Privacy Preserving Authentication of IoT and Blockchain-Enabled Supply Chain Management

A. S. Sangeetha[1], S. Shunmugan[2]

[1]Register No: 20123152292036, Research Scholar, Department of Computer Applications, S.T.Hindu College, Nagercoil, Affiliated to Manonmaniam Sundaranar University, Abhishekapatti, Tirunelveli-627012, Tamilnadu, India.
Email: asn.sangeetha84@gmail.com

[2]Associate Professor, Department of Computer Science, S.T.Hindu College, Nagercoil, Affiliated to Manonmaniam Sundaranar University, Abhishekapatti, Tirunelveli-627012, Tamilnadu, India.
Email: shunsthc@gmail.com

KEYWORDS

IoT, Blockchain, Hyperledger, Smart Contract, Supply Chain

ABSTRACT:

Securing the legitimacy of credentials and protecting the privacy of sensitive information have become crucial in the constantly changing world of supply chain management. Despite the fact that IoT-based supply chain management excels at providing real-time data and prompt responses, it may have trouble maintaining data security, integrity, and trust. The core components of our proposed framework include IoT sensors, smart contracts, and the Hyperledger blockchain. Through this integration, we establish a robust and transparent system for verifying the authenticity of the products. One of the most promising technological advancements is the convergence of Hyperledger blockchain and the Internet of Things (IoT), a synergy that promises to revolutionize the way supply chains are managed and secured. This innovative approach not only enhances trust among supply chain participants but also contributes to the overall efficiency, transparency, and security of global supply chains. This article presents a comprehensive evaluation of our framework's performance, including scalability, security, and usability aspects.

1. Introduction

In the rapidly evolving landscape of supply chain management, the integration of cutting-edge technologies has become essential to address the complexities and challenges that businesses face in today's globalized economy. According to the World Health Organization (WHO), counterfeit and substandard pharmaceuticals are responsible for over a million annual fatalities and $21 Billion in economic damage worldwide. Supply chains have historically been plagued by issues such as transparency, traceability, and trust among stakeholders. Counterfeit products, unauthorized access to data, and inefficiencies in record-keeping have all contributed to significant losses for businesses.

The four types of blockchain are: Public Blockchain, Private Blockchain, Hybrid Blockchain, Consortium or Federated Blockchain. Public Blockchain is permission less which means it allows any participant to participate in the network anonymously. Bitcoin network is an example of public

blockchain. Private Blockchain is a permissioned blockchain which works on access control i.e. it will be managed by an administrator and participants require permission to join the network as it focuses more on privacy. The performance of this network is faster as it has limited number of nodes. For example, Walmart uses the IBM Food Trust platform, which was built using Hyperledger Fabric and runs on the IBM cloud. Hyperledger projects are an example of private blockchain. Hybrid Blockchain is a combination of both private and public blockchain which is widely used in many organizations. It works in a closed ecosystem, can impose or change the rule anytime, lower the transaction cost and protects from 51% attack. The Consortium or Federated Blockchain is similar to hybrid blockchain but it is different in the sense that multiple organizations collaborate in a decentralized network. It is less transparent when compared to public blockchain but it is more secure, efficient and scalable than it. It also has access controls. For example, R3 Corda for financial institutions lowers friction in financial processes and streamlines interbank transfers.

The Internet of Things (IoT) has become more widespread as Information and Communication Technologies (ICT) and Robotics have converged, particularly in Supply Chain Management[1]. Security is a paramount concern due to the susceptibility of IoT devices to cyberattacks, raising issues regarding data privacy and integrity. The most essential concern when using IoT in supply chains is securing IoT devices and data exchanged by the devices. The integration of blockchain with IoT improves the traceability and tracking of commodities from point of origin to point of destination. Due to the traceability of goods during their entire course across the supply chain, blockchain technology can help increase customer trust on products.

This article discovers how the convergence of a permissioned Blockchain network and IoT, a network of interconnected devices capable of collecting and sharing real-time data is poised to disrupt traditional supply chain paradigms and usher in a new era of trust, transparency, and efficiency in the world of commerce.

2. Background

Integrating IoT and the Hyperledger blockchain into supply chain management (SCM) can enhance transparency, traceability, and security. Blockchain-enabled cargo containers and associated sensors will produce an unchangeable, fully traceable system that can be outfitted with smart contracts to automate tasks like payment executions, like clearing customs. When coupled with technology that supports cryptocurrency, blockchain dramatically improves supply chain security across the board[2]. In this section, the structure and features of Hyperledger blockchain, the security issues in IoT-enabled SCM, and the importance of the convergence of IoT and blockchain are discussed.

2.1. Hyperledger Blockchain:

Hyperledger is an umbrella project under The Linux Foundation that has emerged as a strong and adaptable blockchain platform which has support for permissioned networks, modular architecture, and interoperability capabilities, to meet the various demands of enterprise-level applications. As blockchain technology develops, Hyperledger remains at the cutting edge of innovation, enabling

companies to use distributed ledger technology to improve their business processes and build more secure, transparent, and more effective systems. Some of the prominent Hyperledger projects are given in the Table-1.

Table-1: Different Hyperledger projects and their features

Hyperledger Projects	Primary Focus	Use Case	Consensus Algorithm	Smart Contracts/ Chaincodes
Fabric	Enterprise level	Supply Chain Management, Finance and Healthcare	Practical Byzantine Fault Tolerance and Raft, Kafka, Solo	Chaincodes can be written in Go, Node.js, or Java
Sawtooth	Application with high throughput and dynamic participation	Supply Chain Management, Finance and Healthcare	Proof of Elapsed Time (PoET) and supports pluggable consensus	Solidity (Ethereum-compatible) and WebAssembly (WASM)
Indy	Decentralized identity management and verifiable credentials	Background Verification, Digital Identity management	Plenum Consensus Algorithm	No chaincode or smart contracts, instead SDKs and APIs
Composer	To provide a modular, scalable, and flexible framework	Decentralized Applications (dApps)	Proof of Elapsed Time (PoET) and supports pluggable consensus	Composer Modeling Language (CML)
Besu	Ethereum client built on the Java Virtual Machine (JVM) to provide compatibility with Ethereum network	Tokenization of assets, supply chain, finance, identity, and any Ethereum ecosystem	Proof of Work (PoW), Proof of Authority (PoA)	Solidity
Aries	decentralized identity management and interoperability.	Self-Sovereign Identity systems	No Consensus protocol	doesn't directly support smart contracts
Caliper	Designed for measuring the performance of blockchain networks.	Platform-agnostic and can be used to benchmark different blockchain platforms	The consensus mechanism is inherent from the tested platform	Users need to provide the smart contracts they want to test

2.2. Security threats in IoT enabled SCM:

The global IoT industry is expected to reach $1.6 trillion by 2025. As the number of IoT-enabled applications grows, the technology will face new security concerns and issues. Manufacturers will keep on producing devices with poor security as there are no global IoT security standards. Manufacturers who have started integrating Internet connectivity into their devices might not always prioritise "security" during the product development process. IoT physical device attack, Encryption key attacks, Denial of Service(DoS) attack, Firmware Hijacking, Man-in-the-Middle attack, Ransomware attack, Spying, Privilege Escalating attack, Brute Force Password attack are some of the types of security attacks in IoT. In the present centralised Internet of Things (IoT) architecture, data collection and processing from different IoT objects are fully controlled by a third-party central authority, with no explicit limitations on the data's usage[3]. Consent to collection, transparency, and access to personal

information are among the special difficulties to information privacy presented by this extensive data gathering and processing. Moreover, centralized architecture's constraints and the heterogeneity of IoT devices and data create problems and obstacles for the implementation of optimal access control solutions for the Internet of Things. Strong security standards that protect personal data are essential as the number of IoT devices rises. These requirements should include data encryption, behavior monitoring, and having a reaction plan in place for security issues. Elliptic Curve Cryptography[4] is highly efficient, offering robust security with smaller key sizes compared to traditional algorithms like RSA, thus reducing computational overhead. This lightweight nature aligns well with the resource-constrained environment of blockchain-enabled vaccine supply chains, ensuring data integrity and authenticity while conserving energy and memory.

2.3. Importance of IoT and Blockchain Integration in VSCM:

Plans for a pandemic that rely on IoT and blockchain must be devised in order to keep businesses working. According to the World Economic Forum, "Blockchain technology can overcome supply chain issues revealed by SARS-CoV-2 and can enhance economic recovery." Blockchain technology can strengthen Internet of Things' privacy and reliability concerns. Blockchain-enabled IoT applications can keep track of billions of connected devices, enabling device coordination and transaction processing, which significantly lowers the cost of production for IoT sector players. The SSI system relies on decentralized registers of information and digital wallets to manage identifiers, authenticators, data, and verifiable credentials

3. Methodology

By following the below methodology, a robust IoT and Hyperledger blockchain-enabled supply chain management system can be created that enhances transparency, security, and efficiency while ensuring the safe and timely delivery of vaccines/food products.

3.1. Needs Assessment and Planning:

It is necessary to identify the specific needs and challenges of vaccine supply chain, such as temperature control, tracking, and authentication. The key performance indicators (KPIs) such as Vaccine Availability, Lead Time, Fill rate, Order Accuracy, Inventory Turnover, Temperature Control, Distribution Efficiency, Wastage Rate, Order-to-Delivery Time, Vaccine Tracking Accuracy, Customer Satisfaction, Supply chain Visibility, Security and Anti-Counterfeiting, and Supplier Performance need to be defined.

3.2. IoT Device Selection and Deployment:

The IoT devices such as sensors, RFID tags, temperature monitors are suitable for monitoring and collecting data about vaccines. IoT devices are deployed at critical points within the supply chain, including manufacturing facilities, warehouses, transportation, and storage locations. Ensuring strong security standards secure personal data when deploying IoT devices is crucial. This includes encrypting data, keeping an eye out for odd behaviour, and putting a plan in place for handling security problems.

3.3. Data Collection and Monitoring:

The real-time data from IoT devices, including temperature, location, and condition of vaccines are collected. Data analytics can be implemented to process and analyze the collected data for insights into the supply chain's performance.

3.4. Hyperledger Blockchain Integration:

Appropriate Hyperledger framework (e.g., Hyperledger Fabric) based on the supply chain's requirements must be selected. Smart contracts need to be defined to automate processes like quality checks, payments, and alerts based on predefined criteria.

3.5. Data Encryption and Security:

Encryption and authentication mechanisms must be implemented to secure data transmitted from IoT devices to the Hyperledger blockchain.

3.6. Real-time Tracking and Traceability:

IoT sensors and GPS technology must be enabled for real-time tracking of vaccine shipments. The immutable ledger of all transactions ensures the end-to-end traceability.

3.7. Quality Control and Compliance:

Automated quality control checks using IoT sensors to monitor temperature, humidity, and other relevant parameters and compliance with regulatory standards and guidelines by integrating them into the Hyperledger smart contracts must be ensured.

3.8. Alerts and Notifications:

Automated alerts and notifications triggered by IoT data anomalies, such as temperature excursions or delays in transit. These alerts can prompt rapid response actions to prevent spoilage or theft.

4. Blockchain Integrated Vaccine Supply Chain Management (VSCM)

LARRY ST ONGE, DHL President, Life Science and Healthcare, represents covid-19 vaccine distribution as “The biggest global logistics since World War II”. To put an end to the SARS-CoV-2 epidemic, a huge portion of the population must be immune to the virus. Vaccines are the only solution that humanity has depended on to reduce the mortality toll from infections. If a vaccination is not widely distributed and highly trusted, it would not be as successful. Distributors can receive real time information and improved response capabilities to supply chain issues. Stock control and safety monitoring should be improved by the dispensers. Consumers may trust the immunizations and return to normal life with confidence.

4.1. Challenges of VSCM:

The main issue in managing a Vaccine Supply Chain is that each stage's suppliers must be trusted. Humans are untrustworthy, and the system is vulnerable to corruption. Hoarding, fake medical camps, black marketing, suppliers behaving as crony capitalists, resource exploitation, and so on are some of the most common examples. Moreover the challenge of storing the vaccine in cold storage is a

necessity. Nearly 3 million people live in areas that lack temperature controlled storage to deliver the covid -19 vaccines. The journey of a vaccine from production to distribution is complex for many reasons.

4.2. Blockchain and IoT in Vaccine Distribution

Blockchain Distributed Ledger Technology is unique in that it provides a transparent shared system of record that is based on immutable data for all supply chain actors. Throughout shipment, IoT sensors track the temperature of the vaccines. The blockchain ledger records all the key IoT events, such as the time of the vaccine supply, temperature maintained throughout the shipment, duration etc. When the temperature in vaccine storage falls below an acceptable threshold, smart contracts alert all the stakeholders, allowing the supply to be recovered and promptly transported to proper cold storage. There are no arguments about the condition and placement of the vaccination, and there is no need to reconcile a tangled web of distinct siloed systems, because the immutable blockchain data are independently verifiable by every node. The status of vaccine supply is made public, allowing for more informed and effective decision-making. Fig.1. explains the use of IoT and Blockchain in VSCM.

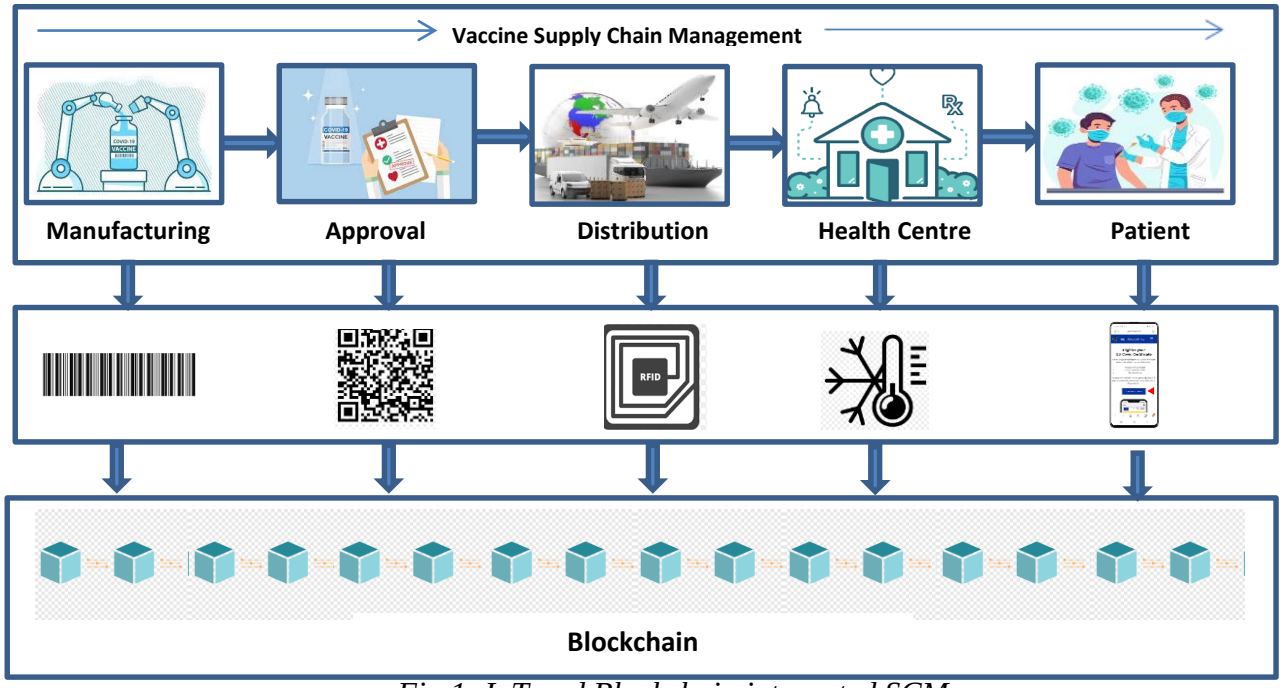

Fig.1: IoT and Blockchain integrated SCM

Pfizer and other leading companies are using blockchain technology to improve the complex vaccine supply chain management. The steps involved in Pfizer vaccine supply chain is given below.

1. The Pfizer vaccines are kept in a specialized container which contains 50 pounds of dry ice filled by hands. This is how the vaccine is kept cold for 10 days.
2. Boxes with 1000 dozes will leave Pfizer's Kalamazoo Michigan with 50 pounds of dry ice in Fedex, UPS and DHL trucks.
3. Depending upon the destination, containers will be delivered by truck or air planes.

4. The containers will have sensors inside to monitor temperature and location as they are shipped.
5. DHL is trading international deliveries that can take as long as 3 days.
6. For every box of vaccine there are dozens of boxes of supporting materials like syringes, swabs and many, shipped separately that must arrive in time to give the lifesaving medicine.

5. Discussion

In the context of vaccine supply chain management, three key concerns are vaccine quality, demand forecasts, and stakeholder trust as these problems are now much more difficult to deal with in light of the latest COVID-19 epidemic[5]. Counterfeit pharmaceuticals account for 70% of all drugs in some countries' supply chains. A recent blockchain trial conducted by KPMG, Merck, Walmart, and IBM instills fresh faith in the system by cutting the time it takes to trace prescription medicines from 16 weeks to just 2 seconds.

[6]proposed a robust Hyperledger blockchain-enabled forward and backward supply chain management system that enables manufacturers to monitor their drug supply to minimize the cost and time to transfer the drug to the end-user. AgriBlockIoT [7] is an integration of IoT and Blockchain implemented over Ethereum and Hyperleger Sawtooth. Pfizer uses an iPhone Operating System based application known as KitChain. It is designed to track and trace the supply chain workflow. It provides an immutable ledger for inventory and shipment tracking. The application is built on top of Hyperledger Fabric, which is an open-source Linux Foundation project. It enables users to send messages between the shippers, recipients and third parties.

In comparison to Ethereum's PoW or PoS consensus process, Hyperledger Fabric uses the Practical Byzantine Fault Tolerance (PBFT) consensus protocol, which offers a lower communication cost for broadcasting messages[8]. As a result, the Hyperledger blockchain's throughput will be increased. Because PBFT cannot tolerate more than 1/3 server failure network, Hyperledger is affected in the event of a crash failure. The supply chains use a query-answer model-based service like Hyperledger to verify the virtual IDs of IoT devices based on their most recent activity. Hyperledger fabric does not have gas fees, so that the transaction cost are generally predictable. Fabric supports Go, Java, and Node.js for writing smart contracts, whereas Ethereum supports solidity, which have a steeper learning curve for developers new to blockchain.

6. Conclusion

This paper explores the modern blockchain technology used in Supply Chain Management by pharmaceutical companies. The integration of IoT and Blockchain technology will be an ultimate way of securing the data from fraudsters and is used extensively in VSCM projects. Blockchain technology is being used by leading organizations like as Pfizer Inc., Premier Inc., McKesson Corporation, and others to improve the difficult process of chargebacks. Hyperledger Fabric undoubtedly stands out as a superior choice for businesses seeking a robust, predictable, and permissioned blockchain solution. Its continuous growth, support from the Linux Foundation, and robust ecosystem make it a strong contender in the ever-evolving world of enterprise blockchain technology.

7. References

[1] A. Rejeb, J. G. Keogh, and H. Treiblmaier, "Leveraging the Internet of Things and blockchain technology in Supply Chain Management," *Futur. Internet*, vol. 11, no. 7, pp. 1–22, 2019, doi: 10.3390/fi11070161.

[2] Deloitte, "IoT powered by Blockchain: How Blockchains facilitate the application of digital twins in IoT," p. 20, 2018.

[3] L. Cocco, R. Tonelli, and M. Marchesi, "Blockchain and self sovereign identity to support quality in the food supply chain," *Futur. Internet*, vol. 13, no. 12, Dec. 2021, doi: 10.3390/fi13120301.

[4] A. Abirami and S. Palanikumar, "ECC Based Encryption for the Secured Proactive Network Forensic Framework," *Iraqi J. Sci.*, vol. 65, no. 1, pp. 381–389, 2024, doi: 10.24996/ijs.2024.65.1.31.

[5] H. Hu, J. Xu, M. Liu, and M. K. Lim, "Vaccine supply chain management: An intelligent system utilizing blockchain, IoT and machine learning," *J. Bus. Res.*, vol. 156, no. March 2022, p. 113480, 2023, doi: 10.1016/j.jbusres.2022.113480.

[6] D. Agrawal, S. Minocha, S. Namasudra, and A. H. Gandomi, "A robust drug recall supply chain management system using hyperledger blockchain ecosystem," *Comput. Biol. Med.*, vol. 140, p. 105100, Jan. 2022, doi: 10.1016/j.compbiomed.2021.105100.

[7] M. P. Caro, M. S. Ali, M. Vecchio, and R. Giaffreda, "Blockchain-based traceability in Agri-Food supply chain management: A practical implementation," *2018 IoT Vert. Top. Summit Agric. - Tuscany, IOT Tuscany 2018*, pp. 1–4, 2018, doi: 10.1109/IOT-TUSCANY.2018.8373021.

[8] A. S. Sangeetha, S. Shunmugan, and G. Murugan, "Blockchain for IoT enabled supply chain management - A systematic review," *Proc. 4th Int. Conf. IoT Soc. Mobile, Anal. Cloud, ISMAC 2020*, pp. 48–52, 2020, doi: 10.1109/I-SMAC49090.2020.9243371.