Turkish Journal of Computer and Mathematics Education Vol.12 No. 11 (2021), 3286- 3298
Research Article

An Approach for Secure Product Traceability in Food Supply Chain Based on Blockchain

Rajvir Kaur
dept. of Computer Engineering & Technology
Guru Nanak Dev University Regional Campus
Jalandhar, India
kaurrajvir174@gmail.com

Sheetal Kalra
dept. of Computer Engineering & Technology
Guru Nanak Dev University Regional Campus
Jalandhar, India
sheetal.ecejal@gndu.ac.in

Varinder Kaur Attri
dept. of Computer Engineering & Technology
Guru Nanak Dev University Regional Campus
Jalandhar, India
Varinder 2002@yahoo.com

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 10 May 2021

Abstract

The emergence of Blockchain technology as Bitcoin, has completely transformed the process of exchanging financial capital, without an intermediary. The huge success of Bitcoin contributed to the rapid advancement and increase interest of the public in Blockchain technology. As people started digging more into the technology underlying Bitcoin, they started realizing that the blockchain capacity is not just confined to cryptocurrencies. It has the potential to impact a much wider domain of applications to solve many of the issues and challenges in real-world scenarios. One such scenario is product traceability in food supply chain (FSC). Traditional traceability systems are vulnerable to various issues and challenges such as lack of data transparency, confidentiality, centralized data storage, mistrust between the parties, product delay which needs to be addressed. This paper proposes a solution for product traceability in FSCs using Hyperledger Fabric (HLF), a permissioned blockchain framework. We keep a track of food products journey from source to destination. All the information associated with food products shipment recorded securely and immutably in a distributed ledger, which is sync and verified with all the participants in the FSC in real-time but can be accessed by the authorized participants only. For managing access rights to the blockchain network resources, access control rules are defined by embedding them in smart contracts. Moreover, REST API allows clients to interact with blockchain network is secured using, OAuth 2.0 authentication strategy. Finally, we evaluate the performance of the designed blockchain-based system for FSC.

Keywords— Hyperledger Fabric, Blockchain, Traceability, Food supply chain, Access Control, Security.

I. INTRODUCTION

Product traceability in safety-sensitive domains such as FSCs is very essential and has been recognized as important food protection and quality tool to increase transparency and guarantee the food product's safety and quality. However, today, most of the traditional product traceability systems can merely track the food products shipment in supply chain and store the orders without ensuring the key features such as confidentiality, auditability, data security, and transparency of data. Moreover, how to share and preserve information in a secure and trusted manner has been the most challenging problem with traditional practices. Thus various research communities focusing on utilizing IoT technologies such as WSNs, RFIDs, to monitor the conditions in food shipment scenarios. However, most of the existing approaches are still depends

upon the centralized cloud infrastructure, that is vulnerable to various security threats [1]. This solution utilizing blockchain technology aims to securely track the food products provenance and existence from the producer to consumer and solves the problem of safe handling of food products that is sensitive to the temperature and time during shipment. The detection and monitoring of food product's temperature conditions and location of the shipment at each point in supply chain help to enhance traceability, transparency, efficiency, and trust in supply chain. Blockchain, a distributed digital ledger stores each transaction history and shares the data with only the authorized participants [2]. By using Blockchain technology and smart contracts the confidential and trusted information about the product is immutably and securely recorded from the start to the end of the FSC. Moreover, the risks and cost associated with the involvement of the human to enforce and execute a contract can be drastically reduced by using smart contracts, that automatically triggers and perform the necessary steps when certain conditions met. Blockchain technology can help to enable secure product traceability across FSC, which eliminates the frauds and improves FSC.

The Rest of the paper is organized as follows: Section II summarizes the related work. Section III discusses the underlying technology and, its features. Section IV introduces the overview, workflow, and architecture of the proposed solution. Section V presents the implementation details, Section VI elaborates on the results of the implementation, Section VII gives the performance evaluation of the proposed solution following a final concluding section.

II. RELATED WORK

In this section, we study and illustrated the related work on blockchain for traceability in FSCs. Considering the issues in FSC, a blockchain and IoT based solution is introduced in [1]. The authors proposed a use-case scenario to track the food from the farm-to-fork utilizing different blockchain platforms. A scheme for soybean traceability is introduced in [3]. In this scheme, they use Ethereum blockchain for executing and tracking the transactions efficiently without requiring any trusted 3rd party authority. Test smart contracts have been implemented that ensure proper interactions between the supply chain participants. Moreover, Tian in [4] proposed a HACCP, blockchain, and IoT based traceability system for tracking of food in supply chain. In this system, the author mainly focuses on the transparency and security of information between all supply chain members to rebuild the consumer's confidence. A Process of the crop plants in various stages from the harvesting of the crop to the retailing has been described. Wang et al. [5] present a product traceability system in supply chain based on blockchain and smart contract. A smart contract is developed to automate the product registration, tracking, tracing and to record the history of product transferring in the blockchain. A mechanism for event response is designed for identity verification of the transacting entities. In order to solve the issues related to traceability in FSC Kim et al. [6] presents an application based on Ethereum, IoT, and smart contract for traceability of food in supply chain. The key objective of this paper is to implement a distributed blockchain ledger for securely recording the information about the food throughout the supply chain. Moreover, Lin et al. [7] developed an EPCIS and blockchain-based prototype system for food traceability. An architecture for managing the data both on and off-chain is proposed that solves the problem of management of a huge amount of blockchain and IoT data. Moreover, they develop a smart contract to secure sensitive data during the interaction between the participants.

III. UNDERLYING TECHNOLOGY

A. Why Permissioned Blockchain?

Different types of blockchain frameworks are available freely classified as follows [14]:

- Permissionless Blockchains: are essentially a permissionless digital ledger that can be accessed by all the network nodes like Ethereum [9]. Anyone can join, can read/write, or participate in the blockchain network [8].
- Permissioned Blockchains: are permissioned digital ledger in which only specific entities with known identities can be granted excess to the blockchain network [8] like Hyperledger Fabric (HLF) [10] blockchain framework. The owner of the network can restrict who can access and do what on the network. For joining the permissioned blockchain network, the participants need permission from the network authority.

Concerning Supply chain traceability systems that usually comprise private and confidential data, a permissioned blockchain: Hyperledger Fabric is the best suitable technology.

B. Key Features of Permissioned Blockchain: Hyperledger Fabric [11]

- Permissioned Network: The HLF allows to create permissioned blockchain network. Using HLF roles can be allocated to the participants, and the actions that can be taken by those roles are confined with the help of the access control list. As the identities of all the participants in the network are known, the trust can be easily established between the participants.
- Confidentiality and Privacy of the Transactions: The HLF blockchain provides the participants of the network with the ability to control the visibility of their transactions. If some network participants want a type of business operation that needs them to limit the transaction visibility to only them, for this purpose a private channel can be created using the HLF.
- Chaincode Functionality: The HLF is programmable by using chaincode. Chaincode can be utilized to automate certain business transaction aspects. Automation of the business processes by using chaincode helps to provide transparency, high efficiency, and trust between the network participants.
- Identity Management: The HLF offers membership identity services that authenticate each participant on the network and also manage the user IDs. Also, an additional permission Layer can be provided with the help of access control lists, through the authorization of certain network operations.

IV. PROPOSED SOLUTION

A. Proposed Architecture

Fig. 1 demonstrates the system architecture of the proposed product traceability solution in FSC. It consists of four main components: HLF Blockchain Network, Rest Server, IoT Sensors, and Client Application.

- HLF Blockchain Network: In this proposed solution a permissioned blockchain network is implemented using HLF framework which allows executing the operations in blockchain network to the authorized participants only. Moreover, a legitimate transaction must always include the participant signature that prevents data leakage possibility and assures no unauthorized party may access or modify the data. HLF Blockchain network comprises components including Peer nodes, Ordering service, MSP, and chaincode.
  - Peer Nodes: Peers are the essential component of blockchain network as various instances of the smart contracts and the ledgers are hosted by these peers. These peers contain smart contracts to write transactions to blockchain ledger. The peer provides several features to the blockchain such as identity authentication, verification of the transactions, and P2P communication.
  - Ordering Service: In blockchain network transactions must be recorded in a consistent order into the shared ledger. Ordering Service in HLF blockchain network guarantees the replicated ledger's consistency. Ordering nodes maintain and records all the valid and invalid transactions in their ledger.
  - Membership Service Provider**:** Every interaction among the nodes in the permissioned blockchain network needs to be authenticated such that every network node must have an identity in order to perform an authentication check. MSP utilizes a certification authority (CA) to issue digital identity to each node in the network by providing cryptographically validated certificates. The MSP maintains and validates the identities by validating the certificates.
  - Chaincode (Smart Contract): A digital contract that contains specific conditions and rules of an agreement among different organizations written in executable code. Smart contract is executed by applications, in order to generate transactions that are further added on the ledger. Usually, in the context of the HLF network, both chaincode and smart contract are used interchangeably but the smart contracts define the transaction logic which is packaged in a chaincode and then deployed on a peer in the blockchain network. After deploying chaincode, all the smart contracts within it are made accessible to the applications.

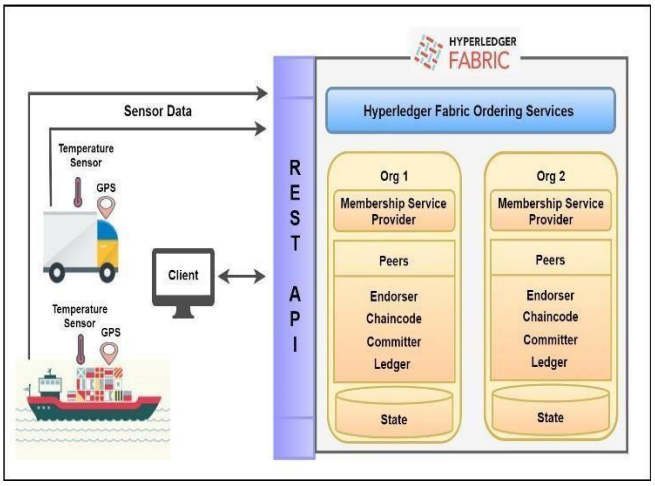

Fig. 1 Architecture of the Proposed Permissioned Blockchain-based solution

- IoT Sensors: In the proposed solution IoT sensors are used for real-time monitoring of shipment conditions from source to destination. IoT sensors sense the temperature conditions and also fetches the current GPS location throughout the food product shipment and send this data into the blockchain via REST API.
- REST Server: REST server is utilized for generating the endpoints of REST API from the food product traceability business network deployed on a Hyperledger Fabric. LoopBack framework is used by REST services that convert the blockchain network into the concept of open APIs. The authenticated participants can interact with the blockchain by calling REST Server via the generated REST API endpoints.

Fig. 2 demonstrates the proposed smart contracts structure

- Client Application: Client application offers an interface to the participants for performing several functions through the REST API such as initiate a shipment for the food products, create a new contract, create different supply chain participants, etc.

B. Proposed Scenario

For implementing the proposed solution, a scenario is created. The producer of the food products sends the products to the trader. The Trader initiates the shipment for the food products and creates a contract with the producer and the transporter for the safe delivery of the food products. The contract contains the arrival date for the shipment, the maximum and the minimum limit of the temperature to be maintained during the shipment of the food products, the price for the successful delivery of the products, and a fine that will be imposed if the conditions mentioned in the contract violates. Before obtaining the shipment of the food products the temperature during the journey is checked by using the IoT sensors. This information is compared with the rules defined in the contract, and fine is assigned accordingly. After obtaining the food products, the price and the fine for the shipment are calculated. In this manner, the producer, transporter will be charged or receive the payments. Blockchain creates a shared and immutable ledger for all the transactions that happen during the shipping of the food products which helps to get the transparent status of the shipping as well as the confidence of the delivery date. All the information about the shipment can be easily tracked and trace at any time. The information on the blockchain is immutable, therefore no one can alter or delete it which makes the information secure and reduces the fraudulent activities during the shipping, product delays, and create trust between the participants.

C. Proposed Smart Contracts

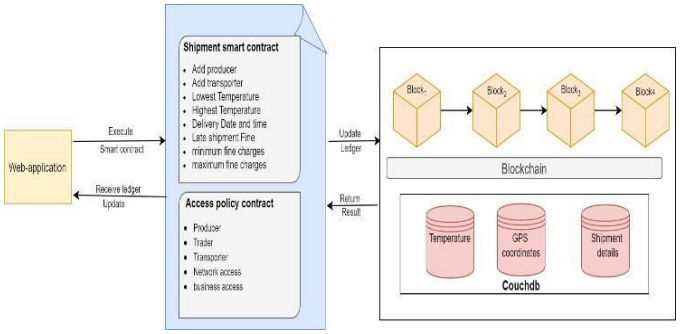

Fig. 3 Proposed Smart Contracts

In this proposed framework, two smart contracts are implemented. These contracts are the Shipment Contract and the Access Policy Contract. The rules for the safe delivery of food products are defined in the shipment contract. Every shipment of products has limits to protect food products from being damaged. The requirements like the date for delivery, and the limits of temperature for safe delivery of products are defined in the contract. If the shipment exceeds the limits mentioned in the contract, the food products are damaged and might become a risk for health, and fine will be imposed on the producer and the transporter according to the conditions mentioned in the contract.

Fig. 3 Access Control Rules

In the access policy contract, an access rule list is defined for managing access rights to the network resources that checks, if the participant in the network has the permission to access or change the resources.

D. Transaction Flow

Fig 4. demonstrates how a transaction executes in the HLF blockchain network. A client utilizes Hyperledger SDK or an application interface to start a transaction. SDK application prepares a transaction proposal and sends it to endorsing peers. The endorsing peers receive this proposal to validate the transaction. After obtaining a proposal, it is transferred to the chaincode function as arguments for simulation of the transaction by endorsing peers. Endorsing peers will verify the transaction proposal format, checks for the transaction proposal duplicity, and also validates the authorization and signatures of the client using MSP. After this, the chaincode will successfully get executed to generate a response value and read/ write set. Once everything is done the endorsing peers will sign this transaction proposal with their certificate and then it is passed back to the client as an endorsement response.

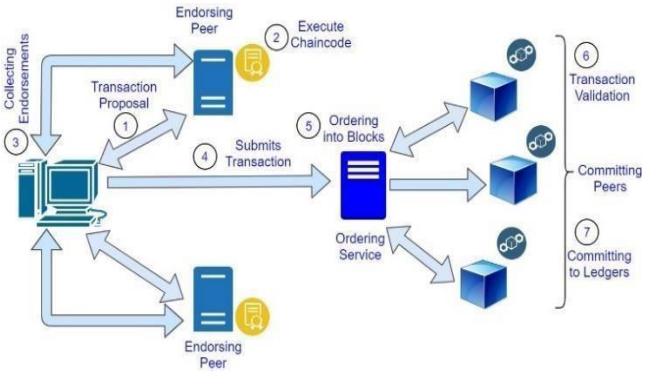

Fig. 4 Transaction Flow [20]

The Application checks the endorsing peer's signatures and also match endorsement responses in order to find whether the proposal responses are similar. The application broadcasts the endorsed transactions comprising read/write sets, Channel

ID, and endorsing peer's signatures to ordering service [12]. The ordering service obtains transactions from the blockchain network's channels, packages those transactions into blocks. Once the ordering service has ordered the transactions inside the block, the transactions are transmitted to the peers who are part of the network. These blocks of transactions are provided to the peers as an invocation response. The peers validate the transactions inside the block to ensure that the transaction policies are fulfilled. Each Transaction inside the block is flagged as a valid transaction or invalid transaction. After committing a block all the peers add that block to their chain. For every legitimate transaction, the execution of write sets takes place and then committed to the blockchain's current state ledger [13].

V. IMPLEMENTATION

A. Development Environment

The proposed solution for Product Traceability in FSC is implemented in the Docker environment. All the work implemented in this paper was conducted on Ubuntu Linux 18.04 LTS with the Intel Core i5-7200U CPU @ 2.50 GHz processor and 8 GB memory. We used HLF (v1.2) framework for implementing the blockchain network. Node (v8.17.0) and Python (v2.7.17) are fabric network prerequisites for developing client SDK. For docker images and container configuration, docker-compose (version 1.13.0) is used. Smart contracts are developed in node.js utilizing Hyperledger Composer which is then deployed on HLF network peers. Hyperledger Composer allows the developers to propose blockchain solutions with the REST APIs which exposes business logic to mobile or web applications. For designing, developing, and testing the blockchain business network definition a Composer web-playground is used. Moreover, we used the composer CLI tool for the deployment of proposed blockchain framework. Each transaction that is submitted via the blockchain business network stored on a blockchain ledger i.e., transaction log. Whereas, the information about the participants and asset's current status is recorded on a state database. In this proposed solution couchDB is utilized as a state database which supports rich queries and particularly deals with JSON documents. Moreover, a web client application was developed by using the angular framework. The authorized participants can perform the operations on web Application which invoke HTTP request such as GET, POST, UPDATE, PUT AND DELETE.

B. Business Network Definition and Deployment

Business network definition is the main concept of the Hyperledger Composer programming model. Hyperledger Composer is utilized for providing a business network definition by utilizing the major components as follows [15]:

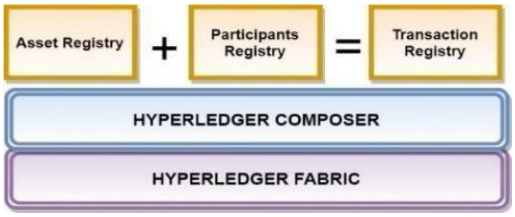

Fig. 5 Assets, Transactions and Participants definition in Hyperledger Composer, running on HLF Environment [19]

- Model File (.cto): defines network entities i.e., Assets, Events, Transactions, and participants inside the blockchain business network.
- Script File (.js): It is a transaction processor file that defines business operations that are required to achieve with the business network. This file also caters to the events and transactions that are defined within a model file.
- Permissions (.acl): This file contains an access control rule list which offers controlled access on the network resources to the participants.
- Query File (.qry): Query file is used for retrieving the data from the HLF blockchain ledger. Bespoke Query language is used for writing queries.

All these four above mentioned files forms the base of the business network inside Hyperledger Composer. These four files are fed into the Hyperledger composer compiler which compiles them into one single .bna file (business network archive) and .card (business network card) which is deployed on a HLF blockchain network. User Credentials and connection profiles are utilized for installing and accessing .bna file to the HLF blockchain network.

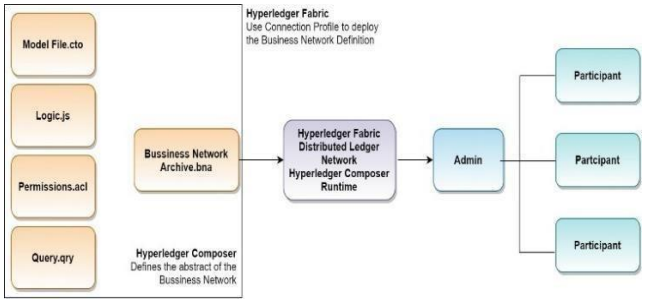

Fig. 6 Hyperledger Composer Architecture

The back-end of the system operates on the Hyperledger composer, connected to the front-end of the web application via REST Server by using REST-API. Fig. 7 demonstrates the system's back-end. At runtime, different Create, Read, Update, and Delete (CRUD) operations can be implemented by the REST server, which helps to control and maintain the Assets, Participants, and also allow to submit transactions.

Fig. 7 Back-end - Hyperledger Composer Rest Server

Fig 8. demonstrate the web application's front-end. This creates an uninterrupted and smooth user-friendly system using which the participants can easily interact with the blockchain system.

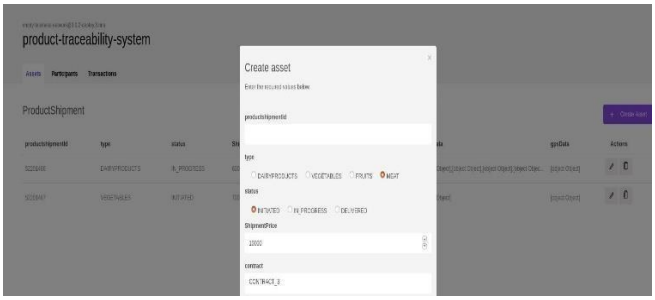

Fig. 8 Create Asset Section on Developed Front-end

C. REST API Security

The Access to REST API which allows users to interact with the permissioned blockchain network must be secured in order to make sure that no unauthorized users can access or manipulate the data using open APIs. In this paper, we use the OAuth-2.0/Passport-GitHub [16] authentication strategy for authenticating the users. Once the authentication is enabled, participants need to provide their credentials in order to perform operations on the REST server such as adding or retrieving data from the blockchain ledger.

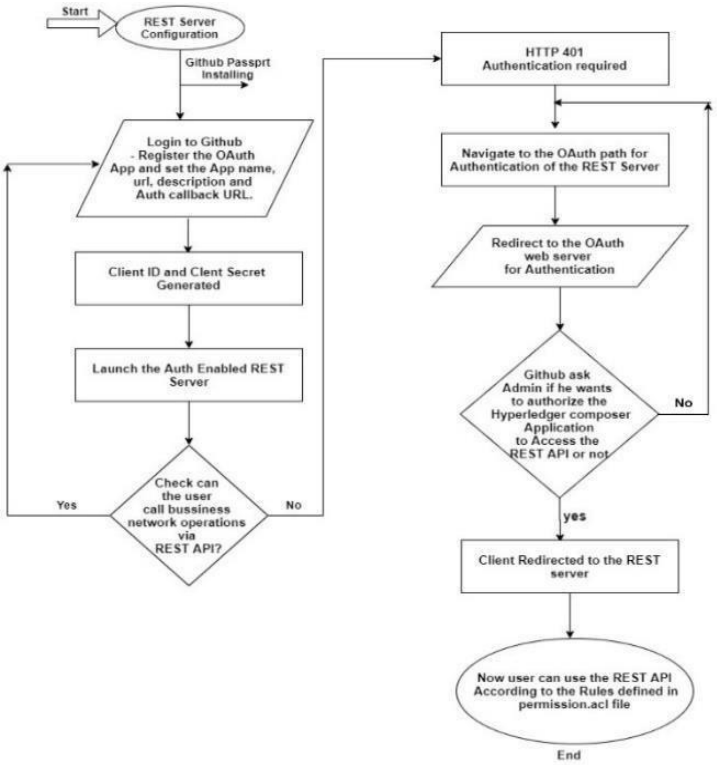

Fig. 9 REST Server OAuth Flowchart

VI. RESULT ANALYSIS

This section will introduce the results of the implemented solution.

A. Transparency: This section presents the transparency of the data from three types of data registries such as Participants, Transactions, and, Assets.

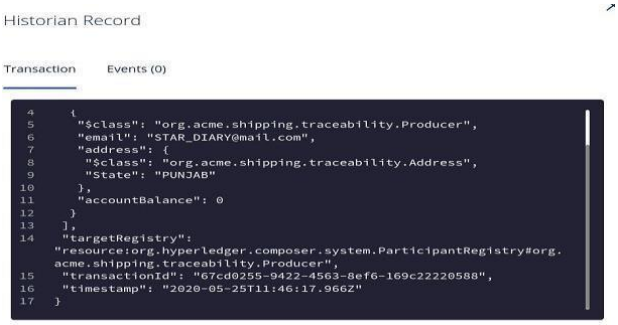

Fig. 10 Participant Data Recorded in the Blockchain

Fig. 10 shows the recorded JSON data about the producer (similarly there is also Trader's and Transporter's data) stored in the blockchain with the information about the resource, transacationId, and the timestamp. HLF guarantees the legitimacy of transactions by ensuring that the administrator of the network in the permissioned blockchain network cannot edit transacationId, and the timestamp fields. Only Hyperledger Fabric adds the values for transactionId and timestamp fields which can be used by all for transparency.

- For every safe and successful delivery of the food product, the shipment contract is developed as shown in Fig. 11 based on which producer and transporter get their payments or penalties (if any).

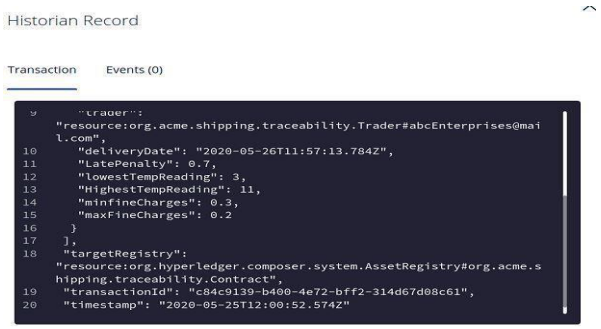

Fig. 11 Contract Asset Data Recorded in Blockchain

- Once the producer and the trader agree on a contract. Shipment Asset is created by the trader for the shipment of the products by the producer. Refer to Fig. 12. Here ShipmentId is the unique identifier for the Asset Shipment.

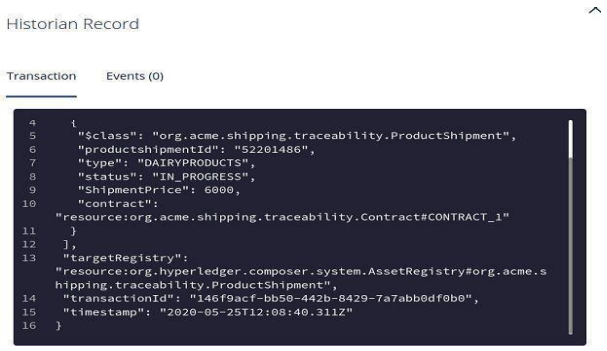

Fig. 12 Shipment Created for Dairy Products, Data Recorded in Blockchain

- Once the Shipment received, the payment for the shipment is made on the basis of the data received by IoT sensors throughout the shipment of the products. Refer Fig. 13. The received shipment can be verified by checking shipment Id.

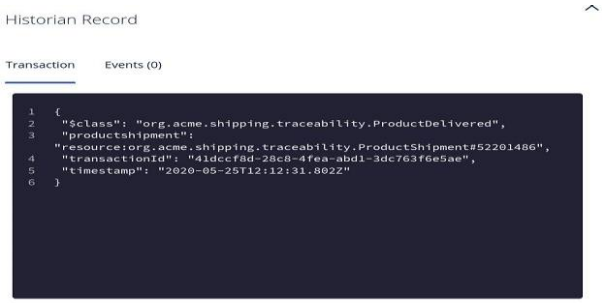

Fig. 13 Shipment Received

B. Traceability

Traceability in FSC is one of the most challenging and problematic areas. However, these challenges can be easily addressed using powerful technology blockchain. As compared to the conventional database systems blockchain records the data immutably and provides the ability to deeply track the shipment records.

Fig. 14 shows the instance of a food product shipment. All the data about the shipment is recorded immutably in blockchain ledger with transactionId and timestamp. The data in the blockchain is tamper-proof and trustworthy. All the data is shared among the supply chain participants. In comparison to a centralized database, systems blockchain provides much faster and clearer traceability of the shipment information which can also help to find the source of many problems.

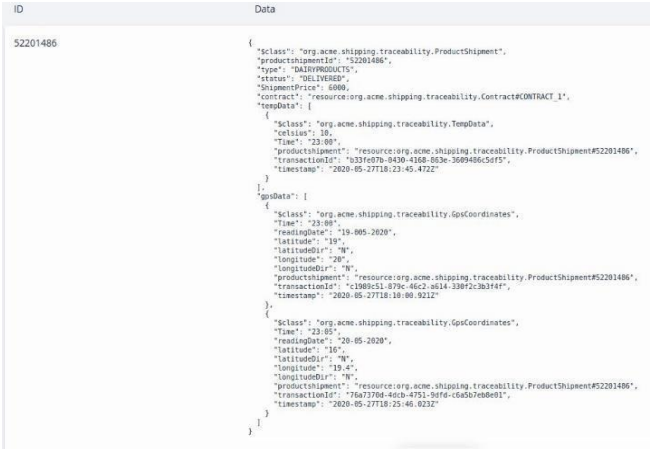

Fig. 14 Instance of a Food Product Shipment Record

C. Confidentiality of Data

As stated before, Traceability and Transparency are very much essential in the FSC. Apart from these, confidentiality is also an important aspect of FSC that needs to be taken into consideration. Without enabling confidentiality among the untrusted participants in the FSC, the entire system will be of no use. In our proposed solution, confidentiality is achieved by using the Access Policy Contract which we have created to control and manage access to the resources in the network by adding the access policies. Fig. 15 shows the result when the Transporter with Id cargo_transporter@mail.com tries to delete the contract data, which clearly shows that such operation is denied as Transporter with ID

cargo_transporter@mail.com do not have ‘DELETE’ access to that resource.

Fig. 15 Access Denied Error

VII. PERFORMANCE EVALUATION

For performance evaluation of the proposed blockchain-based system, an experiment was designed and conducted on Linux- Ubuntu Operating System using Apache JMeter 5.3 [17]. For this experiment, we utilized latency as a main dependent variable and type of request and the number of users was utilized as independent variables. Two main HTTP methods that are associated with the proposed system and used to communicate with the blockchain are GET and POST. GET request is used to retrieve the data from the blockchain, whereas to submit transactions on blockchain network POST request is used. Different types of HTTP methods may perform differently. Moreover, the number of users requesting the blockchain-based system may affect its performance. The performance of the system could decrease with the increase in the number of users. Therefore, number of users and type of request were chosen as independent variables. For evaluating the performance, as stated above, main HTTP methods such as GET and POST are used and the number of users is divided into three different user groups. Those are 100 users, 200 users, and 600 users sending requests to the blockchain system simultaneously. The performance comparison between three different user groups here helps to find out if the system’s performance drops with the increase in the number of users or not.

A. Experiment

For the experiment, a test plan was set-up in Apache JMeter's GUI mode. HTTPs requests (GET/POST) were generated using Apache JMeter and sent to the Hyperledger Composer Rest Server which is connected to the HLF Blockchain-based system in order to submit or retrieve data from the system. Firstly, to assess the impact of the transactions that are submitted by many different users simultaneously on the proposed system's Latency, sample tests, and groups of 100, 200, and 600 sample users were created. Later, the conditions for 100 users, 200 users, and 600 users were administrated for GET and POST requests.

B. Simulation Results

Fig. 16 depicts the average, percentile, minimum and Maximum Latency to execute GET Request in order to retrieve information that is already in the Hyperledger fabric blockchain database. We calculated the proposed permissioned blockchain system's latency by sending HTTPs GET requests by groups of 100, 200, and 600 users to the REST server.

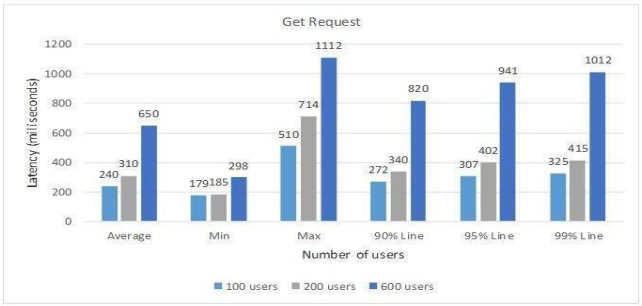

Fig. 16 Latency for GET Request for Retrieving Data from the Blockchain Ledger

The figure shows that the average Latency for a group of 100, 200, and 600 users are 240 ms, 310 ms, and 650 ms respectively. The graph indicates that by increasing the number of users, the system's latency increases. Maximum latency for 100, 200, and 600 users are 510 ms, 714 ms, and 1112 ms, respectively. Furthermore, it is seen in 90%-line case that the system's latency rises by 35 ms when the users increased from 90% to 95 %, and it is same in the case with 95% and 99% percentile line also.

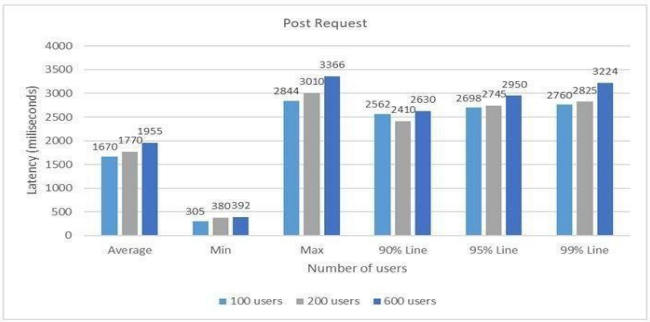

Fig. 17 Latency for POST Request for Posting data into the Blockchain Ledger

Fig. 17 describes the case of submitting data into the Hyperledger fabric blockchain database by sending HTTPs POST requests to the REST Server. The latency for POST request is higher than GET request to the blockchain via REST Server as it requires the peers in blockchain network to perform the process of endorsement, which needs more time. The figure shows that the average Latency for a group of 100, 200, and 600 users are 1670 ms 1770 ms, and 1955 ms respectively. Maximum latency for 100, 200, and 600 users are 2844 ms, 3010 ms, and 3366 ms, respectively. Furthermore, it is seen in 90%-line case that the system's latency rises by 136 ms when the users increased from 90% to 95 %, and it is same in the case with 95% and 99% percentile line also

C. Discussion

With the above observation, it is clearly seen that latency for GET request is better than the POST request. For instance, latency for GET requests over 200 users is 310 ms whereas for the POST request is 1770 ms which means the Post requests are slower as compared to Get requests. This happens in every user group because for writing the new data in the blockchain

and for updating the ledger status it requires more time. Additionally, the latency of the system increases precisely with increase in number of users. From the above experiment, it is depicted that the proposed blockchain system's average Latency for writing details to blockchain and updating the shared ledger status is less than 5 s within the range of users tested. Compared to traditional blockchain systems this is significantly faster. For instance, it takes the bitcoin system about 10 min and in the case of Ethereum, it's 10 to 20s [18] to complete a transaction.

VIII. CONCLUSION

In this paper, we present a state-of-the-art solution for Product Traceability in FSC. The utilization of permissioned Blockchain makes the system tamper-proof and helps to track and trace the product securely throughout the supply chain. All histories related to product shipment are recorded perpetually in the immutable ledger. Tracking and tracing the product on a shared, trusted, immutable, and distributed network provides security and transparency of data, brings trust among the participants, and ensures confidentiality in the complex business scenario. The infusion of smart contracts into the system drastically reduces the shipment delays and also eliminates risks and costs associated with the involvement of the human to enforce and execute a contract by automating the business transaction aspects. Finally, we evaluate the performance of the proposed system under the type of request and the number of users. The solution we proposed offers a secure and efficient approach with little to no risk of fraudulence for traceability of products in FSC with satisfactory performance.

REFERENCES

[1] Caro, M. P., Ali, M. S., Vecchio, M., & Giaffreda, R. (2018, May). Blockchain-based traceability in Agri-Food supply chain management: A practical implementation. In 2018 IoT Vertical and Topical Summit on Agriculture-Tuscany (IOT Tuscany) (pp. 1- 4). IEEE.

[2] Swan, M. (2015). Blockchain: Blueprint for a new economy. " O'Reilly Media, Inc.".

[3] Salah, K., Nizamuddin, N., Jayaraman, R., & Omar, M. (2019). Blockchain-based soybean traceability in agricultural supply chain. IEEE Access, 7, 73295-73305.

[4] Tian, F. (2017, June). A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things. In 2017 International conference on service systems and service management (pp. 1-6). IEEE. 67.

[5] Wang, S., Li, D., Zhang, Y., & Chen, J. (2019). Smart contract-based product traceability system in the supply chain scenario. *IEEE Access*, *7*, 115122-115133.

[6] Kim, M., Hilton, B., Burks, Z., & Reyes, J. (2018, November). Integrating blockchain, smart contract- tokens, and IoT to design a food traceability solution. In 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON) (pp. 335-340). IEEE.

[7] Lin, Q., Wang, H., Pei, X., & Wang, J. (2019). Food safety traceability system based on blockchain and EPCIS. IEEE Access, 7, 20698-20707.

[8] J. Garzik, Public versus private blockchains part 1: Permissioned blockchains (2015) [Accessed 30 May 2020].

[9] G. Wood, Ethereum: A secure decentralised generalised transaction ledger, Ethereum project yellow paper 151 (2014) 1–32.

[10] Introduction to hyperledger fabric [online]: https://hyperledgerfabric.readthedocs.io/en/latest/blockchain.html [Accessed 30 May 2020].

[11] Hyperledger Fabric Capabilities. [online] https://hyperledgerfabric.readthedocs.io/en/release/capa bilities.html [Accessed 30 May 2020].

[12] Thakkar, P., Nathan, S., & Viswanathan, B. (2018, September). Performance benchmarking and optimizing hyperledger fabric blockchain platform. In 2018 IEEE 26th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS) (pp. 264-276). IEEE.

[13] Madala, D. S. V., Jhanwar, M. P., & Chattopadhyay, A. (2018, November). Certificate transparency using blockchain. In 2018 IEEE International Conference on Data Mining Workshops (ICDMW) (pp. 71-80). IEEE.

[14] Pongnumkul, S., Siripanpornchana, C., & Thajchayapong, S. (2017, July). Performance analysis of private blockchain platforms in varying workloads. In 2017 26th International Conference on Computer Communication and Networks (ICCCN) (pp. 1-6). IEEE.

[15] Hyperledger Composer Overview [online] https://www.hyperledger.org/wpcontent/uploads/2017/05/Hyperledger-Composer-Overview.pdf [Accessed 30 May 2020].

[16] Passport-Github2[online] http://www.passportjs.org/packages/passport-github2/ [Accessed 2 june 2020].

[17] Apache JMeter [online] https://jmeter.apache.org/ [Accessed 10 june 2020].

[18] The Mystery Behind Block Time. [online] https://medium.facilelogin.com/the-mystery-behind-

blocktime-63351e35603a/ [Accessed 10 june 2020].

[19] Mukne, H., Pai, P., Raut, S., & Ambawade, D. (2019, July). Land Record Management using Hyperledger Fabric and IPFS. In 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (pp. 1-8). IEEE.

[20] Abhishek, Gunda. "Property Registration and Land Record Management via Blockchains." Diss. INDIAN INSTITUTE OF TECHNOLOGY KANPUR, 2019.