HCIS | Human-centric Computing and Information Sciences

RESEARCH (Research Manuscript) **Open Access**

Human-centric Computing and Information Sciences (2023) 13:04
DOI: https://doi.org/10.22967/HCIS.2023.13.004
Received: January 20, 2022; Accepted: February 5, 2022; Published: January 30, 2023

Supply Chain Management Using an Industrial Internet of Things Hyperledger Fabric Network

Muhammad Rehan[1], Abdul Rehman Javed[2,3], Natalia Kryvinska[4], Thippa Reddy Gadekallu[3,5,*], Gautam Srivastava[6,7,8], and Zunera Jalil[2]

Abstract

Supply chain management (SCM) plays a pivotal role in the industrial life cycle. On-time delivery is necessary for a successful SCM system. To maintain a safe and secure supply of products, mode of transportation and management is equally important. The Industrial Internet of Things (IIoT) eases tracking and tracing of supplies using sensor devices and 5G during the supply chain process. Cold chain and ecologically sensitive products such as vaccines, medical supplies, and food items require a specific temperature to maintain the supplies' genuineness and actuality. A blockchain-based platform (Ethereum) is being used for SCM nowadays. However, it has certain limitations, such as low transaction speed, the requirement for more computation power, and vulnerability to cyberattacks. This research proposes a solution to these problems using a novel approach, named SCMIIOT (supply chain management using industrial Internet of Things). The proposed approach maintains traceability, security, data integrity, transparency, and achieves fast transaction speed. The distributed database system is used to store and transfer transaction ledgers for SCM. In this research, IBM Watson IoT is used as an Internet of Things (IoT) device for input temperature, and the Kubernetes cluster is used as a platform for deploying Hyperledger Fabric. Docker Hub and Hyperledger composer playground provide business network connection for importers, suppliers, retailers, manufacturers, and consumers/end-users. We also demonstrate the working and effectiveness of SCMIIOT through experiments. Results show that SCMIIOT takes only 1 minute to copy local files to storage on the cloud and takes 1 minute to create a genesis block. Similarly, it takes 1 minute for a peer-to-peer connection. Also, the worst-case time complexity of SCMIIOT transaction speed is recorded as 48 seconds on the Watson IoT platform.

Keywords

Supply Chain Management, Blockchain, Industrial Internet of Things, Internet of Things

1. Introduction

***Corresponding Author:** Thippa Reddy Gadekallu (thippareddy.g@vit.ac.in)
[1]Department of Computer Science, Air University, Islamabad, Pakistan
[2]Department of Cyber Security, Air University, Islamabad, Pakistan
[3]Department of Electrical and Computer Engineering, Lebanese American University, Byblos, Lebanon
[4]Information Systems Department, Faculty of Management, Comenius University in Bratislava, Bratislava, Slovakia
[5]School of Information Technology and Engineering, Vellore Institute of Technology, India
[6]Department of Math and Computer Science, Brandon University, Manitoba, Canada
[7]Research Centre for Interneural Computing, China Medical University, Taichung, Taiwan
[8]Department of Computer Science and Mathematics, Lebanese American University, Beirut, Lebanon

Supply chain management (SCM) needs to be tamper-proof, fast, secure, and traceable to meet consumers' demands [1]. While using the industrial Internet of Things (IIoT)-based sensor devices, some challenges such as security, speed, and reliability have to be addressed. With the advent of IIOT, SCM is more vulnerable to cyber-attacks, which is a significant challenge. Supply chain management is about managing information, administration, and modified packaging process and arrangements of supply items in the current era. Beneficiaries of this proposed research work are medical suppliers, food suppliers, heat-sensitive products, and suppliers.

In a general SCM system, the following actors or roles are the key stakeholders: supplier, manufacturer, importer, regulator, retailer, and consumer/end-user. All these actors have their roles and responsibilities. The supplier provides the quality raw material by following the manufacturer's preventive measures; the manufacturer supplies the product to the importer, transfers the product to the regulator, transfers the product to the retailer, and delivers the final product to the consumer/end-user. In all these steps, the supply chain system maintains the actuality and genuineness of the product. A complete supply chain record should be traceable, secure, and tamper-proof from supplier to consumer [2].

A supply chain starts with crude material from a supplier to a creator and terminates with the finished goods' transport to the end-user/client. The SCM is made up of components such as transportation management, storage, inventory management, planning development management, performance management, strategic planning, information technology, and marketing [2]. In a conventional supply chain, complex documents or ledger transactions are maintained manually. It was simple and easy to operate but was costly to manage in terms of time, and it was hard to audit records and predict sales [3]. Rapid advancements in the supply chain were induced after the digitization of the supply chain [4]. The supply chain process involves accessibility, development, and cost of physical resources. Food and drug items often have specific warehouse needs. Besides, ventures see the incentive to share warehouses rather than own warehouses to reduce operating costs. Heat and sensitive ecological supplies require a specific environment for storage. Warehouse containers need to be traceable and transparent to end users. In the whole SCM environment, every step needs to be transparent and traceable to end users. IIoT sensors are available for delicate items that can record temperature, mugginess, vibration, and other ecological conditions [5]. SCM influences supply items, administration, quality, convenience, costs, and most importantly, productive client experience. A smart and well-managed SCM reduces manufacturing costs, preserves product integrity, saves time, and as a result, can give a competitive edge to the company over its peers.

In a conventional SCM, supplies are not secure enough to maintain data integrity and confidentiality due to the involvement of third parties [6]. Blockchain is a straightforward, changeless, and secured distributed system; it is often seen as a game-changer in SCM as it provides a clear supply chain structure. Blockchain offers the following features for SCM: tracking products in the entire supply chain process, authentication, verification of the product's genuineness, sharing the whole chain information between supply chain actors, and providing better auditability. A distributed blockchain-based Hyperledger Fabric network can handle the challenges like traceability, immutability, and detectability and examine the supply item's actuality. Every node in this chain would be secure. A smart contract or chain code is pluggable and flexible enough to accommodate a versatile collection of IIoT [7]. In a supply chain, it can apply to anything from self-executing supply arrangements to the mechanized cold supply chain [8].

Blockchain is a disruptive technology that provides trust and straightforwardness to the business where the value-based procedures are significant [9–11]. It is a scattered, progressed collection of records that works in blocks and exists in various copies spread over diverse peers, customarily known as nodes [12]. Blockchain can be public, private, or based on a consortium.

Public blockchain: This configuration infers that the data and admittance to the system are available to any person who is anxious to take an interest. Bitcoin, Ethereum, and Litecoin blockchain frameworks are a few examples.

Private blockchain: Unlike a public blockchain, the private blockchain is controlled unmistakably by customers from a specific affiliation or endorsed customers.

Consortium blockchain: This type of blockchain involves two or three affiliations. The consortium blockchain network gives controlled access to the system. In a consortium, frameworks are set up and obliged by the preliminary consigned customers.

Advanced SCM demands transparency and secure delivery of product items. In the delivery of heat-sensitive product items, desired temperature and ecological environment are necessary [1]. A little ignorance may be disastrous because medical supplies and other items are sensitive to heat and cannot be compromised. Therefore, real-time tracking of the temperature of the supplies from the manufacturer to the consumer by recording a product's details in an entire transaction ledger is the primary goal of this research [12].

Ethereum network is used for SCM, particularly for delivering heat-sensitive products, but this is vulnerable to a single point of failure and may compromise IoT devices' security. Ethereum network does not have any authorization mechanism for public IoT devices, therefore, there it needs a mechanism to authorize public IoT devices in the network. The authorization mechanism needs to connect all network devices to a centrally administered mechanism that will authenticate and identify IoT devices to enroll in the Ethereum blockchain. Some authors have tried to propose decentralized authorization mechanisms but have not practically deployed them in industry. Ethereum is a public or private blockchain that does not provide the authorization mechanism for interconnecting IoT devices or nodes and cannot bear IoT devices' load. Artificial intelligence (AI) is only possible with sensor devices, so AI devices could not survive without a secure and trustworthy network protocol. Furthermore, the Ethereum network is not pluggable to various IIoT devices, and transaction speed is limited to 300 transactions per second. Hence, the Ethereum network is not feasible for online transactions in SCM [6]. AI IIoT requires a reliable platform that is secure and fast enough to meet consumer demands. SCMIIOT is a permissioned and distributed blockchain network with a flexible and secure architecture.

The main contributions of this research work are:

- Distributed Hyperledger Fabric blockchain network for supply chain management is proposed to handle the single point of failure problem.
- Flexible chain code is used for IIoT device authorization with high throughput transaction speed.
- The Supply chain consensus algorithm provided privileges to access the system to all the stakeholders.
- Minimize the likelihood of cyber-attacks, particularly ransomware attacks using membership service providers and certificate authorities that use cryptographic keys for shared members in the network.

The rest of the paper is organized as follows. Section 2 presents the background of the research study for SCM using AI IIoT. Section 3 offers state-of-the-art related work for SCM. Section 4 discusses the proposed solution using distributed Hyperledger Fabric network. Section 5 presents the experimental setup details for the deployment of the proposed solution. Section 6 evaluates the results and features of the proposed solution. Finally, Section 7 concludes the article with recommendations for future research.

2. Related Work

IIoT has changed manufacturing and the supply chain by tracking records and supplies. The world is moving towards digitization rapidly, and particularly in 2021, digitization is necessary. It has changed the way people communicate, do their businesses, and perform their day-to-day tasks. It has affected the manufacturing and supply chain industry as well. As technology gets advanced, automation comes along. With automation and digitization, comes the possibility of encountering cyber-attacks. Maintaining data integrity, privacy-preserving, and avoiding DDoS attacks is very critical [1].

Blockchain is a stimulating new alternative to the standard money, united banking, and trade procedures that are revolutionizing how we handle cash-related trades. Blockchain is a scattered, progressed record with various copies spread over multiple nodes. A blockchain network is a chain of blocks connected as distributed databases. Each block has the data information, a pointer to the previous block, and a pointer to the next block. In addition, each block has a hash function that validates the block before entering the

chain of blocks in the network. Ethereum is used as a public blockchain to develop smart systems and DAPPs [13].

Kim et al. [14] proposed a Hyperledger Fabric-based blockchain as a service to address IIoT-based AI devices. In this work, the authors addressed the low-power and low-storage IoT devices for configuration and modelling in the blockchain system. Pustisek et al. [7] proposed Hyperledger Fabric, where its architecture, designs, solutions, deployment results, and distributed application programming model are addressed. Blossey et al. [2] proposed supply chain solutions with application perspectives and their limitations are compared with a decentralized system. Pesic et al. [3] proposed multiple solutions for current problems to tackle AI devices and their limitations for usage in currently designed systems. Industrial IoT is used to ease the tracking and tracing tasks for the supply chain using distributed databases and trustless blockchains in future work. Hammi et al. [15] proposed IoT devices' credibility to secure the blockchain network to gain the benefits of IoT devices. Rouhani and Deters [16] proposed an improved blockchain structure. In the enterprise network, the private chain was used to manage IoT device configuration files in a distributed way. It stores the device configuration files on the blockchain by accessing them with a smart contract. Nakamoto [8] proposed a trustless cash system without third-party involvement by using a peer-to-peer network connection. Androulaki et al. [1] proposed an efficient and safe UAV condition monitoring authentication and data integrity scheme by using a blockchain database network.

Reyna et al. [17] proposed a mechanism to monitor food items using immutable blockchain trustless databases. The authors of [2] proposed a scalable and flexible security architecture for IoT devices for wireless AI sensor devices, and its performance was compared with the existing management solutions. They discuss how Ethereum can offer some benefits like tested development architecture and a skilled developer community. Ethereum is an open-source platform primarily used for cryptocurrencies, but developers are also using it for developing smart apps with a combination of IoT devices. Halldorsson et al. [18] proposed an explanation behind the traditional supply chain is the absence of transparency. Decentralized databases are mainly used for the SCM data records and IIoT for sensing data information. The heat-sensitive product industry’s supply chain use case is a complicated landscape, where multiple actors need to work to deliver the goods to the final destination.

In [5], the Kubernetes cluster is a central pillar for all the deployment as all peers, networking, and blockchain are implemented on this platform. On the other side, the Docker Hub meets the requirement of containerized apps to interact and develop. Docker hub brings developers together to work on public or private project repositories. Organizations are perfect for teams that can control who can create and view repositories and push and pull the changes. Two-factor verification builds the security of records by requiring two distinct types of approvals. This guarantees that they are legitimate record owners. Authors in [19] presented an analysis of Internet of Things research in SCM. Authors in [20] presented a survey on SCM. Authors in [21] presented the potential of Industry 4.0 for SCM within the triple bottom line of sustainability. The authors in [21, 22] presented various approaches for SCM. Table 1 summarizes the existing relevant studies [2, 3, 6, 7, 14, 15, 17].

3. Proposed Model

To overcome the limitation of previous SCM approaches, we propose SCMIIOT, a novel method for SCM using distributed Hyperledger Fabric blockchain network. The proposed approach helps in making a traceable, secure, and fast SCM. SCMIIOT can be employed to monitor natural conditions for a blockchain network that incorporates refrigerated medical supplies, garden plant shipments, or any transient things sensitive to temperature, moisture, and time. SCMIIOT uses a distributed network of databases without any third-party involvement. Therefore, it is unchangeable and remotely accessible for real-time data communication.

Table 1. Comparative analysis of existing SCM approaches

Study	Year	Proposed mechanism	Evaluation Method	Limitations
Reyna et al. [17]	2021	Unmanned robotic agriculture transportation	Smart agriculture	Experimented in a closed environment that is not feasible practically
Park et al. [6]	2020	Privacy control of UAVs using blockchain cryptography	Wireless autonomous cryptography hashes	Technology dependent, not pluggable to other devices
Kim et al. [14]	2019	Proposes the direction of recent studies and developments regarding the smart contract	Performance of the blockchain-based solutions	The huge gap between the blockchain-based solution and current applications' performance
Pustisek and Kos [7]	2018	Authenticates the public nodes of IoT devices network that are susceptible to security risks	Practically not applicable, experimented in custom lab	Limited device-to-device communication and is energy inefficient
Blossy et al. [2]	2018	Secure the more significant number of vulnerable IoT devices	Security requirements for IoT along with the existing attacks, threats, and state-of-the-art solutions	Security concerns are only assumed in a simulated environment and are not practically applicable
Pesic et al. [3]	2018	Proposes a framework with layers, intersect, and self-organization blockchain structures (BCS)	IoT device credibility verification method based on blockchain technology	51% of the computation problems are still not effectively addressed
Hammi et al. [15]	2017	IoT devices and remote blockchain clients to further reduce the network traffic and enhance security	RPI v3B embedded system with a wired internet connection	Network load measurements and traffic profiling

In the conventional supply chain business model, a few techniques are utilized to ensure privacy, such as the blend of secure multiparty calculation cryptography strategies with hazard-recognizable proof algorithms from interpersonal organization investigation, differential privacy, bidirectional productivity privacy adaptable validation convention, public-key cryptography, symmetric encryption, message verification codes, and randomized read admittance control. The benefits of these techniques can validate a bunch of labels with less privacy, diminishing trust issues between supply chain proprietors and label producers, lessening computational and correspondence overhead, and decreasing computational exertion. However, these privacy assurance techniques cannot address the privacy insurance dependent on data exchange and sharing. The security instrument of consensus algorithms incorporates the following four perspectives: firstly, uneven cryptography and zero-information proof separate the transaction information from on-chain records, shielding privacy from the hidden algorithm. Secondly, the executive administration's advanced declaration ensures the organization's authenticity on the blockchain. Thirdly, the plan of multi-channel isolates the data between various channels. At last, privacy information assortment further fulfills the requirement for the segregation of privacy information between various organizations inside a similar channel.

Hyperledger Fabric network is used for data communication, and the IBM IoT Watson platform is used for recording temperature statistics. Furthermore, a pluggable chain code is composed to authenticate and authorize incoming IoT device connections safely. In addition to that, a smart contract is also proposed to maintain business requirements. Finally, the Kubernetes cluster is used for network communication (peer-to-peer connection). Fig. 1 thoroughly demonstrates the proposed system architecture.

DHFBN is based on SCM using distributed Hyperledger Fabric blockchain network, for realizing traceability of the supplies, transaction ledger without any third-party involvement, tamper-proof secure transaction ledger with no single point failure, and surveillance of the temperature of storage container using IoT-based temperature sensor devices. This work uses Hyperledger fabric consortium Distributed

Blockchain applications with IIoT devices for heat and ecologically sensitive products. These products can be refrigerated medical supplies, garden plant shipments, or any transient things sensitive to temperature, moisture, vibration, and time to ensure that safe environmental parameter are provided for the shipment [14].

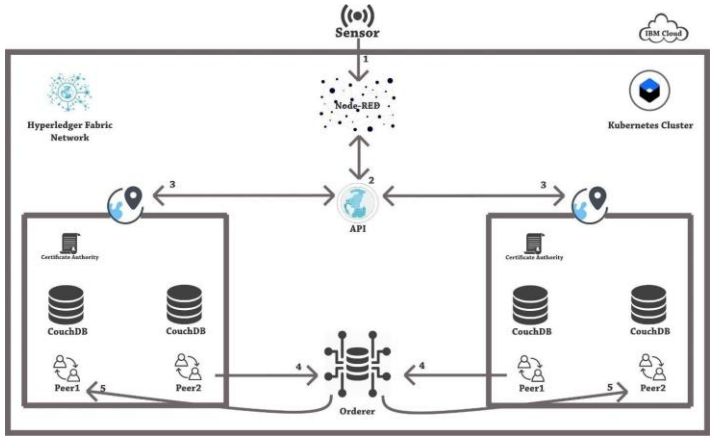

Fig. 1. System architecture.

In response to food contamination scandals worldwide and the significant worldwide problem of contaminated medical supplies, DHFBN tracks and manages the supply chain's temperature using Hyperledger Fabric blockchain technology [23]. We should look at how a transaction is approved to see how Hyperledger Fabric is unique and how it functions in the engine. As an initial step, the client starts a transaction by sending a request to a Hyperledger Fabric-based application client, which presents the transaction proposition for endorsing peers. These peers mimic the transaction by executing the chain code (utilizing a neighborhood duplicate of the state) determined by the transaction and sending back the application's outcomes. Finally, the application consolidates the transaction and communicates it to the ordering service (OS). The OS checks the supports and makes a block of transactions for each channel before transmitting them to all channel peers. At that point, peers will confirm the transactions and submit these transactions [24].

3.1 Components of SCMIIOT

The proposed DHFBM approach is made up of individual components. A brief description of each is as follows:

Chain code: It is a comparable idea to a smart contract in different networks, for example, Ethereum. However, it is a program written in a more significant language, executing against the ledger's current state database.

Channel: It is a private correspondence subnet for sharing confidential data between various network individuals. Every transaction is executed on the channel, which is apparent to the verified and approved parties.

Endorsers: They approve transactions and conjure chain code, sending back the supported transaction results to the calling applications.

Membership service provider: It gives character approval and confirmation forms by giving and approving declarations. It recognizes which certification authorities (CAs) are trusted to characterize the individuals from a trusted space.

Fig. 2 demonstrates the workflow of the proposed SCMIIOT system where the Hyperledger network involves three steps: installation of composer development tools, network configuration, artifact generation, and initiating the service. Finally, the Hyperledger network generates a BNA file deployed locally and on the Hyperledger composer playground.

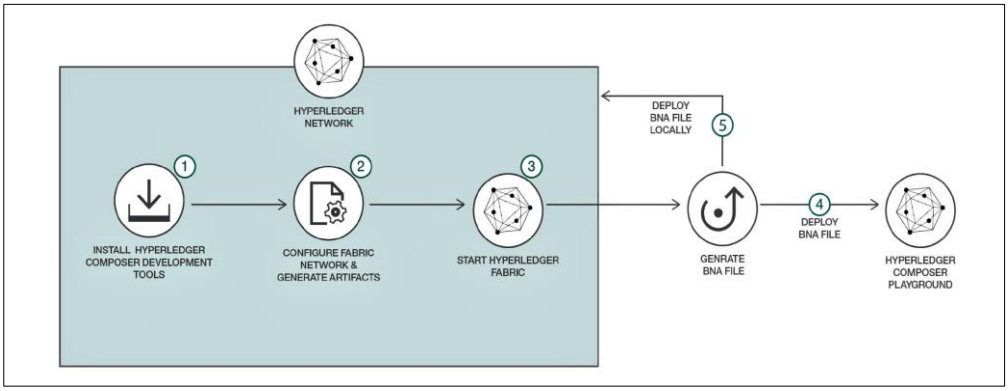

Fig. 2. SCMIIOT system workflow.

Hyperledger Fabric is proposed to create applications or arrangements with a measured design. Hyperledger Fabric permits segments, for example, agreement (consensus) and enrollment (membership) administrations, to be plug-and-play. Its secluded and adaptable plan fulfills a broad scope of industry use cases. It offers a remarkable way to deal with the agreement that empowers execution at scale while safeguarding security and privacy [25].

3.2 Proposed SCMIIOT Algorithm

SCMIIOT involves four actors working around: Supplier, Importer, Retailer, and Regulator. This involves two networks: distributed Hyperledger Fabric blockchain network (DHFBlock) and Hyperledger Fabric business network (HFBusiness).

In SCMIIOT, the createProductlisting function is called when a createProductListing transaction is submitted. It allows a supplier to create a ProductListingContract asset. The transferListing function is called when a transfer listing transaction is submitted by the owner of ProductListingContract. It is submitted either by a supplier to transfer ProductListingContract to an importer or to transfer ProductListingContract to a retailer when the exempt check for the products is completed. The checkProducts function is called when a checkProducts transaction is submitted by the supplier to perform the exempt check for the products present in the ProductListingContract. The status of the ProductListingContract contract will change to CHECKCOMPLETED if all the products are exempted; else the status will change to HAZARDANALYSISCHECKREQ, which means that the supplier needs to provide a hazard analysis report for the products. After submitting the report, the supplier performs the checkProducts transaction to complete the exempt check for the products. The updateExemptedList function is called when a updateExemptedList transaction is submitted by the regulator to update the list of exempted Organization ids and Product ids.

4. Experimental Setup

All details and deployment steps are given in the GitHub repository. The readers may follow step-by-step instructions to achieve desired results (Algorithms 1 and 2).

Algorithm 1. Distributed Hyperledger Fabric Blockchain Network (SCMI-IOT)

Input: *Reading ← CLI Connections*
Output: Network Peers Connections
Evaluation Measures: Localhost Peers, Docker Kubectl nodes, Kubernetes Cluster, REST-API
1: *ConnectCLI* ← [*Input*] {Current Instance}

2: *ConnectLocalHost* ← [*ParsingCouchDB*] {DB Connection}
3: *ConnectDocker* ← [*CLI*] {Kubectl Nodes}
4: *RestApi* ← *CLI* {Connect REST-API}
5: *ConnectChannels* ← [*Peers*] {Join Channel for Peers}
6: *CallKubernetesCluster* ← *IBMCloud* {Connect Watson-IoT IBM *i*}
7: *JoinChannel* ← *NetworkPeers* {Get Network Channels Connection}
8: **return** *NetworkChannelConnection*

Algorithm 2. Hyperledger Fabric Business Network (HFB)

Input: *Reading* ← *CLI Connections*
Output: Network Peers Connections
Evaluation Measures: Composer Playground, NODE-RED, Hyperledger Fabric, Banana File
1: *ConnectHyperledgerComposer* ← *NewBusinessNetwork*
2: *Imports* ← *.BNAfile*
3: *CreateSupplier* ← *GetTokenTest*
4: **if** (*CreateSupplier* ← *GetTokenTest*) **then**
5: *SupplierCall* ← *GetTransactionTest*
6: **if** (*CreateImporter* ← *Manufacturer*) **then**
7: *GetSupplies* ← *RawMaterial*
8: **if** (*CreateRegulator* ← *Supplies*) **then**
9: *RegulateControl* ← *TransactSupplies*
10: **if** (*CreateDistributor* ← *GetTransactSupplies*) **then**
11: *DistributeSupplies* ← *TestSupplies*
12: **if** (*CreateRetailer* ← *GetConsumerSupplies*) **then**
13: *Consumer* ← *TransactSupplies*
14: **end if**
15: **end if**
16: **end if**
17: **end if**
18: **end if**
19: **return** *SuppliesToConsumer* =0

First of all, the installation of prerequisites is required for building a network in the Hyperledger Fabric.

Deployment details are given in the GitHub Link. For experimentations, the following components are required:

- Ubuntu Debian CLI for terminal commands in the Ubuntu operating system.
- Dedicated 2.13 GHz processor and 4 GB RAM for Kubernetes bunch. Kubernetes is a convenient, extensible, open-source stage for overseeing containerized tremendous burdens and administrations.
- Docker Hub is part of Docker for finding and sharing container images with the team. Docker Hub API integrator for rest API.
- Pods and jobs are cloning on the Kubernetes cluster. A job makes at least one pod and guarantees that a predetermined number of them effectively end. As units are effectively complete, the job tracks the fruitful fulfillment at the point when a predetermined number of effective consummations is reached, the errand.
- Channel services on Hyperledger Fabric network using Kubernetes cluster.

Features

SCMIIOT uses Watson IoT to dynamically provide temperature measurements stored on the Hyperledger Fabric network, a framework for traceability applications. The framework is built on Hyperledger Fabric, using most of its features.

- Version 1.4.2 of Hyperledger binaries and Docker images. The framework should work well with little to no changes for versions 1.4.3 and 1.4.4.
- Rich data operations with CouchDB, instead of the default database LevelDB.

- Raft ordering service.
- Chain code is entirely written in JavaScript, using Node.js as the running environment.
- Hyperledger Explorer attached to the Blockchain network.
- Explorer provides a graphical user interface (GUI) to visualize all-important entities in the network, such as organizations, peers, chain codes, channels, and transactions.
- HTTP server communicating with the blockchain network. This server can be hosted in the cloud to handle requests from client apps. The server is written in JavaScript, with Express.js.
- Authentication with JSON web token (JWT).
- Input data validation with Joi/Celebrate.
- Basic error handling.
- Postman collection and environment for convenience when making requests to the HTTP server and the blockchain network.

5. Evaluation and Results

IBM Cloud Kubernetes Service conveys critical assets by joining Docker holders, the Kubernetes innovation, a natural client experience, and inherent security and isolation to robotize the organization, activity, scaling, and checking containerized applications in a cluster of hosts.

In Fig. 3, the persistent volume for data storage and network connection configuration is done using Hyperledger fabric. In Fig. 4, the genesis block of the Hyperledger Fabric blockchain network is created for the interconnection of network nodes. In Fig. 5, Rest-API is called for integration into the Docker Hub repository. Rest API is integrated into the Docker Hub containerized applications where data communication is easily shared between nodes or peers.

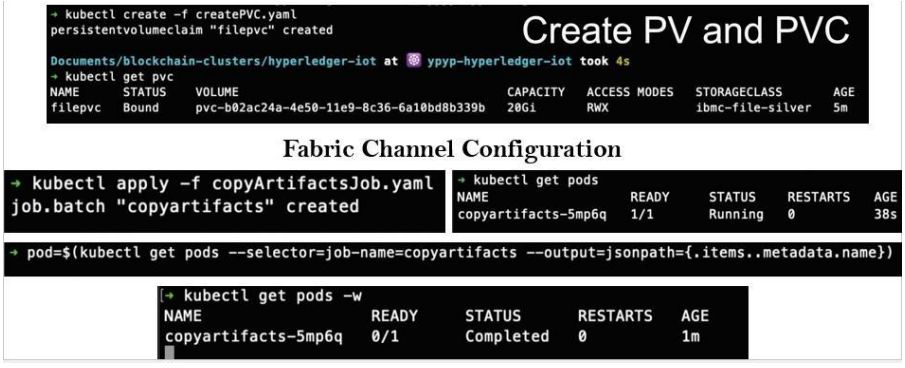

Fig. 3. Deploy Hyperledger Fabric network.

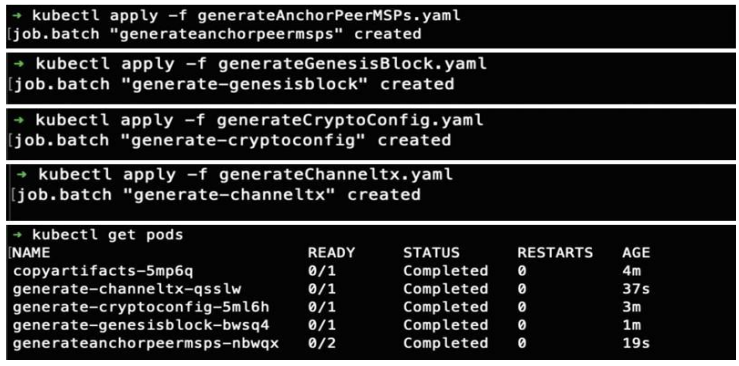

Fig. 4. Hyperledger Fabric channel configuration.

Fig. 5. Network deployment.

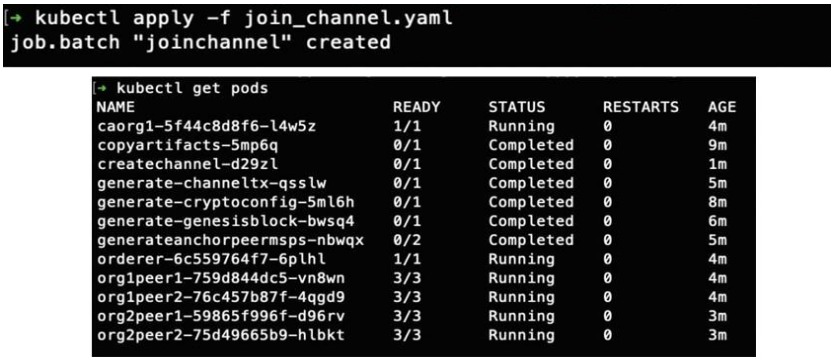

Fig. 6. Network configuration.

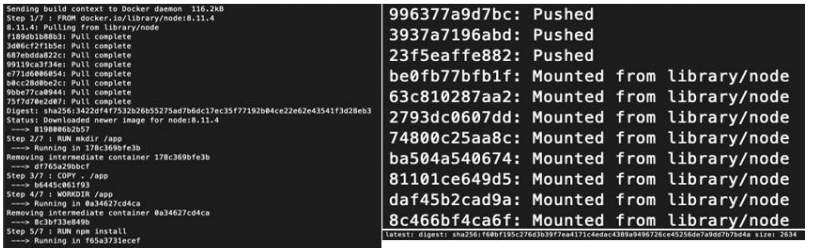

Fig. 7. Deploy Hyperledger Fabric SDK for Node.js.

In Fig. 6, the peer-to-peer connection is established, and channels are joined together to create and trustless and immutable connection.

In Fig. 7, rest API pull and push images from the docker hub to the Kubernetes cluster are depicted. Docker Hub brings developers together to work on a public or private repositories project. Organizations are perfect for teams that need to control who can create and view repositories and push and pull image changes. We perceive the focal job that Docker Hub plays in present-day application advancement and deals with numerous security and substance improvements. Two-factor verification builds the security of records by requiring two distinct types of approval. This guarantees the legitimate record proprietor. Kubernetes cluster is the central pillar for all the deployment as all peers, networking, and blockchain are implemented on this platform. Chain code installation and deployment are presented in Fig. 8. Installation of the chain code jobs is performed on the localhost Ubuntu 18.04 LTS machine. Node-RED containerized code completion, Kubernetes machine-to-machine connection is established, and all anchor peers are executed. All nodes, pods, channels, and jobs run in Hyperledger fabric networks. Localhost external IP is used for the Node-RED dashboard. Network deployment on the Kubernetes cluster is mentioned, in which external IP is used to interact with the system, and internal IP is used to identify the

device. REST decides how the API resembles. REST is a bunch of decisions that engineers follow when they make their API.

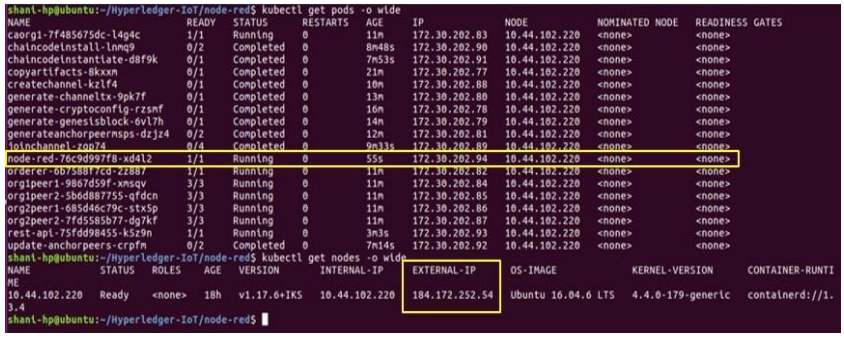

Fig. 8. Access to Node-RED.

Node-RED provides a web interface and artifacts to use and manage network systems. This platform quickly regenerates the network topology's nodes, channels, and pods. The palette of nodes can be effortlessly reached out by inserting the new nodes created by the network, and the streams can be handily shared as JSON documents. Node-RED is a stream-based improvement device for visual programming developed initially by IBM to wire equipment gadgets, API, and online administrations as a component of the IoT. Node-RED gives an internet browser-based stream manager, which can easily make input and output data streaming. A business network for Hyperledger Fabric composition and deployment is achieved through their wallet IDs. Hyperledger composer playground is used to import the .BNA file as a logical data file for data connection. Product listing of food supplies is realized in Hyperledger composer playground using intelligent contracts. Suppliers, Importers, Retailers, and Consumers are created and connected through a Hyperledger Fabric network.

6. Conclusion

SCMIIOT is a novel method for supply chain management using distributed Hyperledger Fabric blockchain network. The proposed approach helps in making a traceable, secure, and fast SCM model. SCMIIOT can be employed to monitor natural conditions for a blockchain network that incorporates refrigerated medical supplies, garden plant shipments, or any transient things sensitive to temperature, moisture, and time. SCMIIOT uses a distributed network of databases without any third-party involvement. Therefore, it is unchangeable and remotely accessible for real-time data communication. Different solutions are proposed to cope with the upcoming challenges in delivering heat-sensitive products, e.g., heat-maintained delivery containers to ensure the product's genuineness. Hyperledger Fabric network for SCM (food supply chain) is an application that can be utilized to follow natural conditions of supply products for a store network that can incorporate refrigerated medical supplies, garden plant shipments, or any transient things that are sensitive to temperature, moistness, vibration, and time. SCMIIOT is limited to a controlled environment. SCMIIOT is not tested in a real-life setting. The future work would include practical deployments of the system to check and test real-life scenarios and adapt to the upcoming Industry 5.0 era [26].

Author's Contributions

Conceptualization, MR, TRG. Funding acquisition, NK. Investigation and methodology, MR, ARJ, NK. Project administration, ARJ, ZJ, NK. Resources, GS, TRG, ZJ. Supervision, ARJ, ZJ. Writing of the original draft, MR, ARJ, ZJ. Writing of the review and editing, TRG, NK, GS.

Software, MR. Validation, ARJ, ZJ, NK. Formal analysis, MR, ARJ, TRG. Data curation, MR. Visualization, MR, ARJ, TRG.

Funding

None.

Competing Interests

The authors declare that they have no competing interests.

References

[1] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, et al., "Hyperledger fabric: a distributed operating system for permissioned blockchains," in *Proceedings of the 13th EuroSys Conference*, Porto, Portugal, 2018, pp. 1-15.

[2] G. Blossey, J. Eisenhardt, and G. Hahn, "Blockchain technology in supply chain management: an application perspective," in *Proceedings of the 52nd Hawaii International Conference on System Sciences*, Maui, HI, 2019.

[3] S. Pesic, M. Radovanovic, M. Ivanovic, M., Tossic, O. Ikovic, and D. Boskovic, "Hyperledger fabric blockchain as a service for the IoT: proof of concept," in *Model and Data Engineering*. Cham, Switzerland: Springer, 2019, pp. 172-183.

[4] M. A. Khan and K. Salah, "IoT security: review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395-411, 2018.

[5] C. Qu, M. Tao, J. Zhang, X. Hong, and R. Yuan, "Blockchain based credibility verification method for IoT entities," *Security and Communication Networks*, vol. 2018, no. 7817614, 2018. https://doi.org/10.1155/2018/7817614

[6] J. H. Park, S. Rathore, S. K. Singh, M. M. Salim, A. E. Azzaoui, T. W. Kim, Y. Pan, and J. H. Park, "A comprehensive survey on core technologies and services for 5G security: taxonomies, issues, and solutions," *Human-centric Computing and Information Sciences*, vol. 11, article no. 3, 2021. https://doi.org/10.22967/HCIS.2021.11.003

[7] M. Pustisek and A. Kos, "Approaches to front-end IoT application development for the Ethereum blockchain," *Procedia Computer Science*, vol. 129, pp. 410-419, 2018.

[8] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," 2008 [Online]. Available: https://bitcoin.org/en/bitcoin-paper.

[9] R. Ch, G. Srivastava, T. R. Gadekallu, P. K. R. Maddikunta, and S. Bhattacharya, "Security and privacy of UAV data using blockchain technology," *Journal of Information Security and Applications*, vol. 55, article no. 102670, 2020. https://doi.org/10.1016/j.jisa.2020.102670

[10] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, T. R. Gadekallu, and G. Srivastava, "SP2F: a secured privacy-preserving framework for smart agricultural unmanned aerial vehicles," *Computer Networks*, vol. 187, article no. 107819, 2021. https://doi.org/10.1016/j.comnet.2021.107819

[11] C. Rupa, G. Srivastava, T. R. Gadekallu, P. K. R. Maddikunta, and S. Bhattacharya, "A blockchain based cloud integrated IoT architecture using a hybrid design," in *Collaborative Computing: Networking, Applications and Worksharing*. Cham, Switzerland: Springer, 2021, pp. 550-559.

[12] I. W. G. Kwon and T. Suh, "Factors affecting the level of trust and commitment in supply chain relationships," *Journal of Supply Chain Management*, vol. 40, no. 1, pp. 4-14, 2014.

[13] J. M. Song, J. Sung, and T. Park, "Applications of blockchain to improve supply chain traceability," *Procedia Computer Science*, vol. 162, pp. 119-122, 2019.

[14] S. Kim, G. C. Deka, and P. Zhang, *Role of Blockchain Technology in IoT Applications*. Cambridge, MA: Academic Press, 2019.

[15] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of Trust: a decentralized blockchain-based authentication system for IoT," *Computers & Security*, vol. 78, pp. 126-142, 2018.

[16] S. Rouhani and R. Deters, “Security, performance, and applications of smart contracts: a systematic survey,” *IEEE Access*, vol. 7, pp. 50759-50779, 2019.

[17] A. Reyna, C. Martin, J. Chen, E. Soler, and M. Diaz, “On blockchain and its integration with IoT: challenges and opportunities,” *Future Generation Computer Systems*, vol. 88, pp. 173-190, 2018.

[18] A. Halldorsson, H. Kotzab, J. H. Mikkola, and T. Skjott-Larsen, “Complementary theories to supply chain management,” *Supply Chain Management*, vol. 12, no. 4, pp. 284-296, 2007.

[19] A. Rejeb, S. Simske, K. Rejeb, H. Treiblmaier, and S. Zailani, “Internet of Things research in supply chain management and logistics: a bibliometric analysis,” *Internet of Things*, vol. 12, article no. 100318, 2020. https://doi.org/10.1016/j.iot.2020.100318

[20] H. Birkel and J. M. Muller, “Potentials of industry 4.0 for supply chain management within the triple bottom line of sustainability: a systematic literature review,” *Journal of Cleaner Production*, vol. 289, article no. 125612, 2021. https://doi.org/10.1016/j.jclepro.2020.125612

[21] S. A. R. Khan, Z. Yu, H. Golpira, A. Sharif, and A. Mardani, “A state-of-the-art review and meta-analysis on sustainable supply chain management: future research directions,” *Journal of Cleaner Production*, vol. 278, article no. 123357, 2021. https://doi.org/10.1016/j.jclepro.2020.123357

[22] C. S. Singh, G. Soni, and G. K. Badhotiya, “Performance indicators for supply chain resilience: review and conceptual framework,” *Journal of Industrial Engineering International*, vol. 15, no. 1, pp. 105-117, 2019.

[23] R. Kamath, “Food traceability on blockchain: Walmart’s pork and mango pilots with IBM,” *The Journal of the British Blockchain Association*, vol. 1, no. 1, pp. 47-53, 2018.

[24] S. Saberi, M. Kouhizadeh, and J. Sarkis, “Blockchains and the supply chain: Findings from a broad study of practitioners,” *IEEE Engineering Management Review*, vol. 47, no. 3, pp. 95-103, 2019.

[25] S. Malik, V. Dedeoglu, S. S. Kanhere, and R. Jurdak, “Trustchain: trust management in blockchain and IoT supported supply chains,” in *Proceedings of 2019 IEEE International Conference on Blockchain (Blockchain)*, Atlanta, GA, 2019, pp. 184-193.

[26] P. K. R. Maddikunta, Q. V. Pham, B. Prabadevi, N. Deepa, K. Dev, T. R. Gadekallu, R. Ruby, and M. Liyanage, “Industry 5.0: a survey on enabling technologies and potential applications,” *Journal of Industrial Information Integration*, vol. 26, article no. 100257, 2022. https://doi.org/10.1016/j.jii.2021.100257