CONTENTS

Contents		Page No
	ACKNOWLEDGEMENT	
	ABSTRACT	
CHAPTER 1	INTRODUCTION	2
CHAPTER 2	RELATED WORKS	5
CHAPTER 3	BLOCKCHAIN TECHNOLOGOVERVIREW	6
CHAPTER 4	SYSTEM ANALYSIS	8
CHAPTER 5	SYSTEM DESIGN	14
CHAPTER 6	MODULE DESCRIPTION	16
CHAPTER 7	SCREENSHOTS	24
CHAPTER 8	CONCLUSION	27

CHAPTER 1

INTRODUCTION

1.1 PURPOSE

Counterfeit medicine authentication is essential for patients' health and business operations. Counterfeiting of several products creates many issues for various manufacturing sectors and causes serious threats to medicine. This is very harmful to public health and also creates profit loss to the pharmaceuticals company. The yearly sales of counterfeit products in the world is 650 billion USD reported on the International Chamber of Commerce of Geneva [12]. To trace counterfeit drugs already several techniques have been used in the medicine supply chain. Authors in [15], proposed the usage of barcode or RFID code on medicine for verifying its legitimacy. Same as, a Data-Matrix tracking process has been proposed in [16], where every medicine has a Data-Matrix where contains Id of Product, Id of Manufacturer ID, unique ID of the package, the authentication code and optional metadata. The central verification register (CVR) is also mentioned. Most of the authors use RFID to their works on the medicine supply chain [1, 2, 16, 17]. But implementation of RFID is costly according to medicine price. In this paper we present a prototype of blockchain system for medicine traceability and regulation that rebuilds the full service architecture, ensuring authenticity and privacy of traceability data, and meantime achieves a ultimately stable blockchain data storage. Pseudocode explains the practical workflow of the medicine supply chain has also been given. This paper is arranged as follows. Blockchain based medicine traceability related works are presented in Section II, Design framework of our prototype is explained from three aspects from four aspects, Medicine Supply Chain Data Storage in blockchain, Detecting counterfeit medicine, and Methodology for the prototype work in Sections III. Then, Section IV explains the implementation and evaluation of the prototype. Finally, the paper is concluded in Section V.

1.2 OBJECTIVES

1.Ensuring Patient Safety:

Verify the authenticity of medicines to prevent patients from consuming counterfeit or substandard drugs, which may have harmful consequences.

2.Supply Chain Transparency:

Enhance transparency throughout the pharmaceutical supply chain, enabling stakeholders to trace the journey of drugs from manufacturing to distribution to end-users.

3.Counteracting Illicit Activities:

Deter and combat the production and distribution of counterfeit drugs by providing a secure and tamper-resistant system for tracking the movement of pharmaceuticals.

4.Authentication of Drug Origins:

Enable consumers, healthcare providers, and regulatory authorities to verify the origin and legitimacy of medications, ensuring they come from authorized manufacturers and distributors.

5.Real-time Monitoring:

Facilitate real-time monitoring of the entire supply chain, allowing for immediate detection of any anomalies or unauthorized access to drug shipments.

6.Data Integrity:

Ensure the integrity of data related to pharmaceutical transactions, preventing unauthorized modifications and ensuring that the information on the blockchain is accurate and reliable.

7.Compliance and Regulation:

Assist pharmaceutical companies in complying with regulatory requirements by providing a transparent and auditable record of the drug supply chain.

8.Efficient Recall Management:

Improve the efficiency of drug recalls by quickly identifying and isolating affected batches in case of quality issues, contamination, or other emergencies.

9.Enhancing Trust:

Build trust among consumers, healthcare professionals, and regulatory bodies by offering a secure and transparent system that guarantees the authenticity of medicines.

10.Cost Reduction:

Reduce costs associated with counterfeit drugs, such as healthcare expenses for treating patients affected by fake medications and the economic impact of lost revenue for legitimate pharmaceutical companies.

11.Interoperability:

Promote interoperability between different stakeholders in the pharmaceutical supply chain, ensuring that the system can be adopted and used seamlessly by manufacturers, distributors, regulators, and other relevant parties.

12.Decentralization:

Leverage the decentralized nature of blockchain to eliminate a single point of failure, making the system more resilient and less susceptible to hacking or manipulation.

13.Privacy and Security:

Implement robust security measures to protect sensitive information while allowing authorized parties to access necessary data, ensuring compliance with data protection regulations.

CHAPTER 2

RELATED WORKS

Nowadays, some technical and practical works which are already proposed in the medicine supply chain to detect substandard drugs with blockchain, but there are some general discussions. Such as, Mettler et al. [5] mainly proposed the possibility to prevent counterfeit medicine in the drug industry using blockchain. Kurki [6] discussed the advantages and instructions for utilizing blockchain within the drug supply chain. Bocek et al. [4] had developed a prototype of Ethereum smart contract based drug supply chain traceability system [7], without explaining the specific design of the workflow. Author in [1] proposed a novel product ownership management system (POMS) of Radio frequency identification (RFID)-attached products for anti counterfeits that can be used in the post supply chain. Similarly, a food company uses RFID to detect hazards in their food supply chain [2]. Author in [3] proposed a hybrid P2P physical distribution (HP3D) framework that used a semi-public ledger and a private ledger blockchain to enhance the validity and security of the information being exchanged. On the above methods, none of them proposed the authentic and automatic verification of drug genuinity from manufacturing to the patient's hand. When we need to prevent counterfeit medicine in the supply chain, blockchain technology makes sure a static chain of transaction ledger, in individual drug levels, every step of the supply chain is tracked.

CHAPTER 3

BLOCKCHAIN TECHNOLOGY OVERVIEW

A blockchain is a decentralized and distributed digital ledger that records transactions across a network of computers in a secure, transparent, and tamper-resistant manner. It consists of a chain of blocks, each containing a list of transactions, and is maintained by a network of nodes.

3.1 KEY FEATURES OF BLOCKCHAIN

1.Decentralization

- Blockchain operates on a peer-to-peer network, eliminating the need for a central authority or intermediary. All participants (nodes) in the network have equal control and authority.
- Decentralization reduces the risk of a single point of failure, enhances security, and fosters trust among participants.

2.Distributed Ledger

- The ledger, containing a record of all transactions, is distributed across all nodes in the network. Each node has a copy of the entire blockchain.
- Distribution ensures that there is no single point of control, making the system resilient to attacks and providing redundancy.

3.Consensus Mechanism

- Nodes on the blockchain network must agree on the validity of transactions through a consensus mechanism. Common mechanisms include proof-of-work (used in Bitcoin) and proof-of-stake.
- Consensus mechanisms maintain the integrity of the blockchain by preventing malicious actors from manipulating transaction history.

4.Immutability

- Once a block is added to the blockchain, it is nearly impossible to alter or delete. Each block contains a unique identifier (hash) based on its content and the previous block's hash.
- Immutability ensures the permanence and integrity of transactions, providing a trustworthy record of events.

5.Transparency

- All participants in the blockchain network have access to the entire transaction history. The information in the blockchain is visible to all authorized users.
- Transparency builds trust among participants, as they can independently verify transactions and the state of the ledger.

6.Smart Contracts

- Self-executing contracts with coded terms and conditions. Smart contracts automatically execute actions when predefined conditions are met.
- Smart contracts automate and streamline processes, reducing the need for intermediaries and minimizing the risk of human error.

7.Cryptographic Security

- Cryptography is used to secure transactions and control access to the blockchain. Public and private keys are used to authenticate participants and ensure data confidentiality.
- Cryptographic techniques provide a high level of security, protecting the integrity and privacy of transactions.

CHAPTER 4

SYSTEM ANALYSIS

4.1 SCOPE

1.Product Authentication:

- The system will verify the authenticity of pharmaceutical products using blockchain technology.
- Verification methods may include QR code scanning, NFC, or an online portal.

2.Supply Chain Traceability:

- The system will provide end-to-end traceability of pharmaceutical products from manufacturing through distribution to end-users.
- Each transaction and movement within the supply chain will be recorded on the blockchain.

3. User Roles:

- The system will support multiple user roles, including manufacturers, distributors, regulatory bodies, and consumers.
- Each role will have specific permissions and access levels.

4. Smart Contracts:

- Smart contracts will be utilized for automating processes, such as product verification, recalls, and compliance reporting.

5. Recall Management:

- The system will facilitate efficient recall processes, enabling quick identification and isolation of affected product batches.

6 Compliance Reporting:

- Compliance reports will be generated and submitted to regulatory bodies to ensure adherence to industry standards.

7. Privacy Measures:

- The system will implement privacy measures to comply with data protection regulations.
- Sensitive data will be handled securely, and access controls will be enforced.

4.1 EXISTING AUTHENTICATION SYSTEM

RFID (Radio-Frequency Identification):RFID technology employs wireless communication and radio-frequency signals to identify and track objects. In the context of combating counterfeit medicines, RFID tags are embedded in the packaging of pharmaceutical products. These tags contain electronically stored information that can be read remotely using RFID readers. The technology enables real-time tracking and authentication throughout the supply chain.

4.1.1 ADVANTAGES OF RFID (RADIO-FREQUENCY IDENTIFICATION)

- Real-Time Tracking
- Automation and Efficiency
- Enhanced Traceability
- Accuracy in Data Collection

4.1.2 DISADVANTAGES OF RFID

- High Costs
- Interception and Disruption
- Limited Range
- Data Privacy Concerns

4.2 PROPOSED SYSTEM

The proposed system is a comprehensive blockchain-based authentication solution designed to effectively combat the global issue of counterfeit medicines within the pharmaceutical supply chain. Leveraging the decentralized and tamper-resistant nature of blockchain technology, the system aims to provide a secure and transparent framework for verifying the authenticity of pharmaceutical products from production through distribution to end-users.

4.2.1 ADVANTAGES OF PROPOSED SYSTEM

- High Security
- Real-Time Visibility
- Trust and Transparency
- Reduced Counterfeiting
- Improved Recall Process
- Global Standardization

4.2.2 DISADVANTAGES OF PROPOSED SYSTEM

- Complexity and Learning Curve
- High Initial Costs
- Scalability Issues
- Energy Consumption

4.3 SYSTEM REQUIREMEMTS

4.3.1 FUNCTIONAL REQUIREMENTS:

1. User Authentication and Authorization:

- Define user roles (manufacturers, distributors, regulators, consumers).
- Implement secure authentication mechanisms.
- Specify access controls for different user roles.

2. Product Registration:

- Enable manufacturers to register products on the blockchain.
- Capture essential product information (e.g., batch number, manufacturing date, expiration date).

3. Transaction Logging:

- Record all transactions related to the movement of drugs through the supply chain.

- Include details such as timestamp, location, and parties involved.

4. Traceability and Transparency:

- Enable traceability of drugs from manufacturing to the point of sale.
- Provide a transparent view of the supply chain to authorized stakeholders.

5 Smart Contracts:

- Implement smart contracts to automate processes (e.g., product verification, recalls).
- Specify conditions triggering smart contract execution.

6 Verification Interface:

- Develop a user-friendly interface for stakeholders to verify product authenticity.
- Support various verification methods (e.g., QR codes, NFC, online portal).

7 Recall Management:

- Facilitate efficient recall processes in case of quality issues or emergencies.
- Specify protocols for identifying and recalling affected batches.

8 Compliance Reporting:

- Generate compliance reports for regulatory bodies.
- Ensure adherence to industry standards and regulations.

4.3.2 NON-FUNCTIONAL REQUIREMENTS:

1. Security:

- Implement encryption for data in transit and at rest.
- Ensure secure key management and access controls.
- Regular security audits and vulnerability assessments.

2. Performance:

- Define performance benchmarks for transaction processing.
- Ensure the system can handle a scalable number of transactions.
- Optimize for low-latency verification.

3. Scalability:

- Design the system to scale horizontally as the number of users and transactions increases.
- Plan for future growth in the number of pharmaceutical products.

4. Interoperability:

- Ensure compatibility with existing pharmaceutical systems.
- Support industry standards for data exchange.

5. Privacy:

- Comply with data protection regulations (e.g., GDPR).
- Anonymize or pseudonymize sensitive data where applicable.

6. Reliability:

- Implement mechanisms for data backup and disaster recovery.
- Ensure high system availability and minimal downtime.

7. Usability:

- Design a user-friendly interface for all stakeholders.
- Provide training and documentation for system users.

8. Legal and Ethical Considerations:

- Adhere to legal requirements related to data storage and sharing.

Consider ethical implications, such as consent for data sharing

4.3.3 HARDWARE REQUIREMENT

- CPU: Intel core I3 processors
- Hard disk Space: 250 Gb
- Display: 15” colour monitor
- RAM: 4Gb or above
- Storage: 512 Gb and above

4.3.2 SOFTWARE REQUIREMENTS

- Operating System: Windows 10 or above
- IDE: VS code, Android Studio, Ethereum
- Front End: Html,Css,JavaScript
- Back End: Node.js, MYSQL

CHAPTER 5

SYSTEM DESIGN

5.1 SYSTEM TOOLS

The various system tools that have been used in developing the front end of the project is being discussed in this chapter.

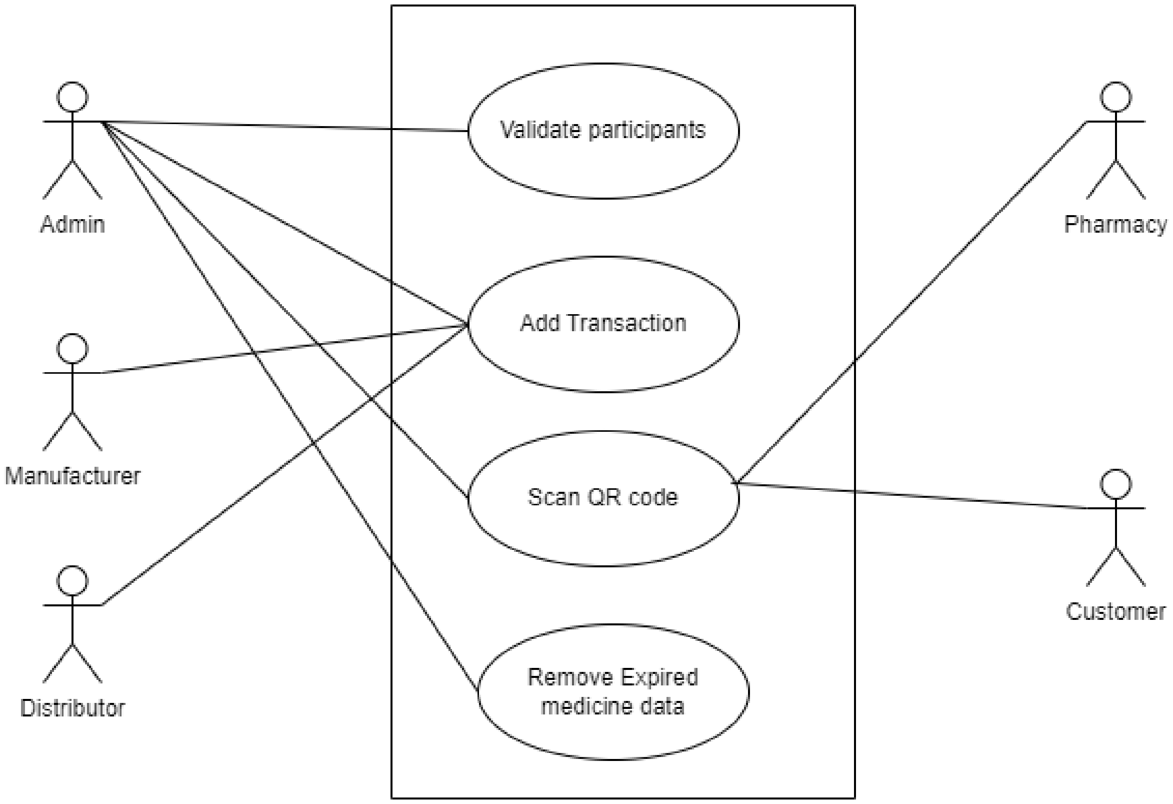
5.1.1 FRONT END

HTML (Hyper Text Markup Language):HTML is a syntax used to format a text document on the web.

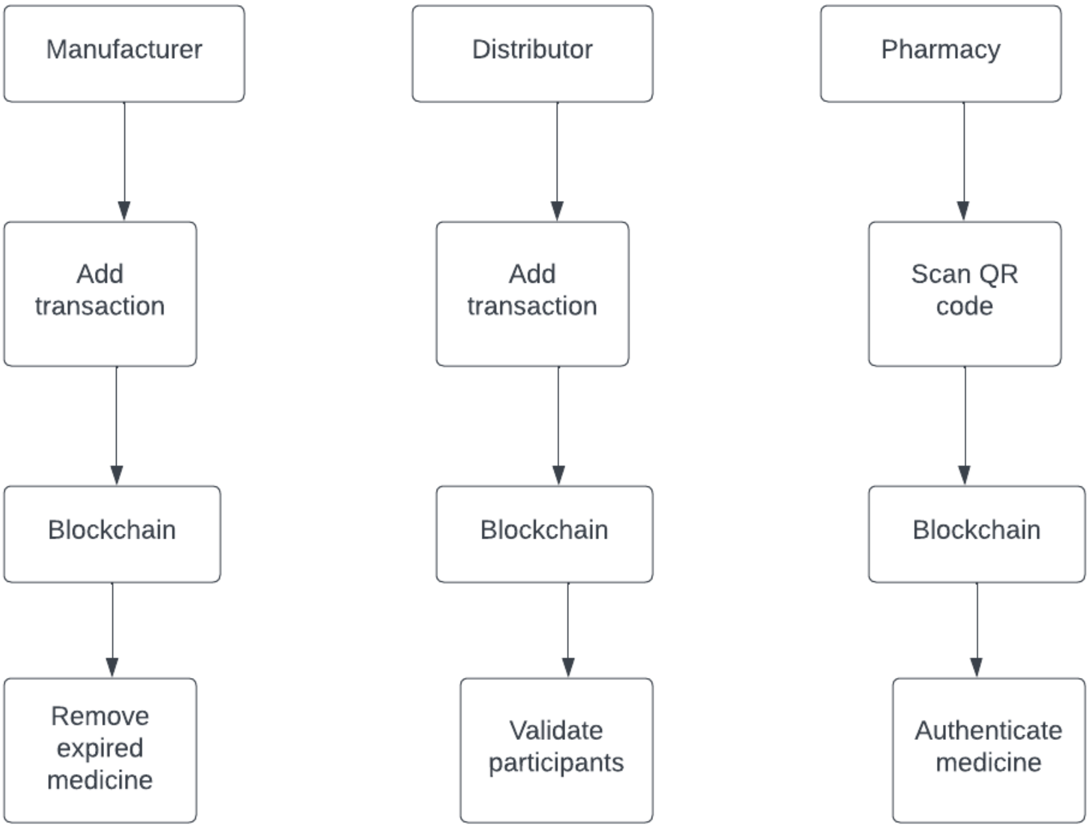
CSS (Cascading Style Sheets):CSS is a style sheet language used for describing the look and formatting of a document written in a markup language.

JAVASCRIPT: JavaScript is a programming language that adds interactivity and dynamic behavior to web pages. It can be used to manipulate the HTML and CSS of a page.

5.2 USE CASE DIAGRAM



5.3 DATAFLOW DIAGRAM



CHAPTER 6

MODULE DESCRIPTION

6.1 USER MODULE

The User Module in a Blockchain Medicine Authentication System is responsible for managing user-related functionalities, including user authentication, authorization, and access control. It ensures that different stakeholders, such as manufacturers, distributors, pharmacies, regulatory authorities, and consumers, interact with the system securely and have access to the appropriate features. Functions of user module:

- User Authentication: Verifies the identity of users attempting to access the system. Implements secure authentication mechanisms, such as username/password, multi-factor authentication, or biometrics. Ensures that only authorized individuals have access to the system.
- User Authorization: Manages user roles, permissions, and access control.Defines different user roles based on the stakeholder category (e.g., manufacturer, distributor, regulatory authority).Assigns specific permissions and access levels to each user role.Controls access to system features and data based on user roles.
- User Registration and Management: Handles the registration of new users and the management of user accounts.Allows new users to register by providing necessary information and credentials.Verifies user information and approval processes, especially for manufacturers and regulatory authorities.
- Profile Management: Enables users to view and manage their profiles.Allows users to update personal information, contact details, and preferences.
- Access Logs and Auditing: Records user activities and access logs for auditing purposes.
- Password Security: Ensures the security of user passwords.

Sub modules in User module:

1. Admin
2. Manufacturer
3. Distributor
4. Pharmacy
5. Customer

6.1.1 ADMIN

The Admin Module in a Blockchain Medicine Authentication System is designed to provide administrative functionalities for system administrators or superusers. These administrators have elevated privileges and are responsible for managing and overseeing the overall operation of the system.

- User Management: Admins have control over user accounts and their permissions.
- System Configuration: Admins can configure system settings and parameters.
- Alerts and Notifications: Admins receive alerts and notifications related to system events.
- Blockchain Management: Admins have control over blockchain-related functions.
- Data Analytics and Reporting: Admins can access analytics and reporting tools.
- System Health Monitoring: Admins monitor the overall health and performance of the system.
- System Upgrades and Maintenance: Admins manage system updates, patches, and maintenance.
- Security Oversight: Admins oversee the security posture of the entire system.

6.1.2 MANUFACTURER

The Manufacturer Module in a Blockchain Medicine Authentication System is dedicated to functionalities related to the production and authentication of medicines. This module is designed to facilitate the activities of pharmaceutical manufacturers, ensuring the generation of unique identifiers, recording production data on the blockchain, and contributing to the overall integrity of the supply chain.

- Generate Unique Identifiers: Enables manufacturers to create unique identifiers for each batch of medicines.
- Record Production Data on Blockchain: Records essential production data on the blockchain ledger.
- Product Traceability: Provides traceability features for manufactured products.
- Integration with Manufacturing Systems: Integrates seamlessly with existing manufacturing systems.
- Quality Control and Assurance: Incorporates features for quality control and assurance.
- Alerts for Counterfeit Detection: Implements alerts for detecting potential counterfeit medicines.
- Production Analytics: Provides analytics tools for production-related insights.
- Product Recall Initiatives: Facilitates the initiation and management of product recall processes.
- Security Measures: Implements security measures to protect production data and identifiers.

6.1.3 DISTRIBUTOR

The Distributor Module in a Blockchain Medicine Authentication System is dedicated to functionalities related to the distribution and authentication of medicines. This module is designed to facilitate the activities of pharmaceutical distributors, ensuring the secure movement of medicines through the supply chain, updating distribution data on the blockchain, and contributing to the overall traceability of pharmaceutical products. Below is a detailed description of the Distributor Module:

- Receive and Verify Products: Enables distributors to receive and verify products from manufacturers.
- Update Distribution Data on Blockchain: Records essential distribution data on the blockchain ledger.
- Integration with Logistics Systems: Integrates seamlessly with existing logistics and warehouse management systems.
- Product Traceability: Provides traceability features for distributed products.
- Quality Control at Distribution Points: Incorporates features for quality control at distribution points.

- Alerts for Anomalies: Implements alerts for detecting potential anomalies or issues in distribution.
- Distribution Analytics: Provides analytics tools for distribution-related insights.

6.1.4 PHARMACY

The Pharmacy Module in a Blockchain Medicine Authentication System is dedicated to functionalities related to the authentication and dispensing of medicines at pharmacy or retail points. This module is designed to facilitate the activities of pharmacies, ensuring the secure verification of medicines, updating authentication data on the blockchain, and providing consumers with accurate information about the products they purchase. Below is a detailed description of the Pharmacy Module:

- Medicine Authentication: Enables pharmacies to authenticate medicines using unique identifiers.
- Consumer Information Access:Provides access to detailed product information for consumers.
- Integration with Point-of-Sale (POS) Systems:Integrates seamlessly with pharmacy Point-of-Sale systems.
- Alerts for Counterfeit Detection: Implements alerts for detecting potential counterfeit medicines.
- Product Recall Notifications: Receives and handles notifications related to product recalls.
- Transaction Logging:Logs transaction data related to the dispensing of medicines.

6.1.5 CUSTOMER

The Customer (Consumer) Module in a Blockchain Medicine Authentication System is designed to empower end-users with tools and information for verifying the authenticity of medicines before purchase. This module ensures that consumers have easy access to product details, including the origin, manufacturing history, and distribution journey, promoting transparency and trust in the pharmaceutical supply chain. Below is a detailed description of the Customer Module:

- Medicine Authentication: Empowers consumers to authenticate medicines before purchase.

- Product Information Access: Offers consumers access to detailed product information.
- Mobile App or Web Interface: Provides a dedicated mobile app or web interface for consumers.
- Alerts and Notifications: Sends alerts to consumers regarding authentication results and relevant information.
- Transaction History: Allows consumers to view the transaction history of authenticated medicines.
- Privacy and Security Measures: Ensures the privacy and security of consumer data.

6.2 KEY GENERATOR MODULE

The Key Generator Module in a Blockchain Medicine Authentication System is responsible for the generation of cryptographic keys used in securing transactions, ensuring data integrity, and providing authentication within the blockchain network. Cryptographic keys play a vital role in the security of blockchain systems, including the authentication and validation of data. Below is a detailed description of the Key Generator Module:

- Public and Private Key Pair Generation: Generates pairs of cryptographic keys for secure communication. Utilizes cryptographic algorithms to create a unique public key and its corresponding private key. Ensures the integrity of the key pair generation process. Employs industry-standard algorithms like RSA or Elliptic Curve Cryptography (ECC).
- Key Storage and Management:Manages the secure storage of generated keys.Safely stores private keys in a secure key vault or hardware security module (HSM).Implements access controls and encryption to protect key storage.Facilitates key retrieval for authorized processes requiring cryptographic operations.
- Key Rotation:Implements key rotation mechanisms for enhanced security.Periodically generates new key pairs to replace existing ones.Ensures a smooth transition from old to new keys to avoid service disruptions.Mitigates the impact of potential key compromise over time.
- Key Distribution: Facilitates the distribution of public keys to relevant parties.Shares public keys with network participants, such as manufacturers, distributors, pharmacies, and regulatory authorities.Uses secure channels or protocols for key exchange to

prevent interception or tampering.Enables participants to verify the authenticity of received public keys.

- Key Revocation: Implements mechanisms for revoking compromised or obsolete keys.Detects compromised keys or those no longer in use.Flags revoked keys to prevent their inadvertent use. Updates relevant participants with information about revoked keys.
- Cryptographic Signatures: Utilizes keys for creating and verifying cryptographic signatures.Signs transactions, data, or smart contracts with the private key to prove authenticity.Verifies signatures using the corresponding public key.Ensures the integrity and authenticity of information recorded on the blockchain.

6.3 VALIDATION MODULE

The Validation Module in a Blockchain Medicine Authentication System is responsible for verifying the authenticity and integrity of data recorded on the blockchain. This module ensures that the information stored in the decentralized ledger is accurate, has not been tampered with, and complies with predefined rules and conditions. Below is a detailed description of the Validation Module:

- Data Integrity Verification: Verifies the integrity of data recorded on the blockchain.Checks the cryptographic hashes or signatures associated with transactions to ensure data integrity.Verifies that data has not been altered or tampered with since its original recording.
- Smart Contract Execution Verification: Ensures the correct execution of smart contracts.Validates that smart contracts have been executed according to predefined rules and conditions. Verifies the outcomes of smart contract transactions against expected results.
- Consensus Mechanism Validation: Validates the consensus mechanism used by the blockchain network. Verifies that the consensus algorithm employed by the network is functioning correctly.
- Public Key Verification: Validates the authenticity of public keys used in transactions. Verifies that public keys associated with transactions are valid and have not been compromised. Ensures that public keys used for cryptographic signatures are legitimate and have the correct ownership.

- Timestamp Verification:Validates the timestamps of transactions. Verifies that transactions are timestamped accurately and consistently.
- Authentication Data Verification:Verifies the authenticity of medicines and associated authentication data.Validates the unique identifiers, cryptographic signatures, or QR codes associated with medicine authentication.

6.4 TRANSACTION LOGIC MODULE

The Transaction Logic Module in a Blockchain Medicine Authentication System defines the rules and logic governing the execution of transactions within the blockchain network. This module plays a crucial role in ensuring that transactions are valid, secure, and adhere to the business logic encoded in smart contracts. Below is a detailed description of the Transaction Logic Module:

- Smart Contract Execution: Orchestrates the execution of transactions based on smart contract logic.Interprets and enforces the rules embedded in smart contracts. Facilitates the execution of business processes encoded in smart contracts, such as authentication, validation, and distribution.
- Transaction Authorization: Ensures that transactions are authorized by the relevant parties. Validates the authorization of participants involved in a transaction.
- Transaction Ordering: Defines the order in which transactions are processed. Manages the sequencing of transactions to maintain a consistent and agreed-upon order. Utilizes timestamps or other consensus-driven mechanisms to establish transaction order.
- Data Input Validation:Validates the inputs provided in transactions.Verifies the format, integrity, and authenticity of data submitted with transactions.
- Consensus Mechanism Integration:Integrates with the chosen consensus mechanism for transaction validation. Ensures that transactions are accepted or rejected based on the consensus of participating nodes.

6.5 BLOCKCHAIN MODULE

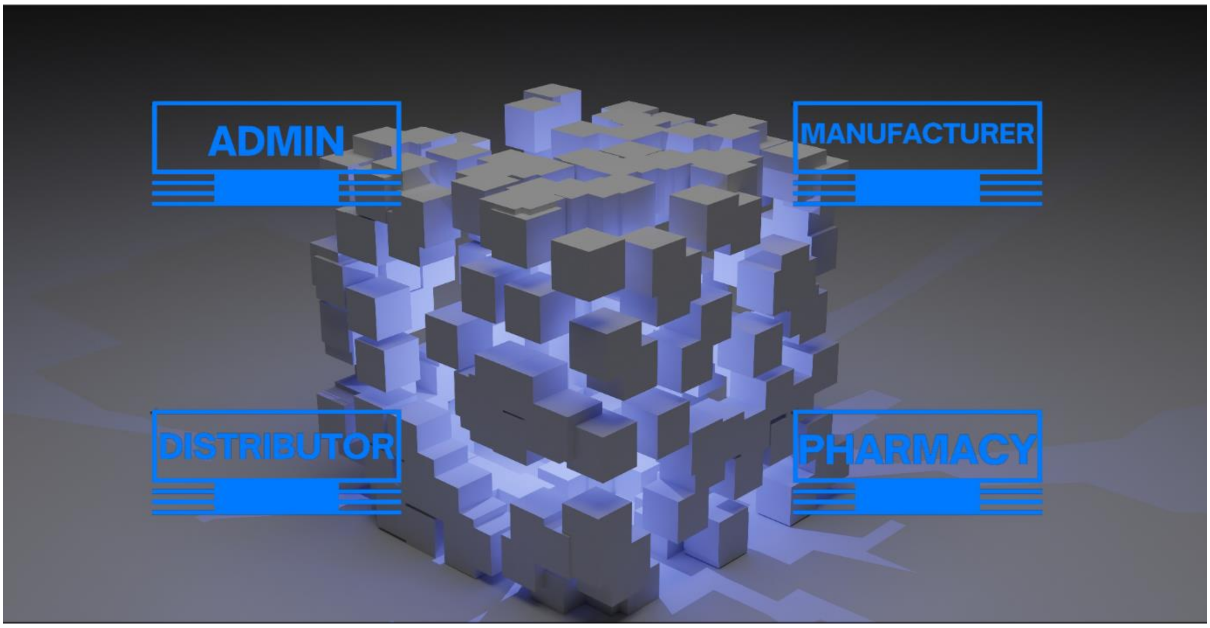
The Blockchain Module is a core component of a Blockchain Medicine Authentication System, responsible for managing the decentralized ledger, securing transactions, and ensuring data integrity across the network. This module incorporates the fundamental principles of blockchain technology, including distributed ledger technology, consensus mechanisms, and cryptographic security. Below is a detailed description of the Blockchain Module:

- Decentralized Ledger Management: Manages the decentralized ledger that records all transactions. Maintains an immutable and transparent record of all transactions within the blockchain.Distributes copies of the ledger across participating nodes in the network.
- Consensus Mechanism Implementation: Implements a consensus mechanism for transaction validation.Chooses and integrates a consensus algorithm (e.g., Proof of Work, Proof of Stake) that aligns with the goals of the authentication system.
- Cryptographic Security: Utilizes cryptographic techniques to secure transactions and data. Implements cryptographic hashing for transaction data integrity.
- Smart Contracts Integration: Integrates smart contracts to automate and enforce business rules. Facilitates the creation and execution of smart contracts that define the logic of transactions.
- Block Creation and Mining: Manages the creation of blocks and the mining process in Proof of Work systems.Gathers transactions into blocks for inclusion in the blockchain. Facilitates the mining process to solve cryptographic puzzles and add blocks to the chain.

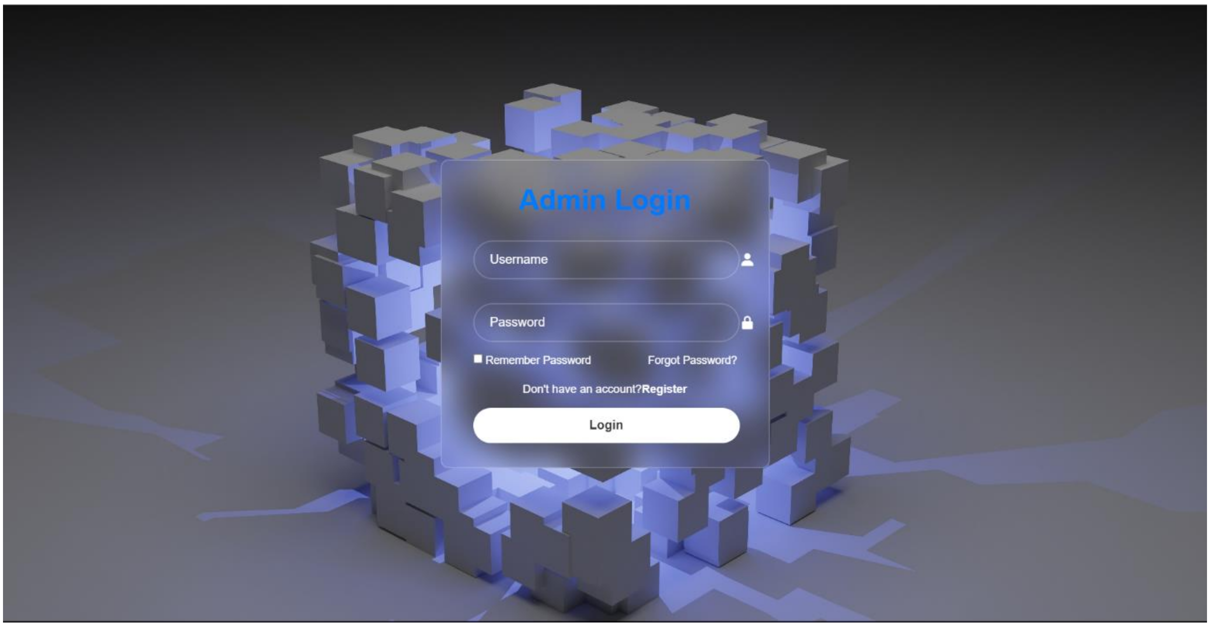
CHAPTER 7

SCREENSHOTS

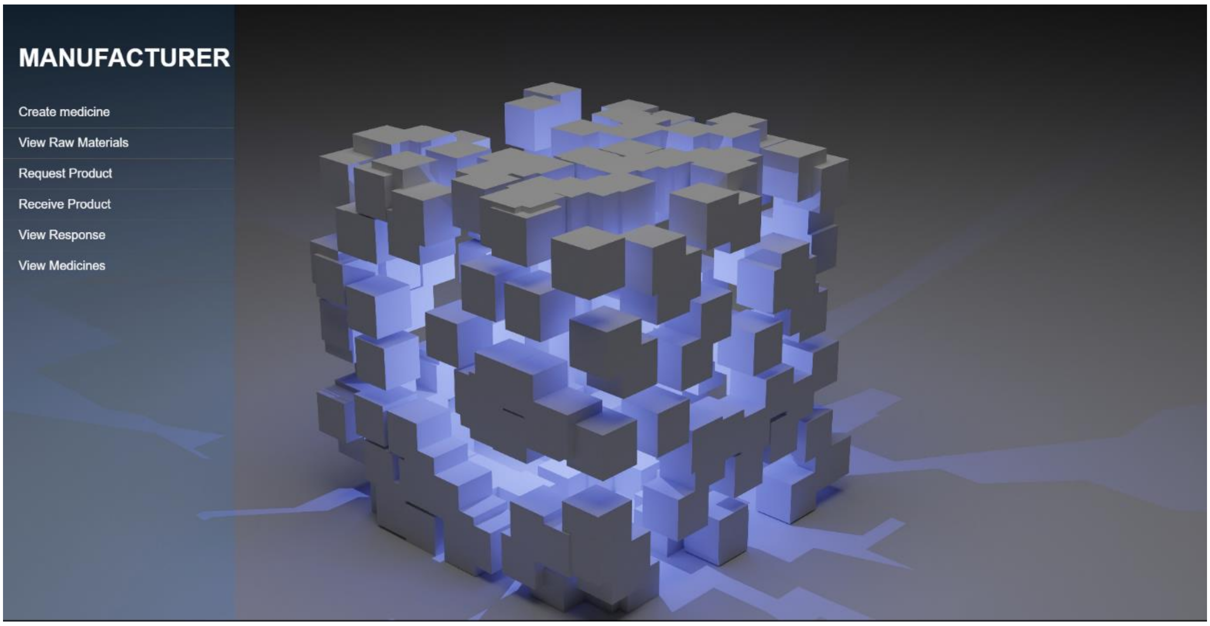
HOME PAGE



ADMIN LOGIN



MANUFATURE LOGIN



MANUFACTURER

Create medicine

View Raw Materials

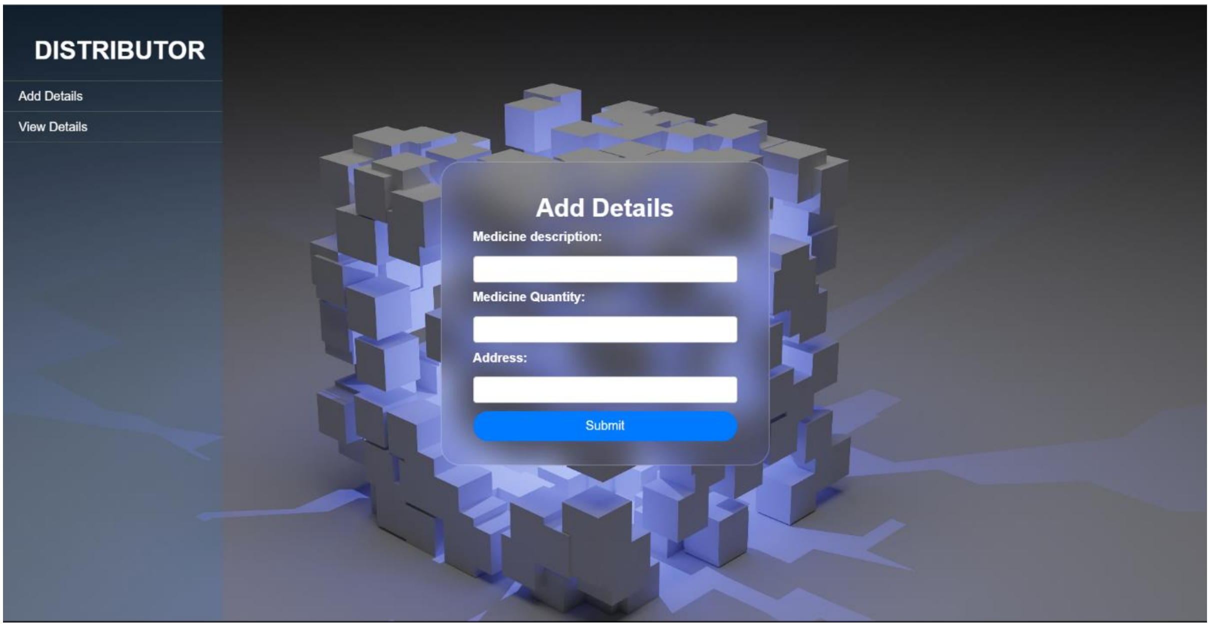
Request Product

Receive Product

View Response

View Medicines

DISTRIBUTOR



DISTRIBUTOR

Add Details

View Details

Add Details

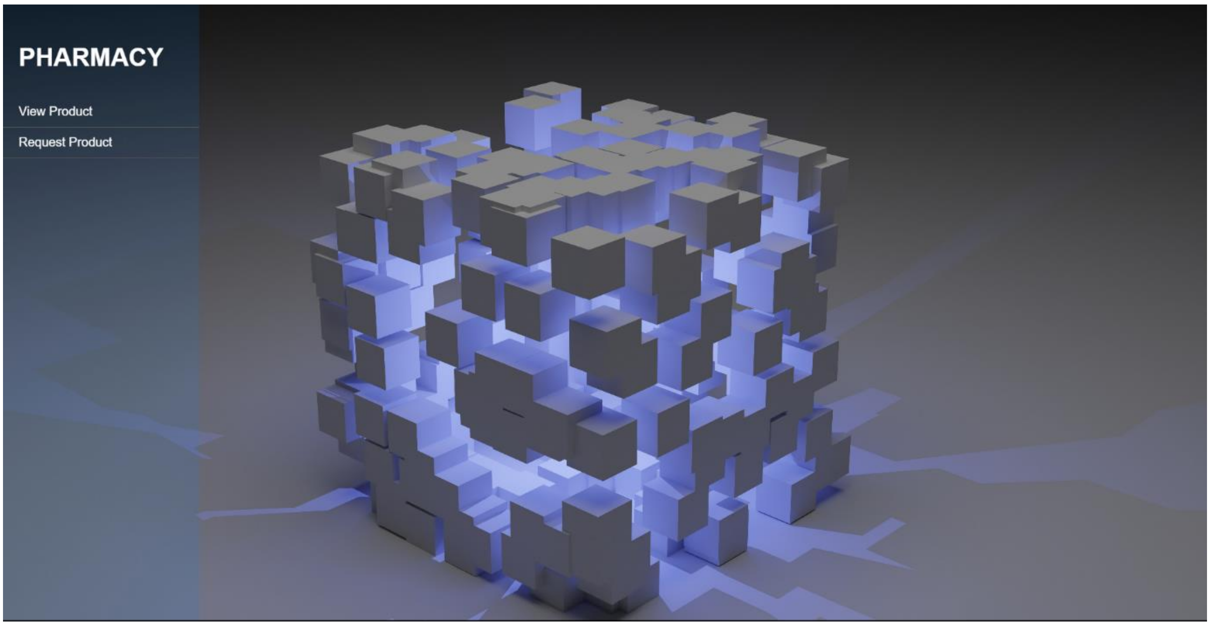
Medicine description:

Medicine Quantity:

Address:

Submit

PHARMACY



CHAPTER 8

CONCLUSION

In this paper, we develop a practical blockchain based secure infrastructure for the medical supply chain among authorized participants on the traditional medicine supply chain. Our application stands on blockchain security to identify the drugs uniquely and individually therefore, a falsified medicine or fraud distributor can be identified easily without any complexity. The prototype reconstructs the whole traditional medicine supply chain service architecture that can provide medicine security as well as authenticity of the manufacturer. It also introduce the current location of every transaction that makes the system more reliable. Optimization of blockchain data storage by removing expired medicine data makes the chain stable and acceptable.