International Journal of Future Generation Communication and Networking
Vol. 13, No. 2, 2020 pp.1147-1159

A Consensus Food Supply Chain Management using Blockchain and IoT Mechanism

N.Prasath,
Associate Professor,
Communication Networks Research Group, Department of Computer Science and Engineering,
KPR Institute of Engineering and Technology, Coimbatore, Tamilnadu, India

Abstract

Now a days many of the food manufacturers, distributors and retailers are focusing on food tracking system in order to improve transparency in the food supply chain. Even through there are many existing methods to track these supply chain in agricultural food sector. Blockchain driven food traceability is allowing the various stake holders a secured information hence there forth it gives confidence over safety and quality of food. Blockchain distributed ledger technology can record transactions between parties in a secure and permanent manner. So a food traceability system using blockchain distributed ledger mechanism and IoT was proposed and implemented to keep track food of supply chain which consist of different participants with different job roles and thereby increasing the trust between the different participants bringing the transparency, in the food supply chain management.

Keywords*: Food traceability, blockchain, Internet of Things, Supply chain management, Agriculture.*

I. Introduction

In recent years, customers are keen in knowing the history of the food cultivated, quality and safety. Since primary need for a customer is to protect their health. But nowadays many of the logistics suppliers don't have the facility to track the information in agriculture food supply chain starting from cultivator to till customer [1].

Using blockchain based applications helps the customer to choose the product and shop, that where to buy and when to buy. It also helps to avoid customers in buying contaminated food, also helps to avoid contaminated food entering into market. Also it gives information about the cultivators/manufacturers, suppliers and retailers to the customer and helps to save time in choosing and buying a product as shown in the figure 1 the food supply chain components. [1]

Nowadays many R&D communities are adopting wireless sensor networks, IoT and RFID tags in order to provide transparency, traceability and auditability features in agriculture and food supply chain in order to track orders and deliveries. However these solutions depend on the centralized cloud infrastructure where there are lack in transparency and there may be lack in availability of data, confidentiality and auditability [1].

In the year 2008, the blockchain was originated from bitcoin technology, which has its main characteristics such as distributed, smart contract, follows asymmetric cryptography, trustless and time stamp. These characteristics in blockchain allows researchers in build mutual confidence and trust by without having centralized authority. Upon inspiring on blockchain technology, this can be used in food supply chain traceability system with distributed participants. The problem of transparency in data management under distributed environment can be solved using this blockchain technology. Along with blockchain by integrating IoT in food industry starting from origin in food supply chain management, i.e., from farmers to customers it's possible to record all the information which are needed at each stage. So because of this cost is minimized, trust is created among customers and profit can be increased. [2]

ISSN: 2233-7857 IJFGCN

The blockchain technology is defined as that its collection of logical blocks, whose data structure is created by linking the blocks together in an order. Each block contains two fields one is block header and the other is block body. It has a collection of tracking records, for example in this paper agriculture tracking records. [2] [3]

The development premise for these communities assumes that data from disparate sources is "open" to being shared, and that semantics in the form of ontology representations. The premise for Bitcoin and traceability block chains assumes that blockchain is needed because data is closed for sharing, that is, it is assumed that self-interested intermediaries tend to hoard and complex business networks like supply chains tend to have no natural intermediaries and hence there is no network-wide record of transactions. They constrain their data with their own meta-data so the need for others to define semantics is not compelling. [2]
The Hyperledger project proposes a set of open-source Blockchain technologies for business applications, like Sawtooth, Fabric, and Iroha [3]. These platforms are designed to be general purpose to accommodate as many use cases as possible, putting forward and emphasizing different features. None of them is built around a cryptocurrency. Nevertheless, many use cases of blockchain involve a form of asset/token transfer [3].

Fig 1: Food supply chain components

By registering and documenting a product's lifecycle across the supply chain nodes increases the transparency and the trust of the participating actors. Moreover, elimination needs to have a trusted third party that can allow for greater scalability, as any number of participants can virtually participate in the chain with the appropriate level of trust, and increased innovation by deploying the dynamics of block chains as enablers of instant payments (through cryptocurrency), smart contracts, and low transaction fees without having the cost overheads of third parties. Last, but not least, a shared, immutable ledger with codified rules can potentially eliminate the audits required by internal systems and processes[4].

From [5] moreover, it has been explained that distributed ledger/blockchain technology must have the ability to operate in a decentralized way without having to trust anyone. Distributed ledger/blockchain technology has the capability to influence how manufacturing supply chains are organized, in particular those in high-tech sectors. For example, the composite materials is a high-tech sector which is having innovative approaches in forming shapes, adapting process and based on the suppliers modifying the materials used in manufacturing process.
In [6], Saw tooth is a general purpose blockchain with a global key-value store as the underlying ledger. The smart contracts are defined by rules performing get/set operations on the store, and they can be written in any programming language so long as it is able to interface with a Saw tooth validator to submit the get/set requests. The security and correctness of smart contracts is challenging no matter which blockchain platform is used, but these Saw tooth features pose some additional challenges for developing smart contracts.

Decentralized autonomous organizations are, however, a special case. In most cases, however, DAOs don't need their own blockchain but are instead higher suited to be built on prime of an existing blockchain with an already existing currency (such as Ethereum).

ISSN: 2233-7857 IJFGCN

From all these survey various techniques are proposed to perform a secure food traceability provenance using blockchain technology. The table represents the Usability, Scalability, Security, Efficiency and performance for each algorithms. In Table 1, the algorithms are compared based on the efficiency, performance, scalability and security factors.[7]

Table -1: Comparisons on General features of various Blockchain techniques

Blockchain	Usability	Scalability	Security	Efficiency	Performance
Ethereum	H	L	M	M	H
Open Blockchain	M	NA	L	L	M
Sawtooth Lake	M	M	M	H	H
Blockstream Sidechain Elements	L	H	L	L	M
Eris	M	L	H	M	M

This paper is structured as followed. We begin with an overview of food supply chain, food traceability, blockchain technology. Next, we demonstrate the conceptual framework of blockchain and Ethereum. After that, we demonstrate the deployment process. Finally, we make a concise conclusion.

II. Related work

Using third party cloud services, as described in previous section an effective traceability can be implemented without using block chain technology. But in recent few years we could witness that in supply chain the Blockchain could act like secure accounting and monitoring technology. Also this systems is decentralized and thus it enable high secure medium for all exchanges in the supply chain [9]. There are four role players in the block chain based supply chain but some of them are not used in the traditional block chain. The entities are Registrars, Standard Organizations, Certifiers, and Actors all their role is to maintain trust [10]. In the supply chain systems participants share their ledger through block chain and smart contracts are used to hold the information that are being changed. Also there by registering the information of participants, which will help us to track the changes initiated by the push mechanism. So the recent alterations that are made are notified by the registered smart contract thus the change of recent information is achieved by using push mechanism [11].

III. Implementation

The process in the Blockchain based supply chain is explained with an architecture diagram as shown in the figure 2. It contains the process of transfer of goods starting from the producer to the consumer. As the Blockchain makes the process transparent every process is visible to everyone. This makes the process impossible to change. Supply chain management includes the integrated designing and planning as well as the execution of various processes.

ISSN: 2233-7857 IJFGCN

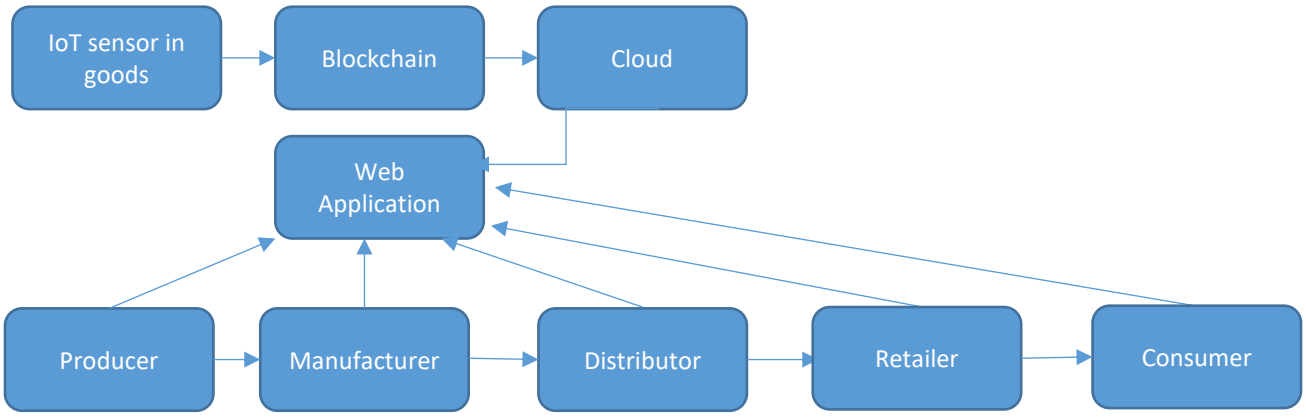

Fig -2: Architecture of the food supply chain system

A. Preparing Sawtooth and Ethereum Blockchain

From the analysis of the different blockchain platforms the most widely used Ethereum blockchain and the new comer Sawtooth Lake blockchain is chosen. The architecture of the both blockchains are studied. The implementation several projects related to the sawtooth and Ethereum blockchain are studied for the implementation of the supply chain in the blockchain.

B. Creating the interface for supply chain

The front-end for the supply chain is created using the basic web designing languages. A login and signup is created for accessing the account for managing the supply chain as shown in the figure 3, the sawtooth front end view. A webpage for displaying the products in the supply chain is created. A separate page for viewing the food products details is created. The location can be traced with the location page where the owner can enter the details of the products in the supply chain.

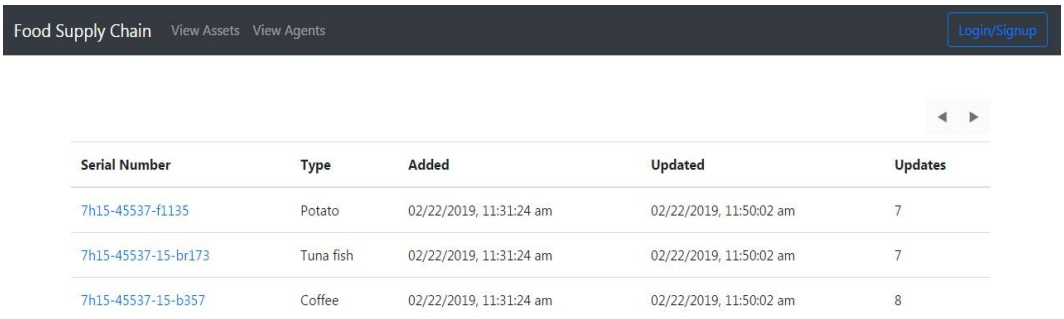

Fig 3: sawtooth front-end view

The above figure 3 depicts the number of food products in the food supply chain. The serial number in the page is unique and it will not be repeated. The creation date and the date of updating the supply chain will be stored in the blockchain and displayed in the front end. The number of updates also available in front end. The serial number is the hyperlink to the page which contains the details of the product.

ISSN: 2233-7857 IJFGCN

Fig 4: Details of the Product

Litke et.al.[4] depicts the details of the products in the food supply chain. The creation date is available in the page. The custodian is updated regularly. The name of the product will be displayed with the weight of the product in the kilogram. The location, temperature and shock is measured by the sensors and the details are updated in a regular interval. The values when clicked it opens another page containing the updates of the sensor values.

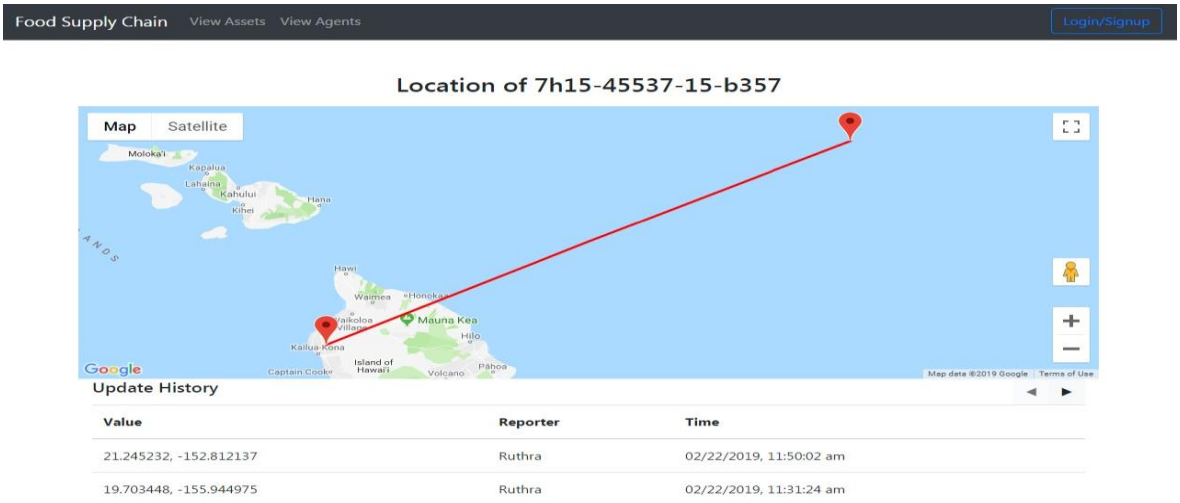

Fig 5: Location Information

Mondragon et.al.[5] depicts the location history of the food supply chain. Separate storage is allocated for the location storage. The Google maps API is connected with the location history. It shows the visual location of the food products in the food supply chain.

ISSN: 2233-7857 IJFGCN

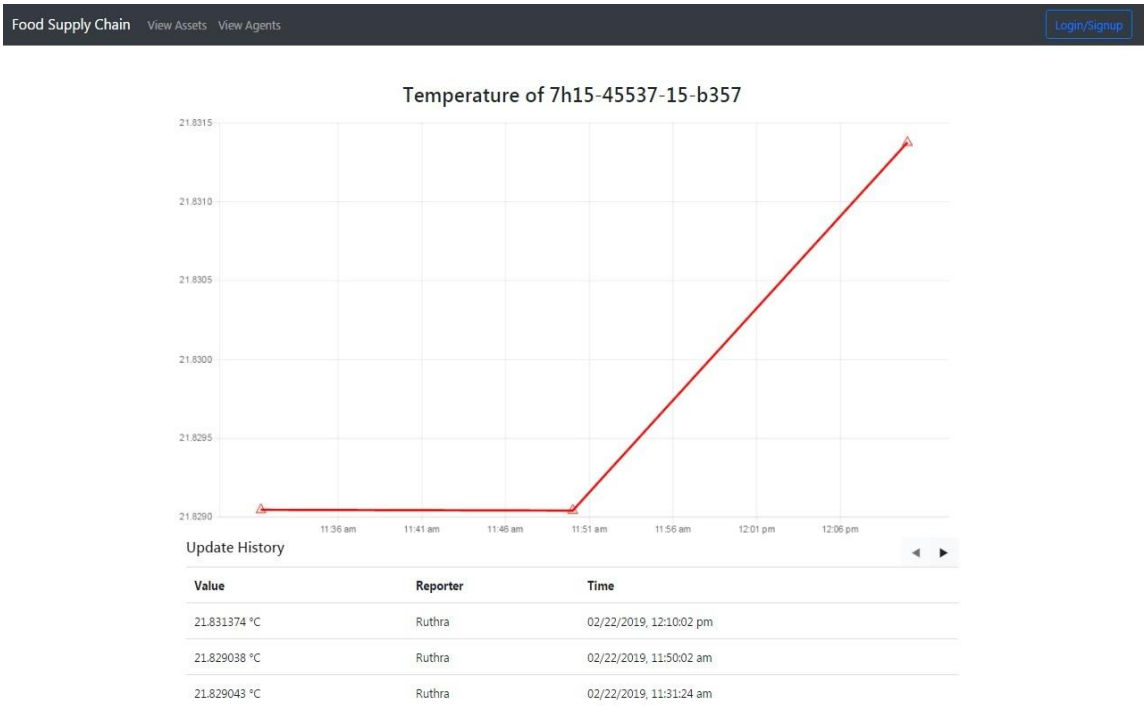

Fig 6: Temperature Information

Figure 6 depicts the temperature history of the food supply chain. Separate storage is allocated for the temperature storage. A dynamic graph is connected with the temperature history. It shows the visual representation of the temperature of the food products in the food supply chain.

Fig 7: Count Information

Figure 7 shows the public key for the users. It can be used for the verification of the agents in the Food supply chain.

C. Securing with blockchain

Every data in the supply chain is hashed with the help of sha-256k1 algorithm and the Elliptical Curve Cryptography algorithm and stored in the database. Authentication and pseudo anonymity of the

ISSN: 2233-7857 IJFGCN

user is promised by using the public key cryptography that works with the private key and public key. The public key thus generated cannot be reversed to find the private key as it uses a mathematical trapdoor function. The hashes are connected with the hashed address. Thus the data is secured with the blockchain as shown in the figure 8.

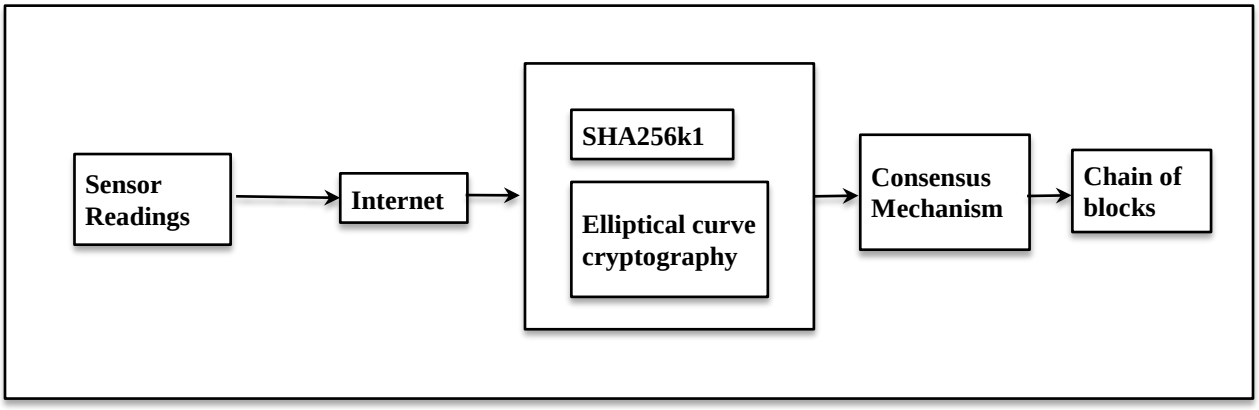

Fig 8: Process in the Blockchain

D. Merging the modules

The modules thus created is merged together. i.e. the front end and the backend is connected. In Sawtooth the JavaScript is used for the blockchain programming and in the Ethereum Solidity is used for the blockchain programming. The implementation is tested with various inputs.

E. Elliptic Curve Cryptography

It's a public key encryption which is based on the theory of elliptical curves. The key is generated by multiplication two large prime numbers and this is used for encryption by using the properties of elliptic curve cryptography. The most important advantage of elliptical curve cryptography is the use of smaller keys to provide security. ECC can provide the security with 164-bit key that other systems provide with 1024- bit key. It is mostly useful for mobile applications as it has the capability to provide high level security with low computing power and battery resource. ECC is a public key cryptosystem which can generate the public key and the private key in order to encrypt and decrypt the data.

Elliptic curves are the binary curves and are symmetrical over x- axis. These are defined by the function as shown in equation 1:

$$y^2=x^3+ax+b \quad (1)$$

i. KEY GENERATION

It is the most important step in which an algorithm is used to generate both public and private keys. Sender encrypts the message along with the receiver public key and receiver decrypts its using private key. [8]
Step 1. Selects a random number dA between the range [1 , n-1].
Step 2. Generates the public key using the formula PA = dA*G
Step 3. Similarly receiver selects a private key dB and generates the public key PB =dB*G.
Step 4. The sender generates the security key "K= dA*PB" and the receiver also generates the security key "K= dB*PA"

ii. Signature Generation

To sign a message m the sender performs the following steps: [8]
Step 1. Calculate a cryptographic hash function
Step 2. Selects a random integer k from [1,n-1]
Step 3. Computes a pair (r,s)
Step 4. r= x1 (mod n) where (x1,y1) =k*G

ISSN: 2233-7857 IJFGCN

Step 5. s= k-1(e+ dA*r)
Step 6. The pair (r,s) defines the signature
Step 7. This signature is sent to the receiver.

iii. Encryption Algorithm

Suppose sender wants to send a message m to the receiver the following steps has to be followed for encrypting the data. [8]
Step 1. Let m has any point M on the elliptic curve
Step 2. The sender selects a random number k from [1,n-1]
Step 3. The cipher texts generated will be the pair of points (B1,B2) where
B1= k*G
B2= M + (k*G)

iv. Decryption Algorithm

To decrypt the cipher text, following steps are performed: [8]
Step 1. The receiver computes the product of B1 and its private key
Step 2. Then the receiver subtracts this product from the second point B2
M = B2- (dB * B1)
M is the original data sent by the sender

v. SHA256k1

The SHA-256 compression function operates on a 512-bit message block and a 256- bit intermediate hash value as shown in the figure 9. It is essentially a 256-bit block cipher algorithm which encrypts the intermediate hash value using the message block as key. Hence there are two main components to describe: (1) the SHA-256 compression function, and (2) the SHA-256 message schedule. [8]

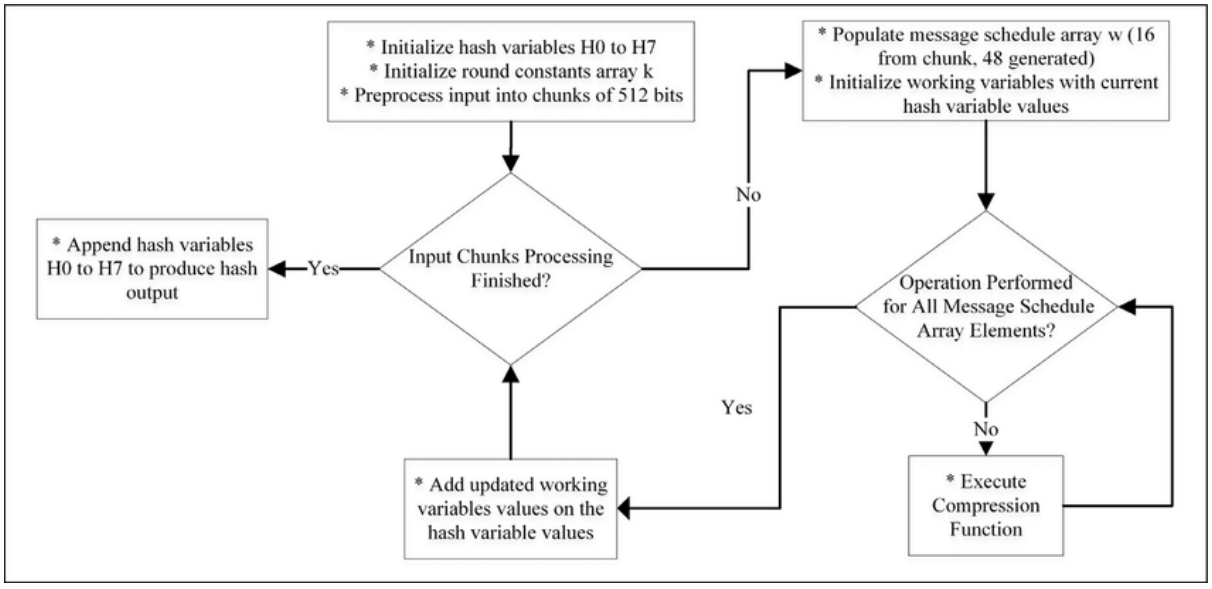

Fig 9: Flowchart of SHA-256

IV Module Description

a) Producing the product

ISSN: 2233-7857 IJFGCN

In Fig 10, after the production of the products the producer enters the details regarding the products within the application designed for the supply chain. The RFID is planted during this step and therefore the details of the products are keep inside the ID. The GPS device is used to trace the products within the time period. As we tend to use smart contracts for the storing information within the cloud using blockchain the device data is autonomously keep within the cloud without any manual work.

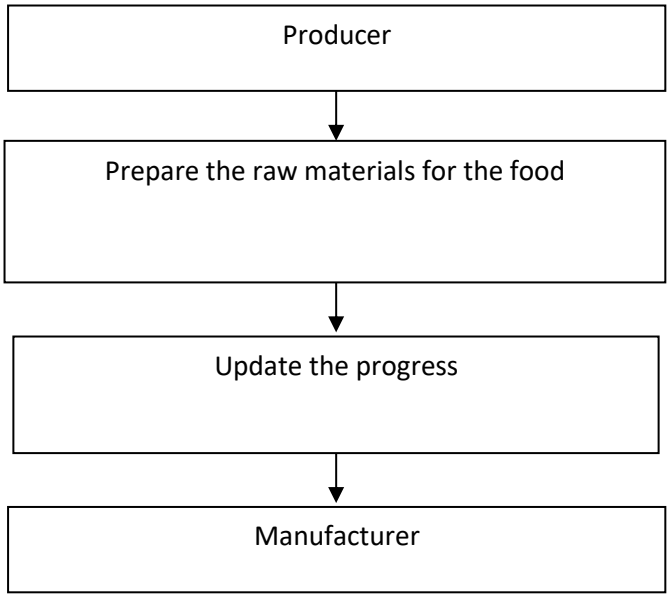

Fig10: Producing the product

b) **Manufacturing process:** In Fig 11, the position of the products is tracked with the web app any time as the goods reach the manufacturer, they will end their work in the products and therefore the timings are updated within the database using the web app.

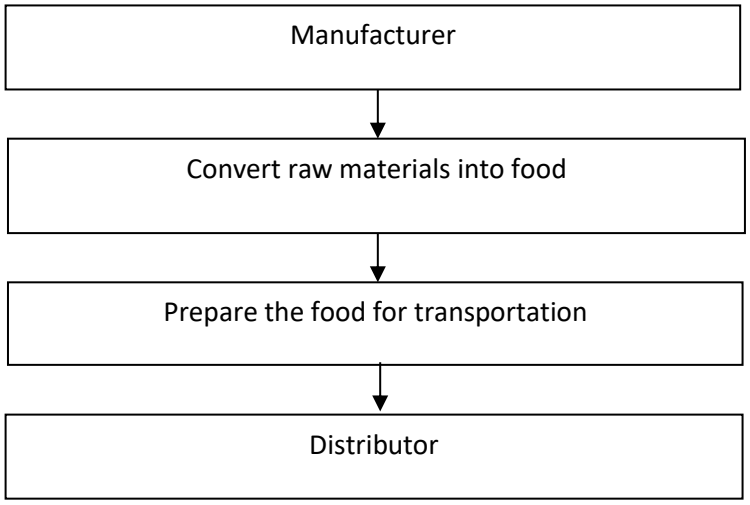

Fig 11: Manufacturing Process

ISSN: 2233-7857 IJFGCN

c) **Distributing the products:** From Fig 12, the products will reach the distributor after the producing process. The distributor will distribute the products to the distributor and the timings are updated to the web app.

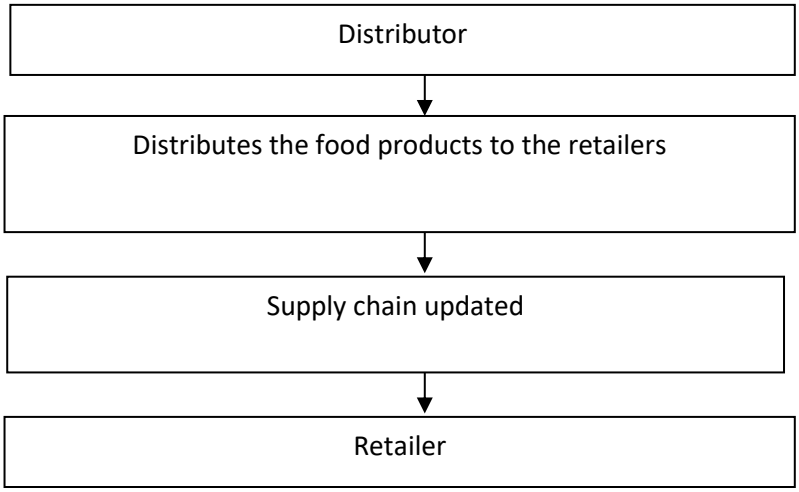

Fig 12: Distributing Process

d) **Selling the products:** In Figure 13, Distributor receives the products from the distributor and the goods are available for the sale in the shop with the ID for the product.

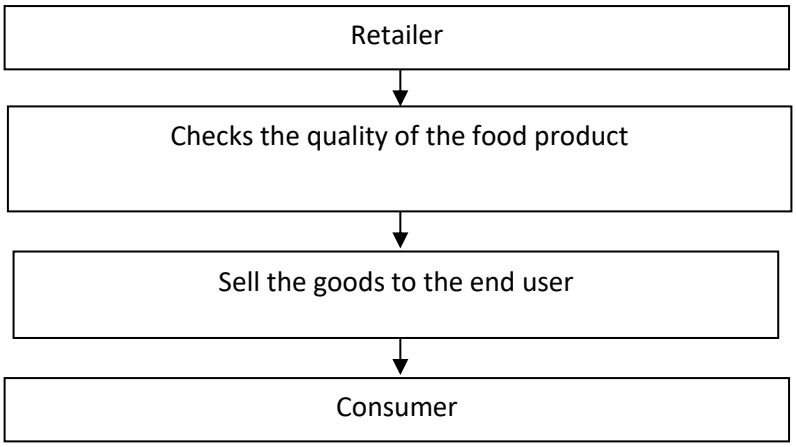

Fig 13: Selling the product

e) **Buying the products:** The customers will visit the retailer's shop and therefore the id is entered to the web app by the customer. The client will get full details regarding the product.

V Results and Discussion

In this paper, the performance of Hyperledger sawtooth and Ethereum is obtained by investigating the Execution time, Average latency, Network transmission and CPU load. This experiment was conducted in both Hyperledger sawtooth and Ethereum blockchain. The experiment results proves that sawtooth outperforms Ethereum through all the performance matrices.

ISSN: 2233-7857 IJFGCN

In Fig 14, Latency is the delay before a transfer of data begins and the latency of the Ethereum and sawtooth is measured and compared. From the comparison, sawtooth lake blockchain is 78.8 % efficient than the Ethereum blockchain.

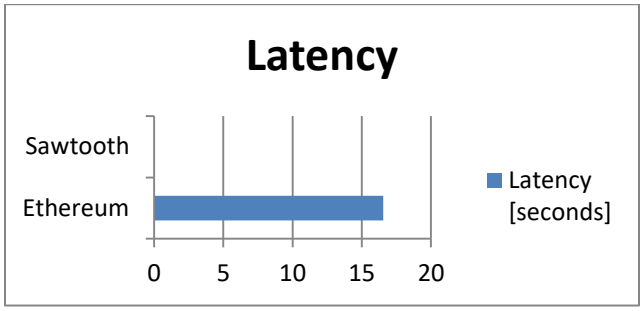

Fig 14: Latency chart

From Figure 15, by comparing the amount of data transferred, the Sawtooth sends less amount of data to the server where the blockchain are stored. Ethereum sends 27.7% more data than Sawtooth.

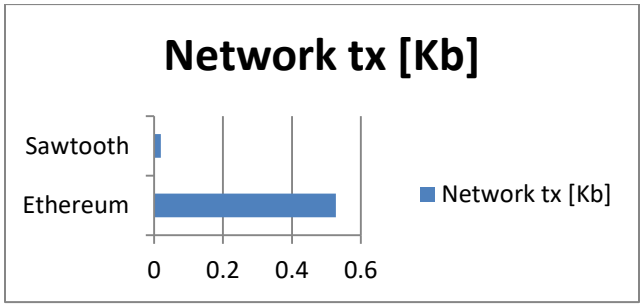

Fig 15: Network transmission chart

From Fig 16, as the data transferred is less in the Sawtooth the amount of data received also less when compared with the Ethereum. It is estimated that Ethereum received 34.7% more data than Sawtooth.

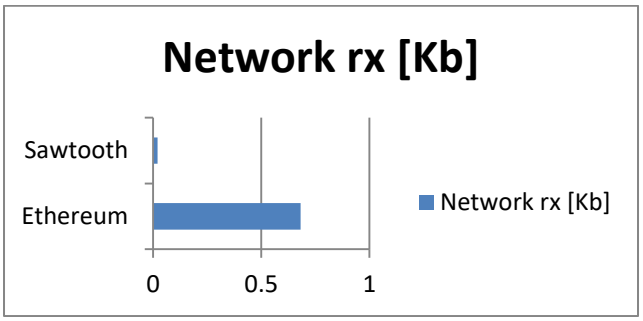

Fig 16: Network Receiving chart

From Fig 17, CPU usage is monitored for the calculation of the CPU Load. From the observation, it is clear that Sawtooth CPU Load is 5.9% lower than Ethereum CPU Load.

ISSN: 2233-7857 IJFGCN

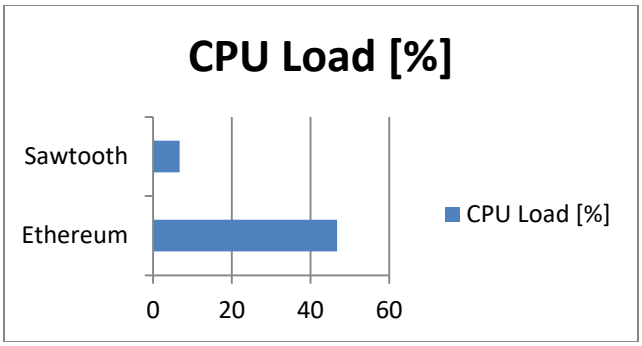

Fig -17: CPU Load chart

Conclusion

In this paper, the IoT and Blockchain technologies is integrated so this helps to create transparent, fault tolerant, immutable and records that can be traced and audited. Test has been carried out using Hyperledger Sawtooth and with Ethereum on various performance parameters like latency, bytes transmitted, bytes received, and CPU load. Based on the test result we could witness that Sawtooth implementation proven better than Ethereum. But both have different stuffs on performance metrics so based on the scenario we need to choose the optimal implementation technique for better results. Ethereum is high scalable and reliable than Sawtooth since it supports more number of participants. If our primary focus is on the cost then it's not advisable to choose Ethereum. But Sawtooth implementations is suitable for devices which don't perform more computation like IoT devices, edge gateways.

References

[1] Caro, Miguel Pincheira, et al. "Blockchain-based traceability in Agri-Food supply chain management: A practical implementation." IoT Vertical and Topical Summit on Agriculture-Tuscany (IOT Tuscany), 2018. IEEE, 2018.
[2] Hua, Jing, et al. "Blockchain based provenance for agricultural products: A distributed platform with duplicated and shared bookkeeping." 2018 IEEE Intelligent Vehicles Symposium (IV). IEEE, 2018.
[3] Malik, Sidra, Salil S. Kanhere, and Raja Jurdak. "ProductChain: Scalable Blockchain Framework to Support Provenance in Supply Chains." 2018 IEEE 17th International Symposium on Network Computing and Applications (NCA). IEEE, 2018.
[4] Litke, Antonios, Dimosthenis Anagnostopoulos, and Theodora Varvarigou. "Blockchains for Supply Chain Management: Architectural Elements and Challenges Towards a Global Scale Deployment." Logistics 3.1 (2019)
[5] Mondragon, Adrian E. Coronado, Christian E. Coronado Mondragon, and Etienne S. Coronado. "Exploring the applicability of blockchain technology to enhance manufacturing supply chains in the composite materials industry." 2018 IEEE International Conference on Applied System Invention (ICASI). IEEE, 2018.
[6] Owens, Luke, et al. "Inter-family Communication in Hyperledger Sawtooth and Its Application to a Crypto-Asset Framework." International Conference on Distributed Computing and Internet Technology. Springer, Cham, 2019.
[7] Rajsingh, Elijah Blessing, et al., eds. Advances in Big Data and Cloud Computing. Vol. 645. Springer, 2018.
[8] Manali J Dubai, T R Mahesh, Pinaki A Ghosh "Design of new security algorithm: Using hybrid Cryptography architecture", 2011 3rd International Conference on Electronics Computer Technology, 2011.
[9] A. Aderibole et al., "Blockchain Technology for Smart Grids: Decentralized NIST Conceptual Model," in IEEE Access, vol. 8, pp. 43177-43190, 2020.

ISSN: 2233-7857 IJFGCN

[10] Saberi, Sara, et al. "Blockchain technology and its relationships to sustainable supply chain management." International Journal of Production Research 57.7 (2019): 2117-2135.
[11] Chang, Shuchih Ernest, Yi-Chian Chen, and Ming-Fang Lu. "Supply chain re-engineering using blockchain technology: A case of smart contract based tracking process." Technological Forecasting and Social Change 144 (2019): 1-11.

ISSN: 2233-7857 IJFGCN