Software Engineering
2026, Vol. 12, No. 1, pp. 1–11
https://doi.org/10.11648/j.se.20261201.11

Research Article

Vaccine Supply Chain Management Through Hyperledger Fabric Blockchain Technology

Gopika Krishnan Suseela[1], Sangeetha Jose[2, *], Jino Joseph[3]

[1]Department of Computer Applications, Al Azhar College of Arts and Science, Thodupuzha, India
[2]Department of Computer Application, Rajiv Gandhi Institute of Technology, Kottayam, India
[3]Department of Commercial Practices, Govt Polytechnic College, Kottayam, India

Abstract

Ensuring transparency, integrity, and security across the vaccine supply chain is essential to prevent counterfeiting, unauthorized data manipulation, and logistical inefficiencies that can adversely affect public health systems. Traditional vaccine supply chain management systems primarily rely on centralized databases, which are susceptible to tampering, single points of failure, and limited real-time visibility for participating stakeholders. These limitations reduce trust among manufacturers, distributors, healthcare providers, and regulatory authorities and increase the risk of counterfeit or compromised vaccines entering the distribution network. This research presents a blockchain-based vaccine supply chain management model developed using Hyperledger Fabric, a permissioned blockchain framework specifically designed for enterprise and healthcare-oriented applications. The proposed system integrates chaincode-driven automation to enforce predefined business rules, SHA3-256 cryptographic hashing to ensure data immutability, and PBFT-based consensus mechanisms to validate transactions reliably in a distributed environment. Role-based authentication is implemented to ensure that only authorized participants can access and update the system, enabling secure and controlled data sharing among all stakeholders involved in the vaccine lifecycle. In addition, a middleware layer developed using the Go programming language and the Gorilla Mux framework facilitates seamless and secure communication between client applications and the blockchain network through RESTful APIs. The proposed architecture enables immutable record-keeping, efficient end-to-end traceability of vaccine batches, and stringent verification of transactions across all stages of the supply chain, including manufacturing, distribution, and administration. Experimental testing conducted through API calls and Postman validates the system's ability to automate operational workflows while effectively preventing unauthorized data modifications. The results demonstrate improved operational reliability, enhanced data integrity, reduced risk of counterfeit vaccines, and increased transparency and trust among stakeholders. This study highlights how permissioned blockchain networks such as Hyperledger Fabric can modernize vaccine logistics and contribute to safer, more transparent, and reliable public health supply chain systems.

Keywords

Hyperledger Fabric, Blockchain, PBFT, Vaccine Supply Chain, Traceability, Decentralization

*Corresponding author: sangeetha.jose@rit.ac.in (Sangeetha Jose)

Received: 13 December 2025; **Accepted:** 25 December 2025; **Published:** 19 January 2026

1. Introduction

The efficient management of vaccine supply chains is critical for ensuring public health worldwide. However, existing systems face significant challenges, including the presence of counterfeit vaccines and a lack of transparency in tracking vaccine distribution. These issues pose serious risks to public health and underscore the urgent need for innovative solutions. In response to these challenges, this paper proposes a decentralized data management system leveraging blockchain technology [1] to enhance the integrity and efficiency of vaccine supply chains.

The current vaccine supply chain ecosystem [2] relies heavily on manual record-keeping and centralized databases, making it susceptible to data tampering, unauthorized access, and operational inefficiencies. Consequently, the reliability of vaccine information is compromised, leading to potential health hazards for individuals receiving counterfeit or tampered vaccines. By harnessing the power of blockchain technology, this paper aims to address these vulnerabilities and revolutionize vaccine supply chain management. Blockchain offers inherent features such as transparency, immutability, decentralization, and traceability [16], which can significantly enhance the security, efficiency, and visibility of vaccine distribution processes. The integration of cryptographic techniques like SHA3-256 ensures data integrity, while consensus algorithms such as PBFT (Practical Byzantine Fault Tolerance) reinforce data consistency across the network. By providing an immutable ledger, blockchain [13] can not only prevent unauthorized alterations but also ensure that all stakeholders have real-time access to vaccine information, reducing delays and fostering greater accountability.

Through the implementation of a decentralized data management system [17], vaccine-related information can be securely stored in interconnected blocks, ensuring tamper-proof records and transparent transaction history throughout the supply chain. Additionally, smart contracts [15] embedded in the system automate key processes, reducing human errors and operational inefficiencies, and further improving overall management. This system not only makes it easier to track [11] vaccines from the manufacturer to the recipient, but it also lowers the risk of fake vaccines getting into the supply chain.

This paper proposes a transparent, tamper-proof distributed vaccine supply chain management system built on Hyperledger Fabric [3], with the potential to transform how vaccines are managed and distributed across global healthcare systems. The solution is designed to increase the resilience and responsiveness of vaccine logistics, ensuring better public health outcomes.

The remaining sections of the paper are organized as follows: Section 2 presents a summary of the literature review, highlighting current advancements in the field. Section 3 discusses the methodology adopted for the proposed system. Section 4 outlines the implementation details, while Section 5 evaluates the results of the system. Section 6 provides the conclusion of the research and explores potential future directions for enhancing the system's effectiveness.

2. Literature Review

Here are some notable works related to vaccine safety that have been addressed using blockchain technology. L. Cui et al. [4] published a paper titled Protecting vaccine safety: An improved, blockchain-based, storage-efficient scheme. The paper introduces a blockchain solution for bolstering vaccine safety, employing trace codes, transactions, and smart contracts. However, while tackling data reliability challenges, it encounters potential efficiency issues and cloud security concerns, prompting the need for additional enhancements to optimize performance in practical vaccine circulation scenarios.

T. Fatokun et al. [5] proposed a blockchain-assisted patient-owned system for electronic health records. The objective of this paper is to implement a patient-centric electronic health record (EHR) system using blockchain to enhance security, privacy, and interoperability. Patients control their records, ensuring secure data exchange. The research includes functional and performance testing, contributing to improved data security, privacy, and interoperability in healthcare. However, limitations include scalability challenges with growing data, bandwidth overhead from mining and communication, and insufficient focus on database security.

F. Jamil et al. [6] proposed a novel medical blockchain model for drug supply chain integrity management in a smart hospital. Objectives include developing a secure drug supply chain record system with Hyperledger Fabric, enhancing transparency in smart hospitals, and providing a global solution to counterfeit pharmaceuticals. Limitations include generalizability, scalability, regulatory considerations, security, privacy, and resource implications, with potential challenges in real-world implementation.

A. R. Nair et al. [7] proposed FAIR, a blockchain-based approach for fair and secure vaccine distribution during pandemics. Utilizing smart contracts and the interplanetary file system (IPFS), it addresses challenges in healthcare supply chains. IPFS is a decentralized peer-to-peer file-sharing system that allows people to access content without the need for a central server. Limitations include potential complexities, costs, scalability issues, and integration challenges with existing systems and data privacy concerns.

I. T. Javed et al. [8] proposed PETchain, a privacy-enhancing technology on a consortium blockchain. PETchain empowers users with control over their data, stored securely on IPFS. It features a user-centric architecture, secure data storage, a trusted execution environment (TEE), auditable logs, and smart contract functionality. The objectives involve PETchain development and a smart contract for access control and performance analysis. PETchain faces challenges including block time variability affecting throughput, trade-offs between transactions per second (TPS) and block time leading to lost blocks, and computational overhead from privacy technologies like homomorphic encryption.

A. Musamih et al. [9] proposed a blockchain-based solution for COVID-19 vaccine distribution addressing transparency, traceability, and security. Features include accountability through Ethereum smart contracts, decentralized availability, protection against attacks, rigorous security analysis, and a comparative advantage over non-blockchain solutions. Limitations encompass scalability challenges, internet connectivity dependence, off-chain storage costs, smart contract customization complexity, and regulatory compliance hurdles.

S. Bhushan et al. [10] proposed a blockchain-powered vaccine supply chain system to tackle distribution challenges, ensuring transparency, authenticity, and efficacy. Features include decentralized smart contracts, tamper-proof administration, internet of things (IoT) integration for temperature monitoring, and public reporting. Limitations involve technology adoption, regulatory hurdles, resource demands, and integration complexities with existing distribution systems.

To address these gaps and improve the current vaccine supply chain, we propose a decentralized vaccine supply chain management system through blockchain technology [20, 21]. Hyperledger Fabric is the technology used. This approach has the potential to bring about transformative improvements by enhancing transparency, traceability, security, and efficiency, ultimately strengthening public health response capabilities.

3. Methodology

The proposed system marks a substantial improvement in addressing the challenges present in the current system. It covers key features, materials, and methods employed in the development. With a focus on leveraging blockchain technology, the outlined system offers innovative solutions to enhance efficiency, security [18], and transparency in the targeted domain.

3.1. Features of Proposed System

The proposed system leverages Hyperledger Fabric with the Practical Byzantine Fault Tolerance (PBFT) algorithm [24] to ensure reliable and secure vaccine data management. PBFT maintains transaction consistency even during network disruptions. The system offers real-time tracking, immutable records, and enhanced transparency, fostering trust in vaccine information throughout the supply chain. Key features include:

1) Decentralization: The system operates without a central authority, distributing control among nodes [22, 25], enhancing trust and collaboration between stakeholders.
2) Immutability: Vaccine records are stored on the blockchain, ensuring they are tamper-proof and resistant to unauthorized modifications.
3) Transparency: All transactions and vaccine movements are recorded on a transparent, immutable ledger, making information accessible and verifiable in real time.
4) Traceability: Each vaccine batch can be precisely tracked throughout its journey, allowing stakeholders to verify its authenticity and movement through the supply chain.
5) Security: The use of blockchain and PBFT consensus ensures robust protection against unauthorized access and malicious activity.
6) Data Integrity: The system guarantees the integrity of the data, ensuring that all information remains accurate and reliable across the decentralized network.
7) Efficiency: The decentralized nature and consensus algorithms improve the efficiency of managing vaccine supply chains, reducing errors and delays.

3.2. Methodology

The methodology for developing the vaccine supply chain management system via blockchain technology involves defining API endpoints and functionalities, structuring data models, developing middleware, integrating with Hyperledger, implementing authentication mechanisms, and conducting testing. Each stage ensures the system's efficiency, security, and reliability in managing vaccine-related information and transactions.

1) API Design: This stage involves defining the endpoints and functionalities that the system will provide through its API (Application Programming Interface). The defined functionalities include registering new vaccines, tracking vaccine batches, verifying vaccine authenticity, and retrieving vaccine information.
2) Data Models: In this phase, data structures are defined to organize and manage information related to vaccine batches. Attributes such as batch number, manufacturer, production date, etc., are identified and structured to facilitate efficient data management. Additionally, structures for transactions and blocks specific to the Hyperledger blockchain are defined to ensure compatibility and interoperability with the chosen blockchain platform.
3) Middleware Development: Middleware development involves implementing a layer of software, typically using a programming language like Golang, to expose the defined API endpoints. Libraries such as Gorilla Mux are utilized for routing and handling HTTP requests, ensuring smooth communication between the frontend and backend components of the system.
4) Hyperledger Integration: This step focuses on integrating the Golang middleware with the chosen Hyperledger blockchain platform, such as Hyperledger Fabric [19] or

Composer. Smart contracts are implemented to define the business logic and rules governing vaccine transactions and authenticity verification on the blockchain.

5) Authentication and Authorization: Authentication mechanisms such as JWT (JSON Web Tokens) are implemented to secure the API endpoints and prevent unauthorized access. Roles and permissions are defined to regulate access to different functionalities within the system, ensuring data security and privacy.
6) Testing: The system was tested to validate its core functionality and reliability. API endpoints were tested using Postman to ensure proper interaction between components and accurate data retrieval. This testing helped verify that the middleware and blockchain integration worked as expected.

3.3. Algorithm

The Practical Byzantine Fault Tolerance (PBFT) algorithm serves as a consensus mechanism engineered to establish agreement within a distributed network of nodes, even when confronted with Byzantine faults. PBFT [14] stands as a pioneering algorithm crafted by Castro and Liskov in 1999. Its innovative design enables nodes in a distributed network to reach consensus even when faced with Byzantine faults, where nodes exhibit malicious or arbitrary behavior. PBFT divides the network into a collection of replica nodes, typically comprising at least 3f+1 replicas, where 'f' symbolizes the maximum number of faulty or malicious nodes the system can endure while retaining consistency. Each replica uses a unique identifier and engages in communication with other replicas across the network. Through its design and operation, PBFT provides a robust framework for achieving consensus in the face of potential faults or adversarial behavior, marking a significant advancement in the field of distributed systems and consensus protocols. The consensus process in PBFT involves several phases:

1) Request: A client sends a request to the network, specifying the operation it wants to be executed.
2) Pre-Prepare: The primary replica (leader) assigns a sequence number to the request and sends a pre-prepare message to other replicas, proposing the operation and sequence number.
3) Prepare: Upon receiving a pre-prepare message, each replica verifies the request and then broadcasts a prepare message to indicate acceptance of the proposed operation and sequence number.
4) Commit: Once a replica receives 2f+1 prepare messages for the same sequence number and operation, it broadcasts a commit message to finalize the decision.
5) Execute: Replicas execute the operation specified in the request, applying it to their local state machine.

3.4. System Architecture

Figure 1 illustrates the proposed framework, a blockchain based system designed for vaccine supply chain management. The proposed vaccine supply chain management system involves multiple actors, including regulatory authorities, manufacturers, distributors, wholesalers, pharmacies/hospitals, and consumers, all working within a decentralized framework powered by blockchain technology.

It visually represents the flow of the entire process, with all information being stored on the blockchain to ensure immutability, transparency, and security of vaccine supply chain management. On the left side of Figure 1, all the actors involved in the supply chain are listed, while on the right side, the specific activities of each actor are detailed. The bottom of the figure contains the flow of the entire process, showcasing the movement of vaccines from the manufacturer to the various actors involved, such as distributors, wholesalers, pharmacies/hospitals, and ultimately to the end consumer. The bottom contains the flow of the entire process, showcasing the movement of vaccines from the manufacturer to the various actors involved, such as distributors, wholesalers, pharmacies/hospitals, and ultimately to the end consumer.

The process begins with manufacturers registering on the system and receiving a unique ID. After registration, they submit requests for vaccine production, which are reviewed and approved by the regulatory authority (admin). The regulatory authority then assigns a unique ID to the manufacturer, who subsequently logs into the system using this ID to proceed with vaccine production. Every step is tracked and stored securely on the blockchain, ensuring transparency, security, and traceability throughout the entire vaccine supply chain. Distributors then transport the vaccines to wholesalers, who in turn supply them to pharmacies and hospitals, with every step of the journey tracked and documented on the blockchain. This ensures transparency, security, and traceability throughout the entire supply chain. Pharmacies and hospitals verify the vaccine's authenticity before making it available to consumers. By utilizing smart contracts, key processes such as vaccine registration and tracking are automated, minimizing the need for manual intervention and further enhancing the system's efficiency. Overall, blockchain technology guarantees the immutability of records at every stage, fostering trust and security in vaccine distribution from production to administration.

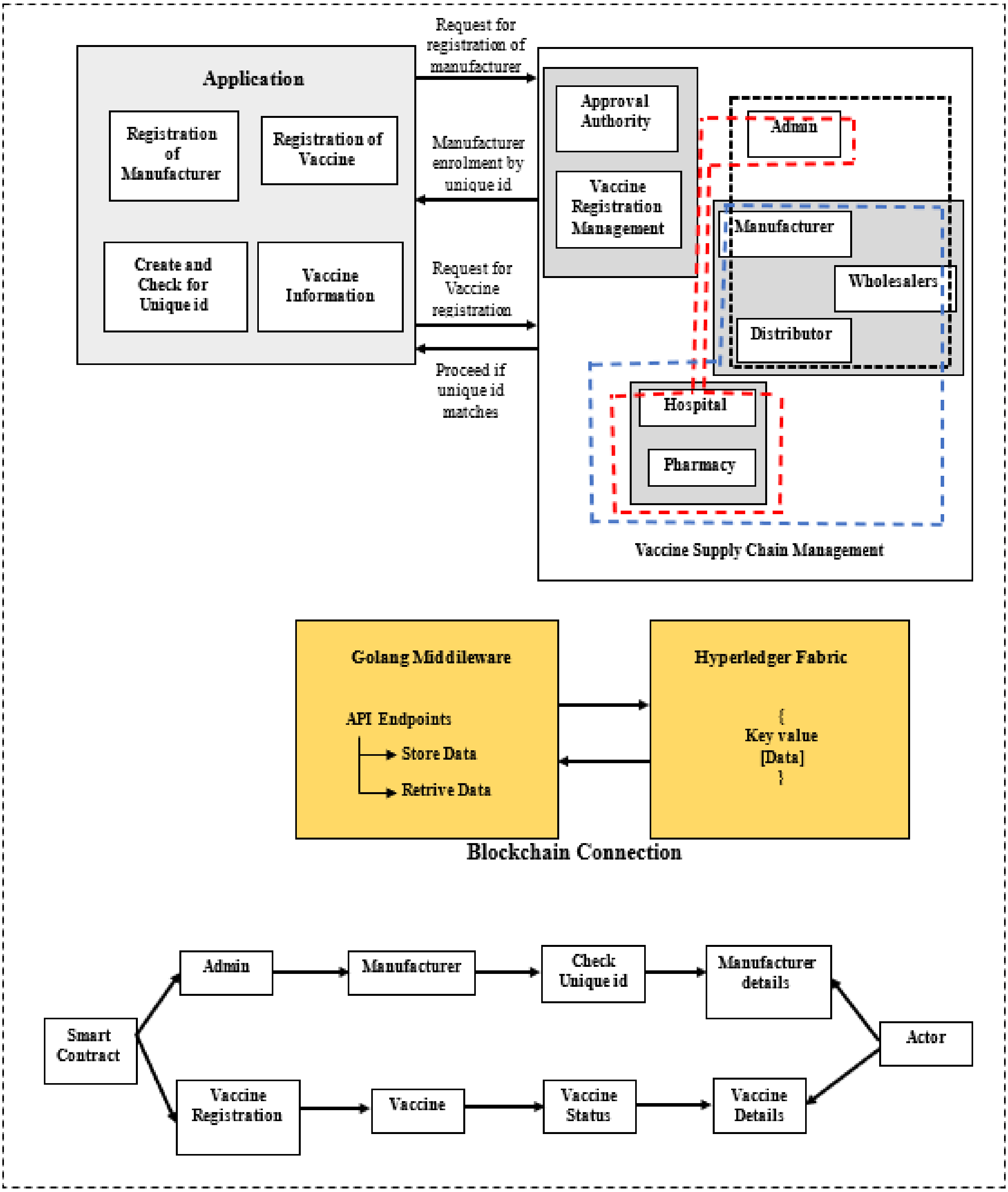

Figure 1. System Architecture.

4. Implementation

This section outlines the steps required to understand the setup and components necessary for the implementation of the vaccine supply chain management system.

4.1. Prerequisites

Before running the system, the following prerequisites need to be installed and configured:

1) Hyperledger Fabric: A blockchain platform used to create a shared and secure system for recording data. It ensures

privacy and scalability by allowing controlled access and different services for managing network members.

2) Docker: A tool that creates virtual containers to run different parts of the system, like network peers and chaincode, in a consistent environment. It helps manage the different components needed for the system to work smoothly.

3) Postman: A tool used to test how APIs work by sending requests and checking responses. It helps make sure the blockchain-based APIs function correctly during system development.

4) Go: Go, also known as Golang, is a statically typed, compiled programming language. It is used for developing chaincode in Hyperledger Fabric due to its efficiency and reliability in executing blockchain operations.

4.2. Running the Hyperledger Fabric Framework

The root directory for the work is fabric-samples. Hyperledger Fabric [23] provides a set of scripts inside the test network directory, which helps in setting up and managing the blockchain network. Below are the steps to configure and run the Hyperledger Fabric node:

1) Navigate to the test-network directory:

cd test-network

This will change the current directory to test-network, which contains the necessary dependencies and scripts for running the Hyperledger Fabric network.

2) Start the Hyperledger Fabric network:

./network.sh up

This command initializes the Hyperledger Fabric network by running the nodes inside Docker containers.

3) Create a Channel:

In Hyperledger Fabric [12], a channel is a communication mechanism allowing participants to interact securely and privately. Creating a channel ensures that transaction visibility is limited to members of that channel. To create a channel, use the following command:

./network.sh create Channel -c channel1

This is a one-time setup, necessary when initializing the network.

4) Deploy the Chaincode (Smart Contract):

To deploy the chaincode (smart contract) written in Go to the newly created channel (channel1), run the following command:

./network.sh deployCC-ccn vaccine1-ccp../fabric-setup/chaincode-go-ccl go-c channel1

This command installs and instantiates the smart contract on the peers of the channel1 network, enabling the functionality for vaccine management on the blockchain.

5) Open a new terminal in the root directory:

After the network setup, open another terminal and navigate to the root directory.

6) Navigate to the Go client directory:

Use the following command to go to the directory where the Go client is written:

Cd fabric-setup/rest-api-go/

7) Run the Go client:

The following command will run the Go client (golang-client), which interacts with Hyperledger Fabric and the frontend:

Go run main. go

4.3. Defining Contract Variables and Modifiers

1) Contract Variables: The smart contract leverages a hierarchical data structure to store and manage vaccine-related information. The core structure, VaccineInfo, contains key attributes necessary for tracking vaccines across the supply chain. Some of the essential contract variables include ID, name, expiry date, and manufacturer ID.

2) Contract Modifiers: The smart contract [15] provides several key functions, or contract modifiers, that interact with the ledger to modify the state of the stored vaccine data. These functions are responsible for adding or updating information on the blockchain, such as adding vaccine details, updating manufacturing and expiry dates, and recording information related to the manufacturer, hospital, and distributor involved in the vaccine supply chain.

4.4. API Endpoints in Go-Client

The Go client serves as the middle layer that interacts with the Hyperledger Fabric blockchain, invoking smart contracts to perform various operations. This middle layer runs a server on port 8080 and acts as both a client and server, enabling interaction with the blockchain. The key API endpoints developed as part of the system for managing vaccine data on the blockchain are given below.

1) [POST] /api/v1/add-vaccine-info:

This API endpoint is responsible for submitting vaccine information to the ledger (blockchain). It interacts with the smart contract to record the necessary details about each vaccine.

Request URL: localhost:8080/api/v1/add-vaccine-info

Request Body Example:

```
{
"VaccineID": "3",
"VaccineName": "Sample Vaccine Name 3",
"AgeGroup": "1-20",
"ContraIndications": "ContraIndications
"MethodOfAdministration":"MethodOfAdministration",
"VaccineDescription": "VaccineDescription",
"PharmaceuticalForm": "PharmaceuticalForm”,
"Precautions": "Precautions"
}
```

This endpoint ensures the proper registration and storage of vaccine information on the blockchain, providing transparency and immutability for the vaccine data. Go-client is designed to facilitate seamless interaction with the underlying blockchain through these APIs.

2) [POST] /api/v1/get-vaccine-details:

This API endpoint retrieves the details of a specific vaccine that has been previously stored on the blockchain. The vaccine information is fetched using the unique VaccineID. This API queries the ledger to obtain the corresponding vaccine details stored in the blockchain.

Request URL: localhost:8080/api/v1/get-vaccine-details

Request Body Example:

```
{
"VaccineID": "1"
}
```

3) [GET] /api/v1/get-all-vaccine-details:

This request is used to get all the vaccine details that have been stored in the ledger.

Request URL: localhost:8080/api/v1/get-all-vaccine-details

Figure 2 presents a code snippet defining a function named createBlockHash. This function generates a SHA-3-256 hash from the provided input content. It takes a string as input and returns a hexadecimal string that represents the resulting hash. This hash can be used for various purposes, such as verifying data integrity or ensuring the authenticity of information.

```go
func createBlockHash(content string) string {

  // Create a new SHA3-256 hasher
  hasher := sha3.New256()

  // Write the content to the hasher
  hasher.Write([]byte(content))

  // Get the finalized hash
  hashBytes := hasher.Sum(nil)

  // Convert the hash to a hexadecimal string
  hashString := hex.EncodeToString(hashBytes)

  // Print the hash
  fmt.Println("SHA3-256 hash:", hashString)

  return hashString
}
```

Figure 2. *SHA-3-256 Hash Generation Function.*

Figure 3 depicts the CheckVaccineExists and GetVaccineDetails functions, which are essential for interacting with the vaccine data stored on the blockchain ledger.

```go
// VaccineExists check the ledger whether the vaccine respective to the particular id exists
func (s *SmartContract) CheckVaccineExists(ctx contractapi.TransactionContextInterface, vaccineId string) (bool, error) {
    vaccineDetailsJSON, err := ctx.GetStub().GetState(vaccineId)
    if err != nil {
        return false, fmt.Errorf("failed to read from world state: %v", err)
    }

    return vaccineDetailsJSON != nil, nil
}

// ReadAsset returns the asset stored in the world state with given id.
func (s *SmartContract) GetVaccineDetails(ctx contractapi.TransactionContextInterface, vaccineId string) (*VaccineInfo, error) {
    vaccineDetailsJSON, err := ctx.GetStub().GetState(vaccineId)
    if err != nil {
        return nil, fmt.Errorf("failed to read from world state: %v", err)
    }
    if vaccineDetailsJSON == nil {
        return nil, fmt.Errorf("the vaccine details %s does not exist", vaccineId)
    }

    var vaccineDetails VaccineInfo
    err = json.Unmarshal(vaccineDetailsJSON, &vaccineDetails)
    if err != nil {
        return nil, err
    }

    return &vaccineDetails, nil
}
```

Figure 3. *Vaccine Existence and Retrieval Functions.*

The CheckVaccineExists function verifies if a vaccine with the specified ID exists, while the GetVaccineDetails function retrieves the complete details of a vaccine based on its ID. These functions play a crucial role in ensuring data integrity and consistency within the vaccine supply chain management system.

5. Results and Discussion

By leveraging Hyperledger Fabric blockchain technology, our proposed system offers a comprehensive solution for managing vaccine supply chains. The following key aspects highlight the system's benefits:

1) Immutability: The SHA3-256 hashing algorithm ensures that data remains unalterable, which strengthens the security and integrity of vaccine-related information. SHA3-256 works by transforming any data into a fixed-size, unique fingerprint, providing a high level of protection against tampering.
2) Data Integrity: PBFT (Practical Byzantine Fault Tolerance) guarantees data consistency by replicating the ledger across multiple nodes. In this process, a leader node broadcasts transactions, and other nodes (replicas) vote on their validity. Once a sufficient number of honest nodes agree, the transaction is committed to the ledger. This multistep process with redundancy makes the system highly resistant to data manipulation by malicious actors.
3) Transparency and Resilience: The adoption of a shared, distributed ledger provides real-time visibility into the vaccine distribution process, fostering transparency and accountability among all stakeholders. This decentralized approach enhances resilience by reducing the risk of single points of failure, ensuring continuous operation even in the event of disruptions.
4) Traceability: The inclusion of unique identifiers in the system enables precise tracking of vaccine batches as they move through the supply chain. This improves traceability and reduces the risk of counterfeit vaccines infiltrating the system.
5) Security: Cryptographic measures, such as public key encryption, ensure that sensitive vaccine-related data is protected from unauthorized access. This enhances overall system security and helps safeguard against potential threats and breaches.
6) Efficiency: Smart contracts automate key processes within the vaccine supply chain, minimizing manual intervention and reducing errors. This results in streamlined management and improved overall efficiency of the system.

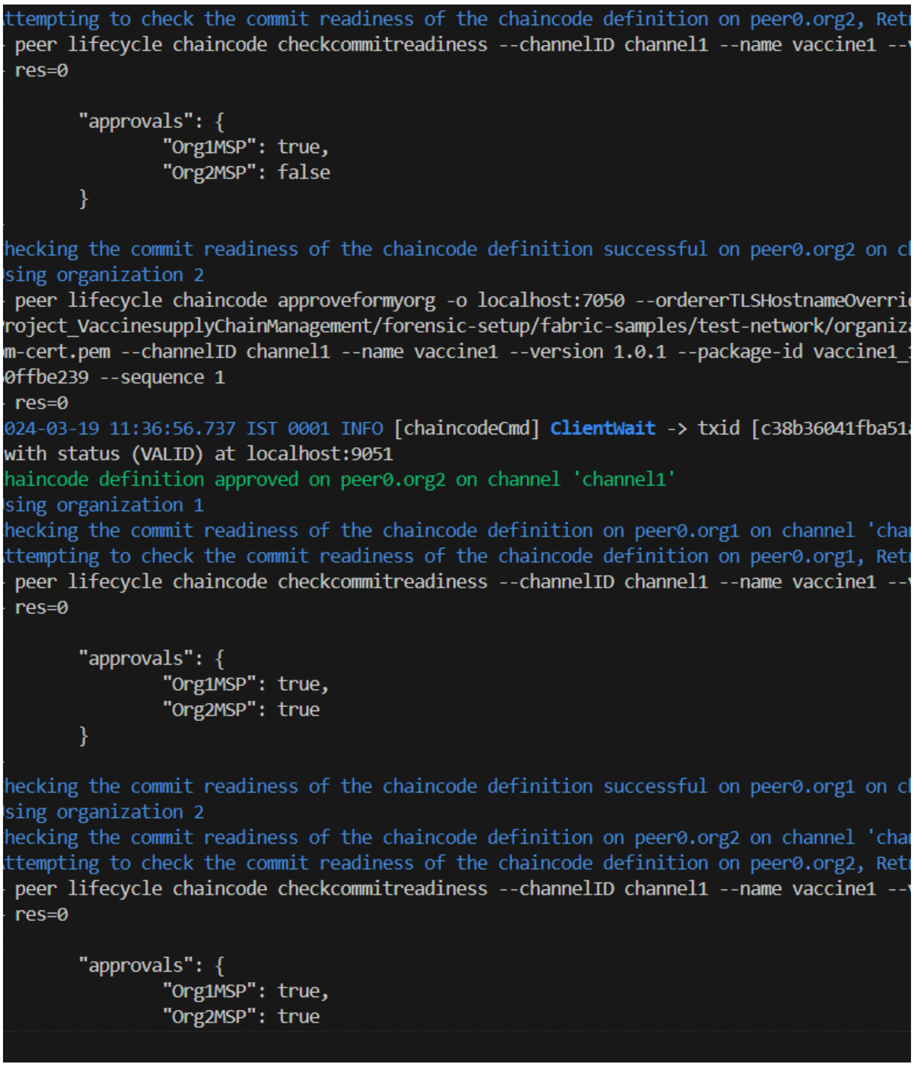

Figure 4. *Smart Contract Deployment.*

Figure 4 illustrates the smart contract being deployed to channel1 on Hyperledger Fabric. The smart contract was successfully deployed using the network.sh script, as confirmed by the command line output. With the contract now in place, it is ready to execute various functions, including adding vaccine information, updating details, and querying the ledger for vaccine status.

Figure 5 depicts a series of transactions executed on a blockchain-based vaccine supply chain management system. Each transaction represents an update to the vaccine information, including its details, manufacturer, expiry date, hospital, and distributor.

```
--> Submit Transaction: AddVaccineInfo, add the given Vaccine info to the chain
Vaccine Info:  {15 Ruby vaccine Recommended for ages 12 to 45 years.   Avoid in individuals with known hypersensitivity to vaccine components. intramus
cular injection vaccine Topical emulsion.   store in cool place  { }   }
*** Transaction committed successfully
VaccineId in AddHospitalDetailRequest 15
DistributorId in AddHospitalDetailRequest 1
2024/05/15 11:41:17 {15 1}
VaccineId 15
ManufacturerId 1

--> Submit Transaction: AddManufacturerInfo, add the vaccine manufacturer info to the chain
*** Transaction committed successfully
VaccineId in AddExpiryDetailRequest 15
ManufacturingDate  in AddExpiryDetailRequest 2024-05-08
ExpiryDate in AddExpiryDetailRequest 2027-06-16
2024/05/15 11:42:16 {15 2024-05-08 2027-06-16}

--> Submit Transaction: AddExpiryInfo, add the vaccine expiry info to the chain
*** Transaction committed successfully
VaccineId in AddHospitalDetailRequest 15
DistributorId in AddHospitalDetailRequest 1
2024/05/15 11:42:51 {15 1}

--> Submit Transaction: AddHospitalInfo, added hospital info to the chain
*** Transaction committed successfully
VaccineId in AddDistributorDetailRequest 15
DistributorId in AddDistributorDetailRequest 1
2024/05/15 11:44:56 {15 1}

--> Submit Transaction: AddDistributorInfo, add the vaccine distributor info to the chain
*** Transaction committed successfully
```

Figure 5. *Vaccine Supply Chain Management Transaction.*

6. Conclusion

The paper addresses the critical challenges faced by the pharmaceutical industry in managing vaccine supply chains by implementing a decentralized system using Hyperledger Fabric. This system enhances transparency, security, traceability, and efficiency in vaccine distribution. By leveraging blockchain technology, it ensures data integrity, mitigates counterfeit risks, and fosters trust among stakeholders. The research introduces a transparent, tamper-resistant ledger system that provides real-time visibility into vaccine movement, prevents data tampering, and reduces the risk of counterfeit infiltration. This ensures the authenticity and integrity of vaccine-related data, ultimately improving public health outcomes.

However, the current work also highlights certain limitations, such as the need for continuous optimization and adaptation to evolving technology and regulatory requirements. Ensuring widespread adoption and interoperability with existing systems presents challenges as well. We plan to extend the performance analysis of the Hyperledger Fabric framework using the Hyperledger Caliper benchmark tool, since it will be crucial to evaluate factors such as throughput, latency, and scalability. This performance analysis will provide valuable insights into system efficiency and help identify areas for optimization. Despite these limitations, the research demonstrates significant progress in revolutionizing vaccine supply chain management through blockchain technology.

In terms of future scope, the system can be further refined and expanded in several ways. Real-world testing in larger environments is essential to validate the framework's performance, particularly in terms of network scalability and user adoption. Enhancing user interaction and integrating features like customer feedback and cold chain monitoring with sensors would further improve the system's reliability and safety. Moreover, strengthening security with multifactor authentication (MFA) would enhance protection against cybersecurity threats. Adapting the framework for diverse global scenarios and improving interoperability with healthcare technologies and standards will also be important for broader applicability and integration into existing infrastructures.

Abbreviations

PBFT	Practical Byzantine Fault Tolerance

SHA3-256	Secure Hash Algorithm 3–256 bit
EHR	Electronic Health Record
IPFS	InterPlanetary File System
TPS	Transactions Per Second
IoT	Internet of Things
HTTP	Hypertext Transfer Protocol
JWT	JSON Web Token
JSON	JavaScript Object Notation
API	Application Programming Interface
Go	Golang Programming Language

Author Contributions

Gopika Krishnan Suseela: Conceptualization, Formal analysis, Investigation, Methodology, Software, Writing – original draft

Sangeetha Jose: Conceptualization, Project administration, Resources, Supervision, Writing – review & editing

Jino Joseph: Conceptualization, Project administration, Supervision, Writing – review & editing

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. Available from: https://bitcoin.org/bitcoin.pdf (accessed April 2019).

[2] Rehman, M., et al. A cyber secure medical management system by using blockchain. IEEE Transactions on Computational Social Systems. 2022. https://doi.org/10.1109/TCSS.2022.3215455

[3] Hyperledger Foundation. Hyperledger Fabric. Available online: https://www.hyperledger.org/projects/fabric (accessed on April 2019).

[4] Cui, L.; et al. Protecting vaccine safety: An improved, blockchain-based, storage-efficient scheme. IEEE Transactions on Cybernetics, 2022. https://doi.org/10.1109/TCYB.2022.3163743

[5] Fatokun, T., Nag, A., Sharma, S. Towards a blockchain-assisted patient-owned system for electronic health records. Electronics. 2021, 10(5), 580. https://doi.org/10.3390/electronics10050580

[6] Jamil, F., et al. A novel medical blockchain model for drug supply chain integrity management in a smart hospital. Electronics. 2019, 8(5), 505. https://doi.org/10.3390/electronics8050505

[7] Nair, A. R., Gupta, R., Tanwar, S. FAIR: A blockchain-based vaccine distribution scheme for pandemics. In Proceedings of IEEE Globecom Workshops (GC Wkshps). 2021, pp. 1–6. https://doi.org/10.1109/GCWkshps52748.2021.9682114

[8] Javed, I. T., et al. PETchain: A blockchain-based privacy enhancing technology. IEEE Access. 2021, 9, 41129–41143. https://doi.org/10.1109/ACCESS.2021.3064896

[9] Musamih, A., et al. Blockchain-based solution for distribution and delivery of COVID-19 vaccines. IEEE Access. 2021, 9, 71372–71387. https://doi.org/10.1109/ACCESS.2021.3079197

[10] Sharmila, S.; Bhushan, S.; Kumar, P.; Garg, A. K.; Nair, S. Blockchain Powered Vaccine Efficacy for Pharma Sector. Computational and Mathematical Methods in Medicine, 2022, Article ID 4862742. https://doi.org/10.1155/2022/4862742

[11] Song, S., et al. Traceability of product supply chain based on Hyperledger Fabric. In 4th International Conference on Advanced Information Science and System (AISS). 2023, pp. 1–6. https://doi.org/10.1145/3573834.3574546

[12] Laishevskiy, A., Barger, A., Gorgadze, V. A journey towards the most efficient state database for Hyperledger Fabric. In 2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). 2023, pp. 1–3. https://doi.org/10.1109/ICBC56567.2023.10174970

[13] Vidwans, S., et al. Permissioned blockchain voting system using Hyperledger Fabric. In 2022 International Conference on IoT and Blockchain Technology (ICIBT). 2022, pp. 1–6. https://doi.org/10.1109/ICIBT52874.2022.9807702

[14] Yu, G., Wu, B., Niu, X. Improved blockchain consensus mechanism based on PBFT algorithm. In 2nd International Conference on Advances in Computer Technology, Information Science and Communications (CTISC). 2020, pp. 14–21. https://doi.org/10.1109/CTISC49998.2020.00009

[15] Aleksieva, V., Valchanov, H., Huliyan, A. Implementation of smart contracts based on Hyperledger Fabric blockchain for insurance services. In International Conference on Biomedical Innovations and Applications (BIA). 2020, pp. 113–116. https://doi.org/10.1109/BIA50171.2020.9244500

[16] Naveen, P., et al. Traceability of tea powder supply chain based on Hyperledger Fabric. In 3rd International Conference on Smart Electronics and Communication (ICOSEC). 2022, pp. 303–307. https://doi.org/10.1109/ICOSEC54921.2022.9952056

[17] Jadhav, S. V., et al. Decentralized data storage solutions using Hyperledger Fabric. In International Conference on Signal Processing, Computation, Electronics, Power and Telecommunication (IConSCEPT). 2023, pp. 1–6. https://doi.org/10.1109/IConSCEPT57958.2023.10170327

[18] Raj, A., et al. Enhancing security feature in financial transactions using Multichain-based blockchain technology. In 4th International Conference on Intelligent Engineering and Management (ICIEM). 2023, pp. 1–6. https://doi.org/10.1109/ICIEM59379.2023.10166589

[19] Kuzlu, M., et al. Performance analysis of a Hyperledger Fabric blockchain framework: Throughput, latency, and scalability. In 2019 IEEE International Conference on Blockchain (Blockchain). 2019, pp. 536–540. https://doi.org/10.1109/Blockchain.2019.00003

[20] Kaushal, R. K., Kumar, N. Exploring Hyperledger Caliper benchmarking tool to measure the performance of blockchain-based solutions. In 11th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO). 2024, pp. 1–6. https://doi.org/10.1109/ICRITO61523.2024.10522188

[21] Abbas, S., Sultana, A., Lin, W. Enhancing throughput in Hyperledger Fabric through endorsement policy strategy. In 27th International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD). 2024, pp. 195–199. https://doi.org/10.1109/SNPD61259.2024.10673946

[22] Owivri, O. C., et al. A decentralised framework for issuing electronic exam pass using Hyperledger Fabric. In SEB4SDG 2024 Conference. 2024, pp. 1–6. https://doi.org/10.1109/SEB4SDG60871.2024.10630342

[23] Wickremasinghe, G., et al. Demonstrating a Hyperledger Fabric-based blockchain with knowledge graphs for a supply chain ecosystem. In IEEE International Conference on Blockchain and Cryptocurrency (ICBC). 2024, pp. 15–16. https://doi.org/10.1109/ICBC59979.2024.10634370

[24] Li, Y., et al. An extensible consensus algorithm based on PBFT. In 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC). 2019, pp. 17–23. https://doi.org/10.1109/CyberC.2019.00013

[25] Capocasale, V., Gotta, D., Perboli, G. Comparative analysis of permissioned blockchain frameworks for industrial applications. Blockchain: Research and Applications. 2023, 4(1), 100113. https://doi.org/10.1016/j.bcra.2022.100113