ISSN No:-2456-2165

Blockchain Based Food Safety

Mithu Raveendran
Dept. of Computer Science
Sahrdaya College of Engineering and Technology
Thrissur, India

Reshma Francis
Dept. of Computer Science
Sahrdaya College of Engineering and Technology
Thrissur, India

Sneha Haridas
Dept. of Computer Science
Sahrdaya College of Engineering and Technology
Thrissur, India

Shyam Krishna K
Assistant Prof. (Dept. of Computer Science)
Sahrdaya College of Engineering and Technology
Thrissur, India

Abstract:- Food safety problems have drawn vast attention after the detection of various cases of food poisoning and contamination. This poses serious threats to public health and in- frastructure and makes adverse impact on social balance. In this scenario, food safety management plays a crucial role in achieving social stability. Nowadays the food supply chain is struggling with issues like fraud and corrupt activities. Monitoring and controlling all the activities involved in the food chain is a very risky process. This kind of monitoring is also expensive because it is a large scale network. Nowadays, most of the organizations are embracing the idea of transparency in the supply chain of food products. In this situation, blockchain is the best technology for providing transparency as well as safety. Blockchain technology stands out as a way to assure immutable and transparent chain of processing and tracing each step of the supply chain at the individual food processing stage. This paper depicts the efficient use of blockchain for food safety. Blockchain's advanced features make it capable of providing a basis for complete traceability of food products, from it's raw state to final state and ensure better performance and security and also ensures the data found in blockchain ensures the food safety standards. The system is implemented in the ethereum truffle platform using Solidity language. The framework represents blockchain-based secure infrastructure for supply chain of food products among all the participants in the chain.

Keywords:- *Blockchain, Ethereum, Food safety, Solidity, Traceability.*

I. INTRODUCTION

Nowadays, the distance that food products travel from producer to consumer has increased as a result of globalization in food trade. Therefore, keeping safety and quality along the food supply chain has become a significant challenge [1]. Some of the benefits of blockchain-based supply chain include improved supply chain decision-making, sourcing, inventory tracking, transparency, and visibility. These benefits not only improve supply chain operations but reduce cost and time [9]. There are many ways to ensure the quality of the food the consumer gets. One of them is the way government tags them or stamps them. The other ways are certification which usually appears in the sticker of the packaged item. But these certifications though ensure the fact that they have met government standards, it has come under the notice that many food products have escaped the government radar and was only taken back after numerous lawsuits. Food products like Maggi, or even some other products that comes under cosmetics, personal hygiene products like shampoos etc., has come into the scene only after it's widespread market distribution. An average consumer may not understand the meaning behind the ingredients or the importance of the concentration of ingredients. There is no definite way to know the path of the product into the market. Many unethical practices, especially in the field of farming, is done by middlemen. As a normal consumer, they don't get the complete information of the product they are buying. Though after extensive investigation they may find the path, but the people involved and whether at each stage, if the quality was maintained, are questions that ponder the mind of all consumers. Through personal efforts and for official purposes, people go behind the market and search to get these information. Still, it's an impossible task for a commoner. Traceability provides a set of information about the source of raw material, process, and location of the product along the supply chain. It also acts as a tracking and communication tool to ensure information accessibility along the supply chain [7]. The traceability is attempted to solve through one among the most recent technologies called blockchain. Blockchain is a cutting-edge technology that has great potential for improving traceability performance by providing security and full transparency [8].

Blockchain is a list of blocks, each of which includes multiple data, managed by a peer-to-peer network adhering to a protocol for inter-node communication. The legerdemain of blockchain lies in the protocol of ratifying new blocks, in the short, consensus mechanism. The majority of the nodes will agree on the existence of each block via consensus algorithm after validating the data in the block. It can be comparatively laborious to tamper the data on the blockchain since most of the nodes will not confess it. There are different kinds of blockchain systems, including permissionless and permissioned blockchains, targeting for different application scenarios. The characteristics of the blockchain technology bring about the aspect of system decentralization at the same time with data

immutability. These properties provide potential opportunities for fulfilling the prerequisite of supply chain data management. By using the blockchain to store and supervise the data flow in the supply chain, the information cannot be easily tampered and serves as reliable proof of existence. Data from various stakeholders in the supply chain can be consolidated into the blockchain system rather than storing seperately in individual systems, which not only helps for the data sharing but save cost and time for data retrieval.

As a permanent and immutable record, blockchain is created by superimposing encrypted data in chronological order. With the nature of tamper resistance, traceability, decentralization and cryptographic security, blockchain technology has become immensely popular in the latest research on food quality assurance. A smart contract being an executable code on the blockchain platform, acts as a digital agreement among participants. Due to data transparency, blockchain enables companies to understand useful information quickly. In addi- tion, the data immutability of blockchain ensures that the data is authentic and that data tampering is impossible. Based on these characteristics, blockchain technology has been widely used, including the Internet of Things (IoT), finance, electronic medical records and energy. A smart contract also acts as a digital agreement among participants. With rights, reducing time and economic costs, smart contracts have been applied in various traditional and emerging fields [2].

The remaining parts of this paper are organized as follows: Section II consists of the related works and identifies the main and unsolved challenges. Section III introduce the preliminar- ies needed for addressing these issues. Section IV shows the evaluation metrics. Section V describes the requirements and architecture of the system. Section VI discusses the system model. Section VII deals with the implementation of the system. Section VIII gives the result analysis and evaluation. The last section concludes the paper and provides a possible optimization direction for further system development.

II. RELATED WORK

Research in traceability using blockchain and how much it can contribute to quality assurance of items has been increas- ing steadily in recent years. In this section, the related works on traditional food monitoring and blockchain technology's role in traceability is reviewed.

A. Using blockchain with EPCIS

In order to track and to prevent food safety problems effi- ciently, blockchain can be used. It is a promising technology for food safety traceability because it is secure, tamper-proof and immutable. In some works like [6], EPCIS short for EPC information services is used along with blockchain to avoid and solve the problem of data explosion, data sensitivity problem and trust transfer. Actually it is a collaborative model consisting of on-chain and off-chain data to improve the performance. Here the EPC network is used in the off-chain module whereas a smart contract is used in the on-chain module. The work is mainly focused on curbing the data explosion menace. This system traces the key traceability information of food. It implements the usage of both the EPCIS and blockchain. On-chain information mainly focuses on the credibility of the information, information discovering services and privacy disclosure. Off-chain focuses on the data preservation and management of the EPC network. This system mainly deals with the data explosion.

B. Food quality assurance using blockchain

It is a quality monitoring system where blockchain together with machine learning is used. This system has the character- istics of high automation and high reliability in which machine learning is used for predicting the quality. The data is stored in the blockchain with the help of a smart contract after each stage. Then the data is compared with one another. The quality of the material especially aroma is evaluated by the PCA method. Then the texture gets evaluated by the HCA method. The GC-MS data are the main elements which are stored on the blockchain. After each production stage, the obtained data are evaluated by models. This process is executed by the quality evaluation contract (QEC). Once the evaluated score is lower than the threshold, the smart contract QEC will create a notification message and terminate the production process [2].

C. Motivation of this paper

As seen in the related works section, there are many papers focusing on the traceability. This work aims to design an optimized monitoring network for the regulation of food safety and also to incorporate blockchain for traceability but also on how these technologies can be merged to ensure quality of the items being supplied. It is an attempt to tackle some key problems listed below.

- How to ensure the quality by using blockchain?
- How to deploy it in the real scenario ?
- How to ensure quality and tracking but keeping informa- tion explosion low?

III. PRELIMINARIES

In this section, we will review the relevant background knowledge that will be used in this paper, including data anal- ysis methods, blockchain, cryptocurrencies and smart contract technologies

A. Blockchain

Blockchain is a decentralized, immutable and shared public ledger. Blockchain is composed of add-on blocks that include all transactions of the data. Each of these blocks is hashed and then it's linked to the next. These records contain a secure, immutable and tamper-proof data. These records are like a chain and maintained by all network nodes. According to the transaction participants, a blockchain can be a public, consortium or private blockchain. A public blockchain allows any node to read or write entries to it at any time. In the consortium or private blockchain, only some trusted nodes are involved in the

ISSN No:-2456-2165

decision to create a new block. Due to this, consortium and private blockchains are applied in iden- tity authentication, copyright management and data storage services [6]. Blockchain by definition is decentralised and any change happening to the content is recorded permanently [4]. The key characteristics of blockchain are decentralization, immutability, transparency, efficiency, security, and anonymity. The blockchain system can be divided into permissioned and permissionless [5].

B. Smart contracts and Ethereum

Ethereum is the blockchain platform that aims to provide smart contracts, which are codes present on blockchain and can be approached by the users of Ethereum. These are capable of receiving and transferring of assets, at the same time perform random calculation [10]. The smart contract is an agreement embedded in the computer code that is managed by a blockchain network. It is a peer-to-peer network of computers. Smart contracts are self-enforcing piece which is automatically executed once it is deployed on a blockchain. Ethereum offers a Turing complete script language and enables users to design any arbitrary smart contracts that can be pre- cisely defined. A smart contract in Ethereum can be written in a high level language, such as Solidity, hyperledger, R3Corda etc. A Solidity program is compiled to a low-level code, which is called an Ethereum virtual machine (EVM) code [2].

The smart contract will be valued and executed without the help of human intervention. It contains a set of rules under which the parties agree to interact with each other. Ethereum is open sourced and hosts a public blockchain [3].

IV. REQUIREMENT ANALYSIS AND SYSTEM ARCHITECTURE

A. User requirements

The food safety system dapp can have many participants who are grouped mainly into three categories viz. end con- sumer, distributor, and an administrator. Their functions, de- mands and roles are briefly summarized below:

- **End consumer:** They are the people who are recipients of the service provided by the dapp. They primarily involve the end customer who buys the food item and opens the Dapp to trace the path of the product. There are various ways to implement the part of getting the product's id number. The demand of an end consumer is to be able to view the path. From the path, the person is able to identify the hands the product has crossed and the contribution of each stop the product has made. Their role is to type in the id number or simply scan the QR code.
- **Distributors (Nodes):** In the usual supply chain, the product begins it's journey from producers to other enterprises involved in the chain and finally to distributors and then to retailers. All these people are represented as nodes through which the product moves. The demands of distributors from this dapp is to have a convenient interface that has the following fields:
  - A field indicating the address to which the product is to be transferred.
  - A field to write down if the quality of the product has been maintained at that stage.
  - A field for marking the value added which can be used to estimate the price.

The role of the distributor is to fill down these fields and initiate the transaction to record the transfer of the token.

- **Administrator:** In real life scenario, usually, blockchain will have humongous data which can be extracted for various other purposes including research. A person or group of persons must be responsible for the periodic maintenance of the network and resolve any technical dif- ficulties. Just like a database administrator, a blockchain administrator is responsible for directly interacting with the blockchain. The demands of the administrator involve the maintenance of the blockchain. Blockchain uses real money to function and has to be funded consistently to maintain. An administrator needs to be ensured that the blockchain stays funded to allow continuous transactions. The role of the administrator is to maintain and fix any technical errors that might pop up. They are responsible for altering the code based on new versions and ensure the code is optimized so as to take up less gas whenever possible.

B. System requirements

The system discussed should be able to satisfy the following requirements:

- Fetch the data - Read the blockchain and take data that corresponds to the situation.
- Make sure the data is visible only to the authorized people when needed - Even though it is public, during large scale deployment of a dapp, it might be needed to hide data. Hiding here implies to show only what's needed whenever needed.
- Ensure the integrity of the data - Here, data can be entered wrongly and then re-entered. In such a case, the wrong data remains in the blockchain because no data is ever erased from the blockchain. But while fetching the data, the system needs to ensure that only the right data is fetched.
- Interactive viewing – The data fetched must be simulated in the front-end in a manner understandable to the con- sumer with relevant details.
- Data in the system must be tamper-proof.
- The total cost of the system should be affordable.

ISSN No:-2456-2165

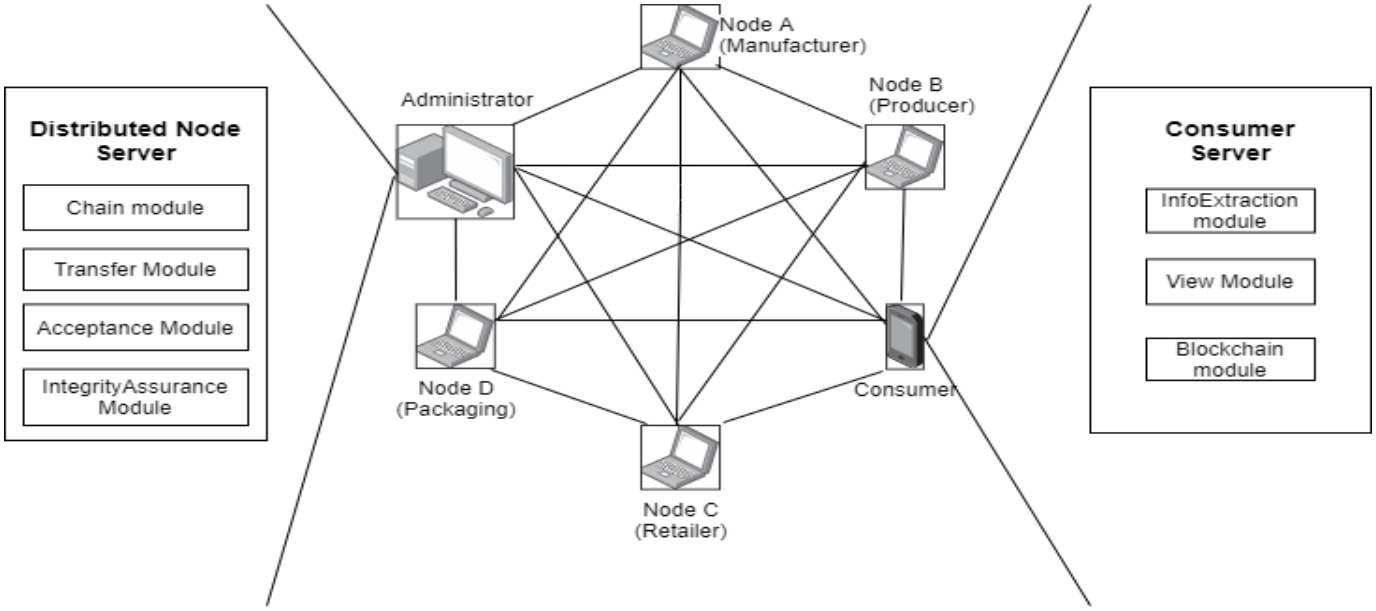

Fig 1:- Architecture of food traceability DAPP

C. System architecture

The proposed food safety traceability dapp based on blockchain consists of two front ends mainly. One is for the distributors to enter data and the other is for the consumer to view the path in interactive or list form. The design of the distributor front-end can be created in any way deemed appropriate based on performance. The design currently followed is in the format of a simple form. The interface is for now done using the IDE called remix. This UI can be used to directly interact with the back end to simulate the working of transfer of the objects. The transfers are stored in the blockchain permanently and can be retrieved when needed through javascript to display it in the consumer UI. The system architecture is shown in figure 1.

The consumer server consists of three main modules. De- tailed description is given below.

- **Infoextraction module:** This module mainly is used to pick out the necessary data based on the food product id. The information what is needed is extracted via javascript. This module can be customized based on industry demands. In other words, priority of people vary according to region. For certain items, the need for knowing the quantity of the value added might not be as important compared to certain other items like medcines etc. Hence, picking the necessary details based on food product id is the main function of this module. In the dapp, only the food product id is taken as input.
- **View module:** This module is responsible for presenting the information in a pleasing manner. This module is an enhanced version of the previous module as this deals with customization of view data. Usually in real life, the journey for most food items is very large and displaying all of them in a screen can be clumsy.
- **Blockchain module:** This is designed to link the client system with the blockchain server which is usually hosted in many server computers. It is through this portal the information is requested or queried.

The distributor-node server consists of five modules. The detailed description is given below:

- **Chain module:** This module deals with the maintenance of the blockchain. It is used to provide options for participants to either act as a full-time node or a part- time node. It is used to allow the entry and exit of nodes. Whenever a new node (say a manufacturer) comes into business, it should be given a choice on it's contribution to the maintenance of the database. Node here implies the various nodes in the supply chain. It has to be authenticated that the node is actually a part of the supply chain. Blockchain is intrinsically reliable as it's working is such that it facilitates transactions between mutually untrustworthy nodes. However, it is important that the manufacturer ensures that the item is sent to the retailer and the address supplied in the Transfer module is of the retailer (or the intended recipient). To authenticate the node is the real node, digital signatures can be used. Each verified node will be registered under government and will be having their own identifying numbers. Apart from this each transaction initiated is encrypted and digitally signed by the private keys of both the parties. The public keys of the companies are public and known beforehand. After transaction both the parties can verify the signature of the companies involved in the transaction and ensure that the node they dealt with was real.
- **Transfer module:** This is the module that contains the logic of the program that does transfer of product items. The node which can be manufacturer, distributor or anyone in the chain can give their address and the address to which they intend to transfer the data and the execute it. This will like other modules cost gas money but this will also cost additional ether (Ether is the currency used in Ethereum).

- **Acceptance module:** This is the module that is used by the receiving node to accept the item. If the item transferred in system's logic using transfer module is not accepted by the intended recipient, the transaction cannot be said as finished. The node which receives the item gets a prompt along with it to authorize the reception of the said item.
- **IntegrityAssurance module:** This module is used to get details regarding the properties pertaining to the prod- uct being passed. The sender can add details regarding the properties such as chemical constituents, physical constituents, appearance, texture etc. This form usually depends on the food product being passed and has to be tailor made for each type. For simulation purposes, a form consisting of two fields can be created and then compared with the norms issued by food safety standards. Only if the input values adhere to the norms, the item shall be accepted into blockchain.
- **Transaction module:** In this module, the transfer module and acceptance module are simultaneously checked and if values returned from both are true, the transaction can be finalized and tagged as complete. This will ensure there is no ambiguity in the path and if anything goes wrong, it's easy to track at which node the product was delayed procurement. This module is important as such details is of very much importance to the authorities.

V. SYSTEM MODEL

The important feature of this dapp is ensuring the integrity of the information stored, ensuring if the food safety standards were kept during it's path, preventing accidental wrong data and reducing the problems of data explosion. Among the modules, some interact with each other like the Transaction module and some other modules interact directly with the blockchain like the Transfer module. Some of the features of the proposed system are:

- **Assurance of integrity:** The important feature of this dapp is ensuring the integrity of the information stored. Blockchain by definition is permanent and data can never be removed. Any attempt to remove or change existing data will reflect throughout the system and hence if any wrong data is entered. All that can be done is enter a tag in the succeeding block indicating the preceeding block had erroneous data. Similarly simply putting journey of the item in blockchain does not ensure or help the con- sumers in ensuring if the food safety standards were kept during it's path. Hence, before allowing the transaction to enter blockchain, the module 'IntegrityAssurance' which is customizable and has to be customized in real life scenario is to be used.
- **Constrained flow of data to the blockchain:** With the IntegrityAssurance module, only the data that satisfies the standards are allowed to enter the blockhain. This prevents accidental data from entering the ledger. It also checks every data that enters the ledger. In this way, we can reduce the data explosion that might happen. Having checked data reduces the problem of extensive cleaning procedures that are usually done before data analysis. The noise in data is considerably reduced.
- **Flaw check in the product path:** While entering data into the blockchain module, If the standards are not met, the data fails to enter the blockchain and transaction is not recorded. If the product appears in another node spontaneously, the break in the path will be seen when the data is retrieved from blockchain which will alert the consumer. This is also a research area where Machine learning and Artificial intelligence algorithms can beused to predict any anomaly or suspicions.
- **Hiding of unrelated or unneeded data:** The Infoextrac- tion and view module together ensures that only informa- tion that is authorized to be seen by the client is shown. Various privilege settings can be used to achieve the same. The view module customizes the view according to the product which is being tracked.

A. Details of implementation

Four types of events are used to simulate the events. They are:

- TransferItem
- AcceptItem
- TransactItem
- IntegrityAssurance

Name of the event	Description of the event	Returns
TransferItem	This event indicates the trans- fer of the item from the sender to receiver. Can be imple- mented in various ways includ- ing using ERC tokens.	-The product id -Address of the sender -Timestamp -Address of the receiver
AcceptItem	The recipient node on receiv- ing the item produces this event to indicate that the item has reached it's destination.	-The product id -Timestamp
TransactItem	This event indicates the trans- action between nodes has been successful.	-Address of the sender -Timestamp -Address of the receiver
IntegrityAssurance	This event indicates that the integrity has been assured by the sender.	-Flag -Product id

Table 1:- Function of the Events

ISSN No:-2456-2165

The system uses Ethereum which is an open source, public, blockchain-based distributed computing platform and hosts smart contract functionality. The smart contract which is a computer protocol intended to digitally facilitate, verify, or enforce the negotiation or performance of a contract is the fun- damental code building block in the development of ethereum applications. It is the starting point in the development of this dapp. The structure of the smart contract is shown in Figure 2. It can be divided into logical layer and data layer. The logical layer consists of various methods and events that per- form the functions of alerting recipient, integrity verification, identification of product id and verification of transactions. The data layer typically consists of two primary objects 1. Node or distributor (which represents the various participants along the supply chain) and 2. Item (which indicates product item). The data is picked up from the data layer via the logical layer using Web3.js or ReactJS. Web3.js is used for simplicity.

Apart from this, the data layer also have blockchain based data such as transaction hash number, block number, age which indicates how long ago the block was created, hex- adecimal address of the sender and receiver, the value of ether exchanged, the gas fee, gas price at the time of creation of the block and the nonce used for that transaction. It also stores the proof of identity of the nodes involved by storing the public key of the nodes. A sample of how data is stored in a mainnet (main network) is shown in figure 3. Various test networks like Rinkeby, Ropsten etc. are used to simulate the working because actual deployment costs real money and is not suitable for development purposes.

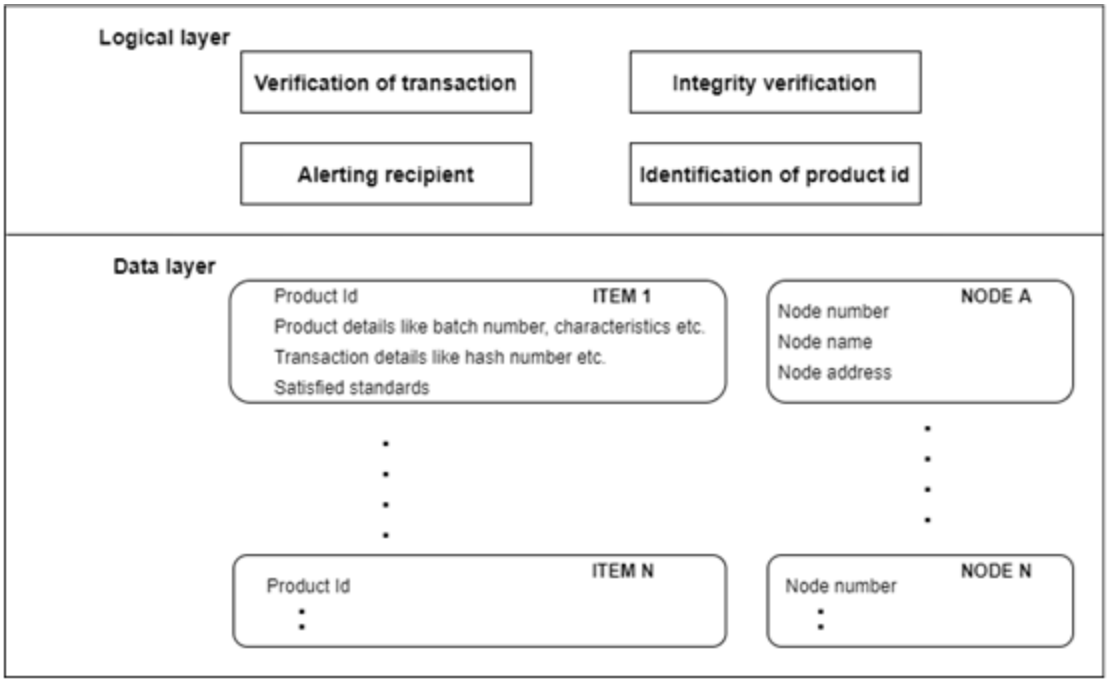

Fig 2:- Structure of smart contract

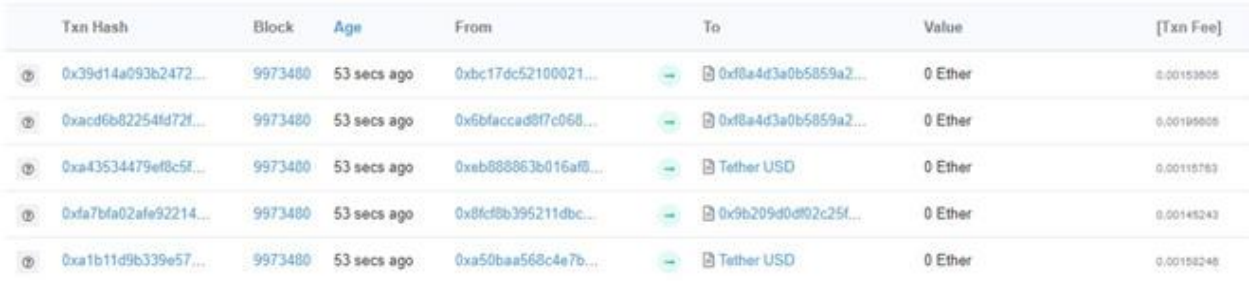

Fig 3:- Storage of data in mainnet

B. Data flow of the system

The dataflow of the system includes the process of upload- ing data to the blockchain ledger, retrieving data from the ledger and finally displaying it appropriately. The working of the system is shown in figure 4. The complete process is explained below:

➢ *Uploading data to the blockchain:*

- Initially, the product starts from a node (say a producer) who produces and can assign a batch number and product number to the item.
- When the producer sends their raw material to a manufac- turer for further processing, they invoke the transferItem module to transfer the item. While doing

so, the details regarding the batch number, product id etc. are entered into the server.
- This prompts the IntegrityAssurance module to confirm whether the raw material being passed has met the food safety assurance standards if applicable.
- Once the IntegrityAssurance module is used to ensure this, the data is uploaded to the blockchain. The product may begin physically moving to the destination.
- Once the transferItem is done, the receiver receives a prompt to acknowledge the reception. This data is then uploaded to the blockchain directly.

➢ *Offline interaction:*
- The transactItem retrieves the product id status and ensures the transaction is complete.
- It updates the status of the product id.

➢ *Retrieval of data:*
- The user enters a product Id (The id could be entered, could be scanned through a QR scanner or even RFID can be used to enter the data. The options are endless). Since the focus is more on the back end, simulation of input is done by typing in the product id.
- The client or consumer side of the module uses it's functions like Infoextraction module to extract the information by keeping the product Id as index. The smart contract's methods are called using Jquery.
- The view module customizes what is needed to be shown and displays or collects information with regard to the characteristics of the product.
- The user can now view the path.

VI. SYSTEM IMPLEMENTATION

The implementation of the modules briefed earlier, along with the origin of events, and retrieval of the data together comprises the working of the Dapp.

➢ **Transfer module:** The transfer module basically engages in transfer of the item. It is called by the sender by interacting with a UI that's visible only to the node system administrators. The transfer module can have an additional form to fill about the product being transferred. Whenever smartcontract is called, this will use some ether from the sender's wallet. For small scale applications, a simple wallet hosted by MetaMask Chrome extension can be used. Figure 2 describes how this wallet connects with infura which is an application that allows the usage of ethereum network without putting up or hosting the node as an ethereum node. In other words, the system can choose not to involve itself in the proof-of-work calculation or any other consensus mechanism.

➢ **IntegrityAssurance module:** Whenever Transfer module is called, it eventually leads to this module which directly deals with the characteristics of the product being passed and compares it with the common or government stan- dards. Only if it meets this standards, the transferItem module is executed. Calling of any module located in the smart contract picks up gas or money and calling of this module too picks up ether. This ether is subtracted from the node's wallet. The IntegrityAssurance module has to be tailor made for the application as various food products has varying demands. Once the integrity is assured, the transaction is initiated. This will cause a huge transfer of money depending on the block size to be transferred to the recipient. Since the sender too shall receive some money this way when other parties send items to this node, this cash runs through this system and doesn't pose much threat to the system. The block is created and can be referred by any party through various websites like etherscan. It can also be hidden for privacy.

➢ **Acceptance module:** Once the recipient receives the item, it calls the acceptance module which will cost some ether again. Absence of calling this breaks the continuity of the flow and this break will be visible when the consumer looks up the track record. When both these modules are returned as true, the transaction can be said as complete and a new block for this is created by calling TransactItem.

The block creation is usually a time consuming process as necessary proof-of-work has to be generated. Hence all these modules will be called in a very smaller pace. This process repeats in all nodes until that item reaches the consumer. The chain module is responsible for the maintenance and hassle free processing of the previous step.

When the consumer picks up the item, he or she looks up the path by calling the Infoextraction module. Calling of this module consumes ether and the data collected by it is accepted by Web3.js. The web3 then uses these data and presents them in a user friendly manner. Infoex- traction extracts all information like transaction block, hash number etc. which are of no relevance to the end consumer. The view module can be called for retrieving only specified information.

➢ **Blockchain module:** This is the fundamental module that acts as a platform for the rest of the modules. This dapp is created in ethereum truffle platform using the language of Solidity version 5.0.0 or above. The cryptographic hash function is used to create the digital signature for each unique block. There is a large variety of hash functions, but the hashing function that is used by the Bitcoin blockchain is the SHA-256 hashing algorithm. This is used to encrypt the event information data and product details from the outside world. The reliability of the sys- tem is guaranteed by the usage of these strong algorithms and harder nonce values. The consensum method for rinkeby test net within which development was made is Proof-of-authority. Most popular versions of blockchain particularly those used for financial purposes use Proof- of-work algorithms to achieve consensus.However, there are other ways like Proof-of-stake, Proof-of-authority etc. In this model, before deploying to the mainnet, the system is tested in rinkeby test network which unlike Ethereum mainnet, is a proof-of-authority network. Proof of au- thority delivers comparatively fast transactions through a consensus mechanism that is based on identity as a

ISSN No:-2456-2165

stake. It registers blocks faster and is not done by a lot of machines computing to create a number satisfying a particular criterion which takes a long time. The proof-of-authority mechanism in a larger sense allows certain nodes or a group of nodes to validate blocks which has it's own advantages such as faster processing, absolutely little to no computing power hence low cost. This is advantageous for development purposes but is not recom- mended in a full-fledged system as it causes the ability to grant permission for block creation in the hands of a few nodes. During development purposes, a lot of money can be saved during testing when Proof-of-Authority is used.

VII. TEST RESULTS AND ANALYSIS

A. *System Test*

For development and testing purposes, five computers along with their ethereum addresses were taken together for a net- work pretending to be intermediary nodes in the supply chain. Since blockchain has consensus algorithm and to perform this, there should be large amount of computers in the network. Hence, the rinkeby test network was used to simulate the events. The details of test environment is given in table 2 and the details of hardware environment is given in table 3.

Development Platform	Sublime Text 3
Operating System	Windows 10 Home
Blockchain Module	Ethereum Truffle v5.0.8
Smart Contract	Solidity v0.5.12
Javascript	Web3.js v1.2.1

Table 2:- Software Environment

CPU	Intel(R) Core (TM)i5-7200
Hard Disk	TOSHIBA MQ01ABD100
Memory	7GB
CPU Cache	4MB
FSB	1000Mhz

Table 3:- Hardware Environment

Other dependencies for running the dapp includes a lightweight development only node server with a version greater than 2.3.0. This also called as lite-server that serves a web app, opens it in the browser, refreshes when html or javascript change, injects CSS changes using sockets, and has a fallback page when a route is not found. Performance of any system primarily depends on the time. The time calling the function and the time in which the block is created are indicators of performance. Creating the necessary proof-of- work or proof-of-authority takes some while which increases as complexity of nonce increases. However this can be reduced to acceptable levels by controlling the nonce values. As figure 4 indicates, even after the function is called and funds transferred, block creation takes more than 10 seconds.

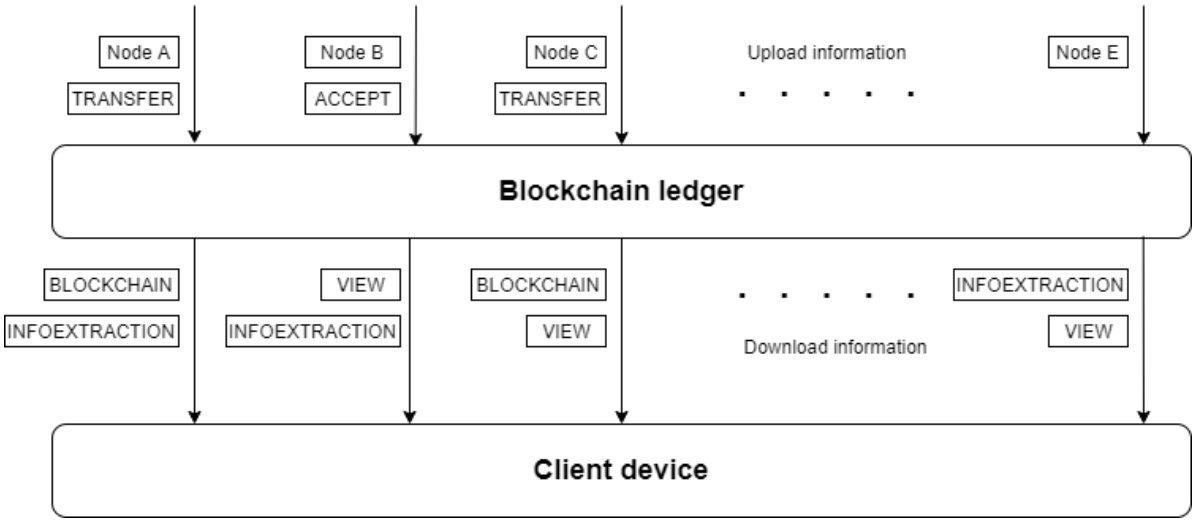

Fig 4:- Working of food traceability DAPP

Features	Traditional sys- tems	ML based sys- tem	Information-based systems (EPCIS etc.)	Traditional file management systems with blockchain	Food safety dapp
Information traceability	Low	-	High	High	High
Data integrity	Low	Medium	Medium	High	High
Privacy Protection	Medium	-	Medium	High	High
Degree of decentralization	Low	-	Low	Medium	High
Amount of on-chain data	-	-	-	Low	Medium
Amount of off-chain data	-	-	High	Medium	Low

Table 4:- Comparison between Various Methods

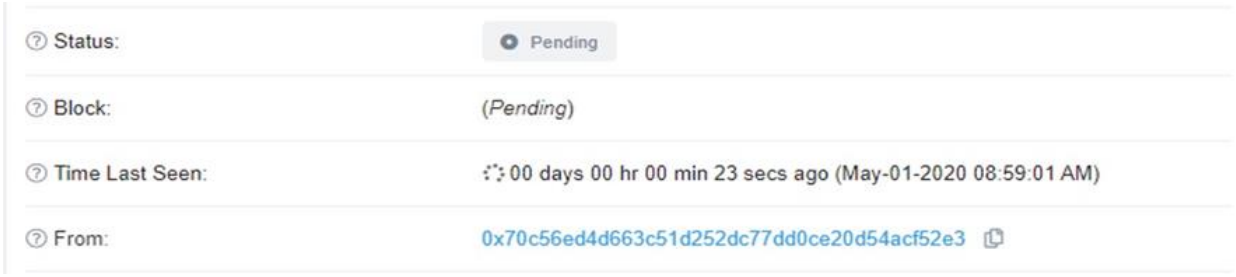

Fig 5:- Delay in block creation

B. Comparison

After successful demonstration of this idea, it can be noted that this idea has the following advantages over the other works previously mentioned:

- **Higher degree of decentralization:** Our system is com- pletely decentralized. We detach the centralized system inorder to ensure the credibility of the system. This is unique to many of the blockchain projects. However, in many of them, important data is stored in offchain manner which compromises with the decentralized storage of data. This idea enables all essential data to be stored in the blockchain.
- **Privacy:** Since our system is decentralized, only the concerned authority can access the data which guarantees privacy
- **Robust and tamper-proof system:** Robustness indicate that any kind of server breakdown will not affect the performance of the system because there are many copies of the data in various systems involved in the blockchain. In traditional systems this is handles by keeping backups. Blockchain is inherently difficult to change because for creating any change, there is a lot of work that needs to be done and those work will be reflected throughout the system which indicates corruption. Integrity of the data can be still maintained because it takes up extensive computer resources to bring about such changes which are not feasible
- **Legitimacy of the data uploaded is guaranteed:** Be- cause of the integrity assurance module one can be sure the data found in the blockchain is true and when it comes to quality of food items, it can be ensured that the quality has been met because it's the system that's comparing the provided standards with the existing standards.
- **Affordability:** This system is affordable as even though it takes ether to transfer object. The money is transferred back to the node when another node transfers any item to this node. The money keeps circulating within the supply chain. Usage of this system will not increase the cost of the item being supplied.
- **Independent of other management systems:** This dapp is standalone and doesn't use any other information service systems or it's APIs for fetching data. However, this can be added based on needs.

Table 4 summarises the differences between the idea of food safety dapp elaborated here versus other systems like the traditional systems, ML based systems which is primarily used to predict quality etc., and Information based systems like EPCIS.

VIII. CONCLUSION AND FUTURE WORK

This work focuses on the solving some of the issues with traditional food traceability system. It can be noticed that various attempts by many scholars have been made with regard to the same and each time a new problem is solved. In this system, the issue of ensuring integrity to the data entered in to the blockchain ledger is solved. Just because there is data in blockchain, it doesn't ensure that the food product has met the quality standards and keeping all sorts of data would create data explosion. Hence, in this system data is thoroughly checked either manually or through a computerised checking before uploading it into the chain. This step depends on the item being processed. To conclude, a decentralized system based on blockchain was designed and transactions were secured using smart contract. Through the comparison with the current systems we arrived at a conclusion that our system not only tracing the food but also ensuring performance in tamper-proof, privacy protection ,degree of centralization and amount of on-chain data. Also we reduced the cost of the traceability system. Our system is basically customer oriented. It helps the customer to get the path of the food from the beginning to end.

For improvements, some of the place where future works on this topic can emphasis upon are:

- Customisation of quality check module – Since the supply chain is vast, there is a large number of items and with each, varies the parameters for standards. It's hard to customize all so some way to solve this is an interesting research area.
- On chain data explosion – Once the customer buys an item say some food product with an expiry date, it's wasteful of memory space to hold on to that transaction in memory for more than 3 to 4 years. There could be a way to stop maintaining that block after a specific threshold. This keeps the on chain data limited.
- Optimisation of consensus algorithm – Depending upon the consensus algorithm used, the speed varies. It's a research area to optimize these algorithms without com- promising on security.
- Use of crypto tokens – Use of cryptographic tokens like ERC 20 etc. eliminates asymmetry of information present during the transfer of ownerships.

ACKNOWLEDGMENT

The author would like to thank the co-members, associate editor and anonymous reviewers very much. Their comments and suggestions are very valuable and helpful to the modifi- cation of this paper.

REFERENCES

[1]. **Aung M. M., Chang Y. S.**, (2014), "Traceability in a food supply chain: Safety and quality perspectives ", *,Food Control, 39, 172–184*

[2]. **Bin yu, Ping Zhan, Ming Lei, Fang Zhou, Peng Wang**, (2016), "Food Quality Monitoring System Based on Smart Contracts and Evaluation Models ", *Natural Science Basic Research,volume4*.

[3]. **Mithu Raveendran, Reshma Francis, Sneha Haridas, Shyam Kr- ishna K**, (2020), "Food Safety using Blockchain", *Recent Trends in Information and its Application,volume3,Issue 1*.

[4]. **Satoshi Nakamoto**, "Bitcoin: A Peer-to-Peer Electronic Cash System ", *www.bitcoin.org*.

[5]. **Hongf Ang Lu, Kun Huang, Mohammad Amin Azim, Lijun Guo**, (2017), "Blockchain technology in the oil and gas industry: A review of applications , opportunities, challenges and risks ", *China Scholarship Council ,volume XX,2017*.

[6]. **Qijun Lin, Huaizhen Wang,Xiaofu Pei and Junyu Wang**, (2016), "Food Safety Traceability System based on Blockchain and EPCIS ", *National Key RD Program of China* .

[7]. **Haleem A., Khan S., & Imran Khan M.**, (2019), "Traceability implementation in food supply chain: A grey-DEMATEL approach ", *Information processing in agriculture 6 (2019) 335–348.*

[8]. **Huanhuan Fenga , Xiang Wanga , Yanqing Duan , Jian Zhangd, Xiaoshuan Zhanga** , (2020), "Applying blockchain technology to improve agri-food traceability: A review of development methods, benefits and challenges ", *Journal of cleaner production.*

[9]. **Banerjee A.**, (2018), "Blockchain Technology: Supply Chain Insights from ERP ", *Advances in computers*.

[10]. **Ghosh A., Gupta S., Dua A., Kumar N.**, (2020), "Security of Cryptocurrencies in blockchain technology: State-of-art, challenges and future prospects ", *Journal of Network and Computer Applications*.