NEXT-GEN PATIENT MANAGEMENT SYSTEM USING BLOCKCHAIN TECHNOLOGY WITH SHA-256 ENCRYPTION

CO8811 – PROJECT REPORT

Submitted by

ANITHA KATHERIN RJ	**211420118006**
SNEHA M	**211420118000**
SWETHA M	**211420118000**

in partial fulfillment for the award the degree

of

BACHELOR OF ENGINEERING

in

COMPUTER AND COMMUNICATION ENGINEERING

PANIMALAR ENGINEERING COLLEGE

(An Autonomous Institution, Affiliated to Anna University, Chennai)

MARCH 2024

BONAFIDE CERTIFICATE

Certified that this project report **"NEXT-GEN PATIENT MANAGEMENT SYSTEM USING BLOCKCHAIN TECHNOLOGY WITH SHA-256 ENCRYPTION"** is the bonafide work of **ANITHA KATHERIN RJ (211420118006), SNEHA M (211421118047), SWETHA M (211421118052)** who carried out the project work under my supervision.

SIGNATURE

Dr.B.ANNI PRINCY M.E., Ph.D.,

HEAD OF THE DEPARTMENT

PROFESSOR,
COMPUTER AND COMMUNICATION ENGINEERING,
PANIMALAR ENGINEERING COLLEGE,
NAZARATHPETTAI, POONAMALLEE,
CHENNAI- 600123.

SIGNATURE

Dr.B.ANNI PRINCY M.E., Ph.D.,

SUPERVISOR

PROFESSOR,
COMPUTER AND COMMUNICATION ENGINEERING,
PANIMALAR ENGINEERING COLLEGE,
NAZARATHPETTAI, POONAMALLEE,
CHENNAI- 600123.

Certified that the above candidate(s) was/ were examined in the End Semester Project Viva-Voce Examination held on 26.03.2024

INTERNAL EXAMINER **EXTERNAL EXAMINER**

ACKNOWLEDGEMENT

We express our deep gratitude to our respected Secretary and Correspondent **Dr.P.CHINNADURAI, M.A., Ph.D.** for his kind words and enthusiastic motivation, which inspired us a lot in completing this project.

We would like to extend our heartfelt and sincere thanks to our Directors Tmt. **C.VIJAYARAJESWARI, Dr. C. SAKTHIKUMAR, M.E., Ph.D**., and **Dr.SARANYASREE SAKTHIKUMAR B.E., M.B.A., Ph.D**., for providing us with the necessary facilities for completion of this project.

We also express our gratitude to our Principal **Dr.K.MANI, M.E., Ph.D.,** for his timely concern and encouragement provided to us throughout the course.

We thank our HOD of Computer and Communication Engineering Department, **Dr. B. ANNI PRINCY, M.E., Ph.D**., Professor, for the support extended throughout the project.

We would like to thank our supervisor, **Dr. B.ANNI PRINCY , M.E., Ph.D.**., Professor, and all the faculty members of the Department of Computer and Communication Engineering for their advice and suggestions for the successful completion of the project.

ANITHA KATHERIN RJ

SNEHA M

SWETHA M

ABSTRACT

Blockchain is evolving to be a secure and reliable platform for secure data sharing in application areas such as the Financial sector, Food industry, Internet of Things, Supply Chain management, and healthcare. In this project, we use Blockchain technology to Secure medical records with the help of Ethereum Blockchain platform by interconnecting nodes. This also includes accessing and managing a large amount of medical data. The proposed model is a multilayer architecture with different entities. The entities are patients, doctors, clinic or hospitals, medical records etc. One of the key aspects of this endeavour is the efficient sharing of medical data. The medical system is to deliver better healthcare services with optimized cost. We use Blockchain technology in this study to safeguard medical data by connecting nodes on the Blockchain platform using secure hash algorithm-256. This innovative approach aims to enchance the efficient security and privacy of patient management system, paving the way for a more advanced and trustworthy healthcare ecosystem. The integration of blockchain ensures transparent and secure patient data transaction, While SHA-256 encryption adds an extra layer of robustness to protect sensitive information. The goal of the system is to provide optimally priced, high-quality medical services. The abstract may also touch upon the potential for improved patient outcomes, reduced errors, and increased trust in healthcare system through the decentralized and tamper-resistant nature of the Blockchain technology.

Keywords : *Blockchain technology; healthcare; smart contracts; data exchange;*

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATIONS

EHR	-	Electronic Health Records
EVM	-	Ethereum Virtual Machine
EMR	-	Electronic Medical Record
DFS	-	Distributed File System
ICT	-	Information Communications Technology
IOMT	-	Internet of Medical Things
POW	-	Proof-of-Work
DPOS	-	Delegated Proof-of-Stake
PBFT	-	Practical Byzantine Fault Tolerance
IPFS	-	Interplanetary File System

CHAPTER - 1

1.1 INTRODUCTION

Blockchain has recently emerged as one of the most promising technologies, attracting the attention of a number of academic studies and industries. Satoshi Nakamoto first proposed this notion in a 2008 white paper[19]. It is defined as a decentralized, appropriated, permanent record that is used to securely save exchanges across multiple PCs in a common organization, without the need for an outsider.

The idea of a distributed ledger, in which transactions are recorded across a network of nodes in an open and unchangeable fashion, is the foundation of blockchain technology. Cryptographic methods like the Secure Hash Algorithm (SHA) are used to encrypt each transaction, which stands for a patient record or interaction, guaranteeing its integrity and authenticity. In addition to protecting the data from unwanted access, this cryptographic hashing makes it possible to efficiently verify data integrity without sacrificing privacy.Additionally, blockchain enables safe and easy data sharing between different healthcare ecosystem participants, such as insurers, researchers, patients, and healthcare providers. Encoded on the blockchain, smart contracts are programmable self-executing agreements that automate and enforce specified criteria for patient data access and exchange. This reduces administrative overhead and improves transparency and confidence between participants.

Beyond patient management, blockchain technology has far-reaching ramifications for the healthcare industry. Evolving use cases include clinical trial data management, pharmaceutical traceability, and supply chain management. Resolving issues, improving implementations, and promoting the continuous

development of nextgeneration patient management systems require constant cooperation between researchers, industry stakeholders, and regulatory agencies. With SHA-256 encryption and blockchain technology coming together, healthcare delivery might be completely changed in this revolutionary environment while maintaining patient data's privacy, accuracy, and efficiency all throughout its lifecycle.

The healthcare industry is changing quickly, and integrating cutting-edge technologies has become essential to improve patient care, expedite procedures, and protect patient data. Blockchain stands out among these technologies as a gamechanger, providing hitherto unseen possibilities for transforming health care systems. Healthcare organizations can develop a cutting-edge patient management system that guarantees data quality, privacy, and efficiency by utilizing blockchain's intrinsic properties of decentralization, immutability, and transparency in conjunction with the Secure Hash Algorithm (SHA).

Blockchain technology's smart contracts have made healthcare arrangements more automated. These self-executing contracts reduce administrative costs and the likelihood of errors or disagreements by encrypting interactions between patients, healthcare providers, and insurance companies and expediting such exchanges. incorporates SHA-256, a powerful cryptographic hash technique, to improve the security and confidentiality of patient data. Its one-way function, which creates a unique hash for each piece of information, guarantees data integrity and privacy. Further enhancing cryptographic assurance is the SHA-256 cryptographic hash function, which is a member of the SHA-2 family of hash functions, which is renowned for its robust security procedures.

Furthermore, by offering a standardized foundation for transferring healthcare data across various platforms and systems, blockchain technology promotes interoperability. Blockchain breaks down data silos and improves the completeness

and accuracy of patient data by creating a single source of truth for medical records. This allows clinicians to make better judgments and improves patient outcomes in general.

Blockchain technology allows healthcare organizations to provide better patient care while reducing the risk of data breaches and noncompliance with regulations. This is achieved by guaranteeing data integrity, privacy, and interoperability. Blockchain is emerging as a key technology that will influence patient management in the future as the healthcare sector continues to embrace digital innovation.

1.2 PROBLEM STATEMENT

Patient management in modern healthcare systems has several difficulties, from privacy concerns and ineffective administrative procedures to data security breaches and interoperability problems. The security and confidentiality of patient data are frequently compromised by traditional patient management systems, which may result in regulatory non-compliance and compromised privacy. Furthermore, incompatible healthcare systems make it difficult for data to be exchanged seamlessly, which makes decision-making and care coordination more difficult. Furthermore, there are serious threats to patient confidentiality and system dependability from cyberattacks and illegal access to centralized data storage models. The issue is made worse by ineffective administrative procedures, which raise operating expenses and lower healthcare practitioners' productivity. Therefore, the requirement for a safe, compatible, and effective patient care system that takes these issues on while utilizing emerging technologies like blockchain to ensure data integrity, and transparency.

Patient privacy and data security are at risk, and there are many obstacles in the way of effective healthcare delivery in the current environment of patient management systems. Data security and confidentiality are seriously jeopardized by the data vulnerability of centralised storage systems to cyberattacks and illegal access. Furthermore, scattered patient data from incompatible healthcare IT systems makes it more difficult to coordinate care and make decisions. Healthcare companies are additionally burdened by complying with strict legal frameworks, which necessitate significant resources to guarantee data confidentiality and privacy.

Furthermore, ineffective administrative procedures lower the overall quality of care by causing delays and mistakes in patient treatment. In addition, patients frequently lack control over their health information, which makes it difficult for them to take an active role in their own care. As a result, creative solutions that prioritize data security, interoperability, regulatory compliance, administrative effectiveness, and patient empowerment are desperately needed to solve these issues. A potential remedy is blockchain technology, which provides decentralized, transparent, and unchangeable data storage while improving security, privacy, and interoperability in patient management systems. Healthcare companies may transform patient care delivery by utilizing blockchain technology, which guarantees smooth data transfer, better care coordination, and increased patient involvement.

1.3 OBJECTIVES

The objective of implementing a patient management system using blockchain technology encompasses a multifaceted approach aimed at addressing critical challenges in healthcare data management. Firstly, the system aims to bolster data security by leveraging blockchain's encryption techniques and decentralized architecture to safeguard patient information from unauthorized access and tampering. Secondly, it strives to enhance interoperability by facilitating seamless

data exchange among healthcare providers, insurers, and other stakeholders, thereby improving care coordination and decision-making. Additionally, the system targets streamlined regulatory compliance, ensuring adherence to stringent healthcare regulations such as HIPAA and GDPR through transparent and auditable data management processes. Moreover, by automating administrative tasks and empowering patients with greater control over their health data, the system aims to improve operational efficiency and patient engagement, ultimately enhancing the quality of care delivery. Furthermore, it seeks to foster collaborative medical research by enabling secure and privacy-preserving data sharing among researchers while protecting patient confidentiality. Ultimately, the overarching goal is to promote trust, transparency, and integrity in healthcare data management, driving innovation and improvement in patient care outcomes.

1.4 METHODOLOGY

A methodical approach comprising multiple crucial phases is employed in the implementation of a blockchain-based patient management system. First, a comprehensive requirement analysis is carried out with the aim of determining the obstacles that are common in the field of patient management, including weaknesses in patient engagement, regulatory compliance, data security, and interoperability. Feedback from stakeholders is obtained in order to comprehend their unique requirements and expectations. The system is then painstakingly created using blockchain technology to solve the problems that have been discovered.

In order to automate business processes and guarantee data integrity, this entails creating the system architecture, data schema, access control mechanisms, and smart contracts. A blockchain-enabled patient management system prototype is created after the design stage, with a focus on key features such patient registration, data entry, access control, and auditability. The system's functionality, security, and

performance are subsequently confirmed through extensive testing and validation processes.

This covers user acceptability testing, penetration testing, and vulnerability assessments. After undergoing validation, the system is put into use in a real-world setting and connected with the current IT infrastructure in the healthcare industry to enable smooth data sharing. Users receive instruction and training to guarantee safe and efficient system use. In order to ensure that the system remains relevant and effective in improving the delivery of patient care, procedures for continuous monitoring, evaluation, and improvement are put in place. These processes are based on user feedback, developing technology, and regulatory changes.

Using blockchain technology to implement a patient management system necessitates a methodical process that includes multiple crucial steps. First, a comprehensive requirements and challenge analysis is conducted with participation from administrators, patients, healthcare providers, and regulatory agencies. The design step, which creates a scalable architecture integrating blockchain to address security, privacy, and interoperability concerns, is informed by this study. In order to guarantee data openness and immutability, smart contracts are designed to automate crucial procedures like consent management and audit trails. After that, a prototype is created with an emphasis on usability and main functionalities, and it is put through a thorough testing process to confirm its functionality, security, and performance.

After a successful validation process, the system is implemented, integrated into the current healthcare infrastructure, and users receive training to ensure optimal utilization. As a result of user feedback and the development of new technologies, the system must be continuously monitored, evaluated, and improved in order to stay secure, compliant with regulations, and relevant. Healthcare firms may more

successfully use blockchain technology with this iterative strategy, which improves patient care delivery, data security, and regulatory compliance.

1.5 LANGUAGE USED

Solidity stands as a specialized programming language designed explicitly for crafting smart contracts on blockchain platforms, notably Ethereum. With its syntax resembling JavaScript and C++, Solidity serves as the primary tool for developers venturing into decentralized application (DApp) development. Smart contracts, the cornerstone of DApps, encode predefined rules and logic, executing autonomously on blockchain networks. Through Solidity, developers can architect a diverse array of applications, spanning from token creation to decentralized finance (DeFi) protocols and supply chain management systems. Solidity embeds features crucial for fortifying the security of smart contracts, including access controls, data encryption, and defenses against common vulnerabilities like reentrancy attacks. As it seamlessly integrates with the Ethereum Virtual Machine (EVM), Solidity facilitates the seamless execution of smart contracts on the Ethereum blockchain, underscoring its dominance in the ecosystem. Supported by a plethora of development tools and a thriving community, Solidity empowers developers to navigate the complexities of blockchain programming with confidence, while continuous updates and improvements ensure its relevance and effectiveness in the ever-evolving landscape of decentralized applications.

Overall, Solidity serves as a foundational tool for building decentralized applications and smart contracts, playing a pivotal role in enabling the decentralized, trustless, and transparent nature of blockchain networks. Solidity plays a central role in driving innovation and adoption within the blockchain ecosystem by empowering developers to build decentralized applications, tokenize assets, innovate in DeFi, govern DAOs, and enhance security and transparency through smart contracts. .

1.6 ORGANISATION

The implementation of a next-generation patient management system, integrating blockchain technology fortified by the SHA-256 secure hash algorithm, marks a significant organizational transformation in healthcare data management. This advanced system fundamentally reshapes the landscape of patient data storage, access, and security within the healthcare ecosystem. Through the utilization of blockchain's decentralized ledger, patient data is encrypted and stored in a manner that ensures immutability and heightened security. Complemented by the SHA-256 algorithm, which generates unique hash values for each patient record, data integrity becomes virtually impervious to tampering or unauthorized alterations. Integral components such as smart contracts enforce stringent access controls and patient consent mechanisms, while interoperability protocols enable seamless data exchange with existing healthcare infrastructure. Operationally, the system streamlines patient registration, medical records management, and data sharing processes, empowering patients with greater autonomy over their health information while simultaneously ensuring compliance with rigorous regulatory standards. The multifaceted benefits of this approach include enhanced data security, improved interoperability, transparency, and patient empowerment. Nonetheless, it is essential to acknowledge and address challenges such as scalability and regulatory compliance throughout the implementation process. Nevertheless, the adoption of the next-gen patient management system signifies a profound organizational commitment to efficiency, transparency, and patient-centric care in the healthcare industry.

CHAPTER - 2

LITERATURE SURVEY

Title 1 : A blockchain based electronic medical health records framework using smart contracts.

Authors: Dr.R.Chinnaiyan,Sahana R,Shreyas N Dass,Vardhini B.

Year : 2021.

Publications: International Conference on Computer Communication and Informatics (*ICCCI* -2021).

The most common concerns in clinical benefits across the country are related to specialists' reference cycles[27], information flow between health-care facilities, and access for patients to their clinical data. Explicit difficulties arise, such as sharing wellbeing records between establishments or clinics, issues with information abuse after sharing, a lack of security, and so on. The Electronic Wellbeing Record (EHR) System on Blockchain addresses these concerns through a collaborative effort of all partners involved. This study analyzes the feasibility of handling clinical records to provide information security, availability, and interoperability in the medical care explicit setting. Information security refers to managing the cost of assurance to ensure that information is available when needed and is not used, granted, accessed, updated, or erased while being stored, recovered, or sent. Information availability refers to the ability to access information despite typical or counterfeit mishaps, equipment, or others. Working on the transparency of health information in the medical care field while ensuring security has been acknowledged as a critical capacity that comprises both individuals and organizations. Traditionally, medical services interoperability has focused on sharing information between business institutions, such as different .

clinic frameworks. The emphasis has recently been on understanding-driven data sharing, in which the exchange of clinical data demonstrates restraint and patientdriven .

Keywords : *medical information exchange, blockchain-based EHR, consent-based health data sharing, and healthcare record management*.

Title 2 : Scalability challenges in healthcare blockchain system –a systematic review

Authors : Mazlan, A.A., Daud, S.M., Sam, S.M., Abas, H., Rasid, S.Z.A., Yusof, M.F.

Year : 2020.

Publications: IEEE Access 8, 23663–23673.

Blockchain innovation is a private, secure [18], dependable, and straightforward data commerce that is carried out decentralizedly. In this case, coordination and approval efforts are improved because the records are scheduled to update on a regular basis and there is no distinction between the two data sets. This audit focuses on how the Blockchain handles adaptation difficulties and provides solutions in the medical care industry through the application of Blockchain technology. Similarly, 16 arrangements fell into two major categories, namely capacity streamlining and Blockchain updates. Nonetheless, obstacles persist, including block size, huge volume of information, exchanges, the number of hubs, and convention problems.

This survey is divided into six parts, which include differentiating proof of exploration inquiry, examination technique, screening of significant articles, key phrasing in light of the theory, information extraction, and planning processes. The selected keywords were used to search through the important articles using the Atlasti software. Thus, 48 codes and 403 citations were arranged.

Keywords: *blockchain, healthcare, scalability, systematic review.*

Title 3 : Digital and decentralized management of patient data in healthcare using Blockchain implementation.

Authors : Erik Westphal and Hermann Seitz.

Year : 2021.

Publications: MINI REVIEW ARTICLE.

Blockchain arrangements provide superior approaches for reliable information to executives[28], particularly in the therapeutic field, while storing and managing sensitive patient information. Numerous institutional and modern offices have previously recognized the significance of innovation in the healthcare field and have also worked out vital thoughts, ideas, and primary use cases, but significant executions and executions are equally unusual.

This brief audit examines flow study on unambiguous Blockchain executions in medical care that go beyond the condition of idea studies or hypothetical execution ideas, and it represents the most encouraging frameworks in light of exact writing research. According to the report, safe and easy access to complete patient information is becoming increasingly important. Blockchain technology can be used to solve these needs in a secure, simple, and automated manner.

Keywords: *medical Blockchain, digital healthcare, patient data management, electronic medical records, decentralized secure storage, health asset monitoring*.

Title 4 : Blockchain technology applications in healthcare: an overreview.

Authors: Abid Haleem, MohdJavaid, Ravi Pratap Singh, Rajiv Suman, ShanayRab.

Year : 2021.

Publications: International Journal of Intelligent Networks 2 (2021).

Blockchain is an arising innovation being applied for making imaginative arrangements in different areas, including medical care[29]. A Blockchain network is utilized in the medical services framework to safeguard and trade patient information through emergency clinics, symptomatic research centers, drug store firms, and doctors. Blockchain applications can precisely distinguish extreme missteps and, surprisingly, risky ones in the clinical field. In this way, it can work on the presentation, security, and straight forwardness of sharing clinical information in the medical services framework. This innovation is useful to clinical foundations to acquire understanding and upgrade the investigation of clinical records. In this paper[29], They concentrated on Blockchain innovation and its critical advantages in medical services. Different Capacities, Empowering influences, and Bound together Work process Cycle of Blockchain Innovation to help medical care around the world are talked about diagrammatically. At last, the paper recognizes and discusses fourteen critical uses of Blockchain for medical care. Blockchain has a definitive impact in taking care of double dealing in clinical preliminaries; here, the capability of this innovation offer is to further develop information effectiveness for healthcare.

Keywords - *Blockchain, healthcare, scalability, systematic review.*

Title 5 : A Blockchain-based platform for healthcare information exchange.
Authors: Shan Jiang, Jiannong Cao, Hanqing Wu, Yanni Yang, Mingyu Ma, Jianfei
Year : 2018.

Publications: 2018 IEEE International Conference on Smart Computing.

These days, clinical organizations and individuals continually generate an astounding amount of information about medical services[16]. It has been shown

that medical care data exchange (HIE) significantly benefits the clinical business. It is important to retain and distribute such a large amount of health care data during testing. They suggest BlocHIE, a Blockchain-based platform for the exchange of medical data, in their study [16].They begin by breaking down the different requirements for exchanging health care information from different sources. They use two roughly related Blockchains to handle different kinds of medical services information in light of the examination. Secondly, they combine off-chain capacity with on-anchor verification to meet the requirements for both security and actual capacity. Thirdly, they provide two important estimates based on reasonableness that will help both the clients' decency and the framework's throughput grow. In order to demonstrate BlocHIE's feasibility and practicability, they implement BlocHIE in a negligible suitable item approach and evaluate the suggested urgent computations extensively.

Keywords - *Blockchain, healthcare, scalability, systematic review.*

Title 6 : Success factor of implementation Blockchain technology in pharmaceutical industry:A literature review.

Authors: Surjandy,Meyliana,Erick Fernando.

Year : 2019.

Publications: Int. Conf. on Information Tech., Computer, and Electrical Engineering (ICITACEE).

The implementation of Blockchain innovation in the medication firm's store network has begun to meet corporate objectives [9]. However, there are still a lot of people that are unaware of the benefits or the implementation. The goal of this project is to advance the use of blockchain innovation in the pharmaceutical industry. As a result, the metaexamination strategy cycle used in the writing survey. The study's aftereffects identified 21 components, with five criteria being considered to be the most important when using blockchain innovation: track, trust,

discernibility, straightforwardness, and continuity. Other pharma enterprises are encouraged to implement Blockchain innovation as a solution to their problems after discovering this achievement factor. The implementation of Blockchain innovation in the medication firm's store network has begun to meet corporate objectives [9]. However, there are still a lot of people that are unaware of the benefits or the implementation. The goal of this project is to advance the use of blockchain innovation in the pharmaceutical industry.

As a result, the metaexamination strategy cycle used in the writing survey. The study's aftereffects identified 21 components, with five criteria being considered to be the most important when using blockchain innovation: track, trust, discernibility, straightforwardness, and continuity. Other pharma enterprises are encouraged to implement Blockchain innovation as a solution to their problems after discovering this achievement factor.

Keywords: *Pharmaceutical Industry, Blockchain Technology, Success Factor, Literature Review.*

CHAPTER - 3

SYSTEM DESIGN

3.1 EXISTING SYSTEM

The current manual system has a lot of paper work. To maintain the Patient records manually, is a Time-consuming task. With the increase in database, it will become a massive task to maintain the database. Requires large quantities of file cabinets, which are huge and require quite a bit of space in the office, which can be used for storing records of previous details. The retrieval of records of previously registered patients will be a tedious task. Lack of security for the records, anyone disarrange the records of your system. If someone want to check the details of the available doctors the previous system does not provide any necessary detail of this type.

LIMITATION

Integrating blockchain technology with the SHA-256 algorithm into a patient management system presents several limitations. Firstly, scalability concerns arise due to the inherent limitations of blockchain networks, particularly in handling high transaction volumes efficiently. The decentralized nature of blockchain may also pose challenges in ensuring data privacy and confidentiality, especially concerning sensitive patient information. Moreover, regulatory compliance, particularly with laws like HIPAA, can be complex given the immutable nature of blockchain and requirements for data deletion and consent management. Implementing such a system requires significant expertise and investment due to the complexity of integrating blockchain with existing healthcare infrastructure. Additionally, the energy consumption associated with certain consensus mechanisms, such as

Proofof-Work, raises environmental concerns and adds to operational costs. Achieving interoperability with legacy systems and other blockchain platforms remains a challenge, further complicating implementation efforts. Lastly, the risk of centralization threatens the decentralization ethos of blockchain, potentially compromising the security and integrity of the patient management system. Addressing these limitations demands careful consideration of technical, regulatory, and operational factors, alongside ongoing research and innovation in blockchain technology within healthcare contexts.

Finally, achieving seamless interoperability with existing healthcare IT infrastructure and electronic health record (EHR) systems remains a considerable challenge. Integrating a blockchain-based patient management system with legacy systems necessitates robust interoperability standards and protocols to ensure smooth data exchange and continuity of patient care.

Despite these limitations, addressing these challenges through collaborative efforts among healthcare professionals, technologists, policymakers, and regulatory bodies can pave the way for the successful implementation and adoption of blockchainbased patient management systems. By acknowledging these limitations and proactively implementing mitigation strategies, stakeholders can harness the transformative potential of blockchain technology while maintaining efficiency, reliability, and security in healthcare data management.

3.2 PROPOSED SYSTEM

In the proposed enhancement of the patient management system, integrating laboratory test results while employing the SHA-256 algorithm for data encryption constitutes a pivotal step towards fortifying security and ensuring data integrity. Laboratory test results, comprising critical health information, undergo encryption using the SHA-256 algorithm prior to integration into the system. This cryptographic

process generates unique hash values for each set of results, bolstering confidentiality and guarding against unauthorized access or tampering . Once encrypted, the laboratory test results are securely stored on the blockchain alongside other patient data, each linked to the patient's distinct identifier. Rigorous access controls are implemented, dictating that only authorized healthcare personnel and patients themselves can access the encrypted results. Smart contracts are employed to automate result-related processes, such as notification of abnormal findings to healthcare providers, enhancing efficiency and facilitating timely interventions. Retrieval of results is facilitated through the patient's identifier, with the SHA-256 algorithm utilized to verify the integrity of the retrieved data, thus ensuring its reliability. Interoperability standards such as HL7 enable seamless exchange of data between the patient management system and laboratory information systems, while adherence to regulatory requirements like HIPAA is ensured through comprehensive audit trails.

User-friendly interfaces empower healthcare providers and patients to interpret and utilize laboratory results effectively, enhancing clinical decision-making and patient care. Continuous monitoring and updates safeguard against evolving security threats, reaffirming the system's commitment to protecting patient data and improving healthcare outcomes.

Through the integration of smart contracts, access controls and consent management mechanisms are enforced, ensuring that patients retain control over their health data while adhering to stringent privacy regulations. Patient identity management isstreamlined through the assignment of unique digital identities on the blockchain, fostering trust and transparency in data handling. Robust encryption techniques, including the SHA-256 cryptographic hash function, fortify data security, protecting sensitive information from unauthorized access or tampering. Interoperability

protocols facilitate seamless data exchange with existing healthcare systems, promoting care coordination and continuity.

BENEFITS

The next-generation patient management system, integrating blockchain technology with the SHA-256 algorithm, presents a paradigm shift in healthcare data management, offering a myriad of benefits across the entire healthcare ecosystem. By employing the SHA-256 algorithm for data encryption, the system ensures unparalleled levels of security, safeguarding patient information against unauthorized access and tampering. The decentralized nature of blockchain storage ensures data integrity and transparency, providing an immutable ledger of patient records accessible to authorized stakeholders. This fosters seamless interoperability and data sharing between healthcare providers, insurers, and patients, facilitating collaborative care delivery and informed decision-making. Moreover, the system empowers patients with greater control over their health data, promoting autonomy and engagement in care management processes.

Through the automation of administrative tasks via smart contracts, the system streamlines operations, reduces costs, and minimizes errors, leading to improved efficiency and resource utilization. Additionally, the transparent and auditable nature of blockchain enhances fraud prevention and regulatory compliance, while facilitating research initiatives and population health insights.

Overall, the integration of blockchain technology with the SHA-256 algorithm in the patient management system represents a transformative advancement in healthcare, promising enhanced security, interoperability, and patient-centered care delivery for the future.

Beyond its immediate benefits, the system's decentralized architecture ensures high system availability and resilience against network disruptions and hardware failures. This resilience, coupled with distributed consensus mechanisms, guarantees data accessibility and integrity even amidst localized system outages or cyberattacks.

Moreover, the system accelerates medical research and innovation by fostering data sharing and collaboration among healthcare researchers and institutions. By securely storing and sharing anonymized patient data, blockchain fuels advancements in personalized treatment approaches and drives healthcare innovation forward.

In essence, the patient management system leveraging blockchain technology with SHA-256 encryption represents a transformative leap forward in healthcare data management. By harnessing the benefits of blockchain, healthcare organizations can enhance patient care quality, streamline administrative processes, and pave the way for a more efficient, secure, and patient-centric healthcare ecosystem.

In summary, the integration of SHA-256 encryption within the patient management system offers a robust foundation for managing patient data securely and effectively. Its contributions to data integrity, security, efficiency, and interoperability bolster the system's resilience against threats and enable healthcare organizations to provide high-quality care while maintaining patient privacy and regulatory compliance.

Additionally, the standardized nature of SHA-256 ensures interoperability and compatibility with existing blockchain frameworks, fostering confidence among healthcare professionals and stakeholders in the security and reliability of the system.

3.3 LIST OF MODULES

Admin

Doctor

Patient

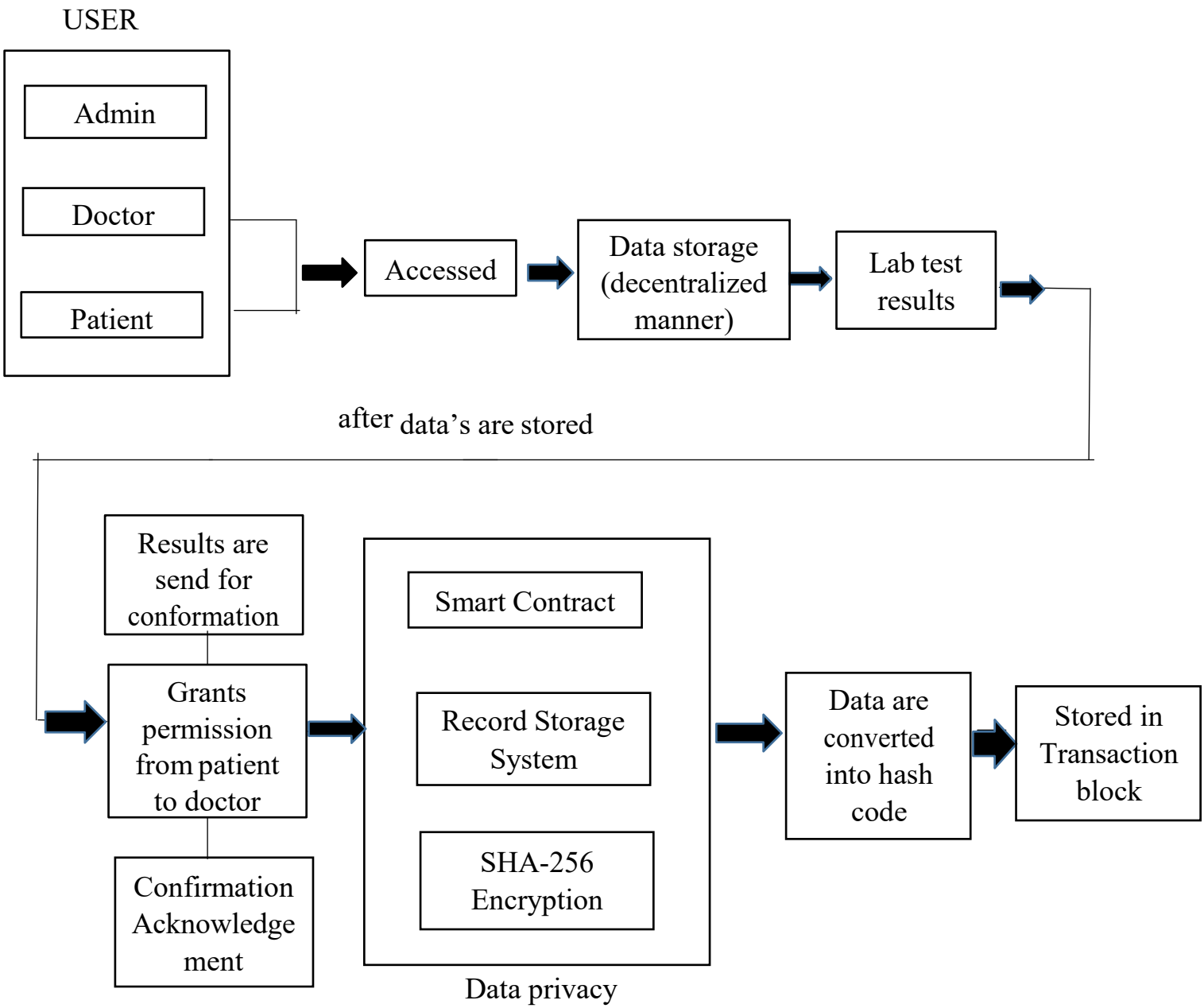

Figure 3.3.1: Block Diagram

ADMIN LOGIN

An admin login function in a patient management system powered by blockchain grants access to administrative features and controls to authorized workers. The administrator enters their credentials to access the login screen; they are safely saved

and validated through the use of cryptographic techniques like hashing and encryption. After the administrator has successfully authenticated, the system gives them access to a dashboard or interface where they can carry out several administrative functions. Managing user accounts, setting up system preferences, keeping an eye on data access and usage, creating reports, and supervising regulatory compliance are a few examples of these duties. To better protect access to important system functions, the admin login function may further include multi-factor authentication or other security measures. Healthcare organizations can guarantee the safe and effective administration of their blockchain-based patient management system while maintaining data integrity and privacy.

The admin login function in a blockchain-powered patient management system is a critical component ensuring secure access to administrative controls and sensitive healthcare data. At the outset, administrators provide their credentials, typically a username and password, which are securely stored using encryption techniques.

Upon submission, the system verifies the authenticity of these credentials through cryptographic methods such as hashing, comparing them with stored records. Successful authentication grants access to an admin dashboard or interface, where authorized personnel can manage user accounts, configure system settings, and monitor activity. To bolster security, additional measures like multi-factor authentication and IP whitelisting may be employed.

Continuous monitoring and logging of login attempts help administrators track access and detect any suspicious activities. Compliance with regulatory standards such as HIPAA and GDPR is maintained through robust access controls and data encryption. Overall, the admin login function plays a pivotal role in ensuring the integrity, confidentiality, and security of patient data within the blockchain-based patient management system.

The admin login specification outlines the detailed requirements and functionalities of the administrative login feature within a blockchain-powered patient management system. Below are the key components typically included in such a specification: Authentication Requirements, Access Control, Security Measures.

DOCTOR LOGIN

In order to guarantee safe access to patient data, a blockchain-powered patient management system's doctor login procedure entails multiple steps. Initially, the physician opens the login portal and inputs their login credentials, which consist of their username and password. These login credentials are safely sent to the blockchain network after being encrypted using cryptographic methods like SHA. The blockchain checks the legitimacy of the doctor's credentials against the data that is recorded on the distributed ledger after receiving the login request. The doctor is permitted access to the system if their credentials match. Multi-factor authentication techniques, including biometric verification or token-based authentication, can be used to further improve security.

After logging in, the physician can safely access patient data, examine medical histories, modify treatment regimens, and get in touch with other healthcare providers within the network. All interactions and changes made by the doctor are recorded on the blockchain, ensuring transparency, accountability, and data integrity.

The doctor login process in a blockchain-powered patient management system involves the encryption of credentials using cryptographic algorithms like Secure Hash Algorithm (SHA) before transmission, verification of authenticity against stored data on the distributed ledger, optional implementation of multi-factor authentication methods for heightened security, and subsequent access to patient

records and interactions within a securely authenticated session, all while ensuring transparency, accountability, and data integrity through immutable transaction records on the blockchain. Step 1-The doctor initiates the login process by accessing the designated login portal or application and They provide their credentials, typically a username and password, to verify their identity

PATIENT LOGIN

The patient login process within a blockchain-enabled patient management system is designed with a focus on security, privacy, and seamless interaction. Initially, patients access the login portal where they provide their credentials for authentication, which may include traditional methods like usernames and passwords or advanced biometric identifiers. Once authenticated, the system conducts verification against the patient's stored credentials on the blockchain, ensuring the integrity and confidentiality of the login process through cryptographic means. Following successful verification, patients gain access to their personalized dashboard or electronic health record (EHR), where they can view medical records, schedule appointments, and communicate with healthcare providers.

Crucially, access control mechanisms implemented via smart contracts on the blockchain guarantee that patients only access and modify their own data, adhering to strict privacy regulations. Throughout the interaction, all activities are recorded as immutable transactions on the blockchain, ensuring transparency and auditability. Upon completion of their session, patients securely log out, triggering additional blockchain transactions to update access logs and confirm the end of the session. In essence, the patient login process within a blockchain-powered patient management system prioritizes robust security measures, patient privacy, and transparent data handling, ultimately enhancing the overall patient experience and trust in the healthcare system.

The patient initiates the login process by accessing the designated portal or application. They provide their credentials, which could be a username/password combination, biometric data like fingerprints or facial recognition, or even a secure digital identity stored on the blockchain. The system verifies these credentials against the patient's digital identity stored on the blockchain, ensuring the authenticity of the user.

Unlike traditional centralized authentication systems where user credentials are stored in a single database, blockchain-based authentication decentralizes this process. Each user's identity and authentication credentials are securely stored and managed on the blockchain network, eliminating single points of failure and reducing the risk of data breaches. Upon successful authentication, the login event is recorded as a tamper-proof transaction on the blockchain ledger.

This immutable record serves as an audit trail, providing a transparent and verifiable history of login activities. Any attempts at unauthorized access or suspicious activities can be easily identified and traced back to their source. After logging in, patients are granted access to their personalized dashboard or EHR based on predefined access permissions encoded in smart contract.

These smart contracts enforce role-based access control, ensuring that patients can only view and modify their own health information while healthcare providers and other authorized entities have access to relevant patient data based on their roles and responsibilities.

Within their dashboard or EHR, patients can securely interact with their health data, such as viewing lab results, medication history, and treatment plans. Any changes

or updates made to the data are recorded as transactions on the blockchain, preserving the integrity and traceability of the information.

The patient login process within a blockchain-enabled patient management system represents a cornerstone of modern healthcare data security and privacy. Initiated by the patient accessing a designated portal or application, authentication unfolds through a variety of secure methods, including traditional credentials or advanced biometrics, all verified against the patient's digital identity stored on the blockchain.

This decentralized authentication framework ensures heightened security by dispersing user data across the network, eliminating the vulnerability of centralized databases. Once authenticated, login events are recorded as immutable transactions on the blockchain ledger, forming an indelible audit trail. Access to the patient's personalized dashboard or Electronic Health Record (EHR) is then granted based on predetermined permissions encoded in smart contracts, ensuring strict adherence to role-based access control principles. Within this secure environment, patients can interact with their health data, confident in the integrity and privacy safeguards afforded by blockchain technology.

Crucially, patients retain control over their data, empowered to manage consent and selectively grant access to authorized parties. Throughout the session, continuous monitoring and logging of user activities further reinforce security measures, enhancing auditability and compliance.

DATA STORAGE

Decentralized data storage, a hallmark of modern distributed systems, revolutionizes traditional data management paradigms by dispersing data across numerous nodes within a network rather than centralizing it in a single location. This approach

ensures redundancy and fault tolerance, mitigating the risk of data loss or corruption due to hardware failures or malicious attacks

Operating on peer-to-peer (P2P) networks, decentralized storage systems empower nodes to communicate directly, facilitating efficient data storage and retrieval without reliance on a central authority. Security measures such as encryption and cryptographic hashing safeguard data privacy and integrity, ensuring that stored information remains confidential and unaltered.

Consensus mechanisms further reinforce data integrity by enabling nodes to collectively agree on the validity of data changes or updates. Incentive mechanisms within some decentralized storage networks incentivize participants to contribute storage resources, fostering network resilience and availability. Notably, in blockchain-based decentralized storage systems, data transactions are recorded on an immutable ledger, enhancing transparency and accountability.

Overall, decentralized data storage offers unparalleled advantages including enhanced security, fault tolerance, and censorship resistance, making it a compelling solution for modern data management challenges.

Furthermore, blockchain's distributed consensus mechanisms, such as Proof of Work (PoW) or Proof of Stake (PoS), ensure that all participating nodes agree on the validity and order of transactions, reinforcing data integrity and resilience against malicious attacks or unauthorized modifications. The use of SHA-256 encryption enhances data security by providing robust cryptographic protection against data tampering or unauthorized access, safeguarding sensitive patient information from breaches and cyber threats.

Moreover, the decentralized nature of blockchain enables secure and permissioned access to patient data, empowering individuals to retain control over their medical information. Through the use of cryptographic keys and smart contracts, patients can selectively grant access to their health records to authorized healthcare providers, enhancing privacy and confidentiality while facilitating seamless data sharing for improved care coordination.

Despite these advantages, it's essential to address challenges associated with blockchain data storage, such as scalability and efficiency. As the system scales and transaction volumes increase, the size of the blockchain grows, potentially impacting storage requirements and network performance. Implementing strategies like data pruning, compression techniques, and off-chain storage solutions can help mitigate these challenges while ensuring optimal resource utilization and system scalability.

In conclusion, data storage in the patient management system leveraging blockchain technology with SHA-256 encryption offers a secure, transparent, and decentralized approach to healthcare data management. By harnessing the benefits of blockchain and SHA-256 encryption, healthcare organizations can enhance data integrity, security, and accessibility while empowering patients with greater control over their medical information. Continued innovation and collaboration are essential to address scalability concerns and optimize data storage solutions for the evolving needs of the healthcare industry.

LABORATORY TEST RESULTS

In laboratory settings,ensuring the integrity of test results is paramount for accurate analysis and decision-making.To achieve this,the Secure Hah Algorithm(SHA) is often employed.This cryptographic algorithm generates a unique hash value from the test results data.The procedure involves collecting the data,processing it using the SHA algorithm to create a hash value, and storing or transmitting this hash

alongside the original data.When verification is required,the original data is hased again,and the resulting hash value is compared with the stored one.A match confirms the data;s integrity, indicating no tampering or alterations.This approach provides a robust mechanism for safeguarding the authenticity and reliability of laboratory test results.

In laboratory settings,test results are often subjected to the Secure Hash Algorithm(SHA) to ensure their integrity and authenticity.The procedure typically involves:

1. Data Collection: The laboratory collects the test results data ,which could include various paramaters , measurements ,and observations.

2.Hash Generation: The collected data is then processed using the SHA algorithm to generate a fixed-size hash value. This hash value is unique to the input data and serves as a digital fingerprint.

3.Storage or Transmision : The generated hash value can be stored alongside the original data or transmitted separately ,depending on the specific requirements and security protocols.

4.Verification: Whenever the test results need to be verified,the original data is hashed again using the same SHA algorithm.The resulting hash value is compared with the previously generated hash value.if they match,it indicates that the data has not been altered or tampered with.

5.Reliability: Employing SHA in laboratory tests enhances the reliability and trustworthiness of the results,providing confidences in their accuracy for informed decision-making.

6.Encryption and Decryption: Utilize encryption techniques to protect sensitive laboratory test results. Only authorized users with decryption keys can access the encrypted data.

7.Blockchain Smart Contracts: Smart contracts can enforce access control policies by defining rules and conditions for accessing laboratory test results. Smart contracts can enforce access control policies by defining rules and conditions for accessing laboratory test results

8.Multi-Factor Authentication (MFA): Implement MFA to add an extra layer of security to the system. Users must provide multiple forms of authentication, such as passwords, biometrics, or security tokens, to access laboratory test results. MFA reduces the risk of unauthorized access due to compromised credentials or stolen passwords.

9.Audit Trails: Maintain audit trails to track and record all access attempts and actions related to laboratory test results.
Audit logs provide transparency and accountability, enabling administrators to monitor user activity and detect any unauthorized access or suspicious behaviour

10.Consent Management: Implement mechanisms for patients to grant or revoke consent for accessing their laboratory test results.
Smart contracts can manage consent agreements, ensuring that only authorized individuals or entities can access patient data with explicit consent.

11,Access Revocation: Ensure that access rights can be revoked promptly when necessary, such as when an employee leaves the organization or a patient withdraws consent.

Smart contracts can automate access revocation processes, immediately removing access permissions for users who are no longer authorized to view laboratory test results.

RECORD STORAGE SYSTEM

Within the patient management system harnessing blockchain technology with SHA-256 encryption, the record storage system is a cornerstone, ensuring the secure and reliable management of patient data. Operating on a decentralized network, this system utilizes blockchain technology's distributed ledger architecture, where each node maintains a copy of the entire ledger, ensuring redundancy and resilience against data loss or tampering. This decentralized approach not only enhances data security but also eliminates the vulnerability of a single point of failure.

The system employs SHA-256 encryption, a robust cryptographic hashing algorithm, to secure patient records before they are stored on the blockchain. This encryption process generates unique digital fingerprints for each data entry, rendering patient information resistant to unauthorized access or modification. Consequently, patient records are shielded from tampering and remain confidential, bolstering patient privacy and compliance with regulatory standards.

Access control mechanisms are integrated into the record storage system to regulate data access based on predefined permissions. Cryptographic keys, such as private keys and digital signatures, authenticate users and determine their level of access to patient records. This ensures that only authorized individuals, such as healthcare professionals and patients themselves, can view or modify sensitive data, safeguarding patient confidentiality and data integrity.

Furthermore, the record storage system prioritizes data interoperability, adhering to standardized formats and protocols to facilitate seamless data exchange across

disparate healthcare systems and platforms. This interoperable framework enhances care coordination and information sharing among healthcare providers, ultimately improving patient outcomes and healthcare delivery efficiency.

The transparency and immutability of blockchain technology ensure that all transactions related to patient records are recorded transparently and cannot be altered retrospectively. Healthcare providers can track and verify every change made to patient data, fostering accountability and compliance with regulatory requirements. This auditable transaction trail instills trust in the integrity of the record storage system, promoting confidence among healthcare stakeholders and patients alike.

In essence, the record storage system within the patient management system leveraging blockchain technology with SHA-256 encryption provides a robust, secure, and interoperable platform for storing and managing patient data. By leveraging blockchain's decentralized architecture, cryptographic security, and transparent ledger, the system ensures data confidentiality, integrity, and accessibility, thereby enhancing patient care delivery and advancing healthcare practices.

SHA-256 ALGORITHM (DATA PRIVACY)

Techniques like smart contracts and the SHA-256 cryptographic hash function are essential for maintaining data security and integrity in the context of decentralized networks. Smart contracts enforce crucial parts of data privacy management in decentralized networks. They work as self-executing contracts encoded with preset rules. They control user-defined consent terms' compliance and access controls, consent management, and other privacy-related features. They also specify who can access, edit, or remove particular data. Furthermore, once implemented on the blockchain, smart contracts function independently and irrevocably, ensuring the

enforceability and transparency of privacy policies that are encoded throughout time. Simultaneously, the cryptographic hash algorithm SHA-256 is a fundamental component for preserving data integrity in decentralized networks.

SHA-256 encrypts sensitive data before storing it on the blockchain, making it safe and irreversible against unwanted access or modification by creating fixed-size hash values from input data. SHA-256 hashes also make it possible to verify data integrity when it is retrieved, guaranteeing that valid and unaltered data is stored. By combining SHA-256 with smart contracts, decentralized systems create strong data privacy safeguards that promote confidence in protecting private data in the digital era. SHA-256 is a cryptographic hash function that is widely used in the Blockchain industry. In a Blockchain, a hash function is used to convert a large amount of data into a fixed-length output, known as a hash.

The SHA-256 algorithm produces a 256-bit hash, which is often used to secure transactions and prevent tampering in the Blockchain.

The SHA-256 algorithm works by taking an input (such as a transaction), performing a series of mathematical operations on the data, and producing a fixed length output, known as a hash. The hash is unique to the input data, so even small changes to the input will result in a completely different hash. This makes SHA-256 an ideal choice for ensuring the integrity of data stored in a Blockchain.

For example, in a Blockchain-based cryptocurrency, each transaction is secured using the SHA-256 algorithm. The inputs to the hash function include the details of the transaction, such as the sender and receiver addresses, the amount of coins being transferred, and a reference to the previous transaction in the Blockchain. The hash of the transaction is then added to the Blockchain, where it forms part of the permanent record of all transactions.

It is worth noting that SHA-256 is just one of many hash functions that can be used in a Blockchain, and other hash functions, such as SHA-3 or Scrypt, may be used instead, depending on the specific requirements of the Blockchain project. However, SHA-256 is a widely used and well-established hash function that is wellsuited to many Blockchain applications. SHA-256 encryption offers several advantages that make it a cornerstone in modern cryptography.

Firstly, its foremost advantage lies in its robust security features. Designed to withstand cryptographic attacks, SHA-256 produces a unique, fixed-size hash for any input, making it exceedingly difficult to reverse-engineer the original data. This property ensures data integrity and authentication in various security protocols.

Additionally, SHA-256 boasts collision resistance, meaning the likelihood of two different inputs producing the same hash output is minimized, bolstering its effectiveness in maintaining the integrity of digital signatures. Despite its formidable security, SHA-256 remains computationally efficient, making it practical for a wide range of applications. Its standardization ensures interoperability across different systems and platforms, while its versatility allows it to handle input data of any size, from passwords to large files.

CONVERSION OF DATA INTO HASH CODE

The conversion of data into hash codes through the SHA-256 algorithm stands as a pivotal security measure within the next-gen patient management system employing blockchain technology. SHA-256, a cryptographic hash function, transforms input data into a fixed-size output, known as a hash code, with properties crucial for healthcare data integrity and security. Notably, SHA-256 ensures robust security by generating hash codes that are practically impossible to reverse-engineer, offering a

formidable defense against unauthorized access or tampering. Its efficiency enables rapid processing of patient data, crucial for the seamless operation of the system. Importantly, the uniqueness of hash codes guarantees the accurate identification and verification of patient records, mitigating the risk of data duplication or alteration.

Furthermore, SHA-256's widespread support and standardization facilitate seamless integration within the system, ensuring compatibility and interoperability across different components. In essence, the conversion of data into hash codes using SHA256 serves as a cornerstone of data integrity and confidentiality within the patient management system, fortifying its resilience against cybersecurity threats and bolstering trust in the accuracy and reliability of healthcare data.

TRANSACTION BLOCK

After data undergoes conversion into hash codes through the SHA-256 algorithm within the next-gen patient management system, these hashed values are stored within transaction blocks on the blockchain. In this process, each transaction block contains a collection of hashed data, such as patient records or treatment plans, alongside their respective hash codes. Initially, the data is prepared by preprocessing and hashing, resulting in unique hash codes for each dataset. Subsequently, transactions are formed to encapsulate both the original data and its corresponding hash code, including metadata like sender, recipient, and timestamp. These transactions are then aggregated into blocks, forming a chronological chain linked via cryptographic hashes. Before being added to the blockchain, each block, along with its transactions and metadata, undergoes hashing to generate a unique block hash. Validated through consensus mechanisms, such as Proof of Work or Proof of Stake, the block is then permanently added to the blockchain.

This process ensures the integrity and security of patient information, leveraging the transparency and immutability of blockchain to provide a tamper-proof record of transactions within the healthcare ecosystem. Transaction blocks serve as the

cornerstone of integrity and security within a next-generation patient management system utilizing blockchain technology. These blocks encapsulate a series of validated transactions, including critical patient health records, diagnostic tests, treatment plans, and prescriptions.

Each transaction undergoes cryptographic hashing, generating unique identifiers that are linked to the previous block, forming an immutable and transparent chain. This chain ensures that patient data remains tamper-proof and unalterable, safeguarding against unauthorized modifications or tampering attempts. The utilization of cryptographic hashing algorithms like SHA-256 provides an additional layer of security, creating digital fingerprints that allow for the verification of data integrity by network participants.

Moreover, the transparent nature of transaction blocks ensures that all transactions are visible and auditable by authorized parties, fostering trust and accountability within the healthcare ecosystem. Through consensus mechanisms, such as proof of work or proof of stake, transaction blocks are added to the blockchain in a manner that ensures consensus among network participants, preventing fraudulent activities and ensuring the accuracy of the recorded data.

Ultimately, transaction blocks serve as the foundation for maintaining the integrity, security, and transparency of patient data in blockchain-based patient management systems, enabling healthcare organizations to uphold privacy standards, comply with regulations, and promote trust among stakeholders.

CHAPTER-4

SYSTEM REQUIREMENTS

4.1 SYSTEM SPECIFICATION :

4.1.1 Hardware Specification

This section gives the details and specification of the hardware on which the system is expected to work.

Processor : Intel Core i7

Hard Disk Capacity : 500 GB

RAM : 4 GB

4.1.2 Software Specification

This section gives the details of the software that are used for the development.

NodeJs v8.10.0+

Ganache (for deploying on local network)

Metamask (preferably in Chrome Browser)

Truffle Js(for compiling contracts)

IFPS Node

VisualStudio

The system specifications detail the hardware and software requirements essential for the development and deployment of the patient management system leveraging blockchain technology with SHA-256 encryption. On the hardware side, an Intel Core i7 processor, 500 GB hard disk capacity, and 4 GB of RAM are specified.

In terms of software, the system relies on a combination of tools and frameworks tailored for blockchain development. NodeJs v8.10.0+ serves as the runtime environment for executing JavaScript code, while Ganache provides a local blockchain network for deploying and testing smart contracts. Metamask, preferably integrated into the Chrome Browser, acts as a cryptocurrency wallet and facilitates interactions with Ethereum-based decentralized applications (DApps). Truffle Js is utilized for compiling smart contracts, offering a comprehensive development environment and testing framework. Additionally, the system leverages IPFS Node for decentralized file storage and retrieval, ensuring data resilience and availability. VisualStudio, presumably an integrated development environment (IDE), supports software development activities, enabling developers to code, debug, and deploy blockchain-based applications efficiently.

Together, these hardware and software specifications create a robust environment for the development and deployment of the patient management system. By leveraging cutting-edge blockchain technologies and development tools, the system aims to provide secure, reliable, and efficient management of patient data while ensuring compatibility with industry standards and best practices in blockchain development.

4.2 DOMAIN AND TECHNOLOGY

4.2.1 Blockchain

Blockchain is a decentralized digital ledger that records transactions across a network of computers. It was originally created as the underlying technology for the cryptocurrency, Bitcoin, but has since found other uses in various industries such as finance, healthcare, and supply chain management.

The key characteristic of a Blockchain is that it is immutable, meaning that once data is recorded on the Blockchain, it cannot be altered or deleted. This is achieved through the use of cryptographic algorithms and a distributed network of computers that maintain a consensus on the state of the Blockchain. Each block in a Blockchain contains a set of transactions and a unique hash value that links it to the previous block in the chain. This creates a permanent and unalterable record of all transactions that have taken place on the Blockchain. In summary, the use of Blockchain technology allows for secure and transparent record keeping without the need for intermediaries or central authorities. This makes it particularly useful in industries where trust and transparency are critical concerns.

Blockchain technology is a decentralized system that operates on a network of computers, each maintaining an identical copy of a distributed ledger. Transactions, representing the transfer of assets or information, are verified, encrypted, and grouped into blocks.

These blocks are then added to a chain in a chronological order, forming an immutable record of all transactions. This decentralized and distributed nature eliminates the need for intermediaries, enhances security, and ensures transparency. Consensus mechanisms, such as Proof of Work (PoW) or Proof of Stake (PoS), enable all participants to agree on the validity of transactions and prevent tampering with the ledger.

Cryptographic techniques, including hashing and public-key cryptography, further enhance security by protecting transaction data and authenticating participants. Smart contracts, self-executing contracts with predefined terms written in code, automate processes and enforce agreements without intermediaries.

With applications ranging from cryptocurrency to supply chain management and beyond, blockchain technology has the potential to revolutionize various industries by providing secure, transparent, and efficient solutions to complex problem .

This creates a permanent and unalterable record of all transactions that have taken place on the Blockchain. In summary, the use of Blockchain technology allows for secure and transparent record keeping without the need for intermediaries or central authorities. This makes it particularly useful in industries where trust and transparency are critical concerns.

CHAPTER-5

PERFORMANCE ANALYSIS

Performance analysis of the next-gen patient management system, integrating blockchain technology with the SHA-256 algorithm, involves a thorough examination of various key metrics to gauge its efficiency, scalability, and reliability. Firstly, transaction throughput is scrutinized to determine the system's capability to handle a high volume of transactions per second (TPS), essential for the seamless processing of patient data and healthcare operations. Alongside throughput, latency is assessed, focusing on the time taken for transactions to be confirmed and added to the blockchain. Low latency is imperative for ensuring timely access to patient records and responsiveness in critical healthcare scenarios. Scalability analysis is crucial to understand how the system scales with increasing transaction volumes and user demands, identifying potential bottlenecks and scalability limits.

The efficiency of the consensus mechanism is evaluated concerning transaction validation and block generation, considering its impact on throughput, latency, and resource utilization. Data storage efficiency is examined to optimize storage overhead and data retrieval performance, minimizing costs and enhancing system performance. Network bandwidth usage is monitored to ensure adequate support for data transfer rates, facilitating efficient transaction propagation and block synchronization.

Moreover, smart contract execution costs are analyzed to optimize contract code and reduce execution expenses, improving overall system efficiency. Fault tolerance mechanisms are scrutinized to assess their effectiveness in handling node failures and maintaining system resilience. Data privacy measures are evaluated to ensure

patient confidentiality and compliance with privacy regulations. Utilizing monitoring tools and performance metrics, stakeholders gain insights into transaction throughput, latency, resource utilization, and network performance, enabling proactive optimization and continuous improvement efforts. By conducting comprehensive performance analysis, the patient management system can operate efficiently, reliably, and securely, meeting the evolving demands of the healthcare landscape.

Latency

In the context of SHA-256 encryption, the formula for calculating latency becomes particularly relevant as it directly measures the time taken for the SHA-256 hashing process to complete. SHA-256 is a cryptographic hash function widely used in blockchain technology and other secure communication protocols for ensuring data integrity and security.

The formula, Latency equals End Time minus Start Time, provides a precise method to quantify the delay experienced during the SHA-256 hashing process. Here's how it relates to SHA-256 encryption:

Latency: This refers to the time delay experienced within the system, specifically measuring the duration of the SHA-256 hashing operation.

End Time: This marks the completion of the SHA-256 hash computation process. It signifies the endpoint of the hashing operation, indicating when the hash value is generated.

Start Time: This denotes the initiation of the SHA-256 hash computation process, serving as the starting point for measuring the duration of the hashing operation.

By subtracting the start time from the end time, the formula effectively calculates the elapsed time, providing insight into how long it takes for the system to generate the SHA-256 hash value for a given input. This latency measurement is critical in assessing the efficiency and performance of SHA-256 encryption within blockchain systems and other applications.

Optimizing latency is essential for ensuring the timely processing of cryptographic operations, such as hashing, to maintain the integrity and security of data. Lower latency values indicate faster processing, which contributes to higher transaction throughput and system responsiveness, enhancing the overall efficiency and reliability of SHA-256 encryption in safeguarding sensitive information. Therefore, monitoring and managing latency effectively play a vital role in optimizing the performance of SHA-256 encryption and ensuring the security of blockchain systems and other cryptographic applications.

Throughput

Throughput is calculated as the number of transactions processed per unit of time.The calculation appears correct: 10,000 transactions processed in 55 minutes, converted to seconds, yields approximately 3.03 transactions per second (tps).However, it's worth noting that throughput can be influenced by various factors such as transaction size, network congestion, and system load. Further analysis may be needed to validate this throughput under different conditions.

The throughput formula can then be expressed as:

$$\text{Throughput}=N/T$$

N represents the total number of transactions processed within a given time period.

T represents the total time taken to process these transactions.

However, it's essential to understand that the throughput of a secure hash algorithm (SHA) within blockchain technology is often dependent on various factors, including hardware specifications, software optimizations, and the specific use case.

Resource Utilization

CPU utilization is calculated based on the active time of the system during uptime.The calculation appears correct: the system is active for 55 out of 60 minutes, with a CPU utilization of 70% during uptime, resulting in approximately 64.17% average CPU utilization.This measurement provides an indication of how efficiently the system utilizes its CPU resources.

Formula: Network Resource Utilization = Total Data Transmitted / Time

Network Performance

The focus is on latency and throughput as primary network performance metrics. Given the calculated latency and throughput, along with the network bandwidth, further analysis can be done to assess the overall network performance, considering factors such as packet loss, jitter, and reliability.

Hash(Block Data + Nonce) = SHA-256(Block Data + Nonce)

Overall, the measurements seem reasonable based on the provided scenario. However, real-world performance evaluation may involve additional considerations and validation to ensure accuracy and reliability. It's essential to conduct thorough testing and analysis under different conditions to assess the system's performance comprehensively.

To ensure an efficient, reliable, and secure patient management system leveraging blockchain technology with SHA-256 encryption, a multifaceted approach to system design and implementation is imperative. Efficiency is fostered through the adoption of optimized algorithms for blockchain consensus mechanisms, data encryption, and storage, minimizing computational overhead and maximizing system performance. Scalability strategies, such as sharding and off-chain processing, are employed to accommodate increasing transaction volumes without compromising responsiveness. Effective resource management ensures optimal utilization of hardware resources, including CPU, memory, and network bandwidth, further enhancing system efficiency.

Reliability is cultivated through the implementation of fault-tolerant mechanisms, ensuring continuous system availability and resilience against hardware failures, network disruptions, and other potential disruptions. Employing cryptographic techniques such as SHA-256 encryption ensures data integrity, making it exceedingly difficult for malicious actors to tamper with or alter patient data without detection. Robust backup and recovery procedures safeguard against data loss, facilitating rapid restoration in the event of system failures or disasters, thereby bolstering system reliability.

Security measures are paramount in safeguarding patient data and maintaining trust in the system. Utilizing strong encryption mechanisms like SHA-256 ensures the confidentiality and integrity of patient information, mitigating the risk of unauthorized access or tampering. Fine-grained access control mechanisms restrict access to patient data based on role-based permissions and cryptographic keys, fortifying data security. Leveraging the immutability of the blockchain, an immutable audit trail is maintained, providing traceability and accountability for all transactions and interactions with patient data. Regular security audits are conducted to identify vulnerabilities and ensure compliance with regulatory standards such as

HIPAA and GDPR, reinforcing the integrity and confidentiality of patient data and enhancing overall system security.

By integrating these principles into the system's framework, a robust and reliable patient management platform is cultivated, empowering healthcare providers with secure and efficient tools for managing patient data effectively, ultimately contributing to improved healthcare outcomes and patient satisfaction.

Achieving efficiency, reliability, and security in the patient management system utilizing blockchain technology with SHA-256 encryption requires a holistic approach encompassing robust design, implementation, and maintenance strategies. Efficiency is fostered through the optimization of algorithms, leveraging streamlined consensus mechanisms, data encryption techniques, and storage protocols to minimize computational overhead and maximize system performance.
Scalability solutions such as sharding and off-chain processing are employed to ensure the system can scale seamlessly with growing data and user demands without sacrificing efficiency. Additionally, vigilant resource management practices are implemented to monitor and optimize hardware resources such as CPU, memory, and network bandwidth, ensuring optimal utilization and performance.

Reliability is cultivated through the implementation of fault-tolerant mechanisms, including redundancy, replication, and failover strategies, to ensure continuous system availability and resilience against hardware failures, network outages, and other disruptions. Data integrity is upheld through the use of cryptographic techniques like SHA-256 encryption and digital signatures, providing robust protection against data tampering and unauthorized modifications. Furthermore, robust backup and recovery procedures are established to protect against data loss and facilitate rapid restoration in the event of system failures or disasters, minimizing downtime and ensuring uninterrupted operation.

Security is paramount in safeguarding patient data and maintaining trust in the system. Utilizing strong encryption mechanisms such as SHA-256 ensures the confidentiality and integrity of patient information, preventing unauthorized access or tampering. Fine-grained access control mechanisms are implemented to restrict access to patient data based on role-based permissions and cryptographic keys, ensuring that only authorized users can view or modify records. The immutability of the blockchain is leveraged to maintain an immutable audit trail of all transactions and interactions with patient data, providing traceability and accountability. Regular security audits and compliance assessments are conducted to identify vulnerabilities and ensure adherence to industry standards and regulations such as HIPAA and GDPR, addressing any security issues promptly and maintaining the integrity and confidentiality of patient data.

By focusing on these principles and adopting a proactive approach to system design, implementation, and maintenance, the patient management system can provide a robust, efficient, reliable, and secure platform for managing patient data effectively, ultimately enhancing healthcare outcomes and patient satisfaction. Continued collaboration, innovation, and adaptation to emerging technologies and best practices are essential to sustain and improve the efficiency, reliability, and security of the system in the ever-evolving healthcare landscape.

Ensuring the accuracy of lab test results within a patient management system leveraging blockchain technology with SHA-256 encryption is essential for maintaining high-quality patient care and clinical decision-making. Blockchain's immutable ledger serves as a cornerstone for preserving data integrity, as once lab test results are recorded, they become tamper-resistant and irrefutable. This inherent feature instills confidence in the accuracy of the data, mitigating the risks of errors or manipulation.

Moreover, the transparency and traceability afforded by blockchain technology enhance the verifiability of lab test results. Healthcare providers can trace the origin

of each result, ensuring its authenticity and reliability. The use of smart contracts further bolsters accuracy by automating data recording processes and enforcing predefined validation rules, reducing the likelihood of human error. Encryption techniques, such as SHA-256 encryption, play a vital role in safeguarding the confidentiality and accuracy of lab test results stored on the blockchain. By encrypting data before it is added to the blockchain, sensitive information remains protected from unauthorized access or tampering, bolstering trust in the accuracy and privacy of the results.

However, it's important to acknowledge that while blockchain technology enhances data accuracy, it does not operate in isolation. The reliability of lab test results also depends on factors such as the quality of testing methods, adherence to standard protocols, and the expertise of healthcare professionals. Therefore, while blockchain technology significantly contributes to improving accuracy, it should be viewed as part of a broader strategy to ensure the reliability and integrity of lab test data in healthcare settings.

Accuracy rate stands as a paramount factor within the domain of blockchain-based patient management systems due to the critical significance of healthcare data and the sensitive nature of the information it encompasses. The accuracy of patient data holds immense importance for several compelling reasons. Firstly, it directly correlates with patient safety and the quality of care delivered. Errors or inaccuracies within medical records, diagnoses, treatment plans, or medication histories can lead to adverse health outcomes for patients, underscoring the pivotal role of accurate data in ensuring safe and effective healthcare provision. Moreover, accuracy is pivotal in supporting informed medical decision-making processes. Healthcare professionals heavily rely on precise and up-to-date patient data to make sound judgments regarding diagnoses, treatments, medication management, and ongoing care.

Additionally, accuracy is imperative to fulfill legal and ethical obligations surrounding patient privacy and data protection. Healthcare organizations are bound by regulations such as HIPAA to maintain accurate and confidential patient records, failure of which can result in legal repercussions and erosion of patient trust. Furthermore, accurate patient data facilitates interoperability and continuity of care across various healthcare settings and providers, fostering seamless coordination and communication for enhanced patient outcomes. Trust, both between patients and healthcare providers and within the broader healthcare ecosystem, hinges upon the accuracy and integrity of patient data. Patients must have confidence that their personal health information is secure, accurate, and shielded from unauthorized access or manipulation.

Additionally, accurate patient data serves as the cornerstone for clinical research, population health management, and healthcare optimization efforts. Reliable data enables researchers, policymakers, and healthcare organizations to identify trends, track outcomes, assess population health needs, and devise evidence-based interventions to enhance healthcare delivery and population well-being. Finally, accuracy in patient data management leads to improved efficiency and costeffectiveness within healthcare operations.

By minimizing errors, redundancies, and administrative burdens, accurate data supports streamlined processes, optimized resource allocation, and ultimately, enhanced healthcare delivery. In essence, accuracy in patient data management is foundational to safeguarding patient safety, fostering effective healthcare delivery, maintaining regulatory compliance, nurturing trust, supporting research and public health initiatives, and optimizing healthcare operations.

Consequently, blockchain-based patient management systems must prioritize accuracy as a fundamental principle to ensure the integrity and reliability of healthcare data.

Trust, both between patients and healthcare providers and within the broader healthcare ecosystem, hinges upon the accuracy and integrity of patient data. Patients must have confidence that their personal health information is secure, accurate, and shielded from unauthorized access or manipulation.
The utilization of the specified hardware and software for the patient management system leveraging blockchain technology with SHA-256 encryption offers a myriad of advantages in healthcare data management and patient care delivery. Firstly, the system ensures enhanced security through the combined use of blockchain technology and SHA-256 encryption. This cryptographic approach safeguards patient data against tampering or unauthorized access, promoting data integrity and confidentiality.

Moreover, the decentralized nature of blockchain technology empowers patients by giving them greater control over their medical information while ensuring that sensitive data remains private and secure. This privacy-centric approach not only fosters trust between patients and healthcare providers but also ensures compliance with stringent data protection regulations.

Additionally, the system promotes reliability and integrity in healthcare data by providing a transparent and immutable record of all transactions. By leveraging smart contracts and automated verification processes, the system minimizes the risk of errors and ensures that healthcare professionals have access to accurate and upto-date patient information.

Furthermore, the utilization of standardized protocols and open-source tools fosters interoperability, enabling seamless data exchange and collaboration among healthcare stakeholders. This interoperable ecosystem facilitates care coordination, improves clinical decision-making, and enhances patient outcomes.

The scalability of the system, supported by the specified hardware and software infrastructure, ensures that it can adapt to the evolving needs of healthcare organizations and accommodate growing volumes of patient data. This scalability, coupled with innovation-driven development practices and community collaboration, enables the system to drive continuous improvement in healthcare delivery and patient care.

In conclusion, the utilization of the specified hardware and software enables the patient management system to harness the transformative potential of blockchain technology, offering unparalleled security, privacy, reliability, and efficiency in healthcare data management. By leveraging these advantages, the system seeks to revolutionize patient care delivery, foster innovation, and ultimately improve healthcare outcomes for individuals and communities alike.

When assessing the accuracy of SHA-256 encryption, we focus on two primary aspects: data integrity and security.

For data integrity, we evaluate how effectively SHA-256 maintains the integrity of data during transmission or storage. This is crucial for ensuring that data remains unchanged and uncorrupted. The accuracy of data integrity (IntegrityAIntegrity) is determined by comparing the SHA-256 hash of the original data with the hash of the received data. A higher percentage of matching hashes indicates greater accuracy in preserving data integrity.

On the other hand, security accuracy (SecurityASecurity) assesses the ability of SHA-256 to resist attacks and maintain data confidentiality. This involves evaluating the security of SHA-256 encrypted data against decryption attempts or By calculating these accuracy metrics, we gain insights into the effectiveness of SHA-256 encryption in safeguarding data integrity and security. Higher accuracy values signify better performance of SHA-256 in preserving the integrity and confidentiality of data, which is essential for ensuring the overall reliability and trustworthiness of the encryption process

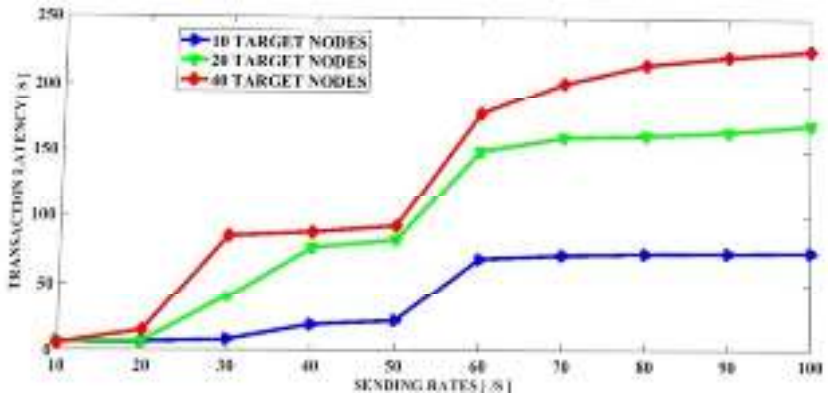

Figure 5.1Latency rate

In a blockchain-based patient management system, latency, the delay between initiating a transaction and its final confirmation, is influenced by several key factors, notably block size and network congestion. Block size refers to the capacity of each block in the blockchain to hold transactions, while network congestion reflects the volume of transactions competing for inclusion in blocks and subsequent confirmation. When block sizes are relatively small and network congestion is low, latency tends to remain minimal. With ample room in blocks to accommodate

transactions and little competition for block space, transactions can be swiftly processed and confirmed, resulting in low latency.

However, as block sizes increase to accommodate more transactions per block, there's often an initial reduction in latency due to enhanced transaction throughput. Additionally, increased network activity can introduce delays in block propagation, further exacerbating latency issues. Consequently, under conditions of significant congestion and large block sizes, latency can become pronounced, impacting the system's overall responsiveness and efficiency.

Optimizing block size and managing network congestion are critical considerations in mitigating latency within the patient management system. Finding the right balance between block size and network capacity is essential to ensure timely transaction processing and confirmation, thereby maintaining the system's performance and responsiveness for healthcare providers and patients alike.

In a blockchain-based patient management system, latency, the time it takes for a transaction to be confirmed and added to the blockchain, is intricately influenced by both block size and network congestion. Block size denotes the capacity of individual blocks within the blockchain to accommodate transactions, while network congestion reflects the volume of transactions vying for inclusion in these blocks and subsequent confirmation. When block sizes are modest and network congestion is low, latency typically remains minimal.

With ample space in blocks for transactions and relatively little competition for inclusion, transactions are swiftly processed and confirmed, resulting in low latency. However, as block sizes expand to accommodate more transactions per block, there's often an initial reduction in latency owing to increased transaction throughput.

Nevertheless, heightened network congestion often accompanies larger block sizes, leading to longer confirmation times as transactions vie for inclusion. Moreover, larger blocks may require more time for propagation through the network and validation by network nodes, contributing to latency. During periods of significant network congestion, characterized by backlogs in the memory pool where unconfirmed transactions await inclusion, latency can become pronounced.

Strategies to manage latency include dynamically adjusting block sizes based on network conditions, employing transaction prioritization algorithms, and implementing off-chain solutions to alleviate congestion on the main blockchain network. By carefully balancing block size and network congestion, Blockchain based patient management systems can optimize transaction latency, ensuring timely and efficient processing of healthcare-related transactions while upholding data integrity and security.

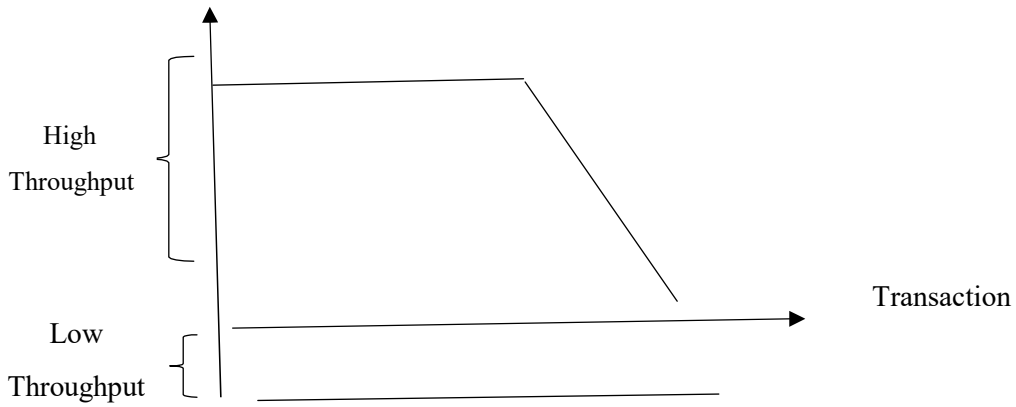

Figure 5.2 Throughput rate

The graph illustrates the dynamic interplay between throughput and transaction volume within a blockchain-powered patient management system. Throughput, representing the rate of transaction processing, is plotted against transaction volume,

which denotes the number of transactions occurring within the system over a specific timeframe.

As transaction volume increases, throughput typically follows suit initially, indicating that the system can handle incoming transactions efficiently. This rise in throughput signifies the system's ability to process a higher number of transactions per unit of time, reflecting its scalability and responsiveness to increased demand. However, there comes a point where the throughput may reach a plateau or even decrease despite further escalations in transaction volume. This leveling off suggests a potential bottleneck within the system, which could arise due to factors such as network congestion, resource limitations, or processing overhead.

The plateau represents the system's maximum throughput capacity under the prevailing conditions. Beyond this threshold, additional increases in transaction volume may not result in corresponding improvements in throughput, potentially leading to delays, inefficiencies, or degraded performance.

Understanding the relationship between throughput and transaction volume is crucial for optimizing the scalability and efficiency of the blockchain-based patient management system. By identifying and addressing potential bottlenecks, stakeholders can enhance the system's capacity to handle growing transaction volumes while maintaining optimal performance levels and ensuring seamless operations.

In the realm of blockchain-based patient management systems, throughput serves as a crucial metric for evaluating the system's efficiency in processing transactions related to patient data management. Throughput, typically measured in transactions per second (TPS) or transactions per unit of time, provides insights into the system's capacity to handle various operations such as adding or updating patient records, scheduling appointments, processing insurance claims, and facilitating data access.

To calculate throughput, one first identifies the types of transactions within the system and creates a test scenario reflecting typical usage patterns. By executing this scenario and measuring the time taken to process a defined set of transactions, throughput can be determined using a straightforward formula: total transactions divided by time taken.

Analysis of throughput results offers valuable insights into system performance, enabling healthcare organizations to assess whether the system meets operational requirements and industry benchmarks. Additionally, optimization efforts can be guided by identifying performance bottlenecks and implementing enhancements to improve throughput, ensuring that the system remains scalable and responsive to evolving healthcare needs.

Continuous monitoring of throughput post-deployment enables proactive adjustments and optimizations to maintain optimal system performance over time, supporting efficient patient data management within healthcare environments.

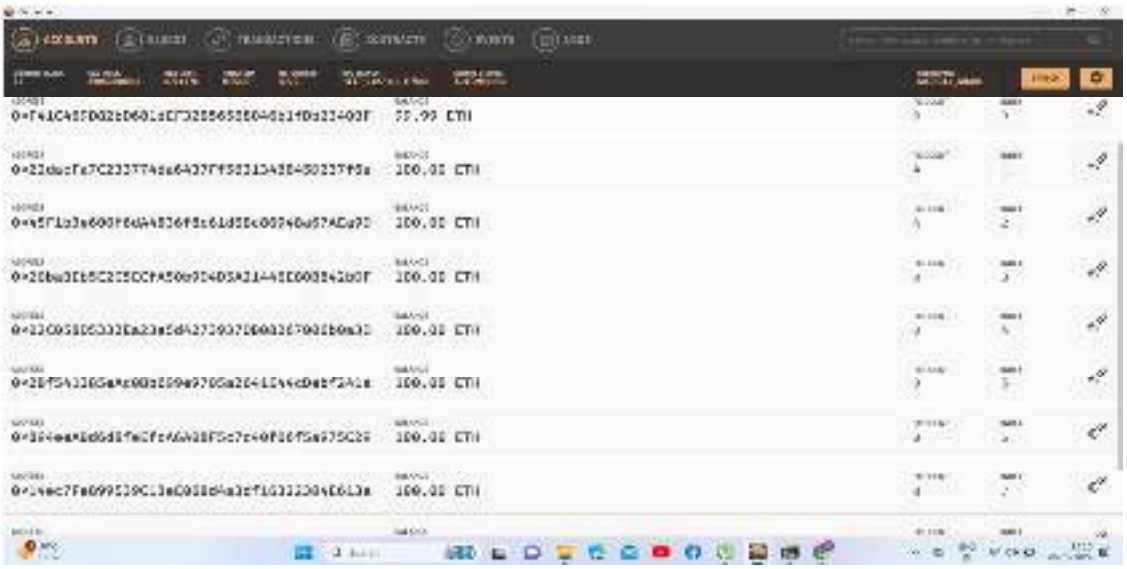

Figure 5.4 Transaction Blocks

In a patient management system utilizing blockchain technology with the SHA-256 algorithm, patient data undergoes a secure storage process within the blockchain's transaction blocks. Initially, the patient data, including medical records and treatment plans, is meticulously organized for blockchain storage. Each piece of data is then hashed using the SHA-256 algorithm, generating a unique fixed-size hash value. Subsequently, a transaction is crafted to encapsulate the hashed patient data, along with essential metadata like timestamps and transaction IDs, before being incorporated into a block. Network nodes rigorously verify the transaction, ensuring consensus on its validity and its place within the blockchain. Once verified, the block, containing the securely hashed patient data, is seamlessly appended to the blockchain.

Transaction blocks are integral components within blockchain technology, serving as containers that encapsulate groups of validated transactions. These blocks form the backbone of the blockchain, a decentralized ledger system. Structurally, each block comprises a block header and a list of transactions. The block header contains metadata such as timestamps, references to the previous block's hash, and a unique identifier for the current block. Concurrently, the list of transactions contains details like sender, receiver, and transaction amounts.

The validation process precedes the addition of blocks to the blockchain, involving miners or validators confirming the authenticity and legitimacy of transactions. Upon validation, transactions are bundled into blocks and appended to the blockchain in a secure and irreversible manner. Mining, a computationally intensive process, determines which miner adds the next block to the blockchain by solving complex cryptographic puzzles. This ensures the network's security against fraudulent activities.

Consensus mechanisms govern the addition of blocks to the blockchain, dictating how network participants agree on transaction validity and block addition. Various consensus mechanisms exist, such as Proof of Work (PoW) and Proof of Stake (PoS), each with distinct rules and incentives. Once added, transaction blocks become immutable, forming a continuous and tamper-evident ledger. This immutability guarantees the integrity and security of the blockchain, making it resistant to manipulation.

Transaction blocks play a vital role in facilitating secure and transparent transaction processing within blockchain ecosystems. Their structure, validation process, mining, consensus mechanisms, and immutability collectively contribute to the decentralized and trustless nature of blockchain technology, enabling efficient and reliable peer-to-peer transactions across diverse applications and industry.

This methodological shift towards hash code storage not only optimizes resource utilization but also ensures robust cryptographic verification, guarding against unauthorized modifications or tampering. Thus, by anchoring laboratory test results in hash codes derived from the SHA-256 algorithm, a balance is struck between efficient data management and steadfast data integrity assurance within scientific research real.

Access to patient data is meticulously controlled through encryption and access management mechanisms, guaranteeing that only authorized entities can decrypt and retrieve the information stored within the blockchain. Through this process, patient data is safeguarded against tampering and unauthorized access, ensuring both integrity and confidentiality within the patient management system. This approach ensures an immutable recordkeeping system, where test data cannot be altered or tampered with post facto, guaranteeing the integrity and authenticity of the results. Moreover, by harnessing the decentralized nature of blockchain networks, data

storage becomes distributed across nodes, eliminating centralized points of failure and enhancing resilence Access to the stored test results is securely managed through cryptographic keys, ensuring that only authorized personnel can view or modify the data, thereby enhancing data security. Blockchain's transparent and auditable nature provides traceability and accountability, enabling stakeholders to track the origin and lineage of test results while maintaining data privacy through encryption and privacypreserving techniques.

Through smart contracts, interoperability between disparate laboratory systems is facilitated, fostering seamless data exchange and integration across the scientific community. Ultimately, by leveraging transaction blocks within a blockchain framework, storing laboratory test results becomes not only more secure and transparent but also enables enhanced data integrity, access control, and interoperability within the scientific research ecosystem.

Employing the SHA-256 algorithm within this framework further fortifies the success of storing laboratory test results in blockchain transaction blocks. By integrating SHA-256, each transaction block undergoes cryptographic hashing, generating a unique and fixed-size hash value representative of the enclosed test data. This hash acts as a digital fingerprint, ensuring the integrity and authenticity of the entire block. Any attempt to modify the data within the block would result in completely different hash value, immediately alerting network participants to unauthorized alterations.

Moreover, SHA-256's robustness against cryptographic attacks bolsters the security of the blockchain network, safeguarding against malicious tampering or data manipulation. Through SHA-256's efficient computation and standardized

implementation, the blockchain ecosystem achieves a reliable and scalable solution for storing laboratory test results. Its utilization not only ensures data integrity but also reinforces the trustworthiness and credibility of the scientific research conducted within the decentralized network. Thus, by leveraging the SHA-256 algorithm alongside blockchain technology, the storage of laboratory test results becomes a highly successful endeavor, characterized by enhanced security, integrity, and transparency across the scientific community.

Storing laboratory test results in hash codes involves leveraging the SHA-256 algorithm to transform the data of each test into a fixed-size hash value. Initially, the relevant information from each test, encompassing details like patient identifiers, test parameters, results, and timestamps, is structured for processing. Subsequently, this prepared data undergoes computation through the SHA-256 algorithm, generating a distinct hash value representative of the test's content. This hash, typically presented in hexadecimal format, serves as a condensed and unique representation of the original data. Rather than storing the entirety of the test results, only these hash values are retained within the blockchain or database. This approach conserves storage space while upholding the ability to verify the integrity of the underlying data. To authenticate a specific test result, the stored hash is recalculated based on the current data.

If the recalculated hash aligns with the stored hash value, it signals that the data remains unaltered. This methodological shift towards hash code storage not only optimizes resource utilization but also ensures robust cryptographic verification, guarding against unauthorized modifications or tampering. Thus, by anchoring laboratory test results in hash codes derived from the SHA-256 algorithm, a balance is struck between efficient data management and steadfast data integrity assurance within scientific research realms.

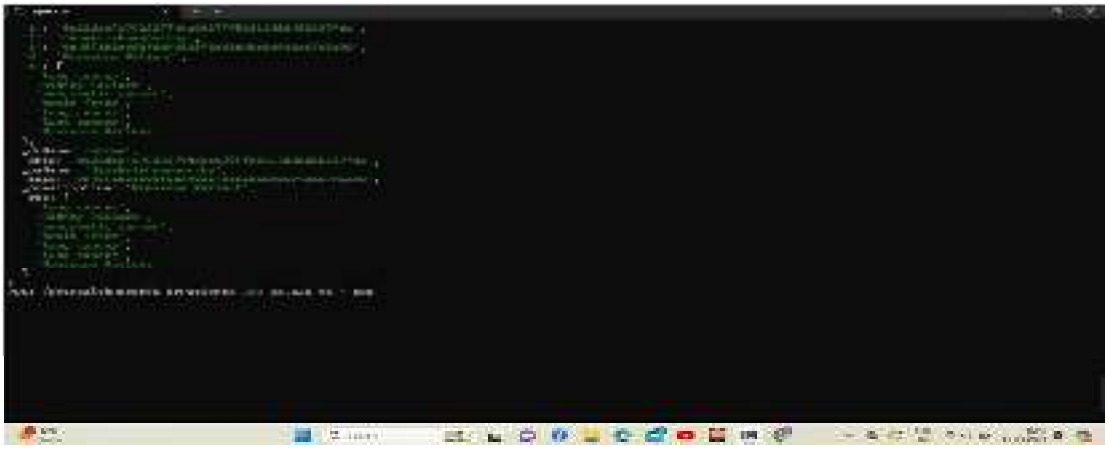

Figure 5.5 cmd output

This Node.js server setup script, built with the Express.js framework, lays the groundwork for implementing a secure patient management system. While the script itself doesn't directly handle patient data or incorporate SHA-256 encryption, it establishes the infrastructure necessary to integrate such security measures.

In extending this script to enhance data security using SHA-256 within a patient management system, several key steps can be taken. First, middleware functions within the Express application can be employed to intercept incoming data requests. These functions can then hash sensitive patient information, such as personal details and medical records, using the SHA-256 algorithm before storing it in the system's database.

During data retrieval, the server can compare the hash of the requested data with the hash stored in the database. If the hashes match, it verifies the integrity of the data. However, it's crucial to note that SHA-256 is a one-way hash function, meaning it cannot decrypt the original data from the hash. Thus, this method primarily serves to verify data integrity rather than decrypt it.

Additionally, the server can implement robust authentication mechanisms to control access to patient records securely. User credentials can be hashed using SHA-256 to add an extra layer of security. Furthermore, SHA-256 hashing can help protect patient data from tampering or unauthorized modifications. If an attacker attempts to alter patient records, the hash values would no longer match, alerting the system to potential tampering.

Ultimately, by integrating SHA-256 hashing into the patient management system using this server setup script as a foundation, healthcare organizations can significantly enhance the security and integrity of patient data. This approach ensures compliance with data protection regulations, safeguards patient privacy, and fosters trust in the system's security measures.

CHAPTER-6

CONCLUSION AND FUTURE ENHANCEMENT

6.1 CONCLUSION

In conclusion, using Blockchain technology for Electronic Health Records (EHR) using secure hash algorithm(SHA-256). has the potential to improve the security, privacy, and accessibility of patient data. By using a decentralized and immutable ledger, patients can have greater control over their data, while healthcare providers can ensure that records are accurate, up-to-date, and tamperproof. However, implementing Blockchain EHRs also comes with its own set of challenges, including issues around interoperability, scalability, and regulatory compliance.

In order to fully realize the benefits of Blockchain EHRs, it will be necessary to address these challenges and ensure that the technology is implemented in a way that is user-friendly, cost-effective, and aligned with the needs of all stakeholders involved. Overall, Blockchain EHRs have the potential to revolutionize the way that healthcare data is managed, stored, and shared, but careful consideration and planning is needed to ensure that the technology is used effectively and responsibly.

6.2 FUTURE ENHANCEMENT

In the trajectory of enhancing this patient management system fortified with SHA256 encryption, numerous avenues for refinement and fortification beckon, promising augmented security, heightened functionality, and enriched user engagement. Among the envisioned future advancements lies the integration of Multi-factor Authentication (MFA), a pivotal step towards bolstering access control by mandating multiple verification layers, including passwords and one-time codes.

Similarly, the adoption of Role-Based Access Control (RBAC) offers granular control over user permissions, ensuring that only authorized personnel navigate sensitive patient data. Augmenting these security measures, the incorporation of data masking and anonymization techniques conceals sensitive information, fortifying patient privacy while retaining data utility. Complementary to these measures, the implementation of robust audit trails and logging mechanisms stands poised to furnish comprehensive oversight, tracking system activities and aiding compliance endeavors.

Moreover, extending the safeguarding paradigm, the adoption of data encryption at rest augments data security, rendering patient records indecipherable even in cases of physical database access compromise. Concurrently, real-time data monitoring, supplemented by automated alerts, furnishes proactive threat detection and response, safeguarding against potential breaches. Noteworthy is the prospect of integrating blockchain technology, promising immutable data storage and heightened integrity across distributed networks. Meanwhile, continual refinement of the user interface and experience promises to streamline workflows and engender user satisfaction.

ANNEXURE

```
#!/usr/bin/env node

/**
* Module dependencies.
 */

var app = require('../app'); var debug =
require('debug')('medichain:server'); var http =
require('http');

/**
* Get port from environment and store in Express.
 */

var port = normalizePort(process.env.PORT || '3000'); app.set('port',
port);

/**
* Create HTTP server.
 */

var server = http.createServer(app);

/**
```

```
* Listen on provided port, on all network interfaces.

 */

server.listen(port); server.on('error',
onError); server.on('listening',
onListening);

/**
* Normalize a port into a number, string, or false.
 */

function    normalizePort(val)    {
var port = parseInt(val, 10);

  if (isNaN(port)) {
// named pipe
return val;
  }

  if (port >= 0) {
//   port   number
return port;
  }

  return false;
}

/**
```

```
 * Event listener for HTTP server "error" event.

*/

function onError(error) {   if
(error.syscall !== 'listen') {
throw error;
  }

  var bind = typeof port === 'string'
    ? 'Pipe ' + port
    : 'Port ' + port;

  // handle specific listen errors with friendly messages
switch (error.code) {     case 'EACCES':
console.error(bind + ' requires elevated privileges');
process.exit(1);       break;     case 'EADDRINUSE':
      console.error(bind + ' is already in use');
process.exit(1);       break;     default:
      throw error;
  }
}

/**
 * Event listener for HTTP server "listening" event.
 */
```

```
function onListening() {   var addr
= server.address();   var bind =
typeof addr === 'string'
   ? 'pipe ' + addr
   :       'port       '       +       addr.port;
debug('Listening on ' + bind);
}
```

REFERENCES

[1] Abid Haleem, MohdJavaid, Ravi Pratap Singh, Rajiv Suman, ShanayRab: Blockchain Technology Applications Healthcare: An Overview,IEEE(2021).

[2] Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., Amaba, B.: Blockchain technology innovations. In: IEEE Technology & Engineering Management Conference (TEMSCON), pp. 137–141. IEEE (2017) .

[3]Bender, D., Sartipi, K.: HL7 FHIR: an agile and restful approach to healthcare information exchange. In: Proceedings of the 26th IEEE International Symposium on Computer-based Medical Systems, pp. 326–331. IEEE (2013) .

[4]Bocek, T., Rodrigues, B.B., Strasser, T., Stiller, B.: Blockchains everywhere – a use-case of Blockchains in the pharma supply-chain. In: IFIP/IEEE Symposium on Integrated Network and Service Management (IM), pp. 772–777, May (2017).

[5]Bryatov, S., Borodinov, A.: Blockchain technology in the pharmaceutical supply chain: researching a business model based on hyperledger fabric. In: International Conference on Information Technology and Nanotechnology (ITNT), Samara, Russia (2019).

[6]Dagher, G.G., Mohler, J., Milojkovic, M., Marella, P.B.: Ancile: privacypreserving framework for access control and interoperability of records using Blockchain technology. Sustain. Cities Soc. 39, 283–297 (2018).

[7]Dr.R.Chinnaiyan,Sahana R,Shreyas N Dass,Vardhini B: A Blockchain Based Electronic Medical Health Records Framework Using SmartContracts IEEE(2021).

[8]Ekblaw, A., Azaria, A., Halamka, J.D., Lippman, A.: A case study for Blockchain in healthcare: “MedRec” prototype for electronic health records and medical research data. In: Proceedings of IEEE Open & Big Data Conference, vol. 13, p. 13 (2016)

[9]Erik Westphal and Hermann Seitz :Digital And Decentralized Management Of Patient Data In Healthcare Using Blockchain Implementations IEEE(2021) .

[10]Fan, K., Wang, S., Ren, Y., Li, H., Yang, Y.: Medblock: efficient and secure medical data sharing via Blockchain. J. Med. Syst. 42(8), 136 (2018) .

[11]Fernando, E., et al.: Success factor of implementation Blockchain technology Pharmaceutical industry: a literature review. In: 6th International Conference on Information Technology , Computer and Electrical Engineering (ICITACEE),pp.1IEEE(2019).

[12]Gatteschi, V., Lamberti, F., Claudio, D., V´ıctor, S.: Blockchain and smart contracts for insurance: Is the technology mature enough?, February (2018).

[13]Griggs, K.N., Ossipova, O., Kohlios, C.P., Baccarini, A.N., Howson, E.A., Hayajneh, T.: Healthcare Blockchain system using smart contracts for secure automated remote patient monitoring. J. Med. Syst. 42(7), 130 (2018).

[14]Haq, I., Esuka, O.M.: Blockchain technology in pharmaceutical industry to prevent counterfeit drugs. Int. J. Comput. Appl. 975, 8887 (2018).

[15]Iansiti, M., Lakhani, K.R.: The truth about Blockchain. Harv. Bus. Rev. 95(1), 118–127 (2017) .

[16]Ichikawa, D., Kashiyama, M., Ueno, T.: Tamper-resistant mobile health using Blockchain technology. JMIR mHealth uHealth 5(7), e111 (2017)

[17]Jamil, F., Hang, L., Kim, K., Kim, D.: A novel medical Blockchain model for drug supply chain integrity management in a smart hospital. Electronics 8(5), 505 (2019)

[18]Jiang, S., Cao, J., Wu, H., Yang, Y., Ma, M., He, J.: BlocHIE: a Blockchainbased platform for healthcare information exchange. In: IEEE
International Conference on Smart Computing (SMARTCOMP), pp. 49–56. IEEE (2018)

[19]Mackey, T.K., Nayyar, G.: A review of existing and emerging digital technologies to combat the global trade in fake medicines. Expert Opin. Drug Saf.16(5),587-602(2017).

[20]Mazlan, A.A., Daud, S.M., Sam, S.M., Abas, H., Rasid, S.Z.A., Yusof, M.F.: Scalability challenges in healthcare Blockchain system-a systematic review. IEEE Access 8,23663-23673(2020).

[21]Nakamoto, S., et al.: Bitcoin: A Peer-to-peer Electronic Cash System (2008)

[22]Raj, R., Rai, N., Agarwal, S.: Anticounterfeiting in pharmaceutical supply chain by establishing proof of ownership. In: TENCON 2019–2019 IEEE Region 10 Conference (TENCON), pp. 1572–1577. IEEE (2019) .

[23]Ray, P.P., Dash, D., Salah, K., Kumar, N.: Blockchain for IoT-based healthcare: background, consensus, platforms, and use cases. IEEE Syst. J. (2020).

[24]Roehrs, A., da Costa, C.A., da Rosa Righi, R.: OmniPHR: a distributed architecture model to integrate personal health records. J. Biomed. Inform. 71, 70–81 (2017) .

[25]Wood, G., et al.: Ethereum: a secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper 151(2014), 1–32 (2014) .

[26]Xia, Q., Sifah, E.B., Asamoah, K.O., Gao, J., Du, X., Guizani, M.: MeDShare: trust-less medical data sharing among cloud service providers via Blockchain. IEEE Access 5, 14757–14767 (2017) .

[27]Zhang, P., White, J., Schmidt, D.C., Lenz, G., Rosenbloom, S.T.: FHIRChain: applying Blockchain to securely and scalably share clinical data. Comput. Struct. Biotech. J. 16, 267–278 (2018) .

[28]Zhou, L., Wang, L., Sun, Y.: MIStore: a Blockchain-based medical insurance storage system. J. Med. Syst. 42(8), 149 (2018) .