FarmaTech

Functional Specification

Faizan Ali Shah & Abhjit Mahal
Student IDs: 21319001 & 21375106

Date Completed: 22/11/2024

Table of Contents

1. Introduction

1.1) Overview

FarmaTech is a blockchain-based web application designed to combat counterfeit medicines by ensuring supply chain transparency and security. It enables drug manufacturers to register their products and generate a unique encrypted QR code for each medicine, which acts as a digital certificate of authenticity.

As medicines progress through the supply chain, authorised distributors, including government bodies like the Health Service Executive (HSE) and Health Products Regulatory Authority (HPRA), can scan the QR code to verify its integrity and update the blockchain with relevant data. This process immediately flags any tampering or discrepancies.

End users such as hospitals, pharmacies, and consumers can scan the QR code to verify the medicine's legitimacy and check for any alerts during its supply chain journey. FarmaTech enhances trust and safety in the pharmaceutical supply chain by offering real-time, secure product verification.

.

1.2) Business Context

FarmaTech is designed to be deployed within the pharmaceutical industry, where the need for secure and transparent supply chain solutions is critical due to the increasing threat of counterfeit medicines. Pharmaceutical companies, healthcare organisations, and regulatory bodies like the Health Service Executive (HSE) and Health Products Regulatory Authority (HPRA) are key stakeholders in this ecosystem. These organisations are focused on ensuring the safety, quality, and authenticity of medicines delivered to consumers.

FarmaTech addresses this by providing a blockchain-based solution that aligns with regulatory requirements and industry standards for supply chain traceability. The system is intended to be adopted by drug manufacturers, distributors, hospitals, and pharmacies to enhance trust, safeguard public health, and ensure compliance with global regulations for pharmaceutical product verification.

1.3) Glossary

Blockchain	A decentralised digital ledger that securely records transactions, ensuring transparency and preventing tampering in FarmaTech's supply chain.

QR Code	A scannable barcode that stores a unique key for each medicine, enabling verification throughout the supply chain.
Hyperledger Fabric	A permissioned blockchain framework used for secure and scalable medicine tracking.
Fabric SDK	A toolkit that enables interaction between FarmaTech's backend and the blockchain for updating and retrieving data.
Smart Contract **(Chaincode)**	Self-executing code stored on the blockchain that governs how transactions are processed.
immutable	A characteristic of blockchain where recorded data cannot be altered, ensuring transparency and security
Instascan.js	A JavaScript library used for scanning QR codes via camera in the FarmaTech application
Geolocation API	A tool used in FarmaTech to track the physical location of medicine scans for supply chain verification.
Drug Manufacturer	An authorised entity that registers medicines and generates QR codes within FarmaTech.
Distributor	Authorised personnel, including government bodies, who verify and update medicine status in the blockchain.
End User	Hospitals, pharmacies, or consumers who scan QR codes to verify medicine authenticity.
Tampering	Unauthorised interference with a medicine that may compromise its safety, flagged within FarmaTech.
CounterFeit Medicine	Fake or unauthorised medicines, which FarmaTech identifies by tracking the supply chain.

2. General Description

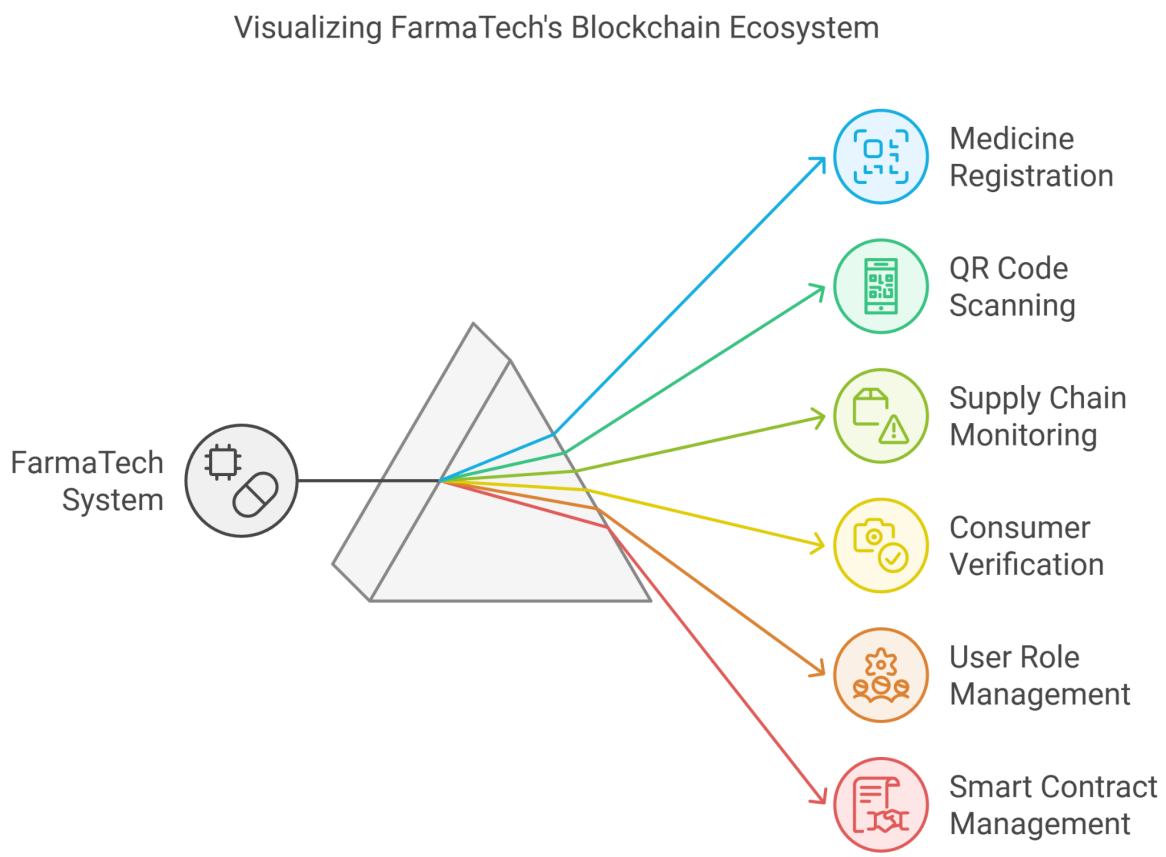

Fig 1: Visualising FarmaTech's Blockchain Ecosystem

2.1 Product / System Functions

Medicine Registration: Drug manufacturers register products and generate unique encrypted QR codes, capturing essential details like name, manufacturing date, and expiration date.

Secure QR Code Scanning: Authorised personnel scan QR codes to verify medicine integrity and update the blockchain with status information.

Supply Chain Monitoring: Tracks medicine conditions and allows users to flag issues such as broken seals or temperature deviations.

Consumer Verification: End users scan QR codes to confirm legitimacy and receive alerts for expiration or counterfeiting.

Detailed Medicine Information: Consumers access comprehensive information about the medicines they use, including manufacturing details and any issues flagged.

Historical Data Access: Provides logs of each medicine's journey for enhanced transparency.

User Role Management: Supports multiple user roles with defined access levels for security.

Blockchain Network Governance: Establishes security frameworks for participants.

Smart Contract Management: Automates processes, such as alerts for expired medicines also shown in fig 1.

Audit Trail: Records all interactions for accountability and thorough investigations.

2.2 User Characteristics and Objectives

FarmaTech serves users, from drug manufacturers to end consumers. Each group has specific needs related to securing the pharmaceutical supply chain, requiring a system that is user-friendly, secure, and transparent.

1. Drug Manufacturers

Expertise: High experience with enterprise systems.

Objectives:

a. Register medicines and generate encrypted QR codes.
b. Ensure regulatory compliance and prevent counterfeit medicines.

Wish List:

c. Automated QR code generation and integration with existing systems.
d. Real-time monitoring of supply chain data.

2. Distributors (Including HSE, HPRA)

Expertise: Familiar with supply chain management and regulatory standards.

Objectives:

a. Verify and update medicine status via QR code scanning.
b. Ensure compliance and prevent counterfeit distribution.

Wish List:

c. Geolocation tracking and real-time status updates.
d. Tools for reporting and auditing.

3. End Users (Hospitals, Pharmacies, Consumers)

Expertise: Minimal technical experience, requiring ease of use.

Objectives:

a. Verify medicine authenticity through QR code scanning.
b. Access detailed information and receive alerts for tampering or expiration.

Wish List:

c. User-friendly mobile interface and instant notifications.
d. Access to supply chain history and issue alerts.

4. Regulatory Bodies (e.g., HSE, HPRA)

Expertise: High knowledge of regulatory and compliance standards.

Objectives:

a. Ensure compliance and monitor the supply chain.
b. Investigate tampering or counterfeit incidents.

Wish List:

a. Immutable audit trails and real-time alerts.
b. Tools for conducting compliance audits and reviews.

2.3 Operational Scenarios

Scenario 1: Medicine Registration by a Drug Manufacturer

Actors: Drug Manufacturer
Preconditions: The drug manufacturer is an authorised user with system access.
Steps:

1. The manufacturer logs into the FarmaTech portal.
2. They navigate to the *Medicine Registration* module and enter the required details: medicine name, batch number, manufacturing date, and expiration date.
3. The system generates a unique encrypted QR code using the blockchain and associates it with the registered medicine.
4. The QR code is printed and affixed to each medicine unit.
5. The blockchain is updated with the registration information, creating an immutable record.

Expected Outcome: The medicine is successfully registered, and the QR code is ready for use in the supply chain.

Scenario 2: Verifying Medicine by a Distributor

Actors: Distributor (e.g., HSE, HPRA)
Preconditions: The distributor has access to a scanning device or mobile app with the FarmaTech system.
Steps:

1. The distributor scans the QR code on a medicine package using the *QR Code Scanning* module.
2. The system retrieves the medicine's details and current status from the blockchain.
3. The distributor verifies the integrity of the data and inspects the medicine for physical tampering or other issues.
4. If the medicine passes inspection, the distributor updates its status via the application.
5. The blockchain records the updated status, including geolocation data and timestamps.

Expected Outcome: The medicine's authenticity is confirmed, and its status is updated in the blockchain. Any tampering is immediately flagged if detected.

Scenario 3: Consumer Scans QR Code for Medicine Verification

Actors: End User (Consumer, Hospital, or Pharmacy)
Preconditions: The end user has a mobile device with the FarmaTech app installed.
Steps:

1. The user scans the QR code on a medicine package.
2. The app displays detailed information about the medicine, including its manufacturing date, expiration date, and supply chain history.
3. If the medicine has expired or is flagged for tampering, the app immediately alerts the user.
4. The user decides whether to use or reject the medicine based on the verification results.

Expected Outcome: The user confirms the medicine's legitimacy and receives alerts for any issues.

Scenario 4: Regulatory Body Investigates Tampering Incident

Actors: Regulatory Body (e.g HPRA, HSE)
Preconditions: A potential tampering or counterfeit issue has been flagged in the system.
Steps:

1. The regulatory body accesses the Audit Trail module within the FarmaTech system.
2. They locate the flagged medicine by searching for its QR code or batch number.
3. The system provides an immutable log of all transactions and interactions involving the medicine.
4. Investigators review the supply chain history, geolocation data, and time stamped events to identify where the tampering occurred.
5. Based on the findings, the regulatory body takes necessary actions, such as recalling the medicine or penalising the responsible party.

Expected Outcome: The source of the tampering is identified, and appropriate actions are initiated to safeguard public health.

Scenario 5: Smart Contract Automates Medicine Expiration Alerts

Actors: End User (Pharmacy, Hospital, Consumer)
Preconditions: The medicine's expiration date is near or has passed.
Steps:

1. The FarmaTech system runs a scheduled smart contract check for all registered medicines.
2. Medicines nearing their expiration dates trigger automated alerts.
3. End users receive notifications via the mobile app, advising them to avoid using expired medicines.
4. The blockchain is updated to record the notification event.

Expected Outcome: End users are informed about expired medicines, reducing health risks associated with their usage.

2.4 Constraints

1. Performance Requirements

1. Real-time QR code scanning capabilities
2. Response time within industry standard parameters
3. Efficient processing of blockchain transactions
4. Speed and Processing

2.5 Compliance Requirements

2.5.1 Pharmaceutical Regulations

1. Maintenance of immutable audit trails compliant with:
    a. Health and Safety Executive (HSE) standards
    b. Health Products Regulatory Authority (HPRA) requirements

3. Blockchain Infrastructure

3.1 Framework Specifications

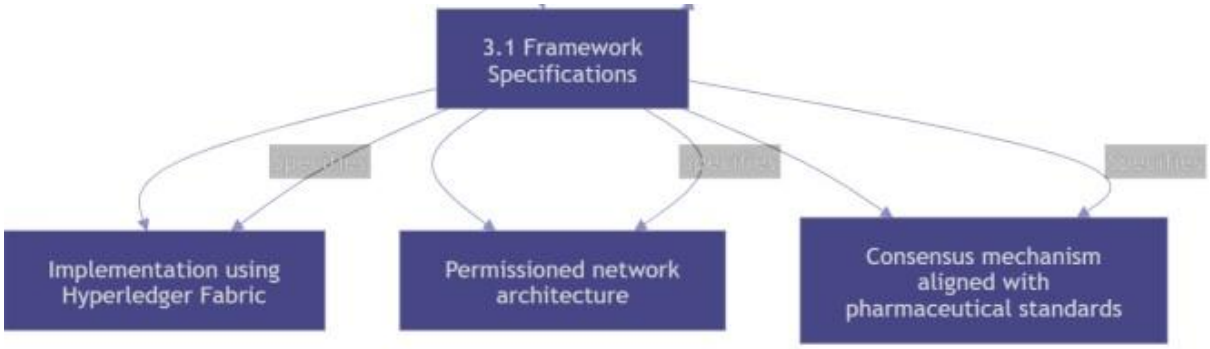

Fig 2: Framework Specification

- Fig 2 shows that only authorised participants can join and interact within the network.
- Provides enhanced security and privacy by restricting access to sensitive data.

3.2 Transaction Management

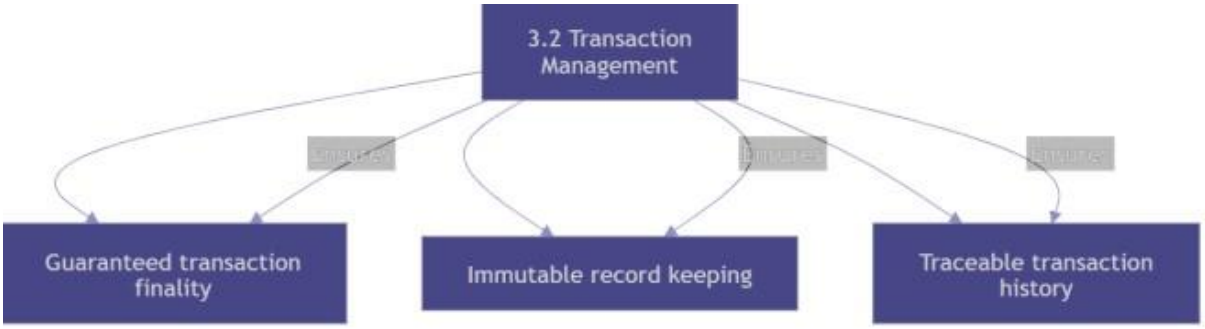

Fig 3: Transaction Management

- Ensures that once a transaction is completed, it cannot be reversed or altered.
- Leverages Hyperledger fabric blockchain technology to maintain an unchangeable ledger.
- Allows all transactions to be traced back through their entire lifecycle.
- Facilitates transparency and accountability within the system.

3. Functional Requirements

3.1. Medicine Registration

Priority Level: High

Description

The system shall provide functionality for drug manufacturers to register new medicines in the blockchain network.

Key Features

1. Product detail registration (name, batch number, manufacturing date, expiration date)
2. Automated unique QR code generation
3. Secure blockchain record creation

Technical Considerations

1. **Integration Requirements**
    a. Seamless integration
    b. Secure API endpoints for data input
    c. Real-time data validation
2. **Security Measures**
    a. Encrypted QR code generation

    b. Duplicate prevention mechanisms
    c. Tamper-proof storage systems

Dependencies

1. Blockchain infrastructure for secure data storage
2. QR code scanning module for verification
3. User authentication system

3.2. QR Code Scanning

Priority Level: High

Description

The system shall enable authorised users to perform QR code scanning for medicine verification and supply chain updates.

Key Features

1. Real-time authenticity verification
2. Supply chain status updates
3. Secure data retrieval

Technical Considerations

1. **Integration Requirements**
    a. Instascan.js implementation
    b. Camera access optimization
    c. Low-latency blockchain queries
2. **Performance Requirements**
    a. Sub-second scanning response
    b. Efficient data retrieval

Dependencies

1. Medicine registration system
2. Supply chain monitoring module
3. Real-time blockchain access

3.3. Supply Chain Monitoring

Priority Level: Medium

Description

The system shall provide comprehensive supply chain tracking and monitoring capabilities.

Key Features

1. Real-time location tracking
2. Status update management
3. Integrity verification

Technical Considerations

1. **Integration Requirements**
    a. Geolocation API implementation
2. **Data Management**
    a. Real-time data processing
    b. Secure storage protocols
    c. Historical data management

Dependencies

1. QR code scanning system
2. Blockchain infrastructure
3. Alert management system

3.4. Consumer Verification

Priority Level: High

Description

The system shall provide end-users with medicine verification capabilities and safety alerts.

Key Features

1. Simple QR code scanning
2. Clear authenticity verification
3. Comprehensive medicine information
4. Real-time alert notifications

Technical Considerations

1. **User Interface**
    a. Accessible design
2. **Integration Requirements**
    a. Push notification system
    b. Real-time blockchain queries

c. Alert management integration

Dependencies

1. QR scanning module
2. Supply chain monitoring system
3. Alert system

3.5. Immutable Audit Trail

Priority Level: High

Description

The system shall maintain a comprehensive, tamper-proof audit trail of all supply chain activities.

Key Features

1. Complete transaction logging
2. Immutable record keeping
3. Advanced search capabilities

Technical Considerations

1. **Blockchain Implementation**
    a. Immutable record architecture
    b. Efficient data retrieval
    c. Secure storage protocols
2. **Performance Requirements**
    a. Quick search response times
    b. Scalable storage solution
    c. Data integrity verification

Dependencies

1. Blockchain infrastructure
2. All functional modules

3.6. User Role Management

Priority Level: High

Description

The system shall implement role-based access control (RBAC) for security management.

Key Features

1. Granular permission control
2. Multi-factor authentication
3. Session management
4. Activity monitoring

Technical Considerations

1. **Security Implementation**
    a. RBAC framework
    b. MFA integration
    c. Session timeout mechanisms
2. **Administrative Features**
    a. Role management interface
    b. Permission assignment tools
    c. Audit logging

Dependencies

1. Authentication system
2. All functional modules

4. System Infrastructure

Fig 4: Blockchain Network Implementation

4.1 Hardware Requirements

1. Deployment flexibility:
    a. Cloud-based implementation
    b. On-premises server deployment
    c. Hybrid deployment options

4.2 Device Compatibility

1. Cross-platform support for:
    a. Smartphones (iOS/Android)

b. Tablets
c. Desktop computers
d. Web browsers

4.3 Integration Requirements

5.1 Geographical Considerations

1. Support for regional deployment limitations
2. Compliance with local data regulations
3. Geolocation service integration

4.4 Security Framework

4.4.1 Access Control

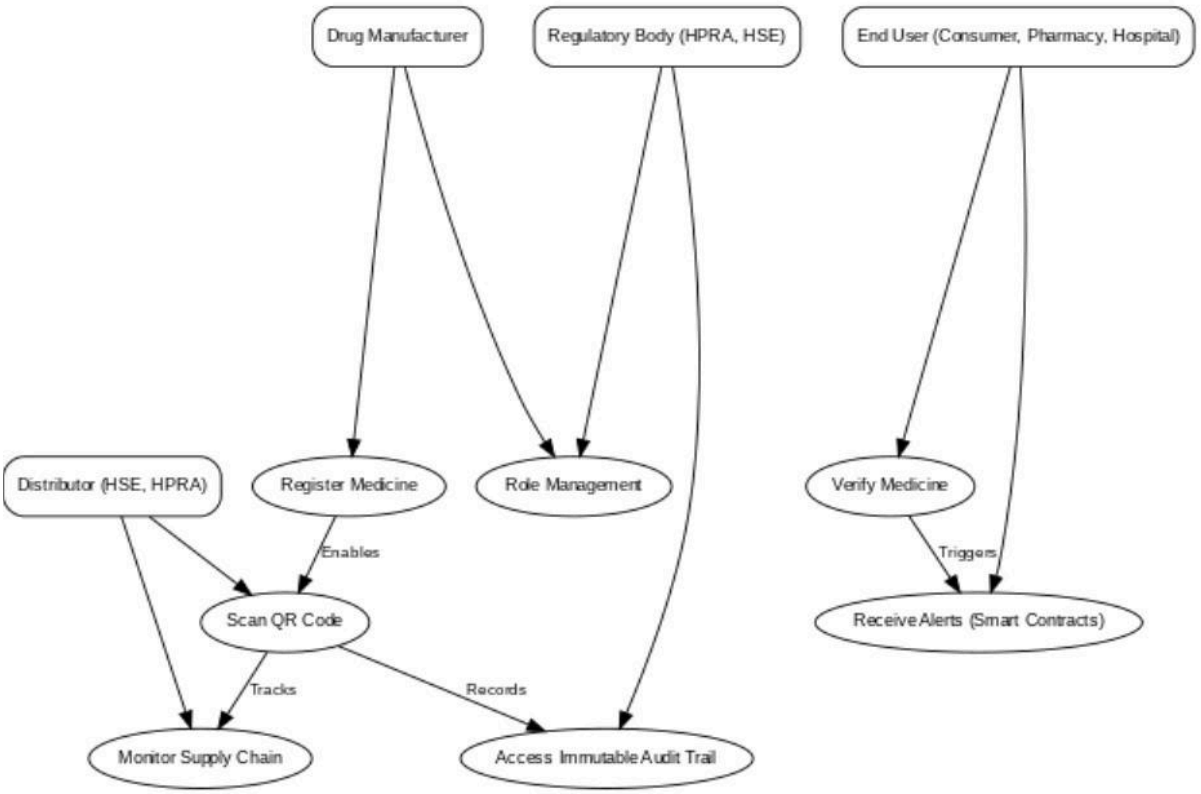

Fig 5: User Access Control Chart

1. Fig 5 describes role-based access control
2. Granular permission management
3. User activity monitoring and logging

4.4.2 Authentication Protocols

1. Multi-factor authentication implementation

2. Secure login procedures
3. Secure QR codes
4. Session management and timeout policies

4.5 System Architecture

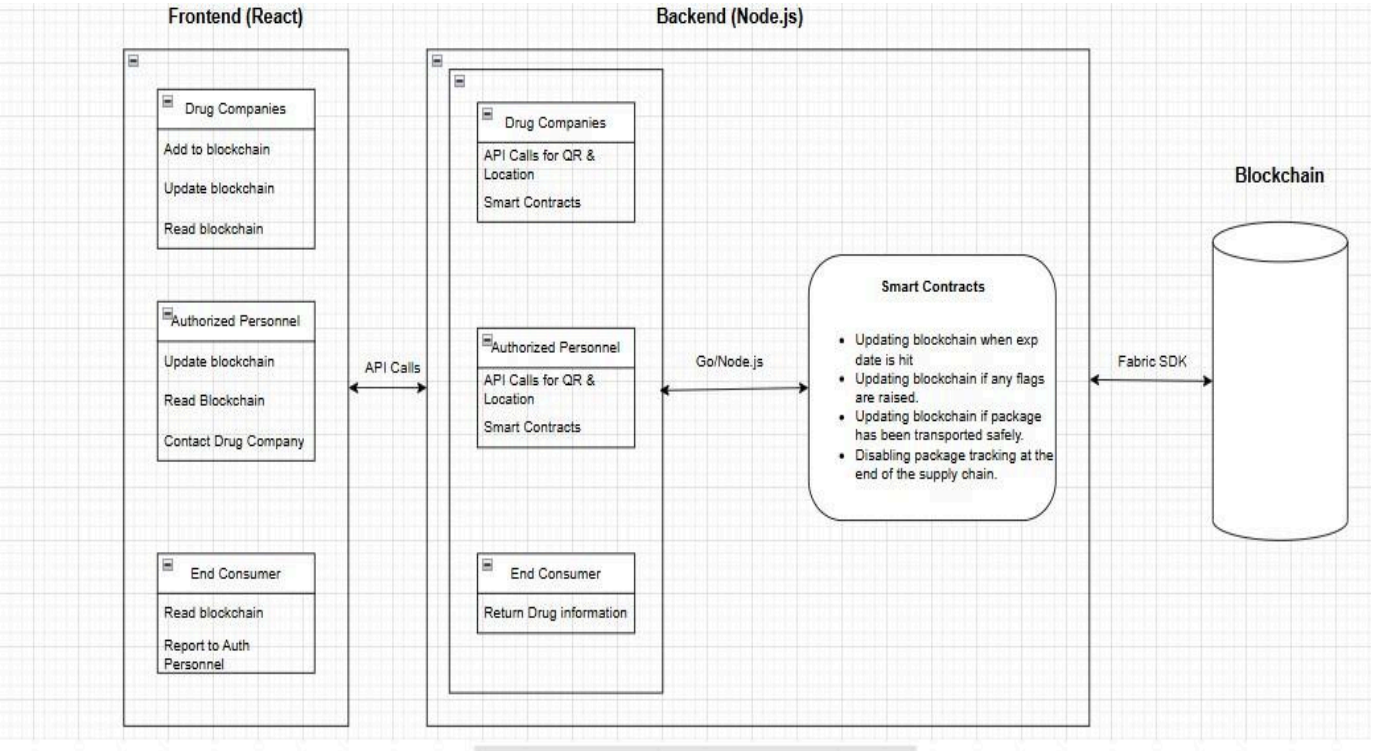

Fig 6: Representation of ou system architecture

4.5.1 User Interface Layer

This layer (frontend layer in fig 6) serves as the entry point for different users interacting with the system. It contains the following modules:

- **Consumer Verification Module**: Accessible to end-users (pharmacies, hospitals, or consumers) to verify the authenticity of drugs by scanning the QR code on products. It displays product details stored on the blockchain, including drug name, manufacturing batch number, expiry dates, and supply chain history.
- **Supply Chain Monitoring Module**: Used by distributors to update and track the movement of drugs in the supply chain. The interface allows distributors to scan QR codes, update the status of the drugs, and monitor their journey through the distribution network.
- **Admin/Manufacturer Interface**: This allows drug manufacturers to add new medicines to the system, registering them along with detailed product information that gets added to the blockchain.

4.5.2 Blockchain Layer

This is the core of the FarmaTech system, where all transaction data and supply chain details are securely stored in an immutable, decentralised manner.

- **Blockchain Network**: FarmaTech utilises a blockchain Hyperledger Fabric to record all product registrations, updates, and transactions. Data on the blockchain is accessible only to users with proper permissions. It ensures that all product details, movement history, and updates are permanently recorded and cannot be tampered with.
- **Smart Contracts**: These are used to enforce the rules for data modification (e.g restricting distributors to only update supply chain status or manufacturers to add drugs). Smart contracts ensure that all interactions with the blockchain adhere to the system's policies and user roles.

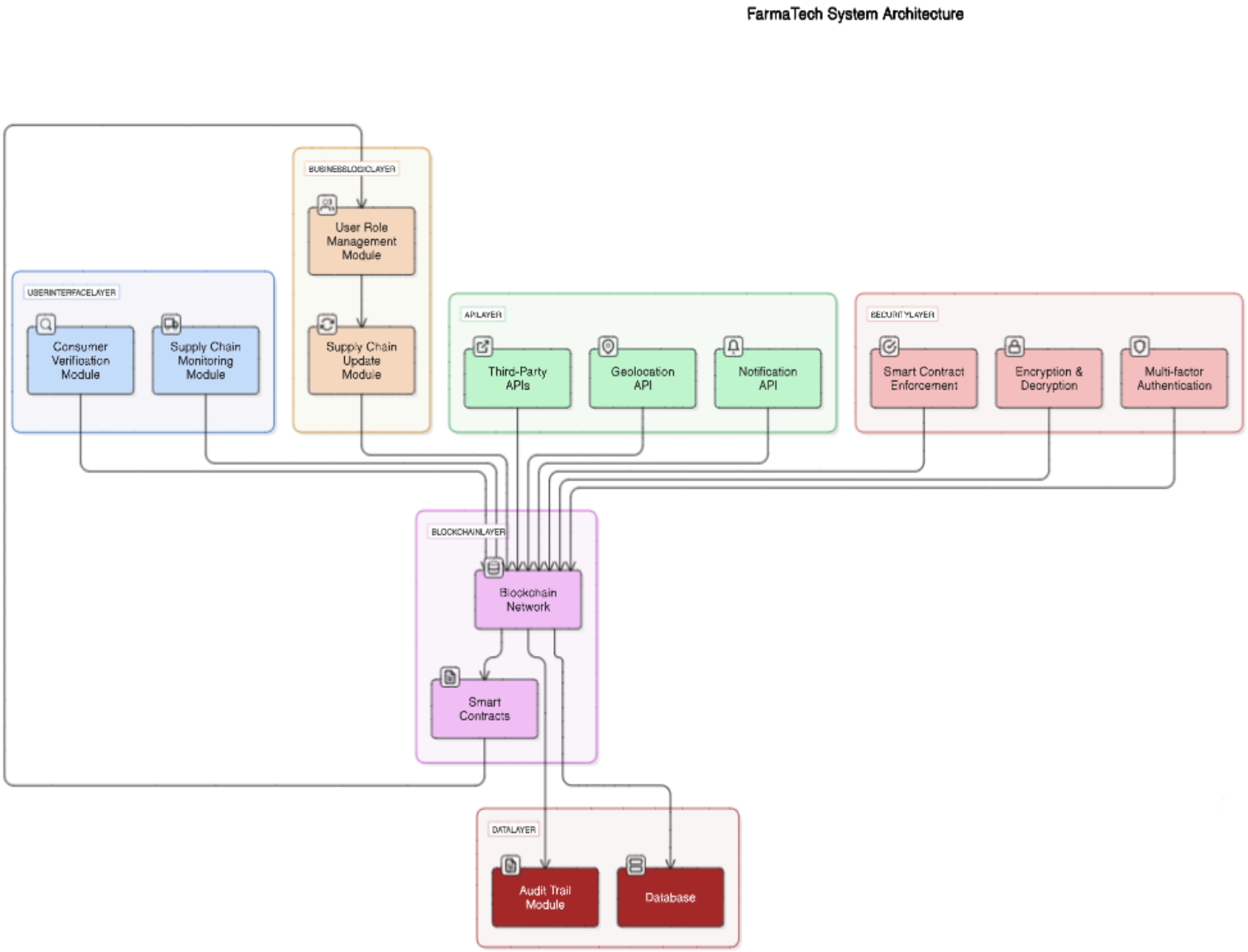

Fig 7: Elaborating on the system architecture

4.5.3 Business Logic Layer

This layer governs the interactions between users and the blockchain, managing permissions and performing necessary calculations.

- **User Role Management Module**: Ensures that each user is granted the appropriate permissions based on their role. Manufacturers can add new medicines, distributors can update supply chain data, and end-users can only view information. Role-based access control (RBAC) ensures proper access rights for each user type.
- **Supply Chain Update Module**: This module is used by distributors to update the status of drugs in the supply chain. These updates are recorded on the blockchain and verified by QR code scanning.

4.5.4 API Layer

The API layer handles communication between various modules and external systems.

- **Geolocation API**: Tracks the real-time location of drugs as they move through the supply chain. Integrated with the blockchain, this data is automatically updated as the drug moves between different points (e.g manufacturer to distributor, distributor to pharmacy).
- **Notification API**: Sends real-time alerts to end-users (pharmacies or consumers) about counterfeit drugs, expired drugs, or irregularities in the supply chain.

4.5.5 Data Layer

The data layer stores all non-blockchain-related information that needs to be retrieved by the system.

- **Database**: A relational or NoSQL database stores supplementary data, such as user credentials, product catalogues, and metadata for blockchain transactions. It supports fast retrieval of user information and status updates without interacting directly with the blockchain.
- **Audit Trail Module**: This logs every action taken within the system (both on the blockchain and in the database) for accountability. Each user interaction with the system is captured to ensure transparency and compliance.

4.5.6 Security Layer

This layer ensures that all data transactions and user actions are secure, and that only authorised personnel have access to sensitive information.

- **Encryption & Decryption**: Sensitive data, such as product information, geolocation, and user details, are encrypted both in transit and at rest.
- **Multi-factor Authentication (MFA)**: Users are required to authenticate through multiple methods to access the system, ensuring only authorised personnel interact with sensitive information.
- **Smart Contract Enforcement**: Only users with specific roles can perform certain actions. Smart contracts enforce these restrictions and maintain data integrity.

System Workflow:

1. Manufacturers register new medicines on the blockchain by inputting details like drug name, batch number, and expiration date via the Medicine Registration Module. This data is permanently recorded on the blockchain, accompanied by a QR code.
2. Distributors use the Supply Chain Monitoring Module to scan QR codes on drugs, which allows them to update the drug's status (e.g., shipped, delivered, in transit). Distributors' access is restricted to supply chain updates and cannot modify product registration details.
3. End-Users (pharmacies, hospitals, or consumers) use the Consumer Verification Module to scan the QR code of drugs they are receiving or purchasing. They can access the drug's complete history from the blockchain to verify its authenticity, manufacturing details, and supply chain journey. They can only view, not modify, any information.
4. The Geolocation API tracks the physical location of drugs as they move through the supply chain. This data, along with any status updates, is recorded on the blockchain for transparency and traceability.
5. The Alert Notification Module sends alerts to the end-users about any issues related to the drugs, such as counterfeiting or expiration, ensuring safety.
6. The Audit Trail Module logs every interaction and update on the system, ensuring an immutable record of all transactions for compliance and auditing purposes.

5. High-Level Design

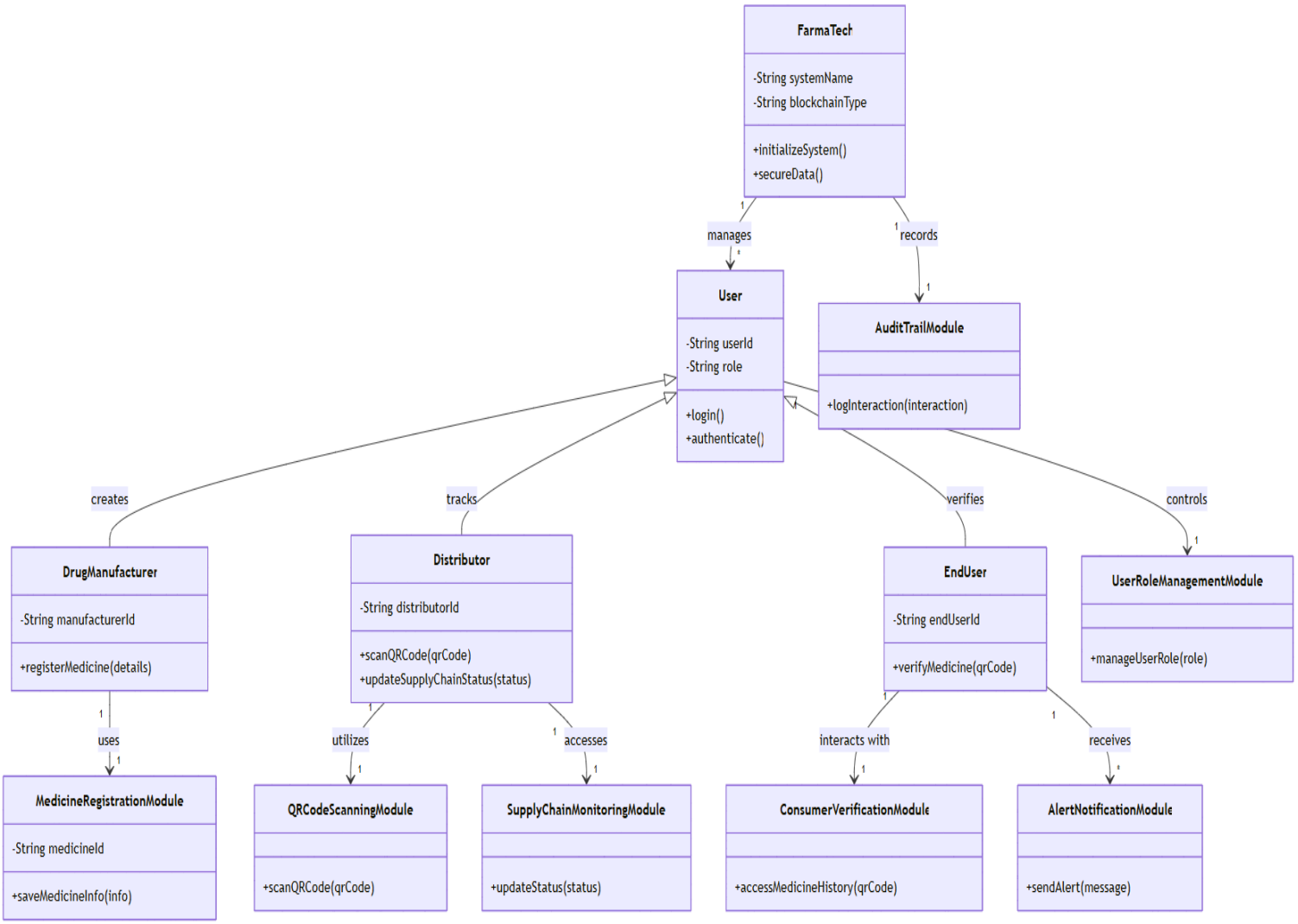

Fig 8: Class Diagram

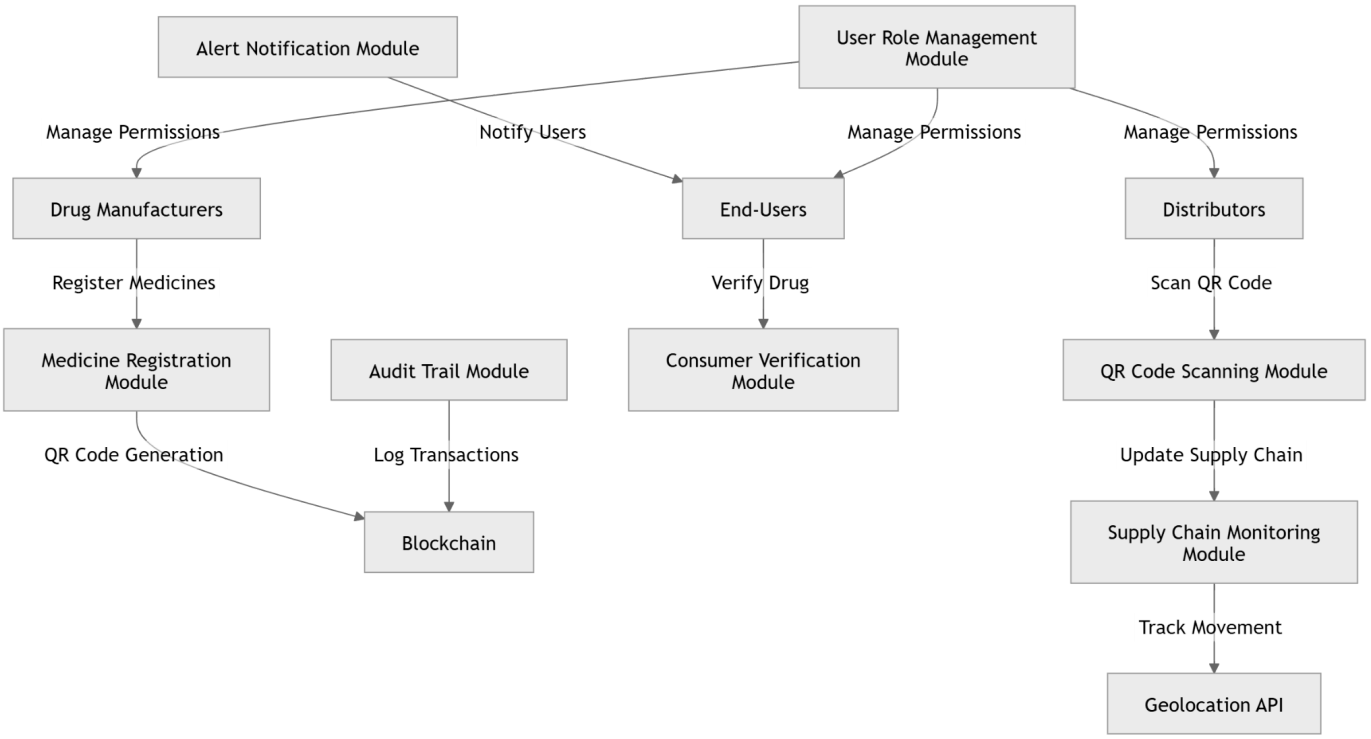

Fig 9

5.1 Blockchain Network Implementation

1. Deploy a permissioned blockchain using Hyperledger Fabric, ensuring secure, immutable, and transparent data storage.
2. Establish a consensus mechanism for transaction integrity, low latency, and high throughput.
3. Configure blockchain governance to restrict access to authorised participants (e.g manufacturers, distributors, regulators).

5.2 Medicine Registration Module

1. Drug manufacturers register medicines via a web-based portal.
2. Collect essential details such as medicine name, batch number, manufacturing date, and expiration date.
3. Generate a unique encrypted QR code that encapsulates all essential information using blockchain integration.
4. Update the blockchain with the registration details, creating an immutable record.

5.3 QR Code Scanning Module

1. Enable QR code scanning via mobile and web applications using the Instascan.js library for fast and accurate detection.
2. Retrieve detailed medicine information from the blockchain in real-time.
3. Integrate Geolocation APIs to record the physical location and timestamp of each scan for enhanced traceability.
4. Update the blockchain with new supply chain status details after every scan.

5.4 Supply Chain Monitoring Module

1. Provide a dashboard for distributors and regulators to track medicine status and integrity.
2. Integrate geolocation tracking for real-time visibility of medicine movement.
3. Implement smart contracts to automate alerts for issues such as tampering, temperature deviations, or broken seals.
4. Record flagged incidents in the blockchain for investigation and accountability.

5.5 Consumer Verification Module

1. Design a user-friendly, cross-platform interface for consumers, hospitals, and pharmacies.
2. Allow users to scan QR codes and instantly verify medicine authenticity.
3. Display comprehensive details, including manufacturing and expiration dates, supply chain history, and tampering alerts.

5.6 User Role Management Module

1. Employ Role-Based Access Control (RBAC) to define and enforce user permissions based on their roles.
2. Implement Multi-Factor Authentication (MFA) for secure user access.
3. Provide administrative tools for managing roles, permissions, and audit logs.

5.7 Audit Trail Module

1. Maintain an immutable log of all interactions, transactions, and status updates.
2. Enable advanced search capabilities for regulatory bodies to investigate flagged incidents.
3. Use the blockchain's inherent properties to ensure data integrity and prevent tampering with records.

5.8 Integration Framework

1. Develop secure REST APIs for interoperability with third-party systems.
2. Design the system for compatibility with smartphones (iOS/Android), tablets, desktops, and web browsers.

5.9 Security Framework

1. Implement end-to-end encryption for all data transmitted between users and the blockchain.
2. Conduct periodic vulnerability assessments and implement secure development practices.
3. Use session management and secure authentication protocols to prevent unauthorised access.

5.10 System Deployment

1. Design the infrastructure for cloud-based, on-premises, or hybrid deployment, depending on stakeholder requirements.
2. Optimise the system for scalability to handle increasing data volumes and user interactions.
3. Ensure performance benchmarks, such as sub-second response times for QR code scanning and real-time blockchain updates.

6. Preliminary Schedule

Phase 1: Planning and Requirements Analysis

Duration: Week 1-6

- Finalise project scope and objectives.
- Refine functional requirements and constraints.

Deliverables:

- Finalised Functional Specification Document.
- Approval from key stakeholders.

Phase 2: System Design

Duration: Week 6-8

- Define the system architecture and third-party integration strategy.
- Develop high-level and detailed designs, including object models and data flow diagrams (DFDs).
- Plan blockchain infrastructure and smart contract requirements.

Dependencies: Completion of Phase 1.
Deliverables:

- High-Level Design Document.
- Approved system architecture blueprint.

Phase 3: Prototype Development

Duration: Week 8-14

- Implement the blockchain network using Hyperledger Fabric.
- Develop core features:
    - Medicine Registration Module.
    - QR Code Generation and Scanning.

    - Basic Supply Chain Monitoring.
- Test the prototype in a controlled environment.

Dependencies: Completion of Phase 2.
Deliverables:

- Prototype of core functionalities.
- Initial test results.

Phase 4: Full System Implementation

Duration: Week 14-16

- Implement all functional requirements:
    - Immutable Audit Trail.
    - User Role Management.
    - Smart Contracts for Expiration Alerts.
- Integrate geolocation tracking and alert systems.
- Develop user interfaces for different user groups.

Dependencies: Successful prototype testing in Phase 3.
Deliverables:

- Fully functional FarmaTech system.
- Detailed documentation for each module.

Phase 5: Testing and Quality Assurance

Duration: Week 16-18

- Perform unit testing for individual components.
- Conduct integration and system testing.
- Gather feedback from stakeholders during User Acceptance Testing (UAT).

Dependencies: Completion of Phase 4.
Deliverables:

- Test cases and reports.
- Approved system for deployment.

Phase 6: Deployment and Training

Duration: Week 18-20

- Deploy the FarmaTech system on cloud or on-premises infrastructure.
- Provide training sessions for Drug Manufacturers, Distributors, and End Users.

Dependencies: Successful completion of testing in Phase 5.
Deliverables:

- Deployed FarmaTech system.
- Training manuals and user guides.

7. Appendices

Specifies other useful information for understanding the requirements.

##High level design

8. References

IBM, director. *Using blockchain to prevent counterfeit drugs in Kenya*. IBM, 2017. *youtube*, https://www.youtube.com/watch?v=11Z4-XYoZAE&ab_channel=IBMResearch.

IEEE. “Blockchain Based Counterfeit Medicine Authentication System.” *Blockchain Based Counterfeit Medicine Authentication System*, IEEE, 26 May 2021, https://ieeexplore.ieee.org/abstract/document/9431789. Accessed 10 11 2024.

Islam, Muhammad Nazrul. “A blockchain based medicine production and distribution framework to prevent medicine counterfeit.” *ScienceDirect*, 2023, https://www.sciencedirect.com/science/article/pii/S1319157823004056#sec6. Accessed 1 December 2024.

Title:Geolocation Tracking with Node.js and GPS: Building Location-Aware Applications
Website title:Medium
URL:https://medium.com/@desmondmutuma35/geolocation-tracking-with-node-js-and-gps-building-location-aware-applications-d04501a5ed90
Date published:August 5, 2023
Date accessed:November 22, 2024
Author:Mutuma Mutwiri, Juanjo Jaramillo, and Shuai Li

Acviss. “Securing Your Business - Strategies to Prevent QR Code Duplication.” *Anti Counterfieting*, Acviss, 02 September 2024, https://blog.acviss.com/securing-your-brand-to-prevent-qr-code-duplication/. Accessed 05 November 2024.