The probability of data availability can be calculated using Equation 5.2 for different patient preferences. We have calculated the probability of data availability for each patient preference by considering the total number of nodes, the total inactive nodes (TIAN%) in % of all nodes, and inactive-data nodes (IADN%) in % of all nodes. In our investigation, TN is kept at 100, and TDN can be 90%, 75%, or 50% according to the patient preference. The IAN values have been taken as 10%, 20%, and 30%, and the IADN has been taken as 0%, 1%, 2%, 3%, 4%, and 5%. First, we have investigated the probability of data availability for different patient preferences at 10% of inactive nodes and 0-5% of inactive-data nodes, which is shown in Table 5.2.

Table 5.2: Probability of data availability at 10% down nodes.

Down data nodes in %	Preference High	Preference Moderate	Preference Low
0	1	0.999980908	0.993472384
1	1	0.999942144	0.992763175
2	0.99999999	0.999183445	0.962006667
3	0.999999186	0.993562236	0.886903568
4	0.999969002	0.968548839	0.788586783
5	0.999864321	0.936827418	0.694371652

Figure 5.5 illustrates the data availability probability with different user preferences at 10% inactive nodes.

Next, we have investigated the probability of data availability at 20% of inactive nodes and 0-5% of inactive data nodes, which is shown in Table 5.3.

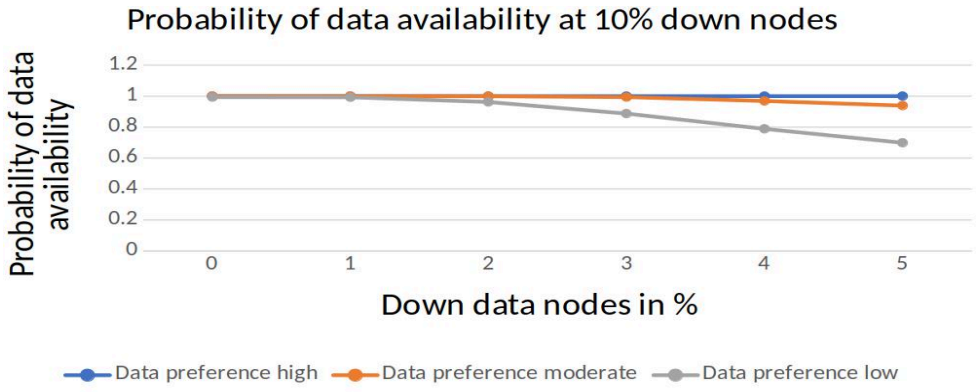


Figure 5.5: Probability of data availability at 10% down nodes.

Table 5.3: Probability of data availability at 20% down nodes.

Down data nodes in %	Preference High	Preference Moderate	Preference Low
0	0.999964426	0.992999224	0.972194988
1	0.999732146	0.991977004	0.933869161

2	0.998476583	0.990632066	0.898397569
3	0.993371798	0.98645864	0.855391381
4	0.977762382	0.95846853	0.733128782
5	0.959678436	0.92646497	0.626173786

Figure Figure 5.6 illustrates the data availability probability with different user preferences at 20% inactive nodes.

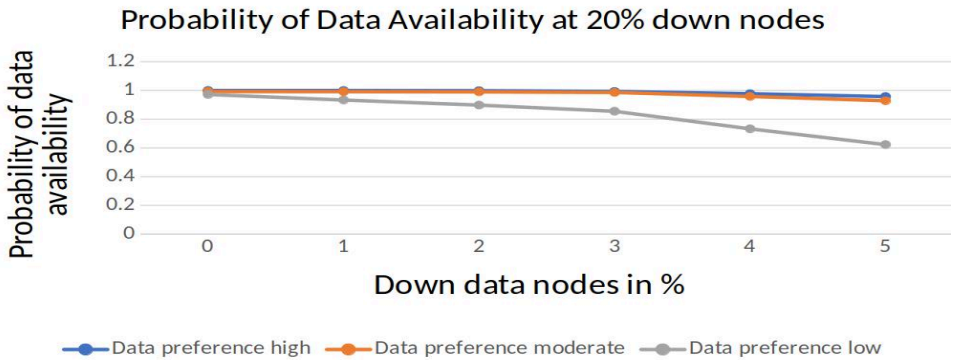


Figure 5.6: Probability of data availability at 20% down nodes.

Finally, we have investigated the probability of data availability for different patient preferences at 30% of inactive nodes and 0-5% of inactive-data nodes, which is shown in Table 5.4.

Table 5.4: Probability of data availability at 30% down nodes.

Down data nodes in %	**Preference High**	**Preference Moderate**	**Preference Low**
0	0.999998264	0.991999594	0.961331795
1	0.999642144	0.990995976	0.925382448
2	0.998083445	0.989968671	0.881029357
3	0.993262236	0.984806468	0.842788793
4	0.968548839	0.946043199	0.727516847
5	0.946325827	0.904382465	0.606825345

Figure 5.7 illustrates the data availability probability with different user preferences at 30% inactive nodes.

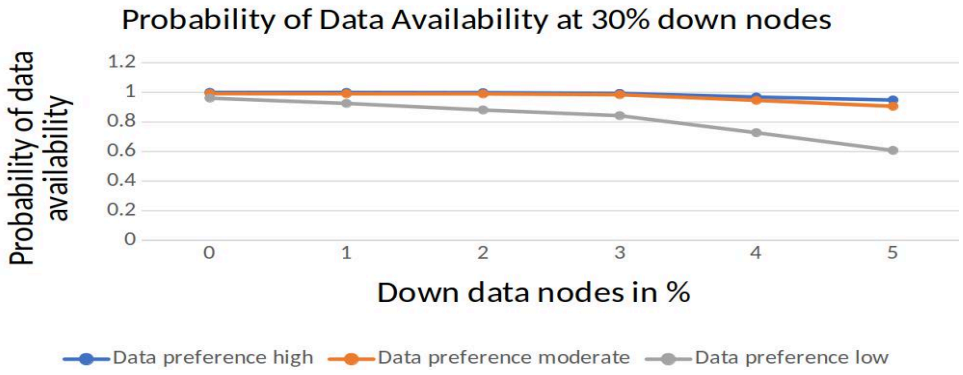


Figure 5.7 Probability of data availability at 30% down nodes.

The obtained results show that relatively better data availability has been achieved at IADN = 0-3% . For high data availability, it is between 0.9999 and 1.0000 at 10% inactive nodes, 0.9933 and 0.9999 at 20% inactive nodes, and 0.9932 and 0.9999 at 30% inactive nodes. For moderate data availability choice, it is between 0.9935 and 0.9999 at 10% inactive nodes, .9864-.9929 at 20% inactive nodes, and .9848-.9919 at 30% inactive nodes. For low data availability, it is between 0.9934 and 0.9869 at 10% inactive nodes, 0.8553 and 0.9721 at 20% inactive nodes, and 0.8427 and 0.9613 at 30% inactive nodes. The probability of data availability obtained is above 90% at 10% down nodes and 0-3% inactive-data nodes. So we have concluded that the optimal probability of data availability is possible at a low storage cost by ensuring that the down data nodes should not exceed 3% of total network nodes.

5.3.4 Execution Cost Analysis

The suggested Ethereum smart contract has been developed using the Solidity programming language. The smart contract of the proposed design has been compiled and deployed in the remix environment for testing. Table 5.5 depicts our evaluation of the execution costs of the smart contract functions.

Table 5.5: Execution costs of the smart contract functions.

Function	Transaction Size (in bytes)	Execution Cost (in Gas)
reportHealthOrganisation	202	49854
approveVaccinationRequest	522	76191
registerNewPatient	650	84395
patientRegistrationRequest	692	119616
addVaccinationRequest	778	121448
addHealthOrganisation	806	128498
addVaccinationCertificate	906	212253

Figure 5.8 shows the remix IDE interface representing the smart contract functions defined in the workflow. Figure 5.9 represents the execution costs of different transaction sizes. The maximum execution cost is in the transaction of the contract, which is equal to 4291404 gas, and all transaction functions have low costs.

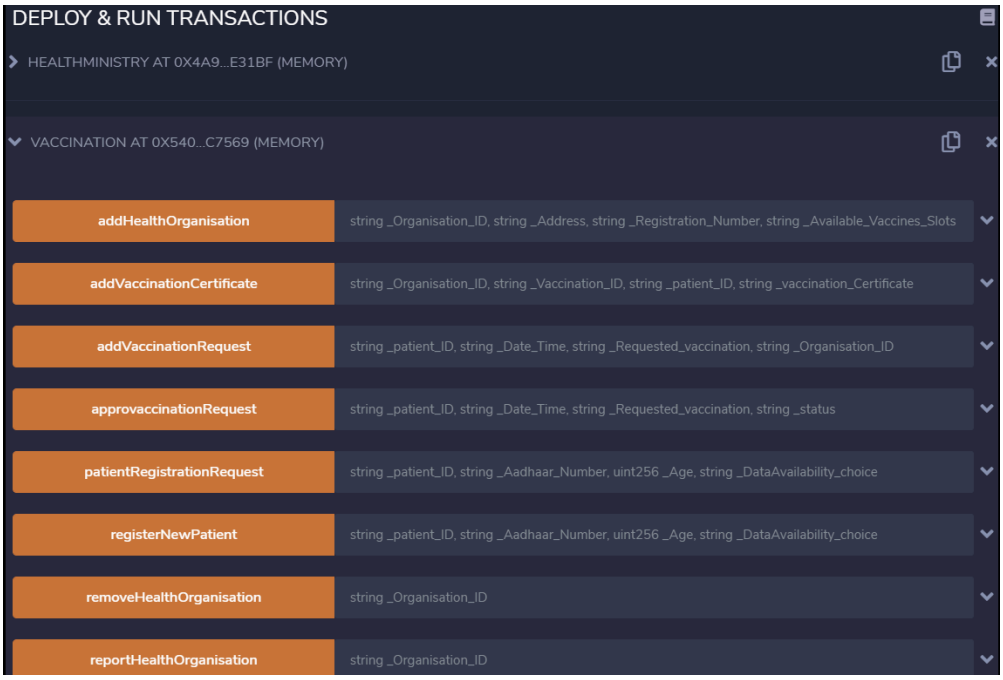


Figure 5.8: Remix IDE interface representing the smart contract functions.

Furthermore, during the testing phase, we decreased the execution fees by introducing various checks in the smart contract. These checks revert invalid transactions to avoid unnecessary execution fees due to the wastage of computation power. For scalability and cost reduction, vaccination records have been stored off-chain through IPFS based on patient preference.

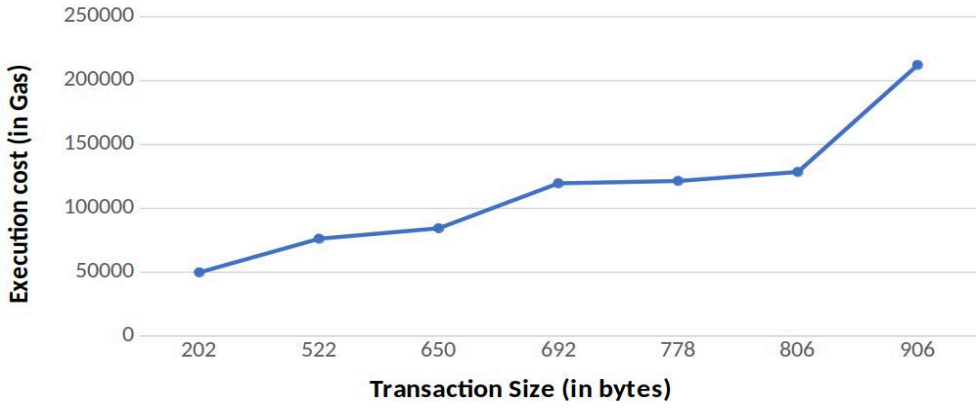


Figure 5.9: Execution costs vs. transaction sizes.

The execution cost can be reduced further by batching multiple transactions into a single transaction.

5.3.5 Energy Efficiency Analysis

For blockchain network development, we have created 1 boot node and 4 peer nodes representing the users (health ministry, health organisation, patient, and requesting entity) in the Ethereum Geth environment. The PoA consensus mechanism has been utilized for mining in the proposed system. Using the puppeth tool, only one admin node representing the health ministry has been authorised to mine blocks. Because the mining process is not completed by all peers, energy waste is reduced. Figure 5.10 represents the block sealing process at node 1 and node 2. It is clear from this figure that node 1 successfully seals a new block by committing new mining work. As only node 1 has been authorised to seal a new block, when node 2 or any other node commits new mining work, block sealing fails with the error message "Unauthorised signer". In this scheme, only one node out of four consumes energy when mining a new block. Hence, the proposed PoA consensus-based system reduces the energy consumption of

sealing new blocks by a factor of 4 as compared to the same system designed using the PoW consensus engine.

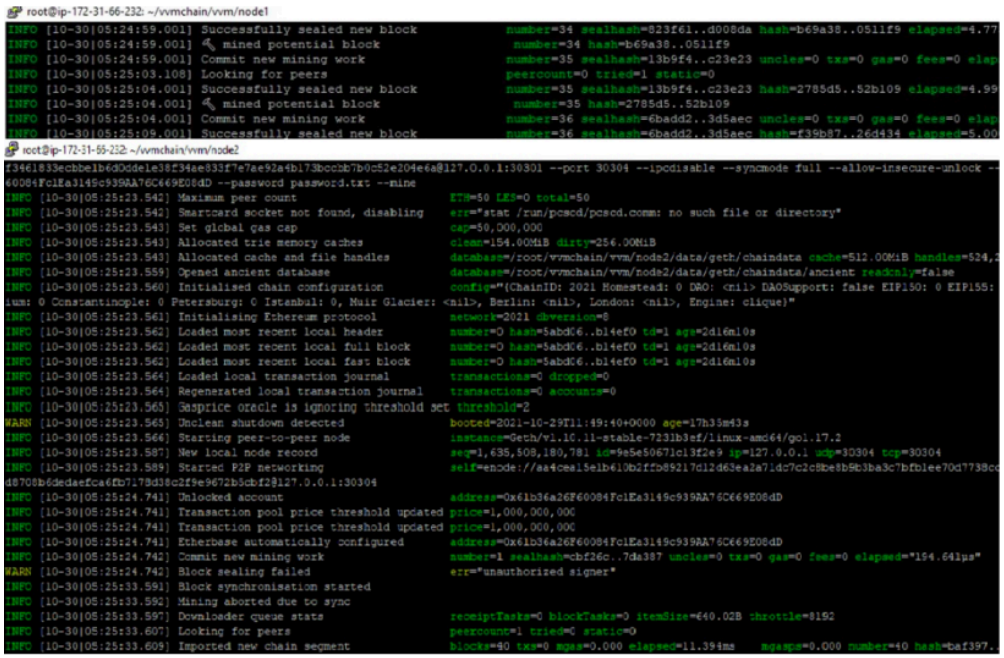


Figure 5.10: Block sealing process at node 1 and node 2.

5.3.6 Comparative analysis

There is limited work related to blockchain-based vaccination systems, almost all of which focuses on COVID vaccination records and COVID vaccine supply schemes. In this work, we have proposed an innovative, scalable, and ideal vaccination record management model based on blockchain. It is not limited to COVID-19 vaccination but is aimed toward creating the vaccination record throughout the patient's life, i.e., from childhood to death. A comparison of the proposed blockchain-based vaccination system with related work in terms of different metrics is shown in Table 5.6.

Table 5.6: Comparison of the vaccination scheme with prior works.

Qualitative metrics	**[14]**	**[15]**	**[16]**	**[17]**	**[18]**	**[108]**	**[109]**	**Proposed work**
Ethereum based	×	×	✔	✔	✔	✔	✔	✔

Smart contract	✔	✔	✔	✔	×	✔	✔	✔
Cost analysis	×	×	✔	×	×	✔	✔	✔
Energy efficient	×	×	×	×	✔	×	×	✔
Scalability	×	×	✔	×	×	✔	✔	✔
Cost efficient	×	×	×	×	×	✔	✔	✔
Availability analysis	×	×	×	×	×	×	×	✔
Validation Mechanism	×	×	×	×	×	✔	✔	✔

×: Unavailable, ✔: Available

The following summarizes the comparison of the proposed work with previous works using different performance metrics:

- Ethereum-based: Because public blockchains have a global presence, vaccination certificates issued on these systems are guaranteed to be widely acknowledged, accepted, and validated across national boundaries. There are few Ethereum blockchain-based systems [16], [17], [18], [108], [109], and very few Hyperledger blockchain based-systems [14] and [15] available. The proposed system is deployed over the Ethereum blockchain for enhanced decentralisation and global validation.

- Smart-contract: The smart contract functionalities used in this system cover the entire vaccination process with access controls, which were missing in the existing works. A novel smart contract algorithm with access control checks is developed, enabling complaints against health organizations and their removal when necessary.

- Cost-analysis: In the proposed system, within the smart contract, various checks are introduced to lower the execution cost. These checks revert invalid transactions to avoid incurring unnecessary execution fees due to computation power waste. The execution costs of various functionalities with different transaction sizes are presented for the proposed system. It

was not evaluated in most of the existing works and was not analyzed to make it lower.

- Energy-efficient: The proposed system is energy efficient in comparison to the existing systems because it is based on the PoA-consensus mechanism, whereas all others are based on PoW.

- Scalability: In the proposed work, we have provided a scalable solution using private IPFS as off-chain storage. Private IPFS was not used in the existing work but has been used with the patient preference option in the proposed scheme.

- Cost-efficient: In the proposed scheme, vaccination certificates are stored off-chain in private IPFS based on patient preference, and the hashes of the vaccination certificates are stored on the Ethereum blockchain.

- Availability analysis: We have analysed the parameters for a private IPFS network to get optimal data availability at a low storage cost. This aspect has not been addressed in any previous work.

- Validation mechanism: Most of the existing works lack validation mechanisms. We have implemented a QR code-based validation mechanism so that vaccination certificates can be verified by any requesting identity globally.

5.4 Discussion

The key results of the vaccination record management system are summarised below:

- Proposal of a decentralized model: This study introduces a scalable and cost efficient decentralized model for managing patients' lifetime vaccination records, utilizing the Ethereum blockchain to enhance decentralization and network security. The hash of vaccination certificates is stored on the Ethereum blockchain, ensuring integrity and validation.

- Development of a novel smart contract algorithm: A novel smart contract algorithm with access control checks is developed, enabling complaints

against health organizations and their removal when necessary. This ensures smooth governance of the vaccination process over the blockchain network, with a focus on low-cost execution for different transaction sizes.

- Off-chain vaccination record storage: Vaccination records are stored off-chain in private IPFS based on patient preference, ensuring scalability, availability, and reduced storage costs.

- Successful deployment of a smart contract: A smart contract has been successfully deployed over the remix IDE, and its performance has been evaluated through analysis of execution costs with varying transaction sizes. The transaction of the smart contract has the highest execution cost, which is equal to 4291404 gas, and all transaction functions have low costs.
- Utilization of the PoA consensus engine: The research employs the PoA consensus engine to reduce resource consumption and accelerate validation.

- Evaluation of data availability probability: The research evaluates the probability of data availability in a private IPFS network based on patient preference, a novel aspect not addressed in previous work. Network parameters are also analyzed to optimize storage costs. At 10% down nodes and 0-3% inactive-data nodes, the probability of data availability obtained is greater than 90%. As a result, the optimal probability of data availability at a low storage cost is possible by ensuring that down data nodes do not exceed 3% of total network nodes.

- Fraud reduction through QR code validation: The proposed design implements QR code-based validation, for effectively reducing fraud in vaccination certification. This also empowers requesting identities to verify vaccination certificates globally in order to accept and trust them.

- Comparative analysis: A comparative analysis demonstrates that the proposed blockchain-based scheme outperforms existing schemes across various performance metrics.

CHAPTER 6

BLOCKCHAIN-BASED SCALABLE DRUG DISCOVERY CHAIN MANAGEMENT SCHEME

This chapter contains the blockchain-based scalable drug discovery chain management system design, implementation and performance testing. This work can help in secure, faster and more efficient drug development.

6.1 Overview

The primary goal of the drug discovery process is to develop a novel, safe, and effective drug for treating diseases in patients. Successful collaboration among organizations involved in this process, along with the integrity of their contributions, is crucial. Traditional drug discovery chains, utilizing centralized systems, are vulnerable to cyberattacks and potential lockdowns. Leveraging the strengths of blockchain technology, with its attributes like accountability, immutability, integrity, privacy, and security, holds great promise for enhancing the management of drug discovery chains.

This study introduces an innovative Hyperledger Fabric-based drug discovery application that empowers permissioned organizations to upload, update, view, and verify contributions. Machine learning (ML) is employed for data preprocessing and feature visualization. Each contribution asset is assigned a unique identifier using the secure hash algorithm (SHA-256) in the proposed framework. The design also facilitates regulatory authorities in issuing certificates, validating ownership of contributions by contributing organizations.

Metadata and InChIKey of drug contributions are stored in the blockchain ledger, while the actual contributions are stored off-chain.

This work seeks to demonstrate how blockchain technology, coupled with machine learning, can significantly enhance and expedite the drug development life cycle, providing a secure and efficient framework. The proposed blockchain-based solution ensures data immutability through the cryptographic SHA-256 hashing algorithm, preventing duplicate contribution recordings. Notably, this study presents an end-to-end decentralized drug discovery application with a front-end interface, a feature absent in previous works. Performance analysis, using the Caliper tool, demonstrates the scalability and promise of the proposed design for drug discovery chain management.

6.2 Proposed Drug Discovery Chain Management Design

Current drug development relies on research institutes and clinical trials, where securing contributions in the drug discovery chain can be fortified through distributed ledger technology. This technology presents the potential to safeguard drug discovery data against ransomware attacks, ensuring a resilient defense. Collaboration among numerous organizations is integral to developing new drugs, and blockchain simplifies the process of uploading, sharing, updating, and validating contributions.

The drug discovery chain encompasses various stages: genomic data collection, target identification, drug development, animal testing, and clinical trials (Phase I, Phase II, and Phase III). In Stage 1, genomic data is collected and sequenced. Stage 2 involves detecting targeted proteins or nucleic acids related to a specific disease. Activities in Stage 3 include drug development, such as forming antibodies to compensate for missing proteins. Stage 4 focuses on pre-clinical testing on animals. Clinical trials progress through stages 5, 6, and 7 (Phases I, II, and III) to accumulate substantial evidence supporting the drug's effectiveness.

In our proposed drug discovery decentralized application (Dapp), data generated at each stage is seamlessly added as a contribution to the blockchain network through a user-friendly web-based interface (UI).

6.2.1 Use-case of Hyperledger-based Drug Discovery Chain

Ensuring the privacy and security of drug contributions is indispensable for the successful and ethical conduct of drug discovery. Data privacy measures play a crucial role in assuring clinical trial participants that their information is not only secure but also protected. Upholding the confidentiality of all contributions is paramount for building trust among research participants and maintaining ethical standards. In our proposed system, we employ Hyperledger Fabric blockchain technology, chosen for its inherent privacy features. Hyperledger, being a natively private blockchain, restricts accessibility solely to authorized users. The ledgers within this blockchain maintain transaction records immutably and are accessible only to permissioned users. Collaboration among multiple organizations is facilitated within the Hyperledger Fabric environment, forming a consortium blockchain network. This framework employs the execute-order-validate transaction model to expedite transaction processing. The SHA-256 algorithm is utilized to cryptographically link transaction blocks, thereby enhancing security.

Different entities within organizations are assigned roles such as user, peer, or admin, while smart contracts, known as "chaincode" in Fabric, define the application logic. Figure 6.1 presents a simplified use-case diagram of the proposed Fabric-based drug discovery chain system, offering a graphical overview of the scenario. For a more detailed description, refer to the subsequent subsections.

In this proposed scenario, users (contributors of drug discovery data) utilize a web application to submit onboarding requests. Onboarded users gain the ability to perform various actions, including uploading, updating, verifying, or viewing drug contributions. Administrative tasks, such as managing user activities and access rights within the blockchain network, are overseen by the admin. Endorsement policies are in place to precisely define access rights, ensuring users only execute authorized actions. X.509 digital certificates and public-private keys are issued by the certificate authorities of respective organizations within the blockchain network.

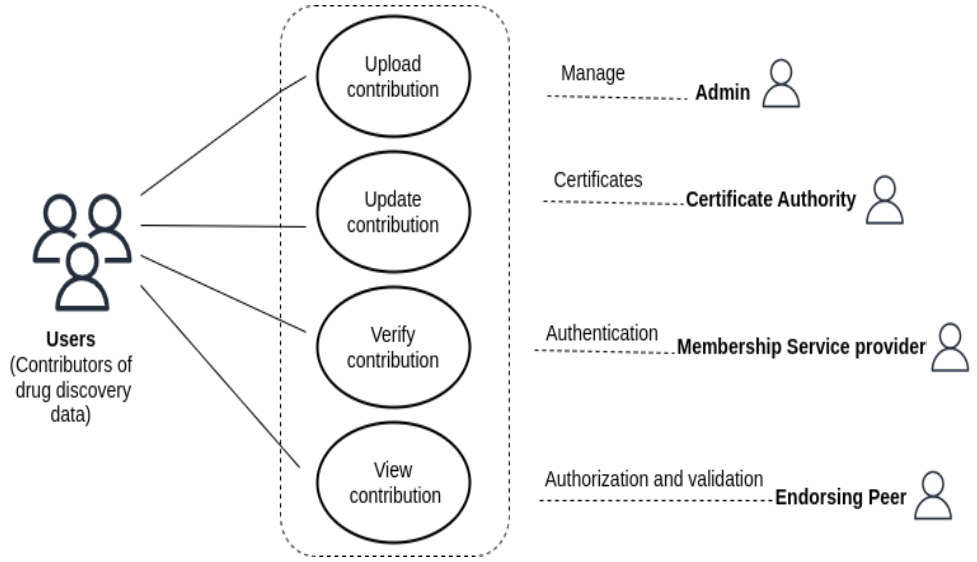


Figure 6.1: Use-case scenario of the fabric-based drug discovery chain.

Users exclusively leverage their digital identities to access the application, with the admin furnishing certificates to identify users within the network. These certificates are provided to users in response to their onboarding requests. Following successful onboarding, users are empowered to initiate transactions related to authorized drug discovery data contributions. The membership service provider conducts backend identity verification using certificates issued by the Certificate Authority (CA). Only users presenting valid certificates are authenticated to invoke transactions; otherwise, an initiation attempt fails.

After authentication, the endorsing peer scrutinizes the user's authorization (access rights) for the intended transaction. Endorsing peers then simulate requested transactions against the predefined transaction logic within the chaincode. The ordering service generates transaction blocks upon receiving responses from endorsing peers, distributing these blocks to all peers on the channel within the Hyperledger Fabric network. Users, upon validation of the transaction block by each peer, receive the network's request response through the web application. This blockchain-based system, as proposed, diligently upholds the privacy and security of contributions throughout the drug discovery process.

6.2.2 Layered Architecture

The proposed model facilitates research organizations in uploading drug discovery contributions onto the blockchain network, empowering supporting entities to access and validate them. Figure 6.2 provides a visual representation of the layered architecture of the proposed drug discovery chain management system.

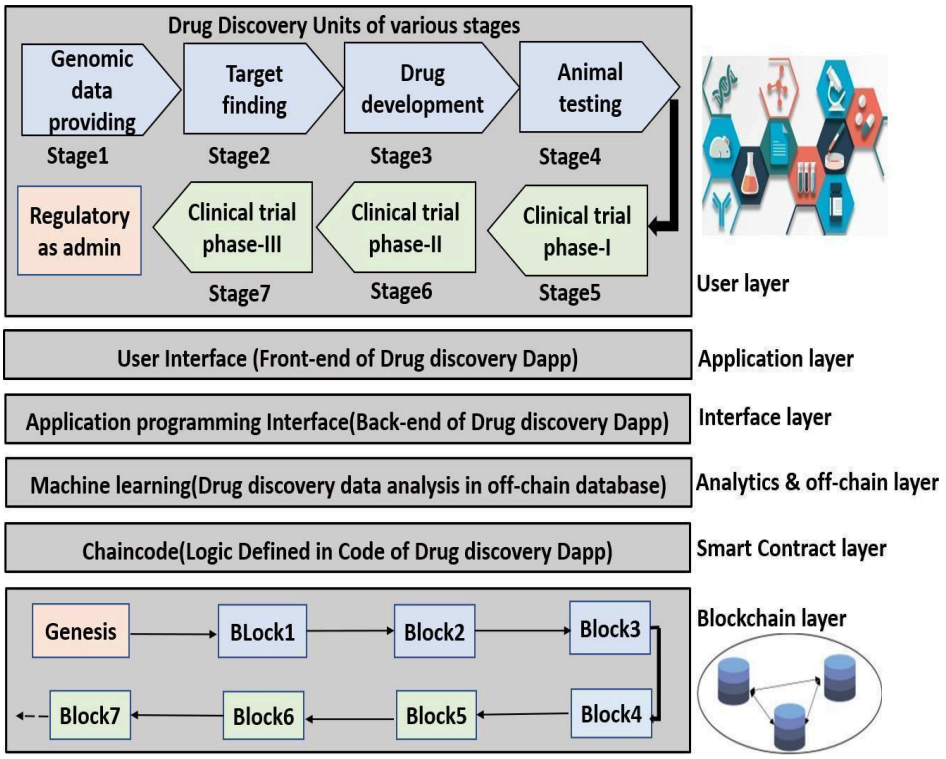


Figure 6.2: Layered architecture of the drug discovery chain design.

This architecture has six layers:

- User Layer: Users are affiliated with various drug discovery units, including genomic data, target finding, drug development, animal testing, and clinical trials (phases 1, 2, and 3). The regulatory authority functions as the admin overseeing the entire system network.
- Application Layer: Serving as the front-end of the proposed drug discovery Dapp, this layer empowers organizations to upload, update, validate, and view contributions on the blockchain ledger. It also facilitates the regulatory authority in issuing contribution certificates.

- Interface Layer: This is the application programming interface, forming the Dapp's back-end to connect the web front-end to the blockchain layer and off-chain storage.
- Analytics Layer: Acting as the preprocessing and visualization mechanism using ML, this layer collects data uploaded by the genomic data provider unit and analyzes the data within off-chain storage.
- Smart Contract Layer: Constituting the chaincode layer, this layer defines the logic of the proposed Dapp.

Blockchain Layer: This layer is responsible for creating the chain of ever-expanding drug discovery data blocks (block 1, block 2, etc.). The first block in this sequence is the Genesis block, which contains network configuration data.In the proposed system, ML models have been developed using ChEMBL bioactivity data. The ChEMBL database encompasses genomic data on over 2 million compounds. Identifying seven target proteins from this extensive genomic database, we utilized ML to visualize their quality scores. Figure 6.3 vividly presents the quality scores of the identified targets through ML.

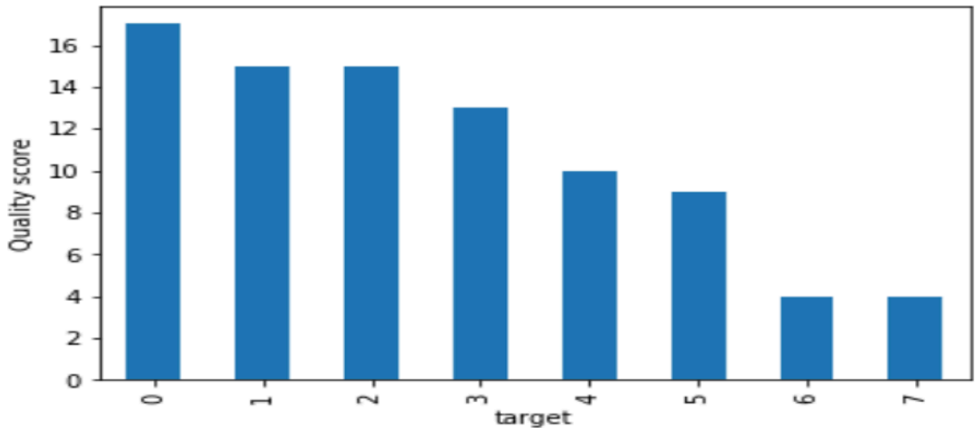


Figure 6.3: ML-based quality score analysis of searched targets.

To plot the quality scores, we employed the Matplotlib library. To enhance the performance of the proposed Dapp, we opted for an off-chain database coupled with a blockchain ledger.

The complete drug discovery contribution data is stored off-chain, while only the contribution metadata and InCHKey are stored on the blockchain network for

validation purposes. This strategic approach contributes to the efficiency of the proposed Dapp.

6.3 Design Implementation

The development environment, resources, chaincode modules, and suggested system architecture are all covered in this section.

6.3.1 Development Environment

Table 6.1 displays the configuration of the suggested scheme on an Ubuntu 64-bit environment (version 20.04.2 LTS) with 12.00 GB of RAM.

Table 6.1: Specifications of the development environment.

Name	Version
Ubuntu	20.04.2 LTS
Docker-engine	19.03.15
Docker-compose	1.24.0
Hyperledger-fabric	2.2.0
Node	10.19.0
Caliper	0.4.2
Python	3.7.2

Docker (v19.03.15) has been used to set up the Hyperledger Fabric environment, and docker-compose (v1.24.0) has been used to configure the Docker containers. For the fabric-SDK-node setup, we used Fabric (v2.2.0) and Node (v10.19.0). The Hyperledger Caliper Tool 0.4.2 version has been used to analyse the performance. ML code has been written in Python (v3.7.2) and is executed on the Jupyter notebook.

6.3.2 Proposed System Assets

The assets in the proposed system consist of drug discovery contribution records and contribution certificates. Research organizations have the ability to create or update contribution assets, each encompassing the following fields:

- Contribution ID: A unique identifier for contributions.
- Organisation Name: Name of the contributing organization.
- Contribution Data: Specific details of the contribution.

Additionally, the research authority can generate contribution certificates as assets, with each contribution certificate asset containing the following fields:

- Certificate ID: A unique identifier for contribution certificates. The certificate ID is a composite key formed by combining the contribution ID and contribution status.
- Contribution Status: Indicates the approval status of contributions.
- Owner: The owner of the contribution.
- InChIKey: The unique hash identifier of the contribution, obtained by applying the SHA-256 hashing algorithm. An InChIKey is a fixed 27-character digital representation of the input InChi string.

6.3.3 Proposed Chaincode Modules

In the proposed model, drug discovery contribution and certificate assets are formatted in JSON, and the chaincodes are scripted in NodeJS. The system incorporates diverse chaincode modules for uploading, retrieving, verifying, and updating contributions, issuing contribution certificates, and accessing contribution histories. Contributions encompass genomic data, target finding data, drug development data, animal testing results, and clinical trial outcomes. The functionalities of the chaincode modules are as follows:

- uploadContribution(): In order to upload a new contribution and store it on the ledger, involved entities call this function. It includes the following fields: contribution ID, organisation name, and contribution data.
- getContribution(): Permissioned entities can retrieve contribution details using this function. It includes the following fields: contribution ID.

- issueContributionCertificate(): This function is exclusively invoked by the regulatory authority to issue contribution certificates. It includes the following fields: contribution ID, contribution status, owner, and InChIKey.
- verifyContribution(): Any registered entity on the network can call this function to validate contributions added by different organisations. It includes the following fields: contribution ID, contribution status, and InChIKey.
- updateContribution(): To update the contribution's ownership or data, the function is called by the contribution's current owner. It includes the following fields: contribution ID, new owner, and new contribution data.
- viewContributionHistory(): Entities use this function to view a contribution's complete history. It includes the following fields: contribution ID.

Figure 6.4 illustrates the workflow of the proposed drug discovery chain. In this scheme, the genomic data unit collects genomic data, the target finding unit identifies target molecules, the drug development unit creates a new drug molecule, the animal testing unit performs pre-clinical testing, and the clinical trial units conduct various testing phases. The different drug discovery units upload their new contributions to the ledger using uploadContribution(). The regulatory authority retrieves contributions made by various organisations using the getContribution() function. The regulatory authority issues unique hash identities for uploaded drug contributions and generates contribution certificates using the issueContributionCertificate() function.

Organizations can utilize verifyContribution() to ensure the integrity of an existing contribution before making updates. Contributors have the capability to update the contribution data field of existing contribution assets through the updateContribution() function. Additionally, organizations can modify the owner field in updateContribution() to facilitate the transfer of ownership for their contributions.

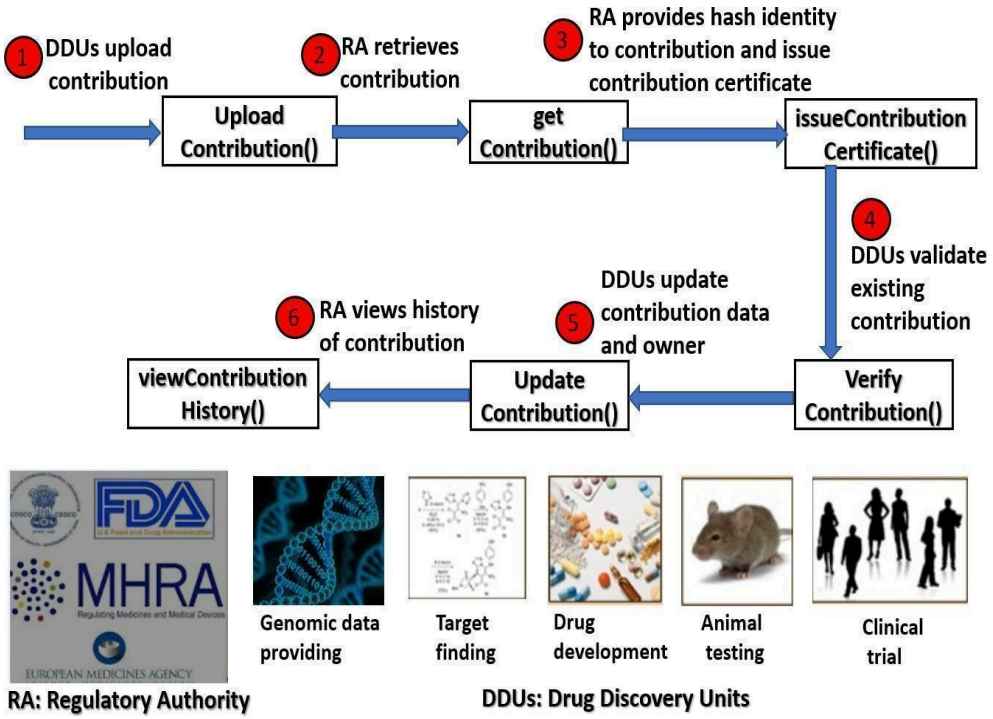


Figure 6.4: Workflow of the drug discovery management design.

Authorized users have the ability to access the comprehensive transaction history of stored contributions on the ledger by invoking viewContributionHistory(). This function also empowers the regulatory authority to validate the integrity of the new drug molecule.

6.3.4 Architecture of Drug Discovery Scheme in the Hyperledger Environment

We employed the Hyperledger Fabric blockchain framework for the proposed drug discovery Dapp. Research organizations can seamlessly contribute drug discovery data at different stages by utilizing the chaincode's upload contribution API across blockchain networks. The architecture of the proposed Hyperledger Fabric-based drug discovery network is illustrated in Figure 6.5. This architecture encompasses a single channel named the "drug discovery channel," one orderer, and three distinct organizations.

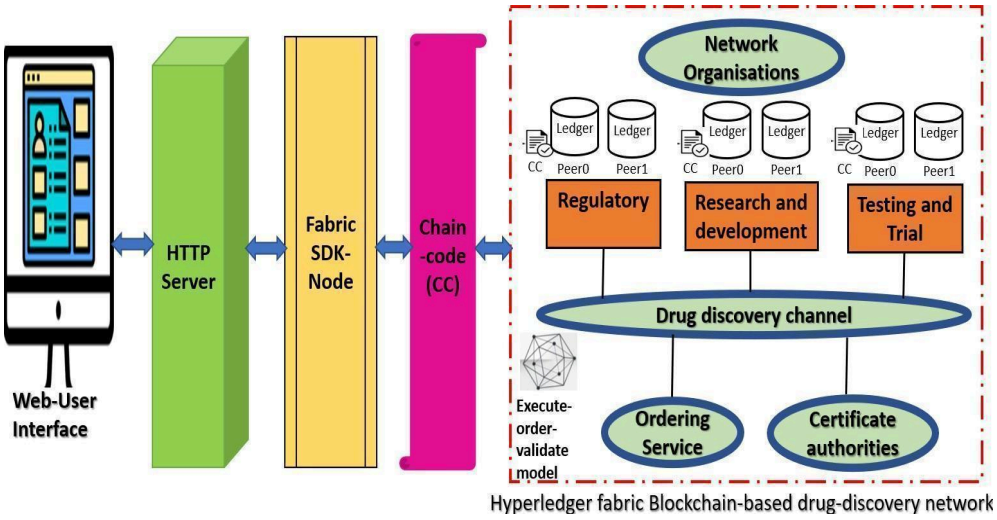


Figure 6.5: Architecture of the Fabric-based drug discovery design.

The three organizations—named "regulatory," "research and development," and "testing and trial"—each house two peers and one Certificate Authority (CA). Every peer deploys a chaincode (CC) named "drug discovery net." The process for submitting a transaction proposal involves several steps:

- Connecting with Fabric Blockchain Network: The Fabric-SDK-node tool is utilized in the system backend to link the user with the Fabric blockchain network. Fabric-node-SDK enables the invocation or querying of chaincode transactions.
- Creating APIs for Web UI Access: Node modules for various application functions are transformed into APIs, serving as endpoints accessed by the client application through HTTP requests. The "Express" library of Node.js establishes an HTTP node server, associating a URL with each node module API for execution and response retrieval.
- Storing User Certificates: The certificates required for user identification on the network are stored in a local file system directory using the FileSystemWallet class instance.
- Defining Connection Parameters: Connection parameters are outlined within a YAML file named the "common connection profile" (CCP), facilitating client connectivity with the Fabric network.
- Establishing Gateway Connection: An instance of the gateway class connects to the network using the user's identity and the CCP.

- Accessing Drug Discovery Network: The user connects to the drug discovery network using the connect() method of the gateway class. Access to the drug discovery channel and chaincodes is achieved through the getNetwork() and getContract() methods, respectively.
- Submitting Transactions: Transactions are submitted using the createTransaction() method, with the chaincode's JSON response relayed to the server.
- Orderer Processing: The orderer inserts the user transaction proposal into a block.
- Peer Validation and Ledger Update: The block is distributed to all peers on the channel, and each peer validates and updates its ledger with the latest block.
- Request Response Handling: The user receives the request response from the network through the web application, completing the recording of drug discovery contribution data in the blockchain ledger.

6.4 Results And Analysis

This section describes the results of the web interface testing, chaincode deployment, application back-end, and suggested drug discovery network configuration. Performance and comparative analysis are also included.

6.4.1 Simulation Results

In the proposed fabric-based drug discovery Dapp, comprehensive entity definitions, including peers, orderers, and certificate authorities, are encapsulated within the crypto-config.yaml file. Network configurations, detailing the capabilities and privileges of distinct services such as channels, orderers, and applications, are outlined in the configtx.yaml file. This file encompasses the genesis block file, channel configuration file, and three subsequent files dedicated to updating the anchor peers in the drug discovery network.

To initiate the foundational crypto-material, specifically X.509 certificates, for all entities, we utilized the cryptogen tool. Subsequently, the fabric configtxgen tool was employed to generate essential channel artifacts, comprising the genesis block, channel, and anchor peer configuration files. Figure 6.6 provides a visual representation of the certificate and channel configuration generation process. The genesis block serves as the inception point for the ordering service, incorporating crucial properties within the orderer profile configuration, such as orderer type, addresses, and batch size. Parameters defining block size limitations, batch timeout, maximum transaction count, and both absolute and preferred block sizes are meticulously specified under the genesis block.

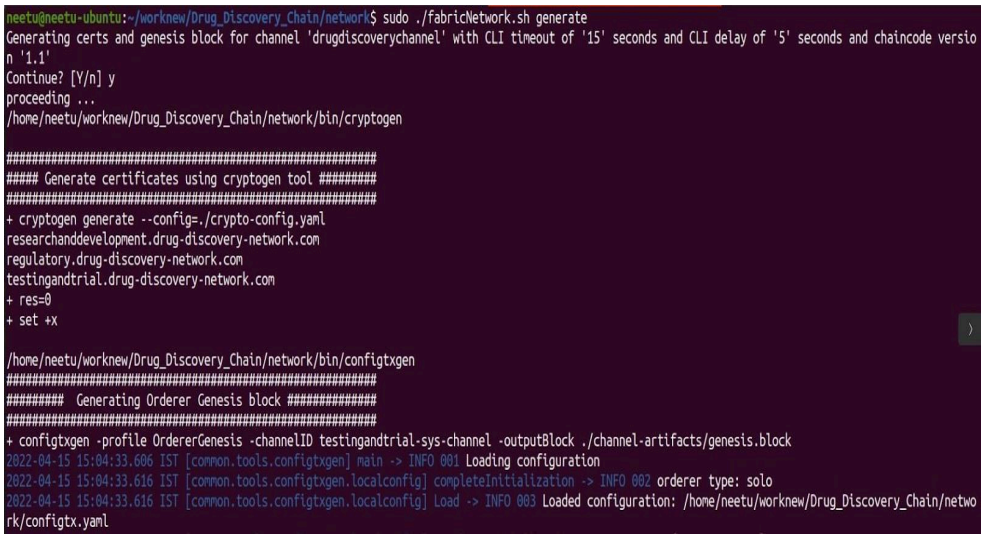


Figure 6.6: Generation of digital certificates and channel artifacts.

The research and development, regulatory, and testing and trial sectors represent the peer organizations within the proposed system. Utilizing Docker, we successfully established and executed the fabric components of the drug discovery network on a local system. As illustrated in Figure 6.7, the Docker containers for the proposed drug discovery network are depicted, showcasing essential details such as container IDs, image names, creation timestamps, status, and assigned port numbers. In total, 12 containers have been instantiated, all operating under the domain “drug-discovery-network.com.” This comprises six containers for peer organizations, three for certificate authorities, one for the CLI, one for chaincode, and one dedicated to the orderer.

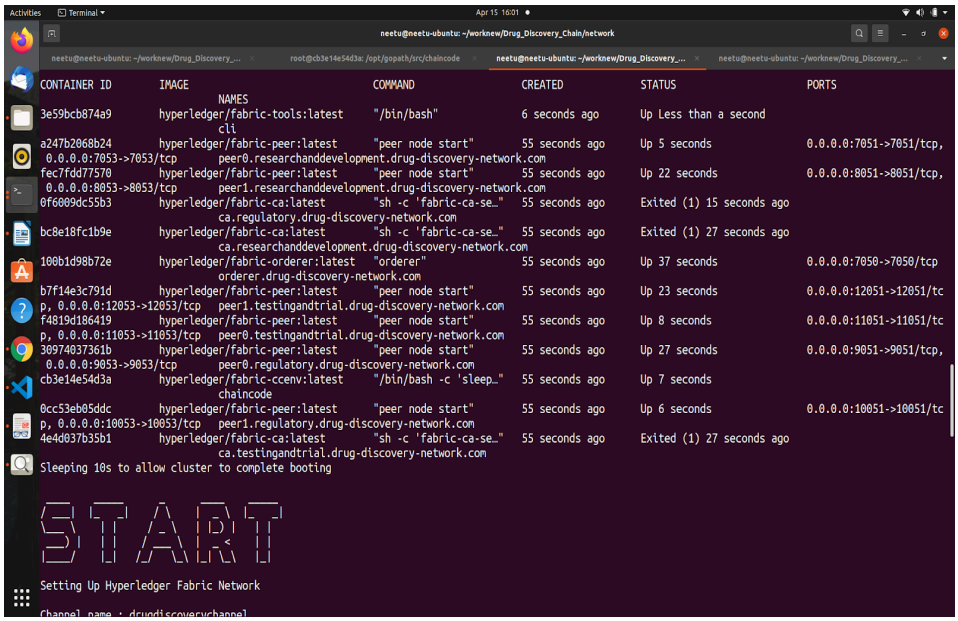


Figure 6.7: Docker containers of the drug discovery design.

Subsequently, a channel was instantiated, and all peers were enrolled in the drug discovery channel, with the anchor peers of drug discovery organizations duly updated. Following this, access to the CLI container was initiated, and a chaincode was installed on endorsing peers to facilitate the testing of APIs. The deployment process of the drug discovery chaincode is visually depicted in Figure 6.8.

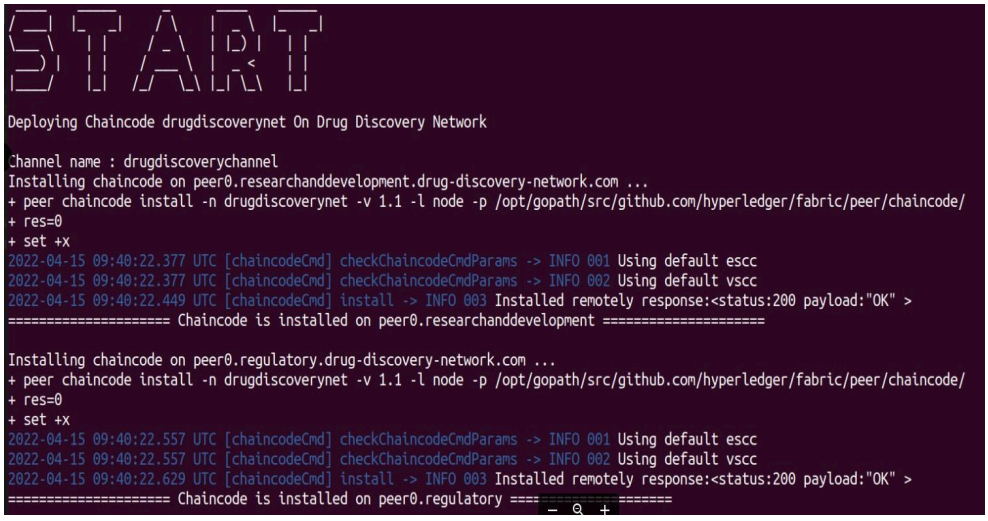


Figure 6.8: Installation of the proposed chaincode.

For the user-friendly interaction with the proposed Dapp, a front-end interface has been meticulously crafted to trigger various APIs. The initial API employed involves adding a user's identity to the wallet. Once successfully logged in using the wallet identity, users gain access to diverse functionalities within the fabric chaincode, including the ability to upload organizational contributions and view contributions. The user interface for logging into the drug discovery Dapp is aptly showcased in Figure 6.9.

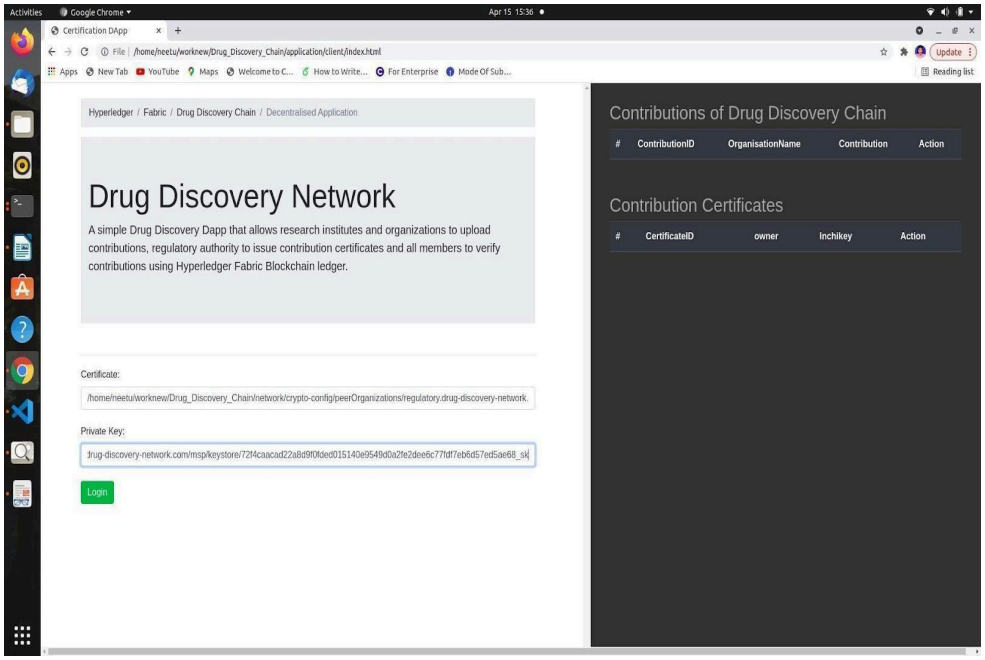


Figure 6.9: Web-interface to sign-in to the proposed Dapp.

To gain entry to the developed Dapp account, users are required to input the certificate and private key paths in the designated field and subsequently press the "login" button. Upon successful authentication, users are granted the ability to either create or update network contribution assets. Figure 6.10 illustrates the user interface for generating a contribution asset on the blockchain. This particular figure exemplifies the process of uploading genomic data as a new contribution asset. To create such an asset, users are prompted to furnish pertinent details, including the contribution ID, organization name, and contribution data. Once the user completes the input and clicks the "create contribution account" button, a contribution creation request is dispatched to the blockchain network. This, in turn, triggers the execution of the "upload contribution" chaincode API on the

blockchain. A positive response results in the creation of a new contribution asset on the UI, accompanied by an alert message stating “Contribution account created.” The successfully added contribution details are then displayed on the right side of the UI. Meanwhile, the backend of the web application undertakes the verification of the filled-out details on the blockchain network. If any contribution fields are left incomplete or contain invalid details, the system responds with an exception and an accompanying error message.

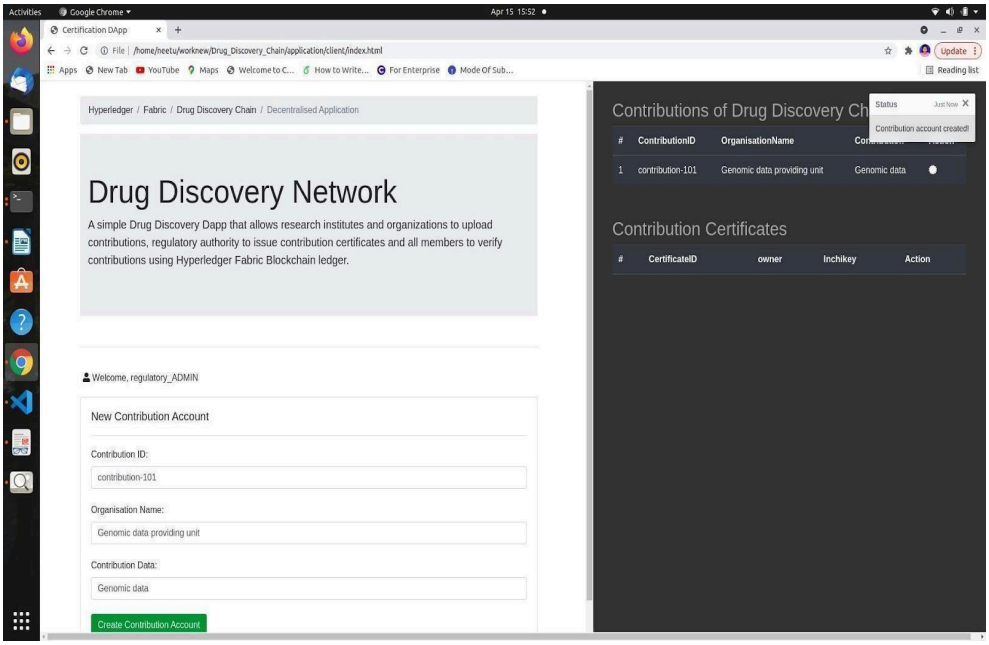


Figure 6.10: User interface to upload a new contribution.

The backend of the drug discovery Dapp, responsible for generating the contribution asset in response, is illustrated in Figure 6.11. The figure exemplifies the seamless creation of the contribution asset, incorporating attributes such as contribution ID, organization name, contribution, organization identity, creation timestamp, and update timestamp. In the Dapp's backend, the response from the blockchain-based drug discovery network is structured in JSON format. Additional contributions, including target molecules, drug molecules, pre-clinical test results, and clinical trial outcomes, can be uploaded in a similar fashion to generate new contribution assets.

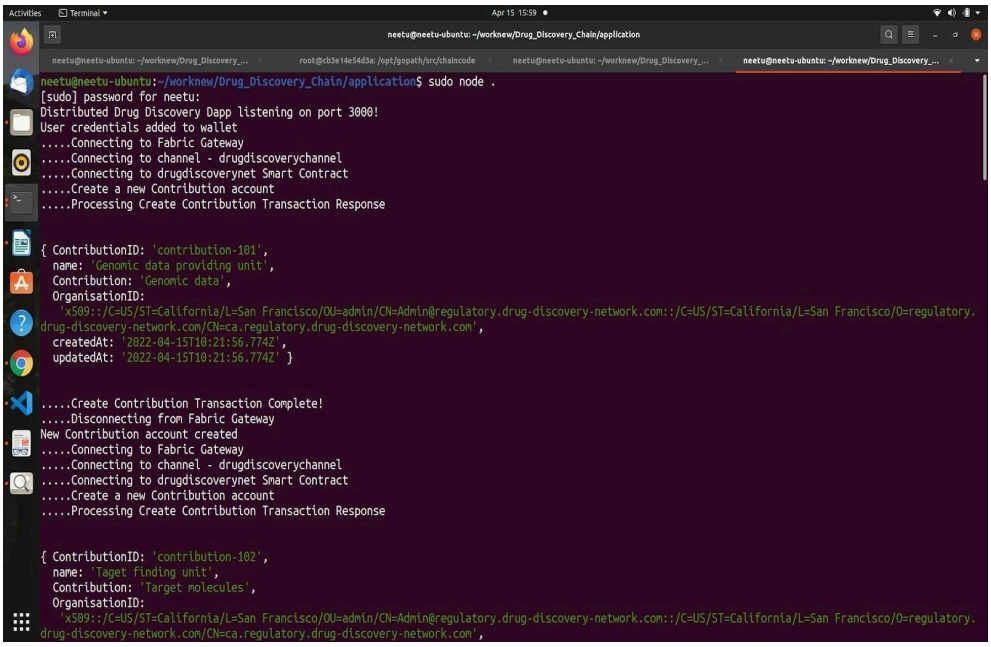


Figure 6.11: Back-end of the Dapp to create a contribution asset.

Furthermore, an API for issuing contribution certificates has been tested, catering to regulatory authorities tasked with issuing contribution certificates. Figure 6.12 visually represents the web interface designed for creating a contribution certificate asset on the blockchain. The regulatory authority can seamlessly issue a certificate for a contribution by clicking on the corresponding icon in the "Action" column. This triggers a request for a contribution certificate within the blockchain-based drug discovery network.

Upon a successful response, a new contribution certificate asset materializes on the UI, accompanied by the message "Certificate issued to contribution." The contribution certificate details undergo verification on the blockchain network through the application's back-end. In cases of invalid details, the system promptly throws an exception, conveying an error message for corrective action. Figure 6.13 provides insight into the back-end functionality of the proposed Dapp, and the creation of the response in the form of a contribution certificate asset.

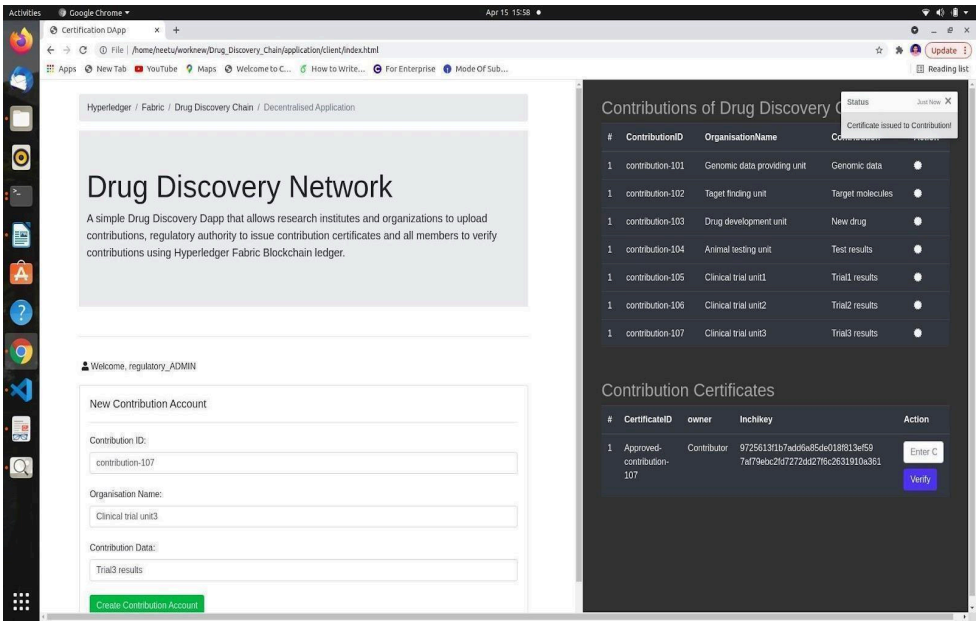


Figure 6.12: User interface to issue a contribution certificate.

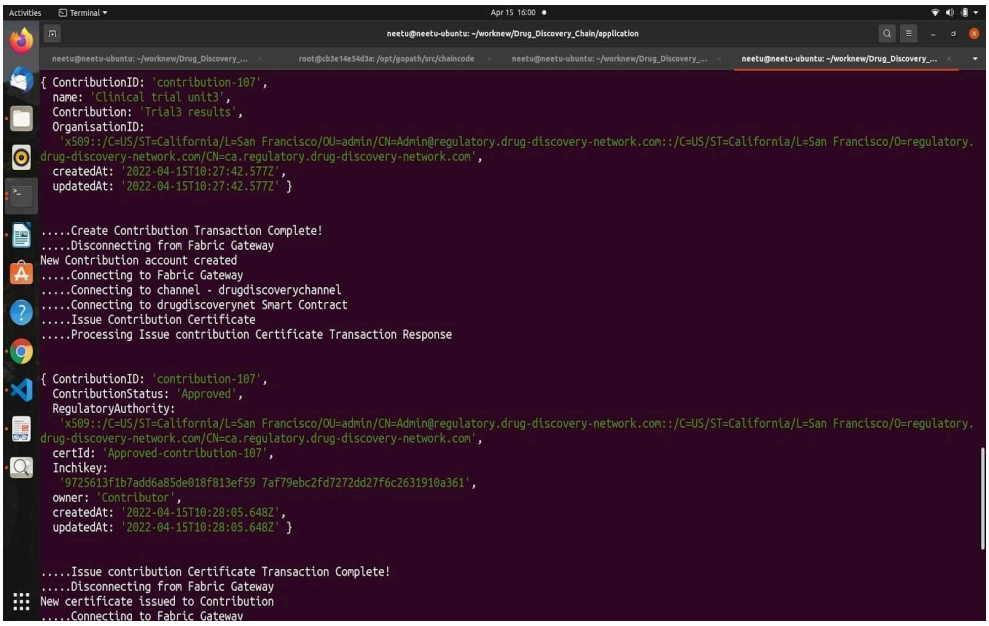


Figure 6.13: Back-end to create the contribution certificate asset.

This asset encapsulates crucial attributes, including contribution ID, contribution status, regulatory authority, certificate ID, InChIKey, owner, created at, and updated at. Once the contribution certificate is issued, its authenticity and validity can be ensured through the "verify contribution" chain code API. Figure 6.14

illuminates the user interface designed for seamlessly validating a contribution asset on the blockchain.

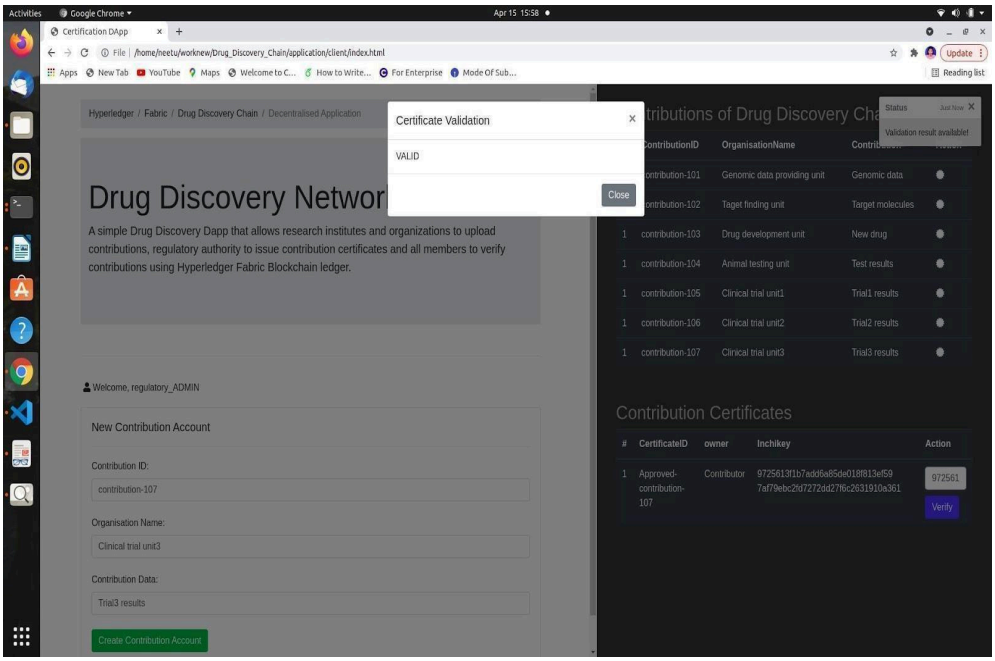


Figure 6.14: User interface to verify contribution assets.

In the input field adjacent to the InChIKey, verifiers can input the current InChIKey for the contribution, validating its match with the stored InChIKey. Upon entering an incorrect InChIKey and clicking "Verify," an alert message promptly indicates "Invalid." Conversely, if the correct InChIKey is entered and the "Verify" button is selected, an alert confirms the certificate's validity. The web application's back-end verifies contribution details on the blockchain network, and any inconsistencies prompt the system to throw an exception with an error message. Figure 6.15 illustrates the back-end of the proposed Dapp, generating responses for the "verify contribution" API. These responses encompass essential attributes, including certificate, contribution data, verifier identity, result, and verification date. The end-to-end application, inclusive of a user-friendly front-end interface and tested APIs, has been successfully developed.

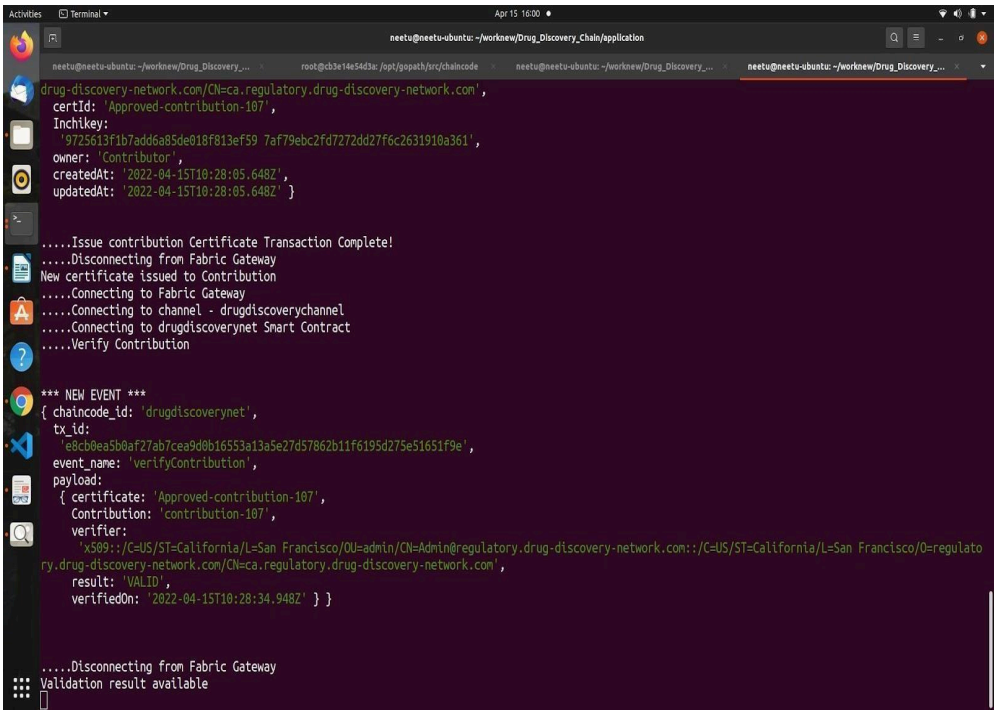


Figure 6.15: Back-end to validate the drug discovery contribution.

6.4.2 Performance Analysis

To assess the performance of the proposed fabric-based design, the Hyperledger Caliper tool is deployed. Key metrics, including throughput (successful transactions per second), latency (transaction confirmation time in seconds), and resource consumption (CPU, memory, traffic-in, traffic-out), are meticulously measured to evaluate the chaincode's efficiency. Several strategies have been implemented to enhance scalability and optimize performance:

- Set the batch timeout to 1 second in the network configuration file.
- Employ event-sourcing within the chaincode to achieve higher throughput. This technique focuses on differences in asset state stored on the ledger.
- Enhance throughput by augmenting the number of endorsers and adjusting block size.

The performance of the proposed drug discovery fabric network has been evaluated across 1, 6, 11, 16, 21, and 26 organisations, considering 1-2 endorsers to observe performance improvement trends. Additionally, variations in configuration block parameters, such as "Max Message Count," "Absolute Max

Bytes," and "Preferred Max Bytes," have been explored to gauge their impact on performance. The "uploadContribution" chaincode API is specifically used for these investigations, with a transaction rate set at 1 TPS and a transaction duration set at 30 seconds.

Figure 6.16 depicts the comprehensive test results obtained using the Caliper tool, specifically focusing on invoking the "uploadContribution" API for 21 organisations.

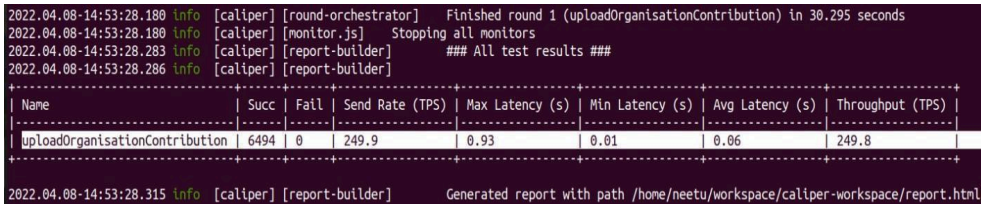


Figure 6.16: Simulation result to measure performance using the caliper tool.

The configuration block parameters, specifically "Max Message Count" set to 250, "Absolute Max Bytes" to 5 MB, and "Preferred Max Bytes" to 1 MB, have been employed for the following result. The test yielded 6494 successful transactions with zero failures. The send rate reached 249.9 TPS, and the achieved throughput stands at 249.8 TPS. Key latency metrics include a maximum latency of 0.93 seconds, a minimum latency of 0.01 seconds, and an average latency of 0.06 seconds. Figure 6.17 illustrates the throughput and latency measurements across up to 26 organisations at various block sizes.

The graphical representation in this figure accentuates that augmenting block size correlates with increased throughput and reduced latency. Specifically, when the block size for measuring chaincode performance is set at 5 MB and 10 MB, the graphs indicate a rapid increase in throughput for six organisations, followed by a gradual decrease for up to 26 organisations.

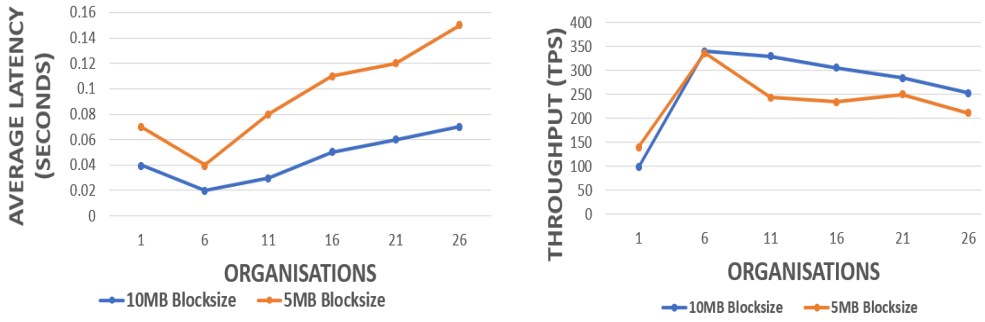


Figure 6.17: Performance analysis at different block sizes.

The throughput observed with a 10 MB block size is notably higher compared to a 5 MB block size. The average latency exhibits a gradual decrease for six organisations before rising steadily for up to 26 organisations. Particularly noteworthy is the substantially lower average latency for a 10 MB block size compared to a 5 MB block size.

Figure 6.18 details throughput and latency measurements across up to 26 organisations, varying the number of endorsers. This figure illustrates that an increase in the number of endorsers can lead to elevated throughput. Throughput experiences a rapid ascent for six organisations before gradually declining for up to 26 organisations. Simultaneously, the average latency follows a gradual decrease for six organisations before an incremental increase for up to 26 organisations. The peak throughput achieved stands at 365.2 TPS with six organisations and two endorsers.

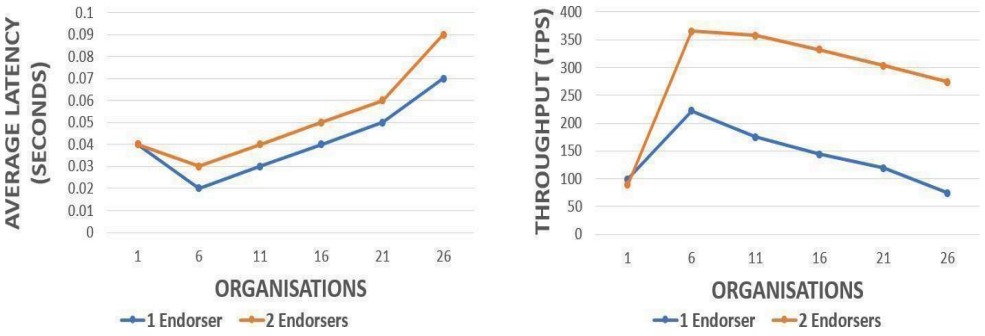


Figure 6.18: Performance analysis at different numbers of endorsers.

The resource utilization of the proposed drug discovery network has been evaluated, focusing on CPU and memory metrics. The system's resource consumption is quantified through measurements of CPU-max, CPU-avg,

memory-max, and memory-min, as presented in Table 6.2. The regulatory organization exhibited an average CPU utilization of 5.84%, with a maximum of 16.34%. Memory resource statistics were measured at a maximum of 58.8 MB and an average of 58.7 MB. The orderer node demonstrated a maximum CPU utilization of 1.54% and an average CPU utilization of 0.49%. In terms of memory, the orderer showcased a maximum utilization of 0.817 MB and an average utilization of 0.131 MB. This substantiates the low resource consumption inherent in the proposed system.

Table 6.2: Resource statistics of the drug discovery design.

Name	CPU% (max)	CPU% (avg)	Memory (max) [MB]	Memory (avg) [MB]
peer0.regulatory.drug-discovery-network.com	16.34	5.84	58.8	58.7
orderer.drug-discovery-network.com	1.54	0.49	0.817	0.131

6.4.3 Findings and Comparison

Key performance insights derived from the analysis include:

- The proposed system attains optimal performance with a throughput of 365.2 TPS, particularly evident when employing six organizations and two endorsers. This pinnacle is reached by augmenting the maximum transactions in a block to 500 and the block size to 10 MB.
- The study reveals that elevating the number of endorsers can effectively yield both high throughput and low latency.
- Comparative performance analysis against a previous model [36] demonstrates the proposed scheme's superior scalability. While the previous model struggled beyond 16 organizations, the proposed system maintained a throughput of 300 TPS and latency of 0.05 seconds under similar conditions.
- In terms of resource utilization, the developed system exhibits low CPU and memory consumption, as validated by the caliper tool.

Table 6.3 presents a comprehensive comparative analysis with prior works, emphasizing the proposed scheme's notable advancements. The existing implementation in [36] lacked various crucial components, such as architecture details, analytics, validation mechanisms, and a user interface. Meanwhile, prior theoretical works [37, 116] offered architectures for collaborative drug development but lacked blockchain integration, along with validation mechanisms, performance testing, and practical demonstrations. In contrast, the proposed scheme encompasses all these aspects, showcasing a robust design.

Table 6.3: Comparison of the proposed scheme with existing schemes.

Qualitative metrics	**[36]**	**[37]**	**[116]**	**Proposed work**
Blockchain-based	✔	×	×	✔
Analytics	×	✔	✔	✔
Architecture	×	✔	✔	✔
Validation mechanism	×	×	×	✔
Web-user interface	×	×	×	✔
Performance analysis	✔	×	×	✔
scalability	✔	×	×	✔

We presented the chaincode test outcomes through both the front-end web UI and the back-end server. Performance metrics were enhanced by systematically increasing the number of endorsers and adjusting block sizes. In our approach to enhance scalability and mitigate storage expenses, we adopted a strategy of storing only metadata on the blockchain ledger, with the remaining data securely stored off-chain.

6.5 Discussion

Key Results of the Drug Discovery Chain Management System are summarised below:

- Decentralized Drug Discovery Chain Model: Introduction of a groundbreaking model utilizing blockchain and ML to manage drug discovery contributions.
- Off-chain Storage: Only essential data, including meta-data and InChIKey, is stored on the blockchain ledger, ensuring improved scalability with the majority stored off-chain.
- ML Integration: Integration of ML for data pre-processing and visualization.
- Novel Chaincodes: Development of chaincode modules facilitating the uploading, viewing, validation, and updating of drug discovery contributions.
- Validation of Contribution Ownership: Implementation of a module issuing a contribution certificate, providing proof of ownership for contributions.
- End-to-End Application with Front-End Interface: Successful creation of a comprehensive decentralized drug discovery application, complete with a user-friendly front-end interface and test APIs.
- Scalability Improvement by Varying Network Parameters: Enhancements in performance parameters through increased endorsers and block sizes, showcasing superior scalability and advanced features.
- Performance Metrics: Peak throughput of 365.2 TPS achieved with six organizations and two endorsers, highlighting high throughput and low latency. Results indicate that adjusting the number of endorsers further improves performance.
- Performance Comparison: Comparative analysis with [36] reveals superior performance in the proposed design. With more than 16 organizations, the proposed scheme demonstrates a throughput of 300 TPS and a latency of 0.05 seconds, outperforming [36] and confirming enhanced scalability.

CHAPTER 7

BLOCKCHAIN-ENABLED TRACEABILITY AND VALIDATION SYSTEM FOR MEDICINE ANTI-COUNTERFEITING

This chapter contains the design, implementation and testing of the blockchain-enabled traceability and validation system for medicine anti-counterfeiting.

7.1 Overview

Medicine counterfeiting poses a significant threat to public healthcare, with the World Health Organization (WHO) estimating that 1 in 10 medical products in developing countries is likely counterfeit, resulting in approximately one million deaths annually. The inadequacies of existing supply chain systems, marked by a lack of transparency, integrity, security, and traceability, contribute to the risks faced by pharmaceutical brands and public health.

This chapter introduces an innovative blockchain-based multilevel security and authentication application designed to combat counterfeiting within the pharmaceutical supply chain. The application leverages a resource-efficient Hyperledger Fabric framework, where multiple computers from various supply chain organizations collaboratively establish a distributed, trustworthy network.

The proposed system targets enhancements in transparency, integrity, and traceability within the pharmaceutical supply chain. It incorporates features such as network security, privacy preservation, real-time tracking, and reliability, all facilitated by Hyperledger Fabric. To bolster authentication and verification, the

system integrates a blockchain-based QR code watermarking layer. A validation module is under development, ensuring buyers can verify the identity and history of serialized medicinal products, while buyer identity validation restricts access to legitimate buyers.

Simulation results and performance measurements demonstrate the effectiveness of the proposed system, encompassing location tracing, QR code authentication, and verification. Using the caliper tool with 100,000 transactions and 8 peers, the system achieved a peak throughput of 417.5 TPS. QR-code authentication performance was assessed under various conditions, including noisy, cropped, and blurred attacks. The supply chain implementation, along with chain code algorithms, is presented, showcasing improved scalability, validation mechanisms, throughput, latency, and resource consumption compared to existing schemes.

7.2 Proposed Medicine Anti-Counterfeiting Design

This section presents a use-case scenario that outlines the essential components and layer architecture of the suggested medicine supply chain design.

7.2.1 Proposed Use case

Counterfeiting is a severe problem in the medicine supply chain, leading to heavy revenue and brand image losses for pharmaceutical companies and posing great risks to public health. since the reliability of counterfeiting methods is still challenging. Thus, in the proposed work, blockchain technology, in integration with IoT technology, has been applied to strengthen medicine supply chain management. Figure 7.1 compares traditional and proposed multiple security-based, reliable BC based medicine supply chain schemes. The figure makes it clear that the proposed approach offers multilayer security. The system offers three levels of verification for medicines, including QR authentication, verification, and traceability. Stakeholders (referred to as organizations in this work) often involved in any supply chain system are manufacturers, distributors, retailers, consumers, and transporters.

The flow of medicine in both traditional and proposed systems is from the manufacturer's end to the consumer's end. In the traditional scenario, consumers cannot validate the origin of medical products and can unknowingly buy fake medicine, which may worsen their health. In the proposed scenario, every consumer can validate the origin of a medicine product by scanning its QR code with a smartphone. A blockchain and IOT based mechanism would detect if a code is invalid or duplicate. In the proposed scheme, the manufacturer first serializes all medicines and then labels them with encrypted QR (E-QR) codes of their serial numbers. Every shipment prepared by the manufacturer has a medicinal box with an E-QR code label that labels cartons inside the box and labels medicine strips inside the cartons. The QR code of a box contains information about the IDs of all cartons packed inside it. Similarly, the code of a carton represents the set of product IDs for all the medicines contained in it.

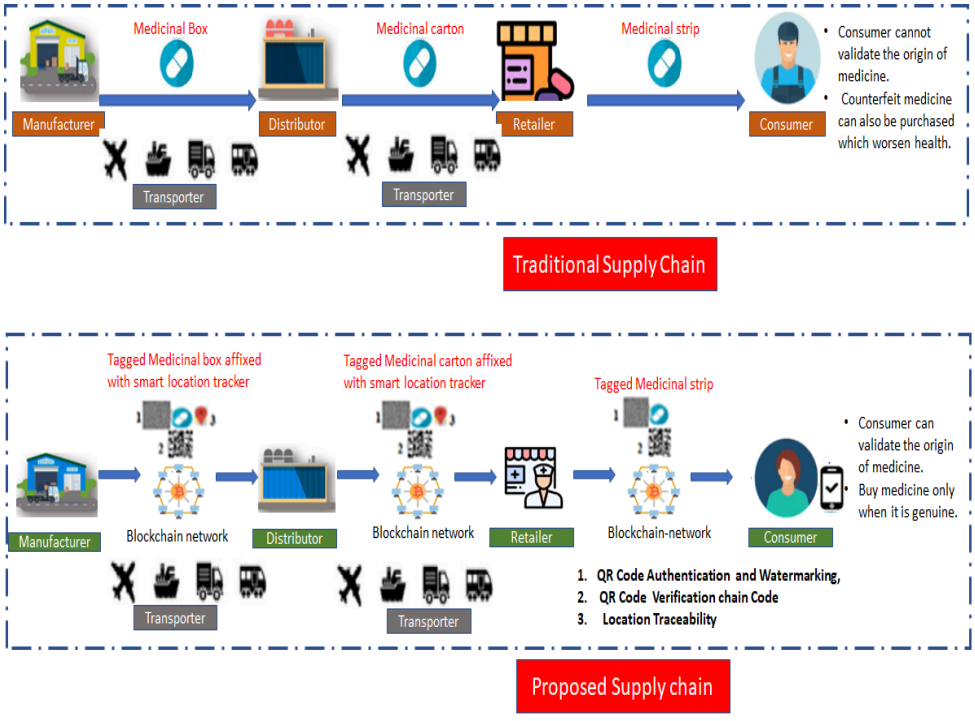


Figure 7.1: Traditional vs. proposed supply chain designs.

Labeled boxes and cartons have been integrated with smart location trackers to track medicine products. In this system, distributors can buy only medicinal boxes, retailers can buy only cartons, and consumers can buy only medicine strips. The manufacturer initially sends a labeled box tagged with a location

tracker to the distributor. A location tracker continuously transmits location data to the blockchain network, achieving real-time tracing and tracking of medicinal products. The distributor can view the E-QR (1) and has to use BC de-watermarking to decrypt the code first, then validate the history of medicinal products that are inside the box by scanning the QR code (2) of the box through the supply chain app from its registered location (3). The distributor then sends labeled cartons tagged with the Smart Location Tracker to the retailer. Retailers can view and validate the history of medicinal products received by scanning the QR code on the carton. Finally, when retailers sell labelled medicine strips, consumers can also validate medicinal products. At each point of exchange, a genuine and unique product ID is validated against the information stored on the distributed blockchain enabled platform.

7.2.2 Anti-counterfeited Supply Chain Components

There are four main components required for building the proposed medicine supply chain, namely, organizations, medicinal assets, smart contract modules, and smart devices. Organizations involved are manufacturers, distributors, retailers, consumers, and transporters. All the medicines produced by manufacturers are medicinal assets. Smart contract modules have a set of APIs (application program interfaces) for various transaction functionalities that return responses after successful execution of a transaction. Various smart contract modules are listed below:

- Onboarding: The function of the onboarding module is user onboarding, i.e. receiving and validating registration requests. Users of all organizations except consumers are required to register on the blockchain network.
- Inventory: It serializes all medicinal products after every production phase and creates an inventory of medicines. The primary purpose of this module is to buffer against uncertainty and provide protection against counterfeiting.
- Ordering: This module involves order collection and processing. It allows buyers to create a purchase order for medicines.

- Shipping: This module facilitates sellers to create medicines shipment.
- Validation: This module is responsible for authenticating stakeholders and allows authorized buyers to validate medicinal product identity. It also allows the transporter to update medicines shipment and retailer to retail medicines after successful validation.
- View: It provides functionality to trace events in the life cycle of the medicinal product from its origin.

Smart devices used in the design include a location tracker and scanner (or smartphone). Location trackers are used for keeping information on real time location, and smartphones are used for validating medicinal assets. Figure 7.2 shows the layered architecture of the proposed supply chain. As a novel addition, BC-based watermarking (BCW) with encryption/decryption capacity is introduced as the third layer of authentication, which makes the system reliable.

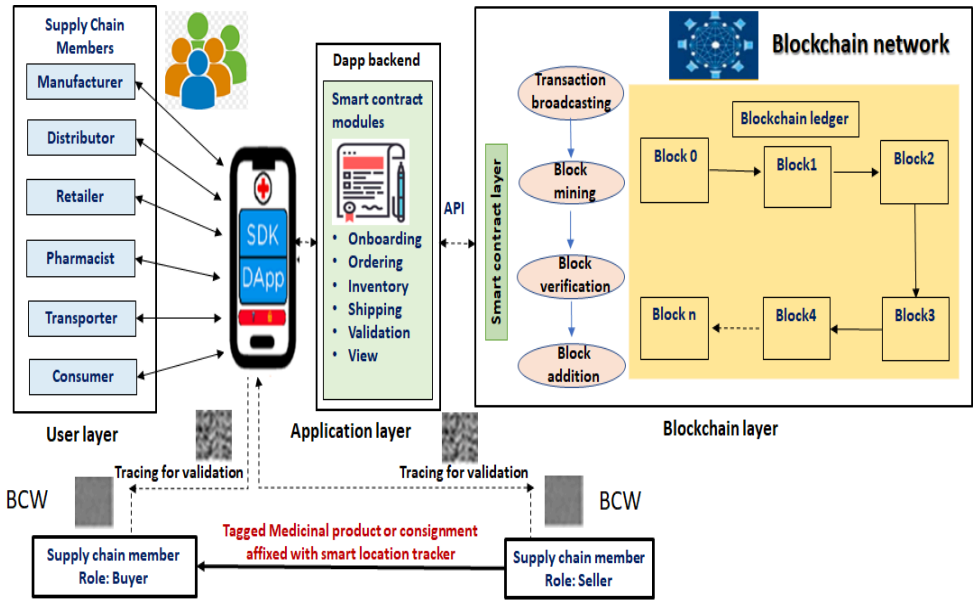


Figure. 7.2: Architecture of the medicine supply chain.

This layered architecture describes the procedure to add medicine supply chain transactions to blockchain when clients invoke smart contract functionalities.

It can be clearly observed from this Figure that each member of the supply chain has authority to verify the medicine. The trunk, box, or strip has a BCW code and has to be decrypted to generate a QR code, which is to be verified first before

access. The distributor's location must be verified across the supply chain for traceability at the manufacturer's end and the retailer's location at the distributor's end. Hence, in this turn, the proposed layered architecture makes the system more reliable. It has three layers: a user layer, an application layer, and a blockchain layer. The user layer has users (supply chain members) of the proposed system that can connect with the application layer for sending transaction requests and receiving transaction states. The Distributed Application (Dapp) layer works as an interface between blockchain clients (users) and blockchain peer nodes for transaction uploading and retrieval. The front end of the Dapp has a set of application program interfaces (APIs) to invoke all smart contract services that are present inside the smart contract layer of the blockchain network.

This layer also returns the transaction states obtained from the blockchain network to the users. The blockchain layer has a decentralized database that stores information sequentially in a chain of linked blocks. The purpose is to create trust among participants in the blockchain network. It performs tasks such as broadcasting of transactions to all peer nodes, mining of transaction blocks, verification of transaction blocks, and appending of blocks into the blockchain ledger (block1, block2. . . blockn). In this layered architecture, medicine is transferred from seller to buyer. Initially, users send registration requests to become part of the blockchain-based supply chain network for different roles. The onboarding module then processes the details provided by the users. Upon validation, the validation system updates user profiles in the ledger. After every production phase, the manufacturer serializes each medicinal product and registers it on the ledger.

Then the manufacturer affixes the medicine shipment with a smart location tracker. After that, the buyer places an order through the ordering module. Upon receiving the purchase order request, the seller creates a consignment shipment corresponding to a transporter. The transporter can update the shipment status when the consignment gets delivered to the buyer's registered location. A buyer has to verify the consignment upon receiving it. Only a genuine buyer with a valid identity can receive the shipment at the defined location. Each buyer needs to validate the ID of a medicinal product by scanning its QR code with the help of a smartphone Dapp. In cases of counterfeiting, the QR code will either be a copy

from a different transaction (already closed or in a different state/location) or not registered with the blockchain network and hence deemed invalid, which can be identified by using a Dapp. Along with Daap, BCW authentication is also available as a third layer.

7.3 Design Implementation

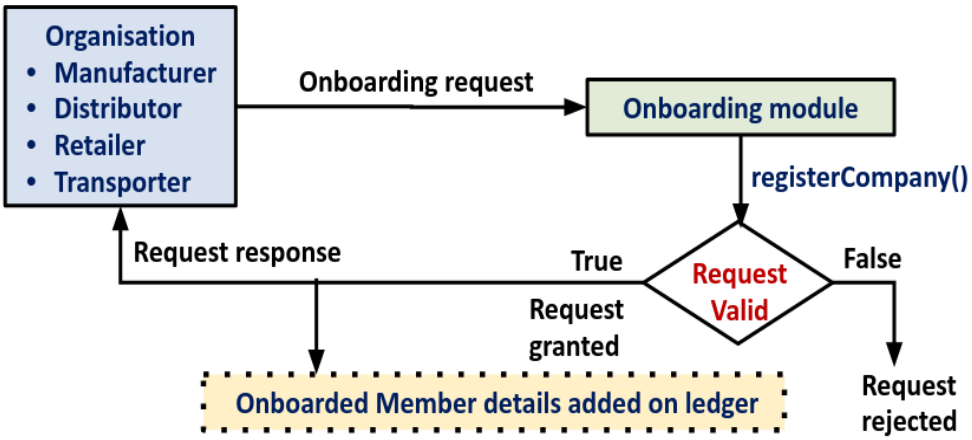
This section covers the implementation of the suggested Hyperledger-based medicine supply chain framework as well as an exploration of chaincode modules.

7.3.1 Workflow

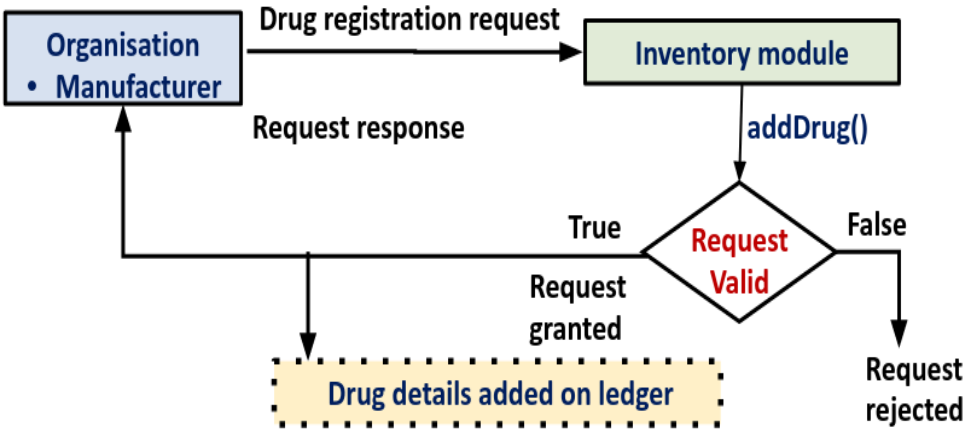
The complete workflow of the proposed system is divided into six chaincode-modules: onboarding, inventory, ordering, shipping, validation, and viewing. These modules process the transaction of medicinal products from the manufacturer's end to the consumer's end. Fig. 7.3 illustrates the workings of the onboarding, inventory, ordering, and shipping modules of the proposed system. The onboarding chain code module collects and validates the enrollment requests placed by different entities. If details are valid, then the onboarding module registers a new entity. If the details are invalid, then the request is rejected. The same module updates onboarded members' details in the ledger.

The chain code of the onboarding module has the following functionalities:

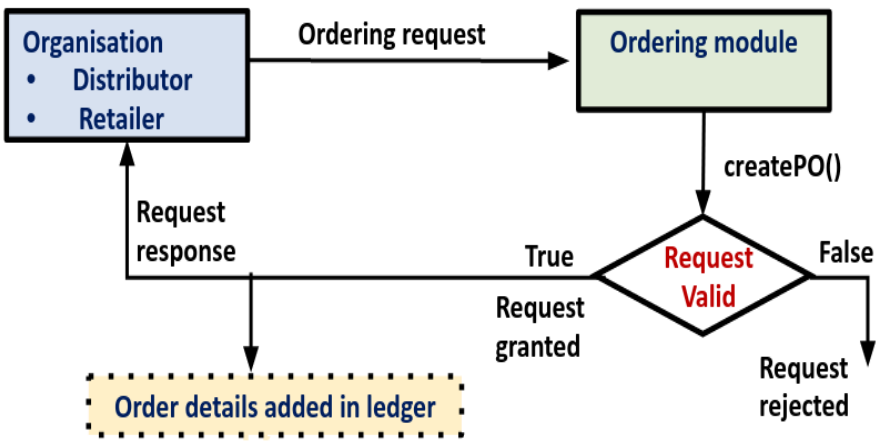
- Register Company: This function is defined to enrol a new user on the ledger in either of the following roles- manufacturer, distributor, retailer, or transporter. It contains following field Company ID, company CRN, company name, location, organization role, and hierarchy key. Company ID field is a composite key that has been determined as a combination of company CRN and company name. Hierarchy key field is 1 for a manufacturer, 2 for distributor, and 3 for retailer organization. Hierarchy key is not defined for transporters.



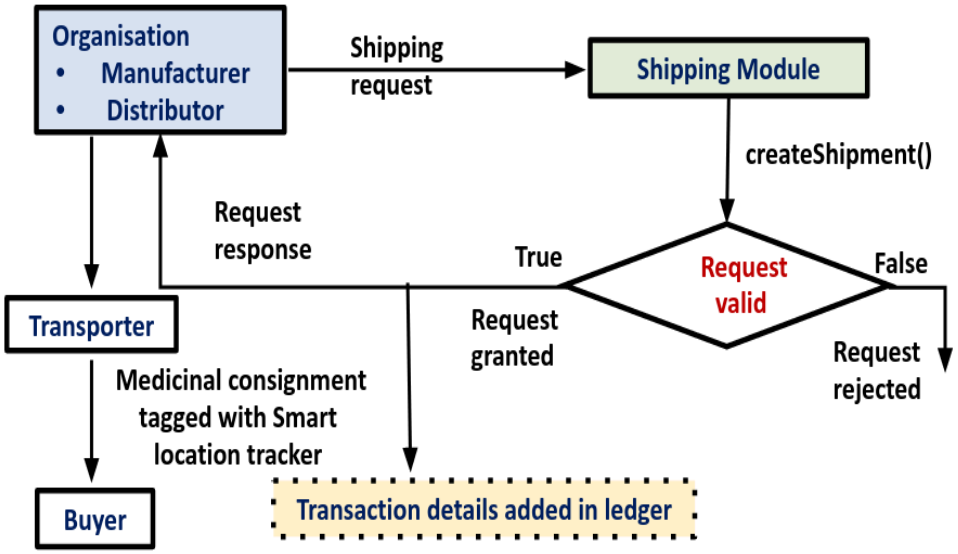
(a) Onboarding Module



(b) Inventory Module



(c) Ordering Module



(d) Shipping Module

Figure. 7.3: Illustrates the workings of various chaincode modules.

The inventory chain code module has functions to register medicinal products on the ledger. If a drug registration request is valid, then the system adds a new drug to the blockchain network. Invalid transaction requests have not been registered in the system. The chaincode of the inventory module has the following functionality:

- addDrug: This function is designed to allow registered manufacturers to be the only ones to register a new medication on the blockchain network. Product ID, drug name, serial number, manufacturer, manufacturing date, expiration date, owner, and shipment are among the fields it contains. The drug name and serial number are combined to create the composite key known as Product ID. When this transaction is first initiated, the manufacturer is the owner and the shipment field is empty.

The ordering module collects and validates order requests placed by enrolled buyers. If the orders are valid, then the order module generates purchase Order IDs; if they are invalid, the request is rejected. The order processing phase has functions to validate orders and generate order IDs. The chain code of the ordering module has the following functionality:

- createPO: This function adds purchase orders to the ledger that are placed by buyer members in order to purchase medication. Distributors and retailers are the only ones who use this function. It has fields for buyer and seller IDs, drug name, quantity, and purchase order ID. The purchase order ID is a composite key that is generated by combining the buyer's CRN and the drug name.

A newly created purchase order is further processed by the shipping module. The chain code of the shipping module has the following functionality:

- CreateShipment: This function is defined to transport the medicinal consignment through a transporter. It is invoked by seller members to respond to the purchase order function. It contains fields such as shipment, transaction creator, list of assets, transporter, and status. Shipment is a composite key that has been determined as a combination of buyer name and buyer CRN.

The buyer ID validation and the medication product ID validation are the two validations included in the validation chain code module. The validation module's operation for validating a medicine consignment is shown in Figure 7.4. Figure 7. 5 illustrates how the view module, which is used to retrieve the medication transaction history, and the validation module, which is used to validate medicine strips, operate.

Before receiving a prescription drug under the suggested system, each buyer must confirm its legitimacy by scanning the QR code on the prescription strip or consignment from the registered location via the supply chain Dapp. This is for both product and buyer identity validation. The blockchain network tracks the movement of pharmaceuticals and uses smart location tracking to determine each buyer's location.

Only customers who present the retailer with a unique identifier (such as a government-issued identification number) will be allowed to validate and purchase medications from a registered buyer location. Only a legitimate buyer with access credentials is able to accept the consignment and verify the medication. If not, the carrier returns the package because the recipient might be

a forger. This verification guarantees that the consignment can only be picked up by an authorized buyer at the registered address.

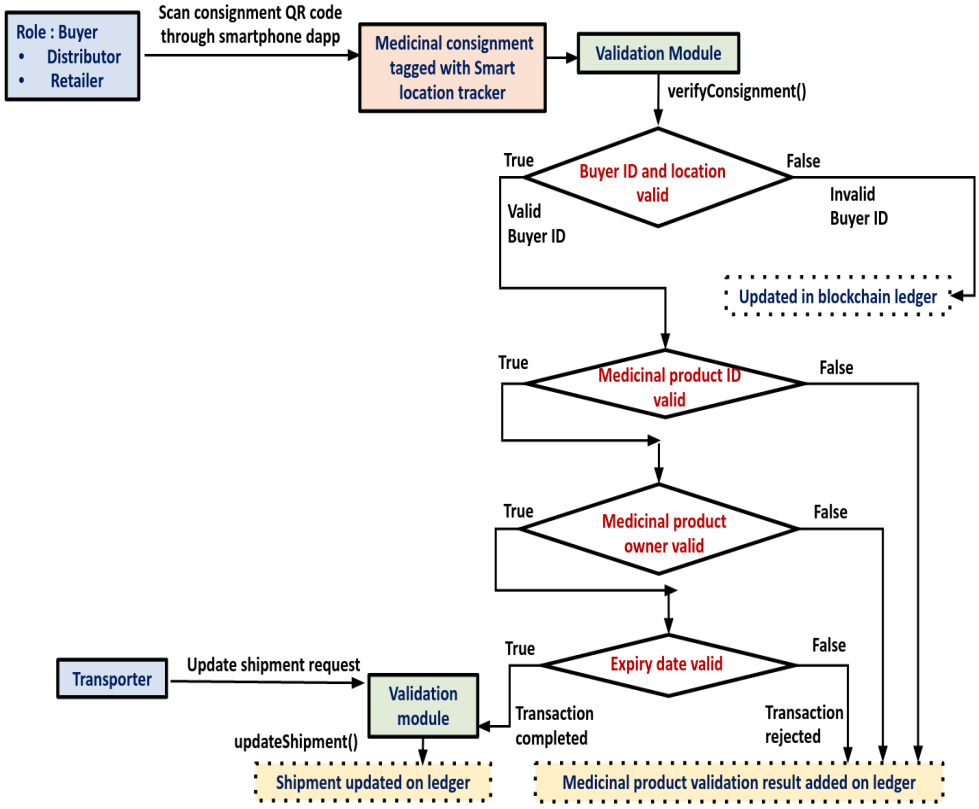
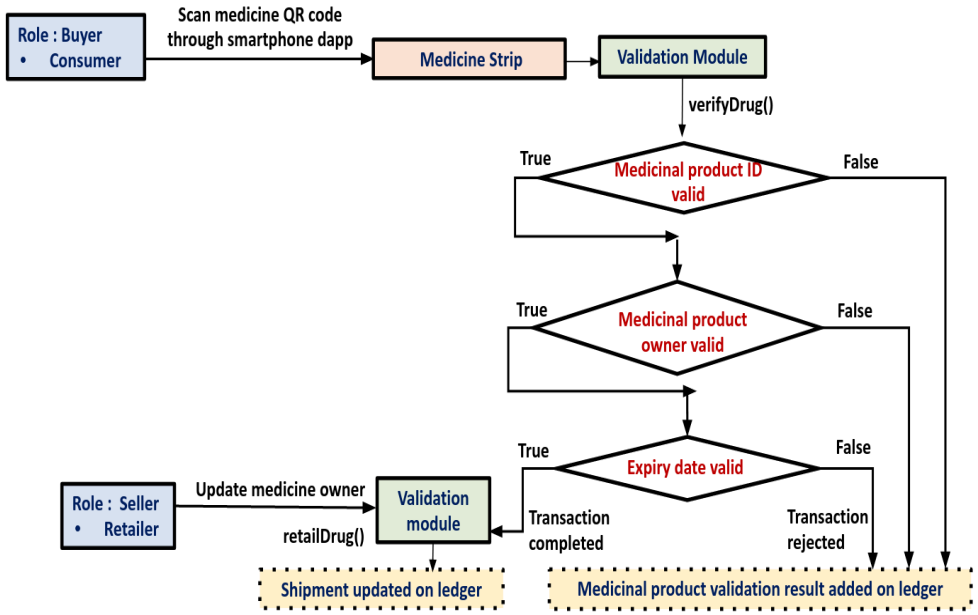


Figure 7.4: Validation module to validate medicine consignment.

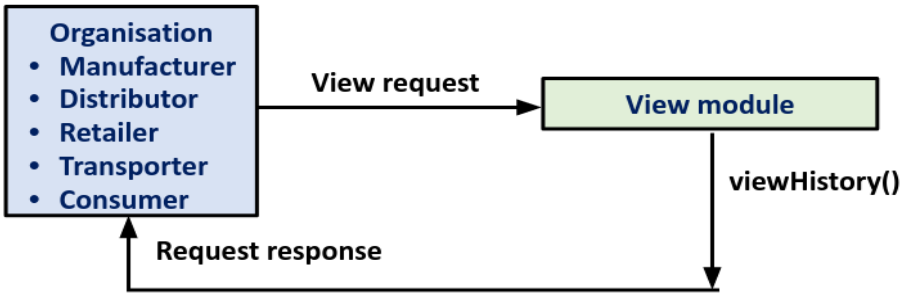
The process of validating an ID for a medicinal product involves three steps. The buyer's scanned ID for the medicinal product will only be accepted at the first level if it matches the transaction that is entered into the ledger. Only when the medicinal product ID is valid will second-level validation be examined; if not, the transaction will be declined. The current owner of the medication is verified at the second level. For instance, the retailer should be the current owner if a customer is purchasingOnly in cases where the owner is also the seller will the third-level validation process be examined; otherwise, the medication will be refused. In order to prevent the sale of an expired product, the third level verifies the medicinal product's expiration date.

Validation checks allow a successful sale of a medicinal product to initiate transaction closure. As a countermeasure against possible counterfeiting, the system rejects the transaction if the validation function returns false, indicating

failed checThis reduces the amount of fake goods in circulation by enabling customers to authenticate prescription drugs using ID scans.



(a) Validation module



(b) View Module

Figure 7.5: Validation module to validate the medicine strip and view module.

The validation modules of the chaincode has following functionalities:

- Verify Consignment: This function validates consignment for distributors or retailers. It includes buyer's CRN, list of assets (medical products), current owner, expiry date, current date, and location. It Outputs validation result and verifier ID.
- updateShipment: It updates shipment status, triggered by the transporter upon consignment dispatch. Fields include buyer's CRN, drug name, and

transporter's CRN. After delivery, updates each medicinal product's shipment information and owner field.

- retailDrug: It enables retailers to sell medicinal products to consumers. Fields incude drug name, serial number, retailer's CRN, and customer's UIN. It updates corresponding drug's owner field with the customer's UIN.
- verifyDrug: It allows consumers to validate medicine strips. fields: include drug name, serial number, current owner, expiry date, current date, and location. It outputs validation result and verifier ID.

The view module, alongside the validation module, manages view requests from authorized users across organizations, retrieving medicine transaction histories for transparency and traceability. The view module has below functionality:

- viewHistory: It allows users from any authorized organization to view the history of a medicinal product from its origin. Fields include drug name and serial number.

7.3.2 Development Environment

An Intel Core i3 8th generation CPU is used in the design and testing of the Hyperledger-based supply chain framework. The operating system employed is Ubuntu 20.04.2 LTS, a 64-bit version. The system is configured with 12.00 GB of RAM to facilitate seamless support for both development and experimental processes, as detailed in Table 7.1. The Fabric network implementation takes place in a Docker environment, leveraging Docker engine (version 19.03.15). Docker-compose (version 1.24.0) is utilized for container and Docker image configuration. Hyperledger Fabric (v2.2.0) and Node (v10.19.0) form the foundation for developing the fabric-node client SDK. Crypto-materials are generated through the crypto-config.yaml file, channel artifacts are created using the configtx.yaml file, and docker-compose.yaml files are deployed for managing Docker containers. The chain code and application files are developed in JavaScript. Testing of transaction proposals is executed through Postman, a simulation software, employing JSON format for transaction requests, including calls such as POST and GET.

Table 7.1: Specifications of the development environment

Name	Version
Ubuntu	20.04.2 LTS
Docker-engine	19.03.15
Docker-compose	1.24.0
Hyperledger-fabric	2.2.0
Node	10.19.0

7.3.3 Hyperledger-based Supply Chain Architecture

A wide range of network participants, including manufacturers, distributors, retailers, consumers, and transporters, are involved in the Hyperledger Fabric-based supply chain. Figure 7.6 shows the architectural representation of this supply chain on the Hyperledger platform. Every participant provides one user and two peers (peers 0 and 1). The anchor peer and endorsing peer are both Peer 0 from all organizations. Using the cryptogen tool, crypto-materials were created for each element in the Fabric network during the pre-setup phase, including peers, orderers, and certificate authorities (CAs). X.509 digital certificates are among these crypto-materials, which are used for user identification. The configtxgen tool was used to create channel artifacts. During the final step of network setup, Docker was used to create on a local machine all the services needed to run the fabric network components. The first step involved creating Docker containers for every peer in a variety of organizations and certificate authorities. We first configure the supply chain network's Docker containers (pharma-network), as shown in Figure 7.7, and then we log into the CLI container. From the CLI container, several crucial tasks are performed, including channel creation, ensuring the inclusion of all peers in the "pharma channel," and updating anchor peers for all organizations.

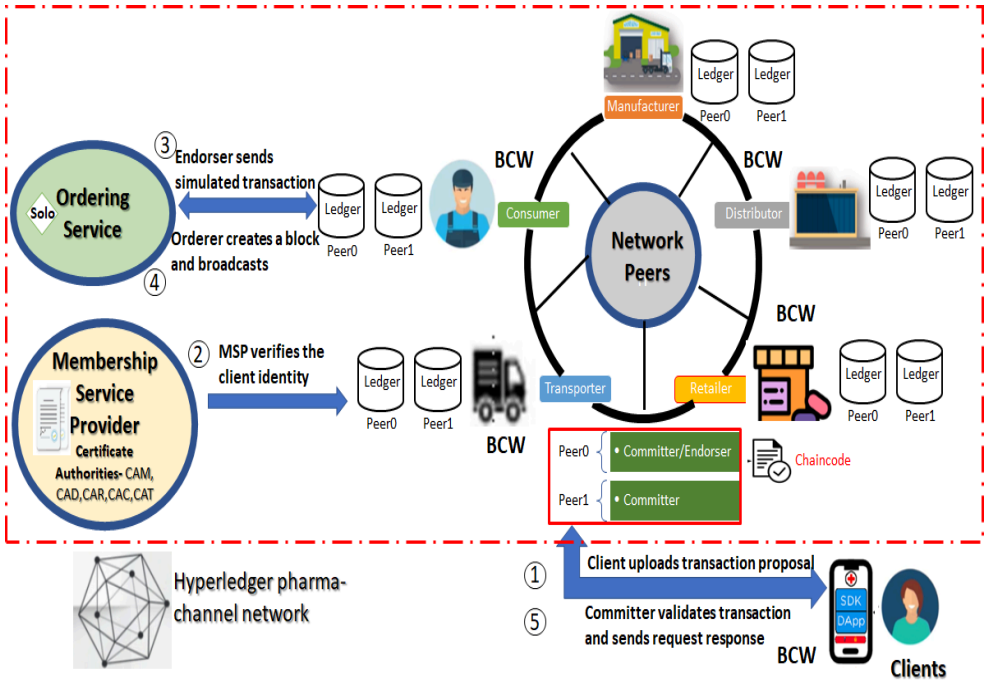


Figure. 7.6: Architecture of the fabric-based drug anti-counterfeiting design.

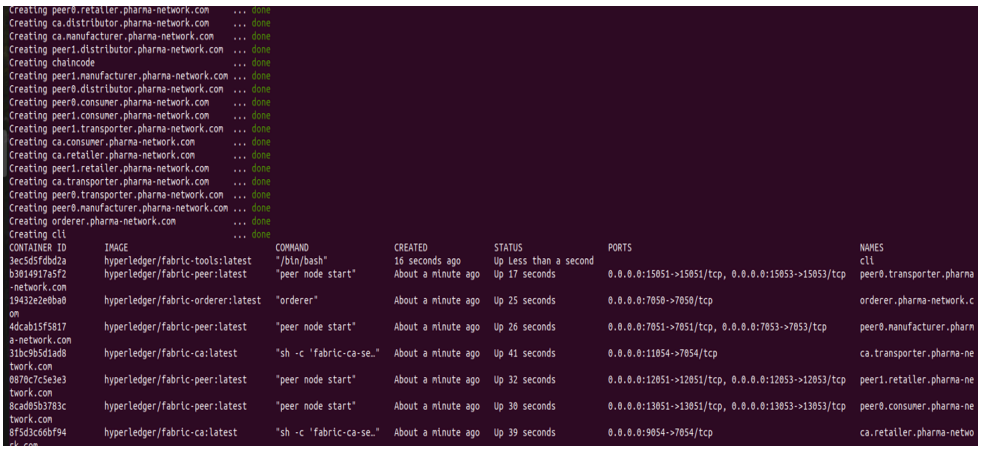


Figure 7.7: Docker containers of the drug anti-counterfeiting design.

Chaincodes have been used by endorsing peers to make it easier to register a business in different organizational roles, order drugs, ship them, validate them, and view them. Each peer receives an identity from the Membership Service Provider (MSP), introducing them to other members of the network and their respective organizations. By giving users representing registered external organizations their credentials (public-private keys), the MSP makes peer identification easier.

Network configuration and initiation are handled by the manufacturer organization, while each organization in the network maintains its own Certificate Authority (CA). The "pharma channel," the only channel in the network, manages the ledger that is only visible to peers who have joined. Each peer signs up for this channel in order to maintain a ledger and access its data.

Ensuring public health safety and combating medicine counterfeiting are the main goals of the blockchain-based system. In order to accomplish this, users must be granted the necessary permissions to invoke chain code functions through the implementation of restricted access controls. Table 7.2 outlines supply chain rights and permissions for different organizations' access controls.

Table 7.2: Access rights of organizations in supply chain design.

Organisation	**Users Role**	**Access Privileges**	**How accessed**
Manufacturer	Seller	Register company, add drug, create shipment, view history	Using public-private key
Distributor	Both seller and buyer	Register company, create purchase order, create shipment, verify consignment, view history	Using public-private key
Retailer	Both seller and buyer	Register company, create purchase order, verify consignment, retail drug, view history	Using public-private key
Consumer	Buyer	Verify drug, View history	Using public-private key
Transporter	Shipment handler	Register company, update shipment, view history	Using public-private key

The X.509 certificates (public-private keys) that authorized organizations have been granted by the certificate authorities allow them to access the fabric pharma-channel network. Within the manufacturer organization, users wield the authority to register a company, add new drugs, create shipments, and access medicine history. Distributor organization users can register a company, generate

purchase orders, create shipments, verify consignments, and view medicine history. Retailer organization users are empowered to register a company, create purchase orders, verify consignments, retail drugs, and view medicine history. Consumer organization users have authority to verify medicines and view their history. Transporter organization users can register a company, update shipments, and view medicine history.

Our ordering service employs a single-node mechanism, Solo consensus, in our implementation. The client application triggers a transaction proposal by invoking smart contract functions, with the Membership Service Provider (MSP) verifying the client's identity for authorization. The proposal is then sent to endorsers, who have deployed the chain codes. Endorsers simulate and validate the transaction based on the chaincode's business logic to achieve consensus. The ordering service captures these endorsed transactions, forms blocks, and broadcasts them to all network peers.

Committer peers validate transactions, with details propagated through the gossip protocol on the pharma channel fabric network, allowing all peers to validate them. After validation, transaction blocks are updated on each committer's peer ledger. Subsequently, the committer sends an asynchronous response to the client application. In Hyperledger Fabric, a transaction is considered final when endorsed, ordered, and validated, indicating compliance with chaincode guidelines and ledger recording.

7.3.4 Blockchain-based Watermarking (BCW)

This study introduces a robust QR code watermarking algorithm bolstered by blockchain technology. The algorithm ensures a dual-layered security approach:

- Embedding a watermark logo into the QR code: This level enhances security by incorporating a visual watermark logo, fortifying the QR code against counterfeiting and tampering.
- Blockchain-based encryption/decryption using SHA256: The algorithm leverages blockchain technology to encrypt and decrypt QR code data, instilling robust anti-counterfeiting measures and elevating overall security.

Figure 7.8 illustrates the block diagram depicting the architecture of the proposed Blockchain-based Watermarking System (BCW system).

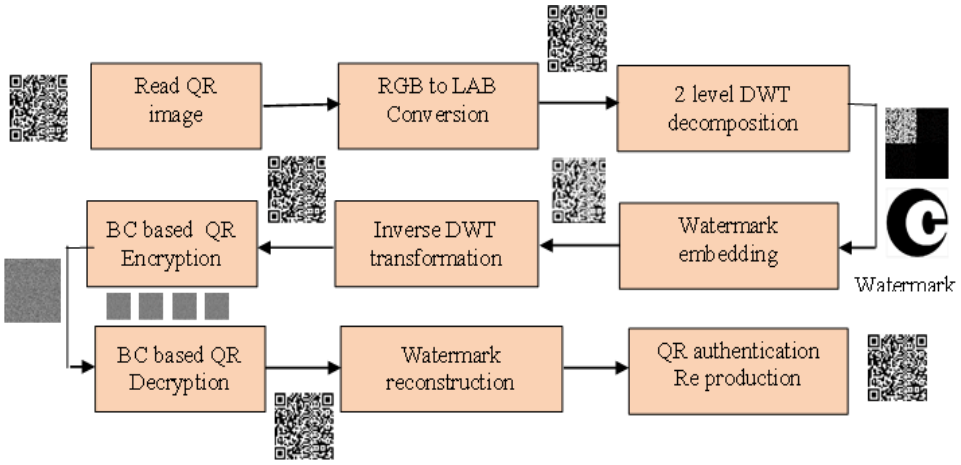


Figure 7.8: QR code watermarking using Blockchain.

7.3..4.1 Embedding with BCW

This work follows the Sobel ED technique and suggests an undetectable ED-based QR code watermarking method. To find the ED, the proper X and Y gradient masking are applied, and they are;

$$F = [(Z7 + Z8 + Z9) - (Z1 + Z2 + Z3)] + [(Z3 + Z6 + Z9) - (Z1 + Z4 + Z6)] \quad (7.1)$$

The edge coefficient of the DWT-LL sub-bands was recommended by the existing watermark insertion algorithm. The dilation coefficient of 2x2 masks across edge components is found. To create the local invisible watermark, the difference between the dilatation and edge elements—which yields the reduced features—is utilized as follows:

$$g(u, v) = f(u, v)^{di} - f(u, v)^{ed} \quad (7.2)$$

Through meticulous scaling parameter estimation, optimized at 0.9 as per valuable insights gleaned from this research, the watermark's invisibility can be maximized. This unveils a first-order scaled improvement in the watermarking rule.

$$W_T(x,y) = (1 - \alpha) * (g(u,v)) + \alpha N_{x,y} \quad (7.3)$$

The second level feature coefficient of the DWT is used as added AWGN noise, which we can refer to as an LL coefficient. Let W_E is embedded watermark as

$$W_E = LL^f_{x,y} + W_T(x,y) \quad (7.4)$$

Lastly, the watermarked QR image is created using an inverse wavelet transform. The proposed block flow of the secured watermark embedding with DWT-Blockchain decryption is shown in Figure 8. Watermarking is included in the LAB space, and the HH coefficient was replaced with the LL coefficient in a recent publication. The mathematical definition of the watermark is an additive signal or content that would be stored as a hidden watermark message b inside the bounds of known undetected distortions represented graphically by mask M. This is expressed as follows:

$$Ow = x + w(M) \quad (7.5)$$

here; x is original image or QRC

$$b = w(M) \quad (7.6)$$

7.3.4.2 SHA 256 based Encryption

The SHA-256 oriented hash algorithm relies on a 256-bit cryptographic hash function, which essentially involves two phases. In the initial step, the provided image is automatically scaled to 512x512 to align with the dimensions required for Blockchain-based encryption and the genesis packet size.

Then, each chain block with 32 bit dimensions combines 512 bits with the input vector X. In the second stage, each block of 512 bits is uniquely represented by;

$$\left[X^{(1)}, X^{(2)}, \cdots\cdots\cdots X^{(m)}\right] \quad (7.7).$$

The next step is to sequentially determine the message block numbers for 64 words or 32 bits each.

$$H^k = H^{k-1} + C^f_{S^{(k)}} * H^{k-1} \quad (7.8)$$

The encrypted QR codes are created by shuffled hash blocks and applied to the outgoing product in the supply chain.

7.4 Simulation Results

This section discloses the test results of the various chain code modules integrated into the proposed system. Snapshots illustrate the simulation results of selected chain code functions. Interaction with the system occurs through Dapp APIs, accessed via the Postman software, with transaction requests communicated in JSON format through POST and GET calls.

The simulation results are categorized into two parts. The initial segment concentrates on simulating the security and traceability aspects of the Hyperledger chain code, showcasing the obtained verification results. In the subsequent part, the simulation outcomes of QR code watermarking using Blockchain encryption are outlined.

7.4.1 Simulation Results of the Implemented Chaincodes

First, we evaluate the register company API, which is used to add various organizations to the ledger. Figure 7.9 depicts the registration process of a manufacturer company, including its name, CRN number, and location, as shown in the Dapp's post call. In a similar manner, we labeled additional organizations as distributors, retailers, or transporters and methodically added and tested them. The Dapp's backend is shown in Figure 7.10, where it is actively listening to client applications and assisting with new company registration. After carefully reviewing the register company API, we tested the addDrug API, which is only intended for manufacturers who have registered on the blockchain. A post-call to the Dapp demonstrating the registration of a medicine called Paracetamol is shown in Figure 7.11. It includes all the necessary information, including the drug's serial number, manufacturing and expiration dates, company CRN, and organizational role. The Dapp's backend, which includes information such as the

product ID, name, manufacturer, manufacturing date, expiration date, owner, and shipment, is depicted in Figure 7.12.

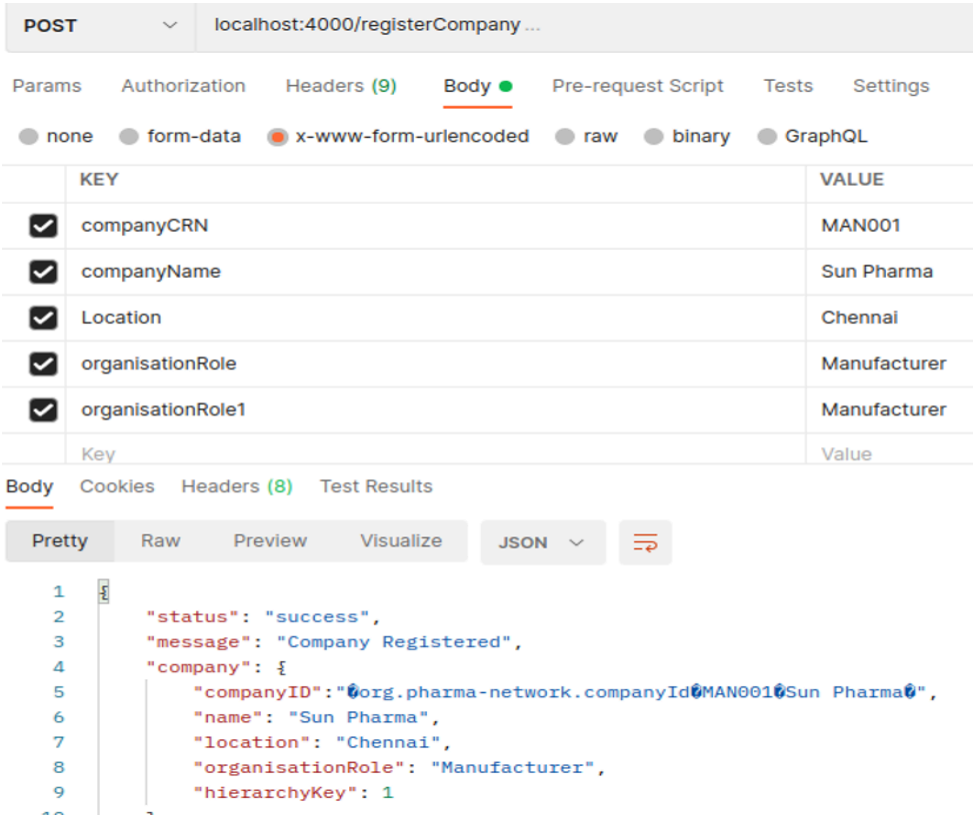


Figure 7.9: Simulation result to register a new company.

```
neetu@neetu-ubuntu:~/workspace/pharma-net/application$ node index.js
Drug counterfeiting App listening on port 4000!
Distributor identity added to wallet.
Retailer identity added to wallet.
Consumer identity added to wallet.
Transporter identity added to wallet.
Manufacturer identity added to wallet.
.....Connecting to Fabric network Gateway
.....Connecting to channel - pharma-channel
.....Connecting to pharma-net Smart Contract
New company registration request
Processing request
{
  companyID: '\x00org.pharma-network.companyId\x00MAN001\x00Sun Pharma\x00',
  name: 'Sun Pharma',
  location: 'Chennai',
  organisationRole: 'Manufacturer',
  hierarchyKey: 1
}
New company is registered
Disconnect from fabric network
.....Disconnecting from Fabric Gateway
Registering a Company
.....Connecting to Fabric network Gateway
.....Connecting to channel - pharma-channel
.....Connecting to pharma-net Smart Contract
New company registration request
Processing request
{
  companyID: '\x00org.pharma-network.companyId\x00TRA001\x00FedEx\x00',
  name: 'FedEx',
  location: 'Delhi',
  organisationRole: 'Transporter'
```

Figure 7.10: Backend to register a new company.

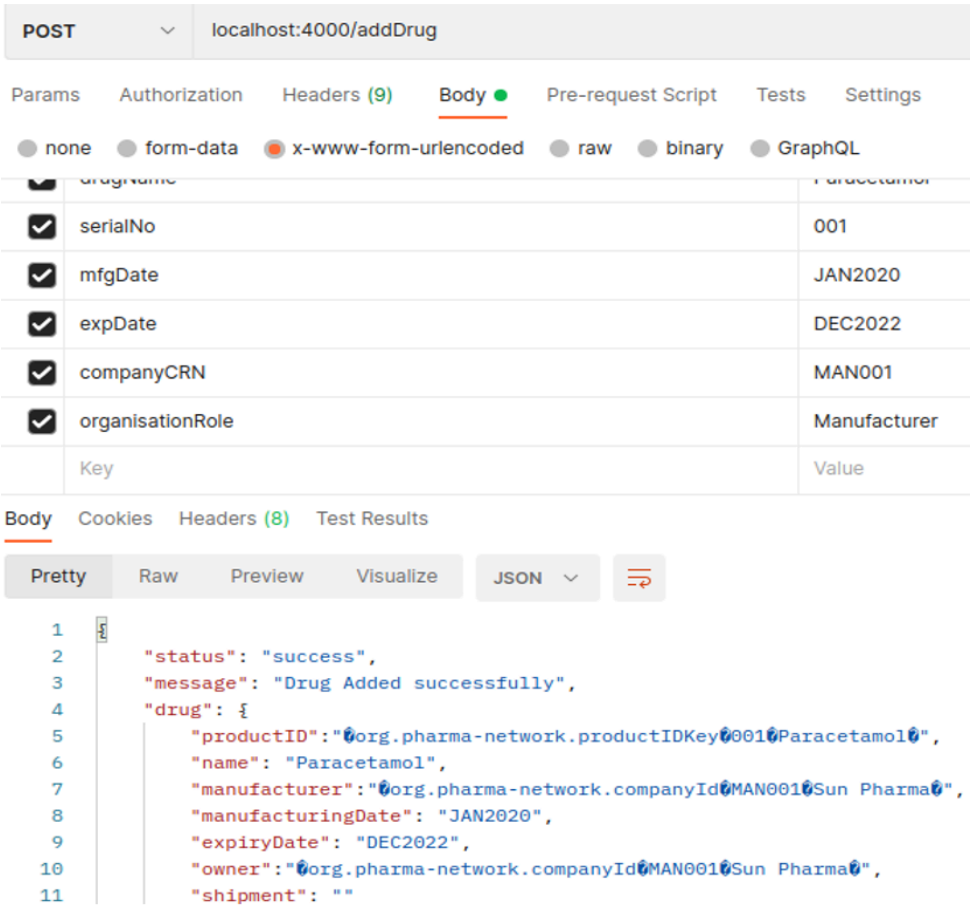


Figure 7.11: Simulation result to register a new drug.

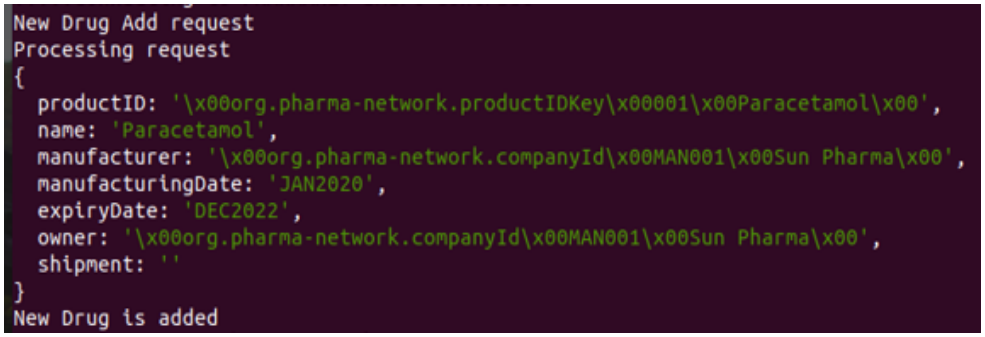


Figure 7.12: Backend to create a new drug asset.

Next, we are testing an API for creating purchase orders, or createPOs, that authorized buyer organizations can use to buy drugs. The post call to the Dapp for generating a new purchase order is displayed in Figure 7.13.

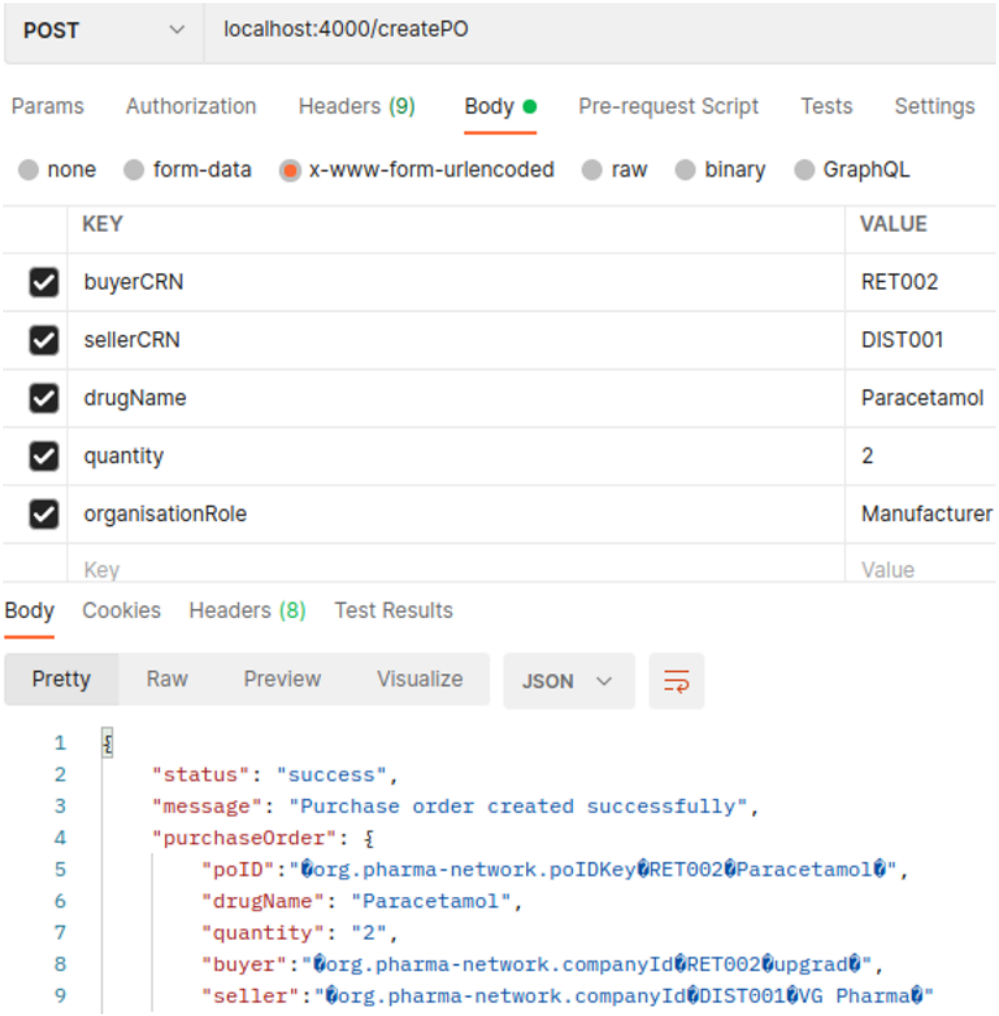


Figure 7.13: Simulation result to create a new purchase order.

It includes drug name, quantity, buyer and seller CRNs, and organization role. Next, an API to create shipments for medicine consignments is being tested. This API can be utilized by authorized seller organizations.

In Figure 7.14, the backend of the Dapp is depicted, illustrating the process of creating a shipment. This involves capturing essential details such as the shipment ID, creator, a list of assets, transporter information, and the current status of the shipment. Figure 7.15 delineates the post call to the Dapp specifically designed for the retailing of medicines. This API is employed by authorized retailers in the healthcare sector. The pertinent details included in this post call encompass the drug name, serial number, retailer, customer details, and the unique identifier (UIN), which utilizes the Aadhar number for reference.

```
Purchase Order Created
Disconnect from fabric network
.....Disconnecting from Fabric Gateway
Creating Purchase Order
.....Connecting to Fabric Gateway
.....Connecting to channel - pharmachannel
.....Connecting to PHARMANET Smart Contract
New Shipmentrequest
Processing request
{
  shipmentID: '\x00org.pharma-network.shipmentKey\x00DIST001\x00Paracetamol\x00'
  creator: '\x00org.pharma-network.companyId\x00MAN001\x00Sun Pharma\x00',
  assets: [
    '\x00org.pharma-network.productIDKey\x00001\x00Paracetamol\x00',
    '\x00org.pharma-network.productIDKey\x00002\x00Paracetamol\x00',
    '\x00org.pharma-network.productIDKey\x00003\x00Paracetamol\x00'
  ],
  transporter: '\x00org.pharma-network.companyId\x00TRA001\x00FedEx\x00',
  status: 'in-transit'
```

Figure 7.14: Backend to create a new shipment.

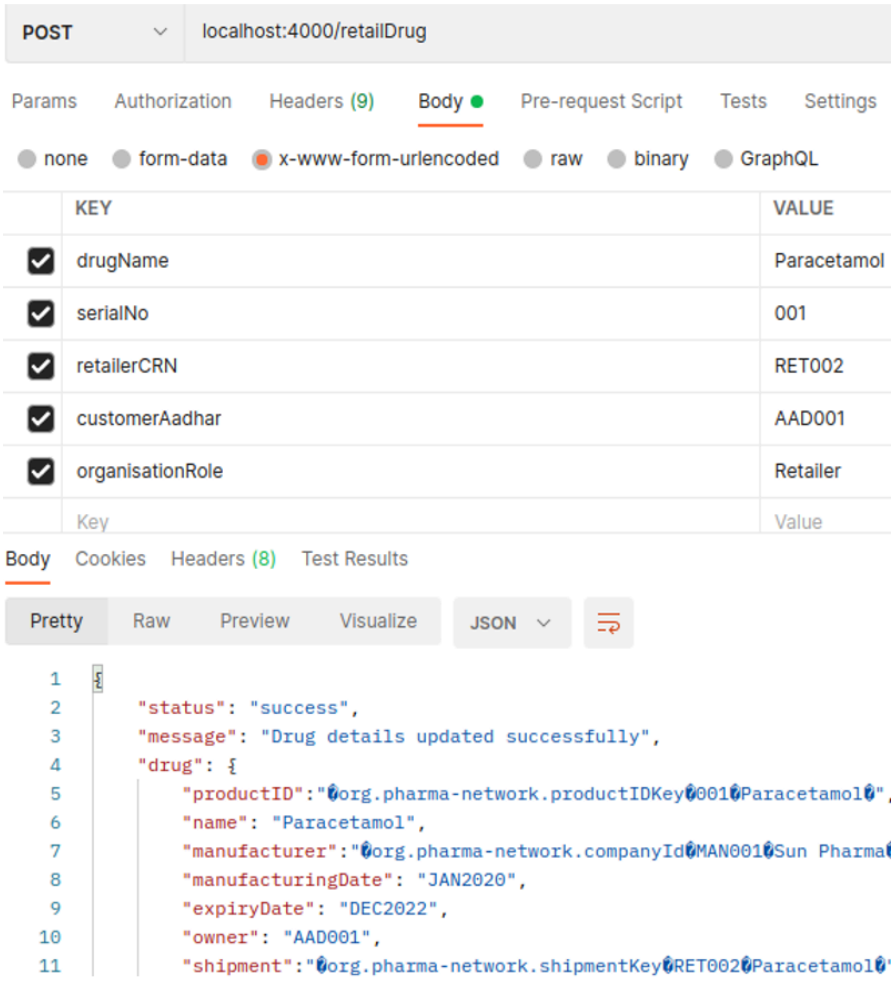


Figure 7.15: Simulation result to retail medicine.

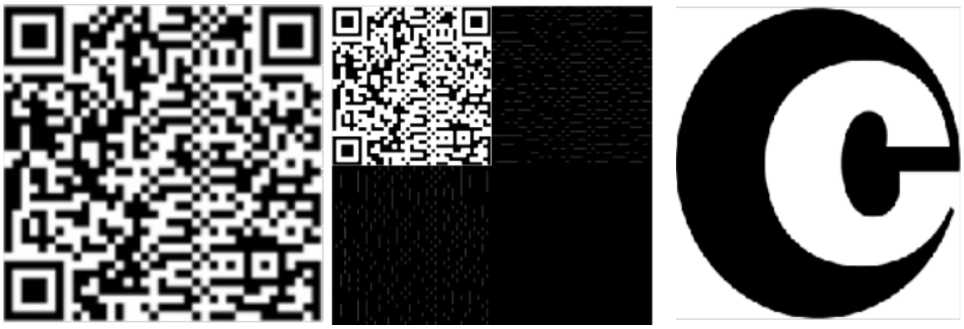
Finally, we are testing a view drug API that allows any authorized user to view a history of medications. The Dapp's backend, which retrieved medication histories with the following information, is displayed in Figure 7.16. It includes the drug name and serial number.

```
View Drug History processed
Disconnect from fabric network
.....Disconnecting from Fabric Gateway
View history of transaction on the drug
.....Connecting to Fabric Gateway
.....Connecting to channel - pharmachannel
.....Connecting to PHARMANET Smart Contract
View Drug current state Initialized
Processing View Drug current state
{
  productID: '\x00org.pharma-network.productIDKey\x00001\x00Paracetamol\x00',
  name: 'Paracetamol',
  manufacturer: '\x00org.pharma-network.companyId\x00MAN001\x00Sun Pharma\x00'
  manufacturingDate: 'JAN2020',
  expiryDate: 'DEC2022',
  owner: 'AAD001',
  shipment: '\x00org.pharma-network.shipmentKey\x00RET002\x00Paracetamol\x00'
```

Figure 7.16: Backend to view medicine history.

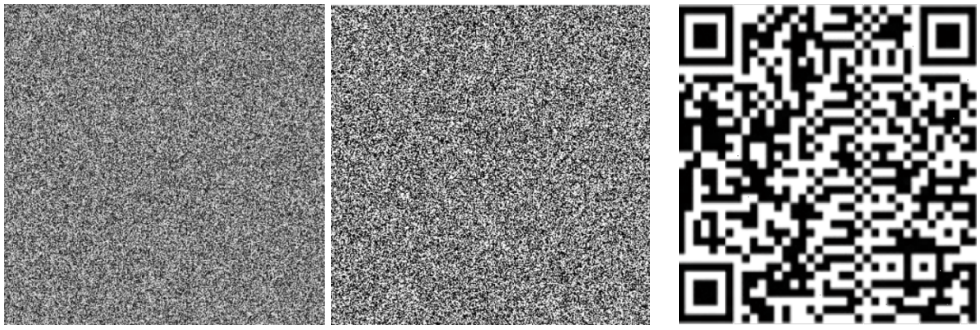
7.4.2 Result of BCW

Figure 7.17 shows the outcomes of the suggested ED wavelet domain invisible watermarking in conjunction with blockchain-based encryption for QR codes that is free from attacks. To improve security, the QR image is watermarked using the DWT-SVD-HD technique and then encrypted using a hash algorithm, as shown in Figure 7.17. The important contributions of the BCW-based QR code authentication technique are shown in this figure.



(a) Original QR Image (b) DWT wavelet decomposition (c) watermark logo

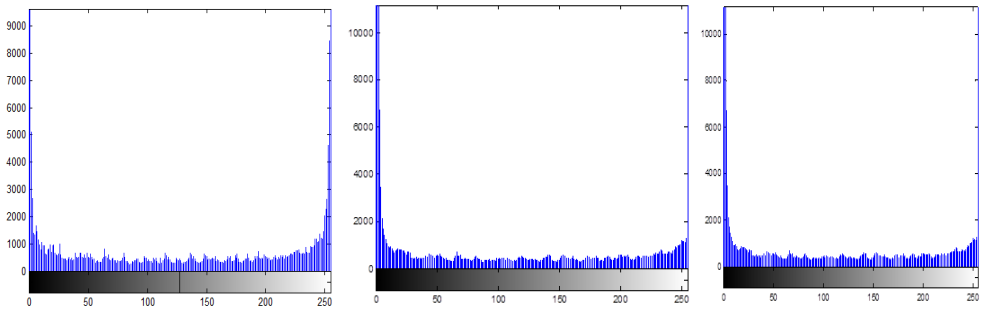
(d) LL wavelet coefficient (e) ED-DWT Watermarked image (f) shuffled image



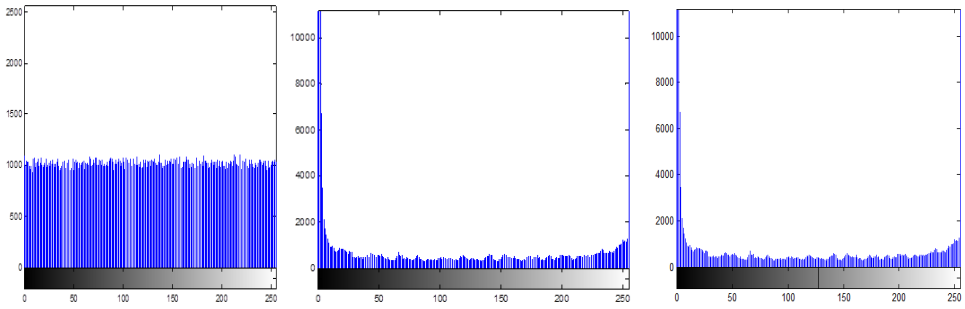
(g) Blockchain Encrypted QR image (h) Decrypted image (i) recovered QR image

Figure 7.17: Results of the QR code BCW validation process.

The step-by-step histogram analyses of the crypto weights are shown in Figure 7.18. It can be seen that the histograms show a high degree of correlation because of the QR image's restricted color features. A well-equalized (flat) histogram of the encrypted data shows the caliber of the encryption standard.



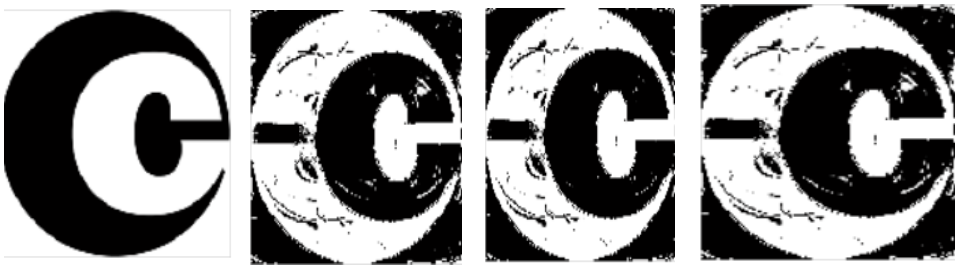
(a) Original QR Histogram (b) Blockchain Watermarked Histogram (c) shuffled Histogram



(d) Encrypted Histogram (e) decrypted Histogram (f) Recovered Histogram

Figure 7.18: Histograms of crypto weight for the BCW operation.

The outcomes of watermark extractions under different attacks, such as motion blur, noise, and filters, are displayed in Figure 7.19.



(a) Original watermark (b) Extracted with Gaussian noise (c) extracted with median Filter (d) Extracted with motion blur

Figure 7.19: Extractions of watermark under various attacks.

The attacks are used on the Blockchain-encrypted QR data in this experiment. The suggested approach works well in every attack since the histograms are already flat and show closely related patterns. Quantitative assessments provide additional support for these conclusions.

7.4.3 Performance Analysis of Fabric-based Framework

To assess the performance of our Hyperledger-based design, we employed the Hyperledger Caliper 0.4.2 framework, a tool adept at furnishing key performance metrics for systems under test. These metrics encompass success rate, throughput, latency, and resource consumption (e.g., CPU, Memory, and IO). The evaluated performance metrics include execution time, representing the duration between transaction request submission and execution; throughput, denoting the ratio of successful transactions to the total time duration in seconds; latency, signifying

the time between transaction request submission and network response; and resource metrics, determined by monitoring CPU, memory, and network I/O utilized by the blockchain system under examination.

Our assessment of the proposed system involved scrutinizing execution time, throughput, latency, and resource statistics. The testing spanned up to 100,000 transactions and 20 peers. To enhance scalability and performance, we configured the block size to 10MB and implemented the event sourcing technique in the chaincode. This technique optimizes storage efficiency by storing only the differential changes in asset state on the ledger.

The peak throughput achieved was 417.5 transactions per second (TPS) under conditions of 100,000 transactions and 8 peers. Figure 7.20 visually presents the Caliper report detailing this result.

```
2022.02.13-20:26:05.069 info  [caliper] [round-orchestrator]    Finished round 1 (addDrug) in 241.243 seconds
2022.02.13-20:26:05.069 info  [caliper] [monitor.js]    Stopping all monitors
2022.02.13-20:26:05.169 info  [caliper] [report-builder]        ### All test results ###
2022.02.13-20:26:05.172 info  [caliper] [report-builder]
+---------+--------+------+----------------+----------------+----------------+----------------+----------------+
| Name    | Succ   | Fail | Send Rate (TPS) | Max Latency (s) | Min Latency (s) | Avg Latency (s) | Throughput (TPS) |
|---------|--------|------|----------------|----------------|----------------|----------------|----------------|
| addDrug | 100000 | 0    | 417.5          | 0.20           | 0.00           | 0.03           | 417.5          |
+---------+--------+------+----------------+----------------+----------------+----------------+----------------+

2022.02.13-20:26:05.238 info  [caliper] [report-builder]        Generated report with path /home/neetu/workspace/caliper-workspace/report.html
```

Figure 7.20: Simulation result of add drug API using Hyperledger caliper tool.

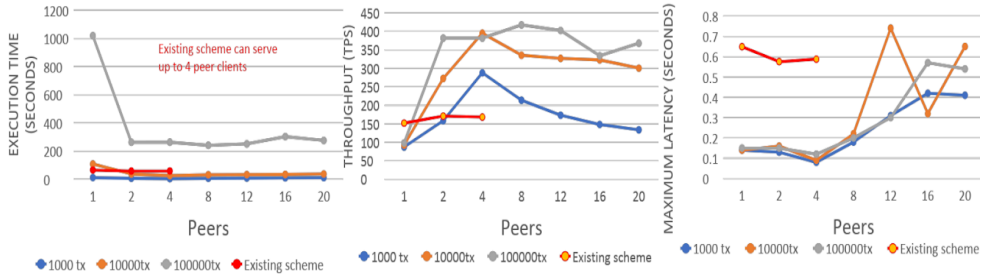
We assessed the proposed system's performance through tests involving varying transaction volumes, reaching up to 100,000, with a single peer. The evaluated metrics encompassed execution time, throughput, maximum latency, minimum latency, and average latency, as illustrated in Figure 7.21. System performance was examined through simulations run at transaction rates (TPS) of 1, 10, and 100. According to our observations, the execution time increases with a higher transaction count and decreases with a lower transaction count.

(a) Execution time (b) Throughput curves (c) Maximum Latency

Figure 7.21: Performance evaluation based on numbers of transactions.

When transaction volumes are lower, throughput is slower initially, but it quickly increases when transaction volumes exceed 10,000. As the transaction volume rises, the maximum latency becomes less noticeable and is more noticeable when there are fewer transactions. These metrics barely vary in the 10–1000 transaction range when using different TPS settings.

Furthermore, we expanded our analysis to assess the system's functionality with various peer configurations using identical metrics. Figure 7.22 presents a visual representation of this thorough assessment.



(a) Execution time (b) Throughput curves (c) Maximum LatencyFigure 7.22: Performance evaluation based on numbers of peers.

To examine the system's performance, we ran simulations with transaction volumes set at 1,000, 10,000, and 100,000. Furthermore, we used 10,000 transactions to benchmark our proposed scheme against an existing one [113]. Our scheme exhibits a notable increase in execution time when the number of peers is limited. However, the execution time settles down to a low level as soon as the number of peers increases enough. In contrast to 1,000 and 10,000 transactions, the execution time for 100,000 transactions is marginally longer. With fewer peers, the throughput performs worse; it peaks at eight peers and then starts to taper off. One hundred thousand transactions were used to reach the maximum throughput. For up to eight peers, latency is continuously low; after that, it varies depending on the volume of transactions. As shown in Table 7.3, we measured CPU-max, CPU-avg, Memory-max, Memory-min, Traffic In, and Traffic Out in order to provide a thorough assessment of resource consumption.

Table 7.3: Resource statistics of the supply chain design.

Name	CPU % (max)	CPU % (avg)	Memory (max) [MB]	Memory (avg) [MB]	Traffic in [MB]	Traffic out [MB]
dev-peer0.manufacturer.pharma-network.com	17.54	5.94	63.9	63.9	1.65	0.543
peer0.manufacturer.pharma-network.com	9.85	5.76	194	194	2.16	3.23
orderer.pharma-network.com	1.55	0.52	58.8	58.7	0.0827	0.141

The CPU utilization of the system's peers was 5.94% on average, with a peak of 17.54%. The average memory utilization was 90.5 MB, with a maximum of 63.9 MB. The maximum CPU utilization for manufacturer peers was 9.85%, with an average of 5.76%. For manufacturer nodes, the maximum and average memory consumption was 194 MB. The orderer node's average CPU utilization was 0.52%, with a maximum of 1.55%. The orderer node's memory usage peaked at 0.827 MB, averaging 0.141 MB. In conclusion, the suggested system shows a comparatively low resource usage.

7.4.4 Performance Evaluation of BCW

The statistical metrics, such as normalized correlation and structural similarity, are used to assess the watermarking performance.

PSNR: The peak signal to noise ratio is the definition of the parameter in mathematics.

$$PSNR = 10 \bullet log_{10}\left(\frac{MAX_I^2}{MSE}\right) \quad (7.9)$$

NC: This quantity, called normalized correlation (NC), should be closer to unity and higher in order to accurately depict how resilient a watermarked standard is to different types of attacks. This parameter's mathematical definition is;

$$NC = \sum_{i,j} d(i,j) * d(i - t, j - t) \quad (7.10)$$

where d is the decision variable, 0 (equal) or 1 (not equal), and S is the frame size.

SSMI: is called the structural similarity measure index. It suppresses the invisible watermarking's quality.

$$SSIM(A,B) = \frac{\mu_A \mu_B + c_1}{\mu_A^{\ 2} + \mu_B^{\ 2} + c_1} + \frac{\sigma_{AB} + c_2}{\sigma_A^{\ 2} + \sigma_B^{\ 2} + c_2} \quad (7.11)$$

where σ_{AB} is the covariance between the A and B matrix, c_1 and c_2 are factors that may be utilised to stabilize a low denominator division.

The quantitative assessment of BCW is detailed in Table 7.4 and Table 7.5. In Table 7.4, a comparative analysis of NC for QR code watermarking against attacks on blockchain encryption is provided, revealing consistent performance across all cases. Table 7.5 delves into the actual accuracy of our proposed method, offering a parametric comparison of watermark attacks applied to BCW images. Table 7.5 indicates an average PSNR of 30.86546 dB and an average NC of 0.974475 for all attacks. The most anticipated speckle noise attack attains a remarkable NC of 0.9995, while the salt and pepper noise achieves the highest structural similarity at 0.9663.

Table 7.4: Comparison of NC for QR Code Watermarking.

Images	**Variance**	**Gaussian Noise**	**Speckle Noise**	**Salt & Pepper**	**Motion Blur**
QR image 1	0.001	0.6610	0.6639	0.6628	0.666
QR image 2		0.6621	0.6632	0.6635	0.662

The findings show improvements, including an average Normalized Correlation (NC) of 0.974475 over all attacks and a higher average Peak Signal-to-Noise Ratio (PSNR) of 30.86546 dB.

Table 7.5: Comparison of PSNR, NC and SSIM under various attacks.

Metrics	Variance	Gaussian Noise	Speckle Noise	Salt & Pepper	Motion Blur
PSNR in dB	0.001	30.54610	33.68161	32.37145	26.86267
NC		0.9990	0.9995	0.9019	0.9975
SSIM		0.8480	0.9396	0.9663	0.8986

7.4.5 Comparative Analysis

In this section, we conduct a thorough comparison of our proposed system's performance and security features with existing works, specifically [44], [9], [113], [126], [127], and [128]. The evaluation in [44] focused on user-based analysis rather than transaction numbers, limiting its applicability. Moreover, their resource consumption was relatively high. In contrast, our design underwent extensive testing with 100,000 transactions and 20 peers, yielding successful results while maintaining reasonable resource consumption. Work in [9] limited testing to a maximum of 250 transaction rates, proving computationally expensive. In contrast, our proposed system demonstrated successful testing up to 1,000 TPS, showcasing scalability and improved performance. Regarding [113], their performance evaluation was capped at 10,000 transactions, and their system struggled to serve more than four users within this range. While they achieved a throughput of 168.3 TPS and a latency of 58.762 seconds with 10,000 transactions and 4 peers, our suggested design achieved a higher throughput of 395.2 and a significantly lower latency of 0.09 seconds under the same conditions, highlighting superior performance and scalability.

The work presented in [126] is less scalable and privacy-preserving due to its reliance on a public blockchain, with performance evaluation limited to 600 transactions. In contrast, our proposed solution utilizes the Hyperledger framework and IoT technology to enhance privacy, scalability, and real-time monitoring over extended distances. Our performance evaluation extends to 100,000 transactions, achieving a maximum throughput of 417.5 TPS and a

latency of 0.15 seconds. We also evaluated performance metrics in terms of the number of peers. Similarly, [127] and [128] suffer from scalability and privacy concerns due to their dependence on public blockchains. [128] is not focused on product traceability, and both works limited their performance evaluations to 1000 transactions. In comparison, our Hyperledger-based design offers superior scalability and performance.

Furthermore, we conducted a comprehensive security and feature comparison with relevant existing works, including [9], [44], [46], [83], [113], [126], [127], and [128]. The advantages of our proposed scheme over prior works are summarized in Table 7.6. A few of the existing schemes are Ethereum-based but the proposed scheme is Our Hyperledger Fabric blockchain-based system aims to enhance privacy and scalability. Unlike some counterparts, we provide detailed insights into the architecture and workflow of our proposed system, incorporating access control OBJs to bolster security. Addressing a common gap in existing systems, we introduce product traceability through a location tracker, recording the product's location on the blockchain.

Table 7.6: Comparison of supply chain scheme with existing works.

Security Features	**[9]**	**[44]**	**[46]**	**[83]**	**[113]**	**[126]**	**[127]**	**[128]**	**Prop -osed**
Privacy	✔	✔	✔	✔	✔	✔	×	×	✔OBJ
Architecture	✔	✔	✔	✔	✔	✔	✔	✔	✔
Access Control	✔	✔	✔	✔	✔	✔	✔	✔	✔
Tracking	×	×	✔	✔	✔	✔	✔	✔	✔
Authentication	×	×	×	✔	×	✔	✔	✔	✔
Performance testing	✔	✔	✔	✔	✔	✔	✔	✔	✔
Scalability	✔	×	✔	×	✔	✔	✔	✔	✔
Product validation	×	×	×	×	×	×	×	×	✔
Blockchain watermarking	×	×	×	×	×	×	×	×	✔

While many prior works restricted their performance evaluations to 1000 transactions, we surpass this limitation by evaluating our system's performance up to 100,000 transactions. Notably, our system demonstrates improvements in throughput, latency, and resource consumption, enhancing both performance and scalability. Additionally, we introduce a product validation mechanism that allows buyers to authenticate products by scanning the QR code, a feature absent in most existing works. Furthermore, we conducted rigorous evaluations of the security layer, focusing specifically on BCW and its resilience against watermarking attacks. The results showcase notable achievements, including a higher average Peak Signal-to-Noise Ratio (PSNR) of 30.86546 dB and an average Normalized Correlation (NC) of 0.974475 across all attacks. Particularly, the exceptional NC value of 0.9995 further substantiates the accuracy and effectiveness of our proposed method in QR authentication security.

7.5 Discussion

Key Results of the Proposed Drug Supply Chain System are summarised below:

- Decentralized Medicine Supply Chain: Implementation of a Hyperledger blockchain-based medicine supply chain integrated with IoT, addressing vulnerabilities in the existing system.
- Novel Chaincode Algorithms: Development of innovative chaincode algorithms incorporating access privilege restrictions and multiple validations, governing the entire workflow of the medical supply chain.
- QR Code Authentication: Introduction of encrypted QR codes with a blockchain-based invisible watermarking authentication method for enhanced reliability. A comprehensive analysis of attacks was conducted for evaluation.
- Validation Mechanism: Empowerment of buyers through real-time validation of serialized medicinal products via encrypted QR code scanning and access to transaction history. Implementation of a buyer identity validation mechanism to ensure only legitimate buyers receive medicinal products, with instant notifications for duplicate QR codes.

- Performance Evaluation: Demonstration of chaincode algorithm effectiveness through simulation results and performance metric evaluation for up to 100,000 transactions. Assessment includes throughput, latency, execution time, and computational resources.
- Improved Scalability: Implementation of a 10MB block size and event sourcing technique in the chaincode to enhance scalability and performance metrics. This technique optimizes storage efficiency by recording only the differences in asset state on the ledger. Highest achieved throughput of 417.5 TPS with 100,000 transactions and 8 peers.
- Performance Comparison: Confirmation that the proposed system handles up to 100,000 transactions with optimal performance. With 100,000 transactions and 8 peers, achieving a throughput of 417.5 TPS outperforms existing schemes, highlighting superior security features and efficient resource utilization, resulting in high throughput and low latency.
- Resource Consumption: Measurement of CPU-max, CPU-avg, Memory-max, Memory-min, Traffic In, and Traffic Out reveals low overall resource consumption in the system.

CHAPTER 8

CONCLUSION, FUTURE SCOPE AND SOCIAL IMPACT

9.1 CONCLUSION

After reviewing the literature, it becomes evident that blockchain design plays a significant role in ensuring the accuracy, trustworthiness, and accessibility of stored data. This technology can be effectively applied to secure EHRs, MPRs, and TMRs, as well as to manage vaccination records, drug discovery and drug supply chains.

Our suggested blockchain-based method for managing electronic health records (EHRs) enables medical facilities to safely share EHRs with patients and authorized requesters. This system ensures the availability of accurate data for future treatments, insurance claims, and drug discovery. Similarly, we introduce a blockchain-based MPR management system to streamline the transfer of medical records between institutions and enable easy access to accurate patient information, protecting against fraudulent practices. For the management TMRs, we present a blockchain-based solution that allows connected medical devices to securely transmit patient data. Healthcare providers can access this data with patient consent, ensuring proper medication recommendations.

Furthermore, our study introduced a blockchain-based vaccination record management system that maintains vaccination records throughout a patient's life. This system ensures secure record uploads and access, benefiting public health and meeting non-medical requirements such as education or employment verification. To address scalability, availability, and cost concerns, vaccination records are stored off-chain using a private InterPlanetary File System (IPFS), respecting patient preferences. The use of QR codes for validation enhances

record authenticity and reduces fraud. Another aspect of our research focuses on a blockchain-based drug discovery chain management system that integrates machine learning. This system enables research organizations to upload drug contributions securely and ensures regulatory compliance through unique asset IDs and certificates. Our system's efficiency is demonstrated through low resource consumption and high throughput. It offers scalability benefits by optimizing block parameters, making it a promising solution for drug discovery management.

Finally, we suggested a multilayer security algorithm for medicine supply chain management that is blockchain-based and Internet of Things enabled. This decentralized, tamper-proof system offers transparent, traceable, and validation-driven capabilities to combat the counterfeiting of medications. A smart location tracker ensures secure product tracking, and QR code authentication prevents counterfeiting. The system's performance is exemplary, handling a substantial number of transactions with superior throughput and low latency. In conclusion, blockchain technology offers versatile solutions across various healthcare domains, ensuring data security, authenticity, and efficiency.

9.2 FUTURE SCOPE

To test scalability further, our future work will include a careful evaluation of the suggested solution across a larger group of organizations. The platform needs to handle a large number of users while maintaining good performance in terms of speed and responsiveness. Ensuring the scalability of blockchain-based solutions is crucial because the sustainability of these systems relies on it. Once data is stored on the blockchain, it cannot be changed, and making corrections in all the blocks is highly expensive. In order to avoid the need for additional data corrections, preprocessing techniques must be used. Furthermore, developers encounter compatibility issues with various blockchain versions due to the absence of standardization, which needs to be fixed.

9.3 SOCIAL IMPACT

This research addresses critical challenges in healthcare by leveraging blockchain technology to enhance the security, accuracy, and efficiency of managing

healthcare data. The solutions presented have the potential to create far-reaching positive social impacts, as outlined below:

- **Improved Patient Safety and Trust:** By ensuring the integrity and reliability of healthcare records, blockchain technology reduces the risks of errors and fraudulent data manipulation. Patients can confidently trust the accuracy of their medical history, leading to better diagnoses, treatments, and overall outcomes. Secure systems also help combat medical fraud, such as impersonation in medical practice registration, safeguarding patients from unqualified practitioners.
- **Enhancing Public Health Preparedness:** Real-time, secure, and scalable systems enable efficient tracking of vaccination coverage, which is critical during outbreaks or pandemics.
- **Revolutionizing Telehealth and Fitness Monitoring:** During pandemics or in remote areas, telehealth has become a lifeline for many. The proposed blockchain-based systems integrate smart devices for real-time fitness monitoring and medication management, providing patients and healthcare providers with secure, actionable insights.
- **Advancing Drug Discovery and Supply Chain Transparency:** Blockchain's role in facilitating collaboration in drug discovery fosters innovation by ensuring the integrity of shared data while protecting intellectual property. The decentralized drug discovery application presented in this research accelerates breakthroughs, which could lower drug costs and improve availability. Furthermore, the blockchain-based drug supply chain solution tackles the global problem of counterfeit medicines. QR code watermarking and distributed collaboration increase transparency and traceability, enhancing trust across the supply chain.
- **Strengthened Data Privacy and Autonomy:** Patients benefit from greater control over their healthcare data, as blockchain allows them to verify and share records securely without intermediary manipulation. This autonomy fosters a patient-centric healthcare system, where individuals are active participants in their health management.

REFERENCES

[1] Farouk, Ahmed, et al. "Blockchain platform for industrial healthcare: Vision and future opportunities." Computer Communications 154 (2020): 223-235.

[2] Pandey, Abhishek Kumar, et al. "Key issues in healthcare data integrity: Analysis and recommendations." IEEE Access 8 (2020): 40612-40628.

[3] Sharma N, Rohilla R. "Blockchain-based approach for managing medical practitioner record: A secured design." Advanced Computing 10th International Conference, IACC 2020, Panaji, Goa, India, December 5–6, 2020, Revised Selected Papers, Part II 10. Springer Singapore, 2021.

[4] Houtan, Bahar, et al. "A survey on blockchain-based self-sovereign patient identity in healthcare." IEEE Access 8 (2020): 90478-90494.

[5] Chukwu, Emeka, et al. "A systematic review of blockchain in healthcare: frameworks, prototypes, and implementations." IEEE Access 8 (2020): 21196-21214.

[6] Hau, Yong Sauk, et al. "Attitudes toward blockchain technology in managing medical information: Survey study." Journal of Medical Internet Research 21.12 (2019): e15870.

[7] Linn, Laure A., et al. "Blockchain for health data and its potential use in health it and health care related research." ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST. 2016.

[8] Lee, Hsiu-An, et al. "An architecture and management platform for blockchain-based personal health record exchange: Development and usability study." Journal of Medical Internet Research 22.6 (2020): e16748.

[9] Tanwar, Sudeep, et al. "Blockchain-based electronic healthcare record system for healthcare 4.0 applications." Journal of Information Security and Applications 50 (2020): 102407.

[10] McKernan, Kevin Judd et al. "The chloroplast genome hidden in plain sight, open access publishing and anti-fragile distributed data sources." Mitochondrial DNA Part A 27.6 (2016): 4518-4519.

[11] Shuaib, Khaled, et al. "Blockchains for secure digitized medicine." Journal of personalized medicine 9.3 (2019): 35.

[12] Ivan, Drew et al. "Moving toward a blockchain-based method for the secure storage of patient records." ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST. Vol. 1170. sn, 2016.

[13] Yue, Xiao, et al. "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control." Journal of Medical Systems 40 (2016): 1-8.

[14] Fiquaro, Monafin Afif, et al. "Vaccination system using blockchain technology: a prototype development." 2021 3rd International Cyber Resilience Conference (CRC). IEEE, 2021.

[15] Yong, Binbin, et al. "An intelligent blockchain-based system for safe vaccine supply and supervision." International Journal of Information Management 52 (2020): 102024.

[16] Deka, Sanjib K., et al. "A blockchain based technique for storing vaccination records." 2020 IEEE Bombay Section Signature Conference (IBSSC). IEEE, 2020.

[17] Carniel, Andrei, et al. "A Blockchain Approach to Support Vaccination Process in a Country." ICEIS (1). 2021.

[18] Eisenstadt, Marc, et al. "COVID-19 antibody test/vaccination certification: there's an app for that." IEEE Open Journal of Engineering in Medicine and Biology 1 (2020): 148-155.

[19] Khan, Abdullah Ayub, et al. "Cloud forensics-enabled chain of custody: a novel and secure modular architecture using Blockchain Hyperledger Sawtooth." International Journal of Electronic Security and Digital Forensics 15.4 (2023): 413-423.

[20] Mariga, Job, et al. "Improving credit information sharing in small economies using blockchain technology." International Journal of Blockchains and Cryptocurrencies 4.2 (2023): 171-185.

[21] Nacer, Mohamed Ikbal, et al. "Missa: a regional approach to maintain validity." International Journal of Blockchains and Cryptocurrencies 4.1 (2023): 26-64.

[22] Sharma N, Rohilla R. "Blockchain based electronic health record management system for data integrity." Proceedings of International Conference on Computational Intelligence: ICCI 2020. Springer Singapore, 2022.

[23] Zhu, Peng, et al. "Enhancing traceability of infectious diseases: a blockchain-based approach." Information Processing & Management 58.4 (2021): 102570.

[24] Marbouh, Dounia, et al. "Blockchain for COVID-19: review, opportunities, and a trusted tracking system." Arabian Journal for Science and Engineering 45 (2020): 9895-9911.

[25] Udokwu, Chibuzor, et al. "Deriving and formalizing requirements of decentralized applications for inter-organizational collaborations on blockchain." Arabian Journal for Science and Engineering 46.9 (2021): 8397-8414.

[26] Naseer, Oumair, et al. "Blockchain-based decentralized lightweight control access scheme for smart grids." Arabian Journal for Science and Engineering (2021): 1-11.

[27] Sharma N, Rohilla R. "A novel Hyperledger blockchain-enabled decentralized application for drug discovery chain management." Computers & Industrial Engineering 183 (2023): 109501.

[28] Omar, Ilhaam A., et al. "Applications of blockchain technology in clinical trials: review and open challenges." Arabian Journal for Science and Engineering 46 (2021): 3001-3015.

[29] Benarous, Leila, et al. "Blockchain-based privacy-aware pseudonym management framework for vehicular networks." Arabian Journal for Science and Engineering 45 (2020): 6033-6049.

[30] Sai, Ashish Rajendra, et al. "Taxonomy of centralization in public blockchain systems: A systematic literature review." Information Processing & Management 58.4 (2021): 102584.

[31] Li, Chunlin, et al. "Lightweight blockchain consensus mechanism and storage optimization for resource-constrained IoT devices." Information Processing & Management 58.4 (2021): 102602.

[32] Dursun, Taner, et al. "A novel framework for policy based on-chain governance of blockchain networks." Information Processing & Management 58.4 (2021): 102556.

[33] Daizadeh, Iraj et al. "Has the COVID-19 crisis affected the growth of United States Food and Drug Administration drug approvals? The answer is not yet! A time series (forecasting) study." Therapeutic Innovation & Regulatory Science 55.3 (2021): 553-557.

[34] Wouters, Olivier J., et al. "Estimated research and development investment needed to bring a new medicine to market, 2009-2018." Jama 323.9 (2020): 844-853.

[35] Deore, Amol B., et al. "The stages of drug discovery and development process." Asian Journal of Pharmaceutical Research and Development 7.6 (2019): 62-67.

[36] Olsson, Christoffer, et al. "A Permissioned Blockchain-based System for Collaborative Drug Discovery." ICISSP. 2021.

[37] Andrews, David M., et al. "Compound Passport Service: supporting corporate collection owners in open innovation." Drug Discovery Today 20.10 (2015): 1250-1255.

[38] Hariry, Reza Ebrahimi, et al. "Towards Pharma 4.0 in clinical trials: a future-orientated perspective." Drug Discovery Today 27.1 (2022): 315-325.

[39] Lewis, David John, et al. "Utilizing advanced technologies to augment pharmacovigilance systems: challenges and opportunities." Therapeutic Innovation & Regulatory Science 54 (2020): 888-899.

[40] Ye, Zongli, et al. "An anonymous and fair auction system based on blockchain." The Journal of Supercomputing (2023): 1-43.

[41] Spjuth, Ola, et al. "The machine learning life cycle and the cloud: implications for drug discovery." Expert Opinion on Drug Discovery 16.9 (2021): 1071-1079.

[42] Radanović, Igor et al. "Opportunities for use of blockchain technology in medicine." Applied Health Economics and Health policy 16 (2018): 583-590.

[43] Boulos, Maged et al. "Geospatial blockchain: promises, challenges, and scenarios in health and healthcare." International Journal of Health Geographics 17 (2018).

[44] Jamil, Faisal, et al. "A novel medical blockchain model for drug supply chain integrity management in a smart hospital." Electronics 8.5 (2019): 505.

[45] Uddin, Mueen et al. "Blockchain Medledger: Hyperledger fabric enabled drug traceability system for counterfeit drugs in pharmaceutical industry." International Journal of Pharmaceutics 597 (2021): 120235.

[46] Liu, Xinlai, et al. "Blockchain-based smart tracking and tracing platform for drug supply chain." Computers & Industrial Engineering 161 (2021): 107669.

[47] Badhotiya, Gaurav Kumar, et al. "Investigation and assessment of blockchain technology adoption in the pharmaceutical supply chain." Materials Today: Proceedings 46 (2021): 10776-10780.

[48] Yiu, Neo, et al. "Toward blockchain-enabled supply chain anti-counterfeiting and traceability." Future Internet 13.4 (2021): 86.

[49] Kshetri, Nir, et al. "Blockchain and sustainable supply chain management in developing countries." International Journal of Information Management 60 (2021): 102376.

[50] Niu, Baozhuang, et al. "Should multinational firms implement blockchain to provide quality verification?." Transportation Research Part E: Logistics and Transportation Review 145 (2021): 102121.

[51] Niu, Baozhuang, et al. "Incentive alignment for blockchain adoption in medicine supply chains." Transportation Research Part E: Logistics and Transportation Review 152 (2021): 102276.

[52] Mettler, Matthias et al. "Blockchain technology in healthcare: The revolution starts here." 2016 IEEE 18th International Conference on E-health Networking, Applications and Services (Healthcom). IEEE, 2016.

[53] Irannezhad, Mandana, et al. "An integrated FCM-FBWM approach to assess and manage the readiness for blockchain incorporation in the supply chain." Applied Soft Computing 112 (2021): 107832.

[54] Balci, Gökcay, et al. "Blockchain adoption in the maritime supply chain: Examining barriers and salient stakeholders in containerized international trade." Transportation Research Part E: Logistics and Transportation Review 156 (2021): 102539.

[55] Patil, Pradnya, M. Sangeeta et al. "Blockchain for IoT access control, security and privacy: a review." Wireless Personal Communications 117 (2021): 1815-1834.

[56] Wang, Xu, Yanjiao Chen et al. "Incentivizing cooperative relay in UTXO-based blockchain network." Computer Networks 185 (2021): 107631.

[57] Fu, Wei, et al. "An improved blockchain consensus algorithm based on RAFT." Arabian Journal for Science and Engineering 46.9 (2021): 8137-8149.

[58] Platt, Moritz, et al. "Sybil attacks on identity-augmented Proof-of-Stake." Computer Networks 199 (2021): 108424.

[59] Khan, Ammar Ahmed, et al. "A blockchain-based decentralized machine learning framework for collaborative intrusion detection within UAVs." Computer Networks 196 (2021): 108217.

[60] Alam, Shadab, et al. "Blockchain-based initiatives: current state and challenges." Computer Networks 198 (2021): 108395.

[61] Wu, Yulei, et al. "Deep reinforcement learning for blockchain in industrial IoT: A survey." Computer Networks 191 (2021): 108004.

[62] Sharmila, A. Helen, et al. "Edge intelligent agent assisted hybrid hierarchical blockchain for continuous healthcare monitoring & recommendation system in 5G WBAN-IoT." Computer Networks 200 (2021): 108508.

[63] Arnold, Rachel, et al. "Continuity: A deterministic Byzantine fault tolerant asynchronous consensus algorithm." Computer Networks 199 (2021): 108431.

[64] da Silva Rodrigues, Carlo Kleber et al. "Analyzing Blockchain integrated architectures for effective handling of IoT-ecosystem transactions." Computer Networks 201 (2021): 108610.

[65] Al-Marridi, Abeer Z., et al. "Reinforcement learning approaches for efficient and secure blockchain-powered smart health systems." Computer Networks 197 (2021): 108279.

[66] Pandey, Prateek, et al. "Securing e-health networks from counterfeit medicine penetration using blockchain." Wireless Personal Communications 117 (2021): 7-25.

[67] Saxena, Rohit, et al. "Efficient blockchain addresses classification through cascading ensemble learning approach." International Journal of Electronic Security and Digital Forensics 15.2 (2023): 195-210.

[68] Liu, Yong, et al. "Fixed degree of decentralization DPoS consensus mechanism in blockchain based on adjacency vote and the average fuzziness of vague value." Computer Networks 199 (2021): 108432.

[69] Goyat, Rekha, et al. "Blockchain powered secure range-free localization in wireless sensor networks." Arabian Journal for Science and Engineering 45 (2020): 6139-6155.

[70] Liu, Yuan, et al. "Proof of Learning (PoLe): empowering neural network training with consensus building on blockchains." Computer Networks 201 (2021): 108594.

[71] Khalid, Sana, et al. "A blockchain-based solution to control power losses in pakistan." Arabian Journal for Science and Engineering 45 (2020): 6051-6061.

[72] Liu, Xuefeng, et al. "MDP-based quantitative analysis framework for proof of authority." 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC). IEEE, 2019.

[73] Omidian, Hossein, et al. "Blockchain in pharmaceutical life cycle management." Drug Discovery Today 27.4 (2022): 935-938.

[74] Reddy, Kotha Raj Kumar, et al. "Developing a blockchain framework for the automotive supply chain: A systematic review." Computers & Industrial Engineering 157 (2021): 107334.

[75] Li, Meng, et al. "LEChain: A blockchain-based lawful evidence management scheme for digital forensics." Future Generation Computer Systems 115 (2021): 406-420.

[76] Jing, Nan, Qi Liu, et al. "A blockchain-based code copyright management system." Information Processing & Management 58.3 (2021): 102518.

[77] Yang, Xuechao, et al. "Blockchain voting: Publicly verifiable online voting protocol without trusted tallying authorities." Future Generation Computer Systems 112 (2020): 859-874.

[78] Ren, Yongjun, et al. "Multiple cloud storage mechanism based on blockchain in smart homes." Future Generation Computer Systems 115 (2021): 304-313.

[79] Ammi, Meryem, et al. "Customized blockchain-based architecture for secure smart home for lightweight IoT." Information Processing & Management 58.3 (2021): 102482.

[80] Delgado-Mohatar, Oscar, et al. "Blockchain-based semi-autonomous ransomware." Future Generation Computer Systems 112 (2020): 589-603.

[81] Huang, Xinyi, et al. "Indistinguishability and unextractablility of password-based authentication in blockchain." Future Generation Computer Systems 112 (2020): 561-566.

[82] Bonnah, Ernest, et al. “A decentralized security approach in Edge Computing based on Blockchain." Future Generation Computer Systems 113 (2020): 363-379.

[83] Agrawal, Tarun Kumar, et al. "Blockchain-based framework for supply chain traceability: A case example of textile and clothing industry." Computers & Industrial Engineering 154 (2021): 107130.

[84] Maity, Meghna, et al. "Stochastic batch dispersion model to optimize traceability and enhance transparency using Blockchain." Computers & Industrial Engineering 154 (2021): 107134.

[85] Chow, Sherman SM, et al. "Editorial for accountability and privacy issues in blockchain and cryptocurrency." Future Generation Computer Systems 114 (2021): 647-648.

[86] Yuen, Tsz Hon et al. "PAChain: Private, authenticated & auditable consortium blockchain and its implementation." Future Generation Computer Systems 112 (2020): 913-929.

[87] Mubarakali, Azath et al. "Healthcare services monitoring in cloud using secure and robust healthcare-based BLOCKCHAIN (SRHB) approach." Mobile Networks and Applications 25 (2020): 1330-1337.

[88] Glicksberg, Benjamin Scott, et al. "Blockchain-authenticated sharing of genomic and clinical outcomes data of patients with cancer: a prospective cohort study." Journal of Medical Internet Research 22.3 (2020): e16810.

[89] Lo, Yu-Sheng, et al. "Blockchain-enabled iWellChain framework integration with the national medical referral system: development and usability study." Journal of Medical Internet Research 21.12 (2019): e13563.

[90] Tang, Fei, et al. "An efficient authentication scheme for blockchain-based electronic health records." IEEE Access 7 (2019): 41678-41689.

[91] Nguyen, Dinh C., et al. "Blockchain for secure ehrs sharing of mobile cloud based e-health systems." IEEE Access 7 (2019): 66792-66806.

[92] Shi, Huixian, et al. "Efficient and unconditionally anonymous certificateless provable data possession scheme with trusted kgc for cloud-based emrs." IEEE Access 7 (2019): 69410-69421.

[93] Beinke, Jan Heinrich, et al. "Towards a stakeholder-oriented blockchain-based architecture for electronic health records: design science research study." Journal of Medical Internet Research 21.10 (2019): e13585.

[94] Hussien, Hassan Mansur, et al. "A systematic review for enabling of develop a blockchain technology in healthcare application: taxonomy, substantially analysis, motivations, challenges, recommendations and future direction." Journal of Medical Systems 43 (2019): 1-35.

[95] Mayer, André Henrique, et al. "Electronic health records in a Blockchain: A systematic review." Health Informatics Journal 26.2 (2020): 1273-1288.

[96] Zhou, Tong, Xiaofeng Li, et al. "Med-PPPHIS: blockchain-based personal healthcare information system for national physique monitoring and scientific exercise guiding." Journal of Medical Systems 43 (2019): 1-23.

[97] Cao, Sheng, et al. "Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain." Information Sciences 485 (2019): 427-440.

[98] Motohashi, Tomomitsu, et al. "Secure and scalable mhealth data management using blockchain combined with client hashchain: system design and validation." Journal of Medical Internet Research 21.5 (2019): e13385.

[99] Vazirani, Anuraag A., et al. "Implementing blockchains for efficient health care: systematic review." Journal of Medical Internet Research 21.2 (2019): e12439.

[100] Guo, Rui, et al. "Flexible and efficient blockchain-based ABE scheme with multi-authority for medical on demand in telemedicine system." IEEE Access 7 (2019): 88012-88025.

[101] Liu, Xiaoguang, et al. "A blockchain-based medical data sharing and protection scheme." IEEE Access 7 (2019): 118943-118953.

[102] Wang, Yong, et al. "Cloud-assisted EHR sharing with security and privacy preservation via consortium blockchain." IEEE Access 7 (2019): 136704-136719.

[103] Daraghmi, Eman-Yasser, et al. "MedChain: A design of blockchain-based system for medical records access and permissions management." IEEE Access 7 (2019): 164595-164613.

[104] Shahnaz, Ayesha, et al. "Using blockchain for electronic health records." IEEE access 7 (2019): 147782-147795.

[105] Esmaeilzadeh, Pouyan, et al. "The potential of blockchain technology for health information exchange: experimental study from patients' perspectives." Journal of Medical Internet Research 21.6 (2019): e14184.

[106] O'Donoghue, Odhran, et al. "Design choices and trade-offs in health care blockchain implementations: systematic review." Journal of Medical Internet Research 21.5 (2019): e12426.

[107] Sanka, Abdurrashid Ibrahim, et al. "A systematic review of blockchain scalability: Issues, solutions, analysis and future research." Journal of Network and Computer Applications 195 (2021): 103232.

[108] Bennacer, Sara Ait, et al. "Design and implementation of a New Blockchain-based digital health passport: A Moroccan case study." Informatics in Medicine Unlocked 35 (2022): 101125.

[109] Nabil, Shirajus Salekin, et al. "Blockchain-based covid vaccination registration and monitoring." Blockchain: Research and Applications 3.4 (2022): 100092.

[110] Berdik, David, et al. "A survey on blockchain for information systems management and security." Information Processing & Management 58.1 (2021): 102397.

[111] Zhang, Guipeng, et al. "Blockchain-based privacy preserving e-health system for healthcare data in cloud." Computer Networks 203 (2022): 108586.

[112] Motohashi, Tomomitsu, et al. "Secure and scalable mhealth data management using blockchain combined with client hashchain: system design and validation." Journal of medical Internet research 21.5 (2019): e13385.

[113] Kumar, Chand, et al. "MedHypChain: A patient-centered interoperability hyperledger-based medical healthcare system: Regulation in COVID-19 pandemic." Journal of Network and Computer Applications 179 (2021): 102975.

[114] Miyachi, Ken, et al. "hOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design." Information Processing & Management 58.3 (2021): 102535.

[115] Heller, Stephen R., et al. "InChI, the IUPAC international chemical identifier." Journal of Cheminformatics 7.1 (2015): 1-34.

[116] Ekins, Sean, et al. "The collaborative drug discovery (CDD) database." In Silico Models for Drug Discovery (2013): 139-154.

[117] Nguyen, Thanh Son Lam, et al. "Impact of network delays on Hyperledger Fabric." IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). IEEE, 2019.

[118] Thakkar, Parth, et al. "Performance benchmarking and optimizing hyperledger fabric blockchain platform." 2018 IEEE 26th international symposium on modeling, analysis, and simulation of computer and telecommunication systems (MASCOTS). IEEE, 2018.

[119] Küsters, Ralf, et al. "Accountability in a permissioned blockchain: formal analysis of Hyperledger Fabric." Cryptology ePrint Archive (2020).

[120] Yu, Helen et al. "Leveraging research failures to accelerate drug discovery and development." Therapeutic Innovation & Regulatory Science 54 (2020): 788-792.

[121] Tseng, Jen-Hung, et al. "Governance on the drug supply chain via gcoin blockchain." International Journal of Environmental Research and Public Health 15.6 (2018): 1055.

[122] Çolak, Murat, et al. "A multi-criteria evaluation model based on hesitant fuzzy sets for blockchain technology in supply chain management." Journal of Intelligent & Fuzzy Systems 38.1 (2020): 935-946.

[123] Hulseapple, Cheryl et al. "Block verify uses blockchains to end counterfeiting and 'make world more honest'." Accessed: Jun 5 (2015): 2020.

[124] Mackey, Tim K., et al. "A review of existing and emerging digital technologies to combat the global trade in fake medicines." Expert Opinion on Drug Safety 16.5 (2017): 587-602.

[125] Chang, Shuchih Ernest, et al. "Supply chain re-engineering using blockchain technology: A case of smart contract based tracking process." Technological Forecasting and Social Change 144 (2019): 1-11.

[126] Anita, N., et al. "Blockchain-based anonymous anti-counterfeit supply chain framework." Sādhanā 47.4 (2022): 208.

[127] Anita, N., M. Vijayalakshmi, et al. "A Lightweight Scalable and Secure Blockchain Based IoT Using Fuzzy Logic." Wireless Personal Communications 125.3 (2022): 2129-2146.

[128] Shi, Shuyun, et al. "A blockchain-based user authentication scheme with access control for telehealth systems." Security and Communication Networks 2022 (2022).

[129] Alsadi, Mohammed, et al. "TruCert: Blockchain-based trustworthy product certification within autonomous automotive supply chains." Computers and Electrical Engineering 109 (2023): 108738.

[130] Chauhdary, Sajjad Hussain, et al. "An efficient evolutionary deep learning-based attack prediction in supply chain management systems." Computers and Electrical Engineering 109 (2023): 108768.

[131] Wang, Jin, et al. "Data security storage mechanism based on blockchain industrial Internet of Things." Computers & Industrial Engineering 164 (2022): 107903.

[132] Omar, Ilhaam A., et al. "Blockchain-based supply chain traceability for COVID-19 personal protective equipment." Computers & Industrial Engineering 167 (2022): 107995.

[133] Xie, Rongsheng, et al. "Anti-counterfeiting digital watermarking algorithm for printed QR barcode." Neurocomputing 167 (2015): 625-635.

[134] Zheng, Zhaohui, et al. "A system for identifying an anti-counterfeiting pattern based on the statistical difference in key image regions." Expert Systems with Applications 183 (2021): 115410.

[135] Zhu, Peng, et al. "A blockchain based solution for medication anti-counterfeiting and traceability." IEEE Access 8 (2020): 184256-184272.

[136] Chow, Yang-Wai, et al. "QR code watermarking for digital images." Information Security Applications: 20th International Conference, WISA 2019, Jeju Island, South Korea, August 21–24, 2019, Revised Selected Papers 20. Springer International Publishing, 2020.

[137] Cardamone, Nicolò, et al. "DWT and QR code based watermarking for document DRM." Digital Forensics and Watermarking: 17th International Workshop, IWDW 2018, Jeju Island, Korea, October 22-24, 2018, Proceedings 17. Springer International Publishing, 2019.

[138] Xun, Yijing, et al. "Dual anti-counterfeiting of QR code based on information encryption and digital watermarking." Advances in Graphic Communication, Printing and Packaging: Proceedings of 2018 9th China Academic Conference on Printing and Packaging. Springer Singapore, 2019.

[139] Liu, Jiannan, et al. "Application of QR Code Watermarking And Encryption in the Protection of Data Privacy of Intelligent Mouth Opening Trainer." IEEE Internet of Things Journal (2023).

[140] Mannepalli, Praveen Kumar, et al. "Block chain based robust image watermarking using edge detection and wavelet transform." (2021).

[141] Rawat, Paresh, et al. "Robust Digital Medical Image Watermarking and Encryption Algorithms Using Blockchain over DWT Edge Coefficient." Blockchain for Information Security and Privacy. Auerbach Publications, 2021. 95-112.

[142] Ramanand Singh, P. Rawat, et al. “Invisible Color Image Watermarking using Edge Detection And Discrete Wavelet Transform Coefficients”,

International Journal of Innovative Technology and Exploring Engineering (IJITEE) Volume-9 Issue-1, November 2019.

[143] Sharma N, Rohilla R. "A multilevel authentication-based blockchain powered medicine anti-counterfeiting for reliable IoT supply chain management." The Journal of Supercomputing (2023): 1-44.

[144] Haouari, Mohamed, et al. "A novel proof of useful work for a blockchain storing transportation transactions." Information Processing & Management 59.1 (2022): 102749.

[145] Song, Hongyu, et al. "Proof-of-Contribution consensus mechanism for blockchain and its application in intellectual property protection." Information Processing & Management 58.3 (2021): 102507.

[146] Spataru, Alexe Luca, et al. "A high-performance native approach to adaptive blockchain smart-contract transmission and execution." Information Processing & Management 58.4 (2021): 102561.