HBRP PUBLICATION

Recent Trends in Information Technology and its Application
Volume 3 Issue 1

Food Safety using Blockchain

Mithu Raveendran[1], Sneha Haridas[2], Reshma Francis[3]*, Shyam Krishna K[4]
[1,2,3]Student, [4]Assistant Professor
Department of Computer Science,
Sahrdaya College of Engineering and Technology, Thrissur, India
Corresponding Author
E-Mail Id: *reshmatfrancis@gmail.com*

ABSTRACT

Food safety management is an inevitable issue in the field of human health and social stability. It is expensive to monitor all entities that are involved in the food chain because it's a large scale network. Traditional supply chain and management systems have various issues like data invisibility, tampering and sensitive information disclosure. The existing traceability systems adopt either centralized architecture or distributed architecture. Blockchain is a disruptive technology consisting of blocks where each block contains a hash of the previous block, thereby creating a chain of blocks. The concept behind blockchain is a mutual trust based on cryptographic techniques. A traceability system based on blockchain can help to increase the efficiency of managing the supply chain. Advantages of blockchain include better visibility of data. The cost of tampering with data is high hence it is reliable. Until now, many researchers came with their version of implementation of blockchain for this purpose but each one has some restrictions. The proposed method has better performance in various aspects like transparency, security, traceability and better management of sensitive data.

Keywords*: Blockchain, food safety, solidity, smart contracts, ethereum*

INTRODUCTION

Most of the food industries faced food quality related problems. Examples of such incidents are the Sudan red, Melamine, and Horse meat, which not only affects the health of consumers, but also affects the stability of social economy. There is about high percent of the total production of fresh meat, vegetables and fruits are under the poor logistics which result in huge waste and increased cost[11]. So we need to portrait the issues in food industries. So according to the consumers they want to know the sources of products. However, most existing traceability systems tend to lack transparency, reliability and performance. When a food quality related problem is arising the traditional supply chain nodes doesn't involve in the prediction of root issues. Food security and quality assurance has become increasingly difficult in times of growing global flows of products. Food traceability turns to be very challenging for all the authorities. Providing an effective food quality traceability system is one of the main features to protect food quality and safety.

The traditional food traceability system has many issues. Firstly there will be a centralized system who masters all the information also, the information providers can tamper with information that is not favorable to them, while the consumer can hardly identify with the naked eye. Secondly, food industry chins involving many links, elements and participants. So it will tend to large communication cost. At last, information sharing between different nodes in the supply chain is very difficult to manage. Without information sharing and management, the industry data

is fragmented [3]. However, if the food industry data is shared, development of the food industry will experience great benefits which will be of use to research been carried out on minimization of the industry chain, and also increase the food quality supervision and anti-tampering abilities[11].

GENERAL BACKGROUND

In the past few years, to combination of blockchain technology with supply chain has become a new trend. Blockchain technology has advantages like decentralization and anti- tampering, and shows bright future to attenuate the availability chain management. The present researches mainly add two directions. One is to revamp the entire blockchain system from underlying architecture to meet the wants of the appliance in supply chain management. The opposite is to make use of the prevailing mainstream blockchain architectures to optimize system security and solve some pain points of the availability chain management. A blockchain based distributed permission management system was developed so as to record the identities within the nodes of supply chains through blockchain and supply permission verification feature for the knowledge interaction between different nodes [13]. There is an agricultural product supply chain traceability system supported blockchain and RFID technology. This technique achieved automatic collection and storage of data through RFID systems and blockchain technology[14]. Ganeshan and Harrison defined supply chain management as, "A supply chain may be a network of facilities and distribution options that performs the functions of procurement of materials, the transformation of those materials intermediate and finished products, and therefore the distribution of those finished products to the customers"[17]. Lee and Corey in 1995 defined it as, "The integration activities happening among a network of facilities that procure staple, transform them into intermediate goods then final products, and deliver products to the buyer through a distribution system"[18]. Christopher in 1998 defined SCM as, "The supply chain is the network of a corporation that's involved, through upstream and downstream linkages, within the different processes and activities that produce value within the sort of products and services within the hands of ultimate customer"[19]. The food processing defines because the agro industrial system aims for plantation, cutting, transport, and processing from farm to mill and mill to market [20].

PROBLEM DEFINITION

Traditional food supply chain management system has a centralized server who masters all the information. The in-formation in the server and the others in supply chain is not transparent. The information providers could tamper with the information which is unfavorable to them. Hence there will be corruptions and lack of accountability in the supply chain. Updations that are done by different nodes in the supply chain will not be immediately visible to all. The problem is to automate the updation process that happens in between each of these nodes. Where the only update we see are the start and end points of the travel path, and any inconsistency arriving middle this process is neglected. For example, a smartphone's GPS[5] history would give the information about path, and in how much time it was covered, but not if the smartphone goes out of range of the GPS satellite.

MOTIVATION

Food security and quality assurance has become increasingly difficult in times of growing global flows of products. Especially, the traceability of food turns to be very challenging to the authorities.

Additionally, it concerns the verification of food authenticity, for instance the right declaration of the geographical origin, variety and cultivation. Such quality parameters justify higher prices and thus, they're often within the focus of food fraudsters. A number of those qualities are often monitored by objective analytical methods, but not all of them. The protection of food safety and quality continuously poses new challenges for politics, industry and science. this is often particularly in line to the statement by the planet health organization that quite 23 million people suffer from contaminated food in Europe per annum of these affected, about 5,000 people die. On the one hand, the problems raised include conscious food fraud, because counterfeiters generally have a high level of ingenuity and knowledge domain, which makes it rather difficult to seek out the perpetrators guilty. On the opposite hand, despite the high standards of hygiene and measures for quality assurance, inadvertent contamination and residues within the end products occur again and again. These include, for instance, pathogenic germs, Noro viruses or salmonella, but also chemical compounds.

In addition, defined and consistently observed transport or storage conditions play an important role within the assessment of food quality. These all are happens thanks to the lack of traceability and quality of the foods[13]. For ensuring the traceability of food trade networks blockchain algorithms incorporate a high potential, as data are often stored in a un-modifiable way and enabling quick tracking across all process steps, in order that stakeholders also as commodities or semi- finished items are often identified much faster. Traceability system supported the blockchain has gained much popularity because its decentralization and data tampering prevention might provide solutions to the shortcomings of conventional systems[1].

OBJECTIVES

- Propose a model that incorporates blockchain and traceability. The model will be having high precision and stable performance.
- By this model supply chain systems can run smoothly and handle enormous amounts of data.
- The blockchain operates on a distributed platform, so in this model each participant has access to exactly same ledger.
- The proposed system guarantees the accessibility of sharing data among enterprises in specific supply chain and the inaccessibility of other enterprises.
- Proposed model provide mechanism to guarantee the quality and legitimacy of the data uploaded to the blockchain

LITERATURE SURVEY

Blockchain

Blockchain is a distributed ledger technology which is man- aged in a decentralized way. The idea behind the blockchain technology originally arises from the financial environment, whose basis for conducting transactions is a trusted instance such as a bank. However, this may become a serious issue if the intermediary follows its own interests and/or misappropriates funds. This technology allows transactions to be per-formed independently of a third party. It was first popularized by bitcoin. On the Bitcoin blockchain, transaction history will be given, everyone can check and verify transaction records digitally to prevent double spending the digital currency. Everyone in this blockchain is free from the need of a centralized mediating entity. Blockchain is also called distributed ledger technology. This is composed of many blocks and these blocks will be with data records. Each and every block will contain

a timestamp and also a hash value which represents the previous block. By this hash value the communication between the blocks can be established [5].The blockchain will be distributed on the computers of all subscribers, so that a peer-to-peer network is obtained. In these networks everyone has the same rights and regulations. Whenever the new data entry is created, it is first checked by all peers then only it is transferred to the blockchain (consensus principle). At the same time, the blockchain is stored on the computers (nodes) of all participants, so that all those partners have the same information and any manipulations on data cannot be done. In this technology a consensus is generated and maintained in a decentralized manner[2].

Blockchain showcases some similarity with the internet like an open, global infrastructure that allows companies and individuals making transactions to cut out the mediator, reducing the cost of transactions and the time lag of working through third parties. It is based on a distributed ledger structure and consensus process. By this structure the transactions are created and shared between the computers on a network. The ledger is not owned or controlled by one central authority, and can be viewed by all the participants on the network [2]. Based on the application field, the blockchain can be divided into three types that are public blockchain, consortium blockchain and private blockchain [11]. Currently, for tracking the products we utilize the technologies like IOT, RFID (radio-frequency identification) tags, sensors, barcodes, GPS tags, and chips [21].

Blockchain is the best technology which tracks all the transactions so that they can be easily available to every person and Blockchain keeps all the transaction secure as well[26]. In the year 2014, second generation "Ethereum" blockchain was designed by Buterin [25]. It was created in such a way, that a person with less technical skills can also be worked and established on Decentralized-application (DApp) [26] on the blockchain. Ethereum has its own currency called "Ether" and also, has a virtual machine (Ethereum Virtual Machine) EVM. Solidity programming language is used for creating dapps.

Public Blockchain

By this type of blockchain every node is freely to join or quit from the network at any time. All nodes have same rights, with a collective maintenance of one chain by the whole network making it a decentralized network. Regardless of the adoption of PoW and PoS algorithms, the performance becoming quite slow due to the transaction verification requirements across the network. A typical example for the public blockchain is Bitcoin. Public blockchains used in cryptocurrencies are publicly available and do not require a higher instance. This makes them very transparent, but also comparatively slows [11]. In a public blockchain, anyone without the permission of a centralized entity can [30]:

- Validation of transactions in the network can be run on their local devices.
- Verify a block of transactions, writing data to the blockchain, thus participating in the consensus process ("Proof-of-Work"), and earning network tokens in the process, by simply installing an application on their device.
- If the block included in the blockchain is valid then download the wallet and send transactions through the network.
- Public block explorer software is used to see all trans- actions that happened on the blockchain, and perform an analysis on all blockchain-related data stored on a full node.

While tokenized incentives make the

untrusted networks safe, they also make them slow. Public and permission less networks can only handle a few transactions per second, which makes them unfeasible for large-scale applications with high transaction volumes.

Private Blockchain

A private blockchain is an invitation-only network which is governed by a single entity. The entries to the network need permission to read write or change the blockchain. To protect commercial confidentiality there will be different levels for accessing and encrypting the information. With- out making data public, private blockchain allows users to employ distributed ledger technology. But this affects the decentralization property of the blockchain. Some definitions says that private blockchain is not a blockchain but it is a central database[9]. Private Blockchains efficient, more cost- effective and then public blockchains. Public blockchain re- quires a lot of time and energy to validation of transactions and its services provided only to the single entities. The cardinality of nodes is small and the permissions of each node are controlled internally. The network has excellent privacy and maintenance is very easy. Private blockchains are only accessible to certain participants, so data privacy can be guaranteed. Furthermore, read, write or administration rights can be limited. The verification of the data sets is usually the responsibility of a participant or company. As a result of this development, the distributed structure is lost, but data backup is still cryptographically performed. In comparison to a public blockchain, this system is faster[11].

Consortium Blockchain

Any node can join or quit the blockchain network after get- ting authorization from the entity. Each node can have different functions in the network. The entire network is organized as a unit forming an alliance to mutually maintaining the operations of the blockchain network. The transaction speed is faster than the public chain, and each node has low accounting costs and can be regulated. A typical example is hyperledger fabric[15]. A consortium blockchain is a mix of public and private execution, as a group of participants secure a consensus. In this way, a quick execution of the transactions can be ensured, and at the same time a decentralized administration can be guaranteed. Compared to other blockchain, the consortium blockchain can satisfy multi scene applications. It provides better performance than the public blockchain, it supports the identity certificate service, which can provide higher security and better controllability and it can be independent of tokens, has high scalability, and is easy to apply to the expansion of various fields[27]. It meets the requirements of food industries and maintains the policies of management agencies about the food security. The industries or any person with authorized certificates can only act as a participant in the blockchain network. By this we can ensure reliability of each node and can manage security in the transactions. According to these features mentioned, the consortium blockchain was used in the construction of food security system[11]. Bitcoin uses a proof of work algorithm to compute a new hash, where a certain number (nonce) from the total hash, the timestamp and a check number of the previous block must be determined. The nonce cannot be calculated, but determined only by trial and error. This process is performed by many computers (miners) in parallel; whereby the computer that is able to determine the hash, receive a distinct amount of bitcoins. This process is repeated every 10 minutes on an average[2]. As an alternative to Bitcoin, the Ethereum system was introduced in 2015, which is based on a different

algorithm that does not require special hardware equipment. This allows more capacity to be used so that a new block can be generated every 15 seconds[24]. Therefore, this method is significantly faster and many more transactions can be performed. In addition, operators are proposing a switch from the Proof of Work process to the more power-efficient Proof of Stake approach, which uses a weighted randomization to select a participant to create the hash. In this manner, it is no longer the number of computer capacity, but the share of the currency (Stake) which is deposited as a kind of pledge and retained in potential fraud attempts. In this way, the system should be resource-saving and secure[3].

Originally developed for the trading of cryptocurrencies (Blockchain 1.0), the blockchain technology is increasingly used in other areas. These include the introduction of the already mentioned smart contracts, which are mainly known under the term Blockchain 2.0. Smart Contracts are digital contracts that automatically come into effect in the so-called if-then conditions without human supervision. In this context, a common example is the function of a vending machine, which dispenses the corresponding drink after the money, has been withdrawn. Smart contracts are digital contracts that automatically come into effect in if-then decisions without human supervision. In this context, a frequently used example is the function of a drinks vending machine, which dispenses the corresponding drink after the money has been paid[16]. Applications of blockchain technologies that are not directly related to financial transactions are assigned to the third-generation blockchain (Blockchain 3.0). For the sake of completeness, as a further development of the blockchain, the tangle technology should not be left unmentioned, in which some scientists see a greater potential. In this approach, the data will no longer be stored as blocks, but as a directed acyclic graph, creating a kind of mesh in which the data can be processed much faster compared to the blockchain. This technique could better address the scalability issue of throughput, latency, and capacity.

In order to make a feasible solution for the traceability system based on blockchain, the main issues, including data explosion on the blockchain, trust transfer, and sensitive in- formation disclosure, have to be solved[1].

Trust Transfer

Trust transfer takes place when information interaction occurs between two non adjacent transaction nodes in the supply chain. For example if we consider four nodes of a supply chain namely manufacturer A, distributor B, distributor C and retailer D. (A, B), (B, C) and (C, D) are direct- trust pairs (direct transaction happens within each direct-trust pair). Beyond the direct trust pair levels, data request will not always proceeded. Consider node D send a request for data to A. By considering the security conditions the node A will verify the authenticity of the sender. If there is no direct connection between nodes, then authenticity verification is little bit difficult. Node B and C will capture the event data and trust relation is recorded. Due to the absence of direct relation between A and C, node C cannot provide a requisite proof to the node A. Similarly node D is unable to get proof from B. We can use interaction and iterative cooperation to find veracity of this indirect relation is one of the possible solutions to this problem. At the same time this procedure will make burden to the system[1].

Data Explosion

Another issue of the blockchain-based traceability system is data explosion. The

information explosion is that the rapid increase within the amount of published data and huge growth in data. Because the amount of obtainable data grows, the matter of managing the knowledge becomes harder, which can cause information overload. Since each block of nodes of the blockchain stores the full data set, data explosion problem tends to happen on the blockchain when the traceability data grows eventually. Data explosion will increase the value of the entire system, and reduce the performance of knowledge query and data management, and thus hamper the appliance of blockchain within the traceability system to an excellent extent[1].

Sensitive Information Disclosure

In the tracking system, some information is sensitive and can only access by trusted partners. The transaction details and unique identities of the nodes are sensitive. Because of the transparent feature of blockchain the disclosure of sensitive information will be happen. Therefore, it is imperative to design a classification for the information to be uploaded on the blockchain so that the safety of sensitive information can be guaranteed [1].

Blockchain in the Food Industry

The Blockchain Technology can be used in the food industry for very different issues. A large field of application concerns the traceability of food. In this regard, first attempts have already been made in cooperation with the American retailer Walmart and the IT company IBM. Using the example of mangos and pork, the two partners demonstrated the strength of the system in 2017. While the hitherto customary trace- ability of shipping documents and invoices for these products took several days, the use of blockchain technology made it possible to trace the entire supply chain within a few seconds. In the future, recall actions should be able to take place much faster and more purposefully. In addition, the blockchain technology allows a more determined detection and elimination of contamination sources, so that food crises such as the above-mentioned EHEC outbreak can be correspondingly reduced much faster[22]. Further, to the automation and digitization of documents, smart sensors can be also used to secure additional accompanying data. These include, for example, temperature loggers whose data records are transferred directly to the blockchain[8]. In this way, cold chains should also be counterfeit-proofed and food safety should be better monitored[2]. Ensuring traceability even within very complex and global supply chains implies that food fraud can be more efficiently contained. It is estimated that a total of 10 percentage of food products traded on the world are counterfeit. Sometimes such manipulations do not strike at all, since there is often no direct danger to health, for example when different qualities of raw materials are used, which relate to the place of cultivation, varieties or production methods [18]. The promotion of food with such parameters is often applied to justify higher selling prices. Such products are also widely preferred by many consumers. This reason makes the counterfeit with food very lucrative. In addition, deliberate manipulation of food may also be associated with a direct health risk, for example if a surrogate with allergenic potential is used to stretch the products. In such cases, a life-threatening danger can arise for predisposed allergy sufferers[10].

The use of digital recording and tracing approaches can also have a positive effect on the idea of sustainability. These include quality parameters based on consumer confidence like animal welfare, working conditions or special environmental requirements that cannot be analyzed by instrumental laboratory methods. For some of these parameters often also special seals are used (fair trade, marine stewardship

council etc.), which can also be retraced only poorly. Also in this area, the blockchain technology could be helpful[2]. Furthermore, the waste of food can be reduced, because on the one hand more contaminated batches can be narrowed down and on the other hand the shelf life of food during the transport and storage process can be monitored in more detail[11].

One-dimensional barcodes or two-dimensional QR codes (quick response) are particularly suitable, because they are compact and space saving. These metadata can be read out by the consumers using their own smartphones. Consumer information is of overriding importance, as there has been increasing interest in the past few years[29]. At the same time, the growing uncertainty caused by various food crises and scandals can be mitigated and consumer confidence be improved. This criterion is also a priority for the honest food producers and distributors, as such scandals adversely affect the entire industry[5]. In particular with regard to the implementation of Blockchain and the Internet of Things, there are still many other possibilities, whose full potential cannot yet be correctly estimated at the present time[26]. The interaction between the digital and the real world is becoming increasingly relevant across all economic sectors. The synchronous networking and simultaneous monitoring of all production and process flows enables a just-in-time coordination in the food industry, where production capacities can be directly adapted to the demand related behavior of the consumer[18]. The purchase of food could be done fully automated. By this, both unnecessary costs and over productions could be avoided and flows of goods significantly accelerated. The aim is a self-controlling process chain. The basis is the automatic identification of objects by labeling them using radio frequency identification systems or even simple barcode, thus making them automatically controllable. Further advantages could be achieved through the direct involvement [2].

Smart Contract

A smart contract is a self-enforcing piece of software. Smart contracts are managed by peer-to-peer network computers. These are the rights management tools which provide coordination and enforcement framework for agreements between users. There is no need of legal contracts. They can be used to frame simple agreements between two parties, the bylaws of an organization, or to create tokens[30]. It is a computer protocol designed to digitally facilitate, verify, or force the negotiation or performance of a contract and it allows transactions without a mediator. Based on the predefined agreements smart contracts will be triggered. These contracts are the self- executing agreements.

The contract will be validated and executing the code is done without the help of human intervention. That is why the smart contract is called “smart”. Agreements in the contracts are triggered automatically if the conditions in the contract are met. Imagine something along the lines of the automatic debit used by merchants to take payment from your bank account, based on pre-agreed conditions (full payment, part payment, minimum amount etc.) on a pre-agreed day or date[10]. It contains a set of rules under which the parties of that smart contract agree to interact with each other. The agreement automatically enforced if the predefined rules met. Contracts provide different methods for maintaining the assets and accessing the rights between two or more nodes. It is similar to cryptographic box. If the conditions are satisfied then the cryptographic boxes unlock the value or access. Smart con-tracts, provide a public and verifiable way

to hold governance rules and business logic in a few lines of code, which can be checked and enforced by the majority consensus of a P2P network[30]. Physical world and blockchain is communicated by the trusted intermediates like Oracle. It is an important part of the smart contract ecosystem and holds data to the blockchain network. Blockchain can access the data from the outside only through the oracle. Sensors, internet of things and weather stations are hardware based oracles. Stock exchange index and expiration date are comes under the category of software based oracles. The consensus is collected from the group of nodes. And based on this consensus, the consensus based oracle is working. The events in the smart contracts can be triggered by consensus oracle. Moreover, inbound oracles pass external data to smart contracts and outbound oracles communicate smart contract-based data to the outside world[10]. Ethereum is the first blockchain platform that focuses on providing a Turing-complete 3 smart contract-based system and decentralized applications. Hyperledger Fabric and R3 Corda are some of the other DLTs that are used to create smart contracts[2].

Proof of Work

We need a proof-of work system to implement a distributed timestamp on a peer-to-peer network. The proof-of-work involves scanning for a worth that when hashed, with SHA-256. The hash value starts with variety of zero bits. The typical work required is exponential within the number of zero bits needed and may be verified by executing one hash. The timestamp network implement s the proof-of-work by incrementing a nonce within the block until a worth is found that provides the block's hash the specified zero bits. Once the CPU effort has been expended to form it satisfy the proof-of-work, the block can't be changed without redoing the work. As later blocks are chained after it, the work to change the block would come with redoing all the blocks after it[12]. In some situations we will follow the majority decisions to reach a final decision. In the case of blockchain it can be solved by proof- of-work. If the majority were supported one-IP-address–one-vote, then everyone in the network ready to allocate many IPs. Proof-of-work uses one-CPU-one-vote. The lengthy chain represents the majority decisions. This has the best proof-of- work implemented. By average targeting a mean number of blocks per hour, we can resolve proof-of-work problem and also we can enhance the system speed.

Consensus Algorithm

The creation of new blocks and appending them to the blockchain is done by consensus algorithm. The most used algorithms are proof-of-work (PoW), proof-of-stake (PoS), and proof-of-authority (PoA). Blockchain follows a PoW consensus model. By solving a computationally intensive puzzle the node gets right to publish the next block. The solution is very easy to correct and thus it helps other nodes to validate and update the blockchain. The node which solves the puzzle wins the reward and this process is called mining.

Ethereum

Ethereum is an open source, and a public blockchain. It supports a modified version of consensus via transaction-based state transitions. Ether may be a cryptocurrency generated by the Ethereum platform and wont to compensate mining nodes for computations performed. Each Ethereum account has an ether balance and ether could also be transferred from one account

to a different Ethereum virtual machine is a decentralized virtual machine provided by Ethereum blockchain platform. This will executes the code or scripts in the public nodes. The instruction set provided by virtual machine is turing complete. Platform provides a mechanism for transaction pricing which is called "gas". The "gas" is used for the allocation of resources on the network. The language solidity are going to be used for implementing any systems in Ethereum[2]. Like other blockchains, Ethereum features a native cryptocurrency called Ether (ETH). ETH is digital money. ETH has many of an equivalent features. it's purely digital, and may be sent to anyone anywhere within the world instantly. the availability of ETH isn't controlled by any government or company - it's decentralized, and it's scarce. People everywhere the planet use ETH to form payments, as a store useful, or as collateral.

The Ethereum community is that the largest and most active blockchain community within the world. The core protocol developers, cryptoeconomic researchers, cypherpunks, mining organizations, ETH holders, and anarchists are included in this. A number of the few apps built using ethereum are CryptoKitties, a game where you collect and breed digital collectible cats and Cent which may be a social network where you'll earn money by posting. DAI which is a stable cryptocurrency that holds value at $1 USD, and Gitcoin, a network of incentivized open-source developers[31]. During state transitions Ethereum performs using accounts and balances. Bitcoin uses another way. Ethereum transaction doesn't depend on unspent transaction outputs. The state refers to the balances that are available in the accounts and some related data. The state is stored in Merkle Patricia tree not in the blockchain. A cryptocurrency wallet stores the general public and personal "keys" or "addresses" which may be wont to receive or spend ether. These are often generated through BIP 39 style mnemonics for a BIP 32"HD Wallet". In Ethereum, this is often unnecessary because it does not operate during a UTXO scheme. With the private key, it's possible to write down within the blockchain, effectively making an ether transaction[32]. For creating the smart contracts for Ethereum blockchain we will choose Solidity programing language. That is why the solidity is called as contract oriented language. By this language we can store all the information about blockchain transaction in smart contracts. Solidity is a high level programing language like JS, python etc. it can be used for executing code on the Ethereum virtual machine [4].

RELATED WORK

The decentralized method like blockchain, a reliable database is maintained to store data. Using cryptography it will creates blocks through any number of nodes. By this feature we can call it as chain of blocks. Each block contains the data of all transactions in the system within a period of time and it create digital fingerprinting which can be used to verify the validity of the information and connect with the next block [23]. There will be large number of blocks in the network. These blocks are connected to each other in linear fashion. Every block in the network are aware about the hash of the previous block. The technology can be viewed as a general term for technical schemes. This is similar to NoSQL databases, and it can be accessed through many languages in programing. Through PoW, PoS and DPOS this type of realizing can be

achieved. Blockchain is decentralized, immutable, reliable, untrustworthy and a distributed ledger technology. The proposed system is mainly focused on a decentralized system and traceability of the product. The consumer can trace the path of the product by scanning the QR code and can get idea about the quality of the product. So consumer come to know the quality of the product and also can trace the path [6].

The existing works are related to IoT, Social network analysis, and supply chain and so on. These works are not that much secured because any time corruption can occur. In order to avoid this corruption, this work is mainly concentrated on decentralized blockchain. RFID based system in a supply chain by calculating the performance increasing in efficiency, security, accuracy and visibility. Their study shows how the product value, lead time and demand uncertainty of the market influence the performance of the RFID system in the supply chain. Blockchain can be seen as a distributed database or ledger, a chronological chain of blocks and each block stores all information of network activity since the block is added to the chain[23]. Every user can add the data in the blockchain in the form of a transaction and any user can check the data at any time. That is why blockchain data is called as public. The changing of data in the blockchain is strictly prohibited. On this distributed network the entire history is maintained among the all nodes. Security and trust is achieved through the mining process. All the nodes can verify the validity of the information that relies in the chain.

In the mining process, new transactions are verified by the nodes in the whole system known as “miners” before being added to blockchain. Miners add new blocks on the chain or new transactions on the block by a consensus algorithm, which must be confirmed by majority or all the nodes in the system, like a voting operation, as the valid data. Once the transaction is confirmed by a sufficient number of nodes, it becomes a valid and permanent part of the database[23]. The features of blockchain include no single entity can control the whole network, immutability and, remove the need for a central entity. These features can improve the security and transparency of decentralized systems. However, blockchain technology has scalability issues in terms of throughput, latency, and capacity when faces enormous data in a real business environment. In decentralized system there is no centralized authority. If any node crashes the other nodes will not be affected. So blockchain system is robust. All activities of each and every node are transparent, so blockchain is called trustless. It is collectively maintainable because all the blocks of system maintained by all the nodes in the system. Every node in the network will holds a copy complete data, so the system is reliable. The core problem solved by the blockchain technology is how to create a trust free environment for business and management activities within the situation of data asymmetry. The blockchain can guarantee the safety of the entire network by employing a mathematical algorithm mechanism [23] dependency from bottom to top, Network, Consensus, Storage, View, and Side Planes. An application of blockchain technology consists of a number of smart contracts. A sensible contract is an instance of a computer virus that runs on the blockchain, *i.e.,* executed by all consensus nodes. A program code, a storage file, and an account balance will be contained. By posting a transaction to the blockchain any user can create contract. The program code of a contract is fixed when the contract is made, and may not be changed.

PROPOSED SYSTEM

Architectural Diagram

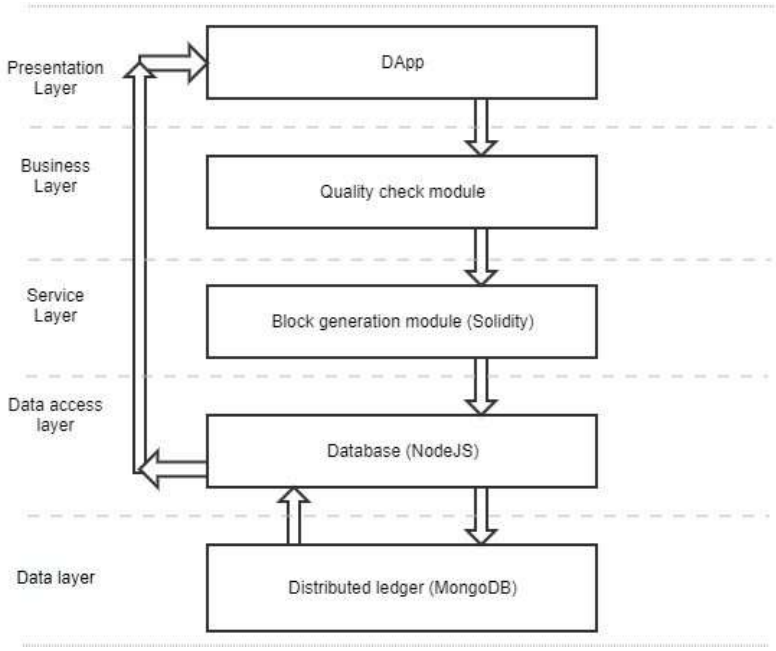

Fig. 1: *Architectural Diagram of Proposed Model.*

Figure 1 is the conceptual model that defines the structure, behavior, and more views of the proposed system. It primarily concentrates on the internal interfaces among the system's components or subsystems.

The top most layer is the presentation layer which is composed of many views that are suitable for each actor in the use case. The peers have one type of view through which they can enter and view details. The end consumer will be redirected to a view that shows the flow of the product. The authorities and governmental agencies shall be given another view through which they can collect the relevant details. All this are done through a single DApp.

The business layer consists of checking the data that comes through the DApp if it meets the business requirements. If it does, it is implemented as a block lying in the service layer. This layer is can be created using Ethereum or any other IDE that supports development of blockchain. This is only done after getting enough PoW from the peer nodes.

Once the block is created it's added to the distributed database. The database used is not a relational database. MongoDB etc. can be used. The data layer can be accessed by the data access layer using languages like NodeJS.

Whenever data is to be retrieved, the request goes through the DApp, the data access layer collects the data from the database and sends it directly to the presentation layer.

Flowchart

The following flowchart (Figure 2) represents the workflow or process in the proposed system. It's a diagrammatic representation of the algorithm stated earlier. It can be used in analyzing, designing, documenting or managing the system. The flowchart described here is

only detailing the procedure happening at one peer in the P2P network. The same events are happening simultaneously to all the nodes present in the network all the time the network is active.

Flowchart starts and the node (receiver peer) receives the input details from the sender peer (both belonging to the same network). The details can be of any format and maybe even embedded in a QR Code, or RFID tag. This detail of the incoming package is entered into the ledger after computing necessary PoW. After the transactions in the block are validated, the block is appended into the distributed ledger. Then the details of the package, especially the parameters of the input concerning with the safety and security standards of the food are tested to see if it satisfies the general criteria set by the receiver, governmental agencies etc. If it satisfies, then a new block is appended into the ledger which behaves like an acceptance block indicating the package received has been accepted and passed onto the next level for processing.

If the quality constraints are not satisfied, then the package is rejected instantly and the software controlling this goes to the previous state for receiving new inputs. Rejection of the package of a particular identity can be identified by tracing the chain and observing that, there is only identity block and no acceptance block for package of that id.

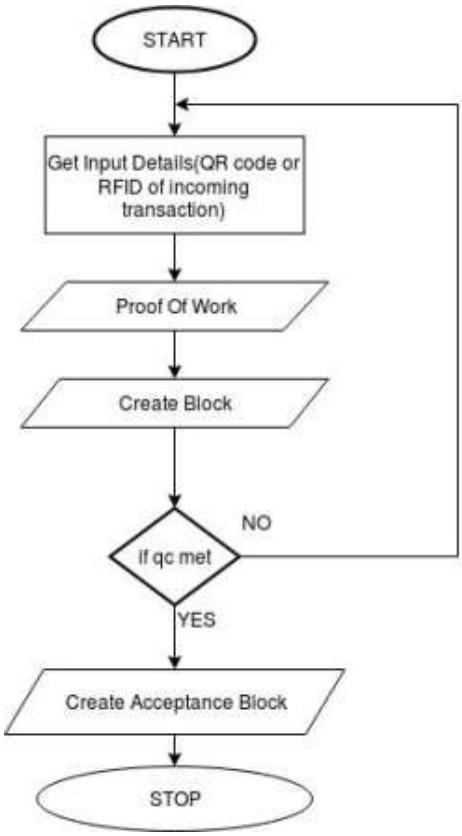

Fig. 2: *Flowchart of Proposed Model.*

Block Diagram

Figure 3 gives the block diagram of the proposed model. The block diagram starts with the receiving of details by one peer from another peer in the network. The data received is usually preliminary information regarding the content or package of the food item. This data has to be stored in a

distributed ledger or a distributed database. The parameters of the package received are then verified if it meets the demands of the industrial quality or as specified. If it succeeds, then a new block is generated for the same package indicating it has met the requirements and is suitable for further processing. The process repeats where this package is processed and sent to the next peer and this process repeats itself.

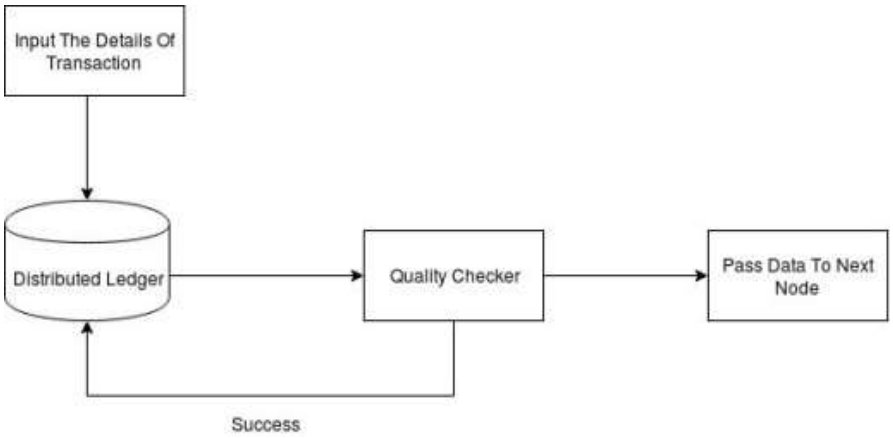

Fig. 3: *Block Diagram of Proposed Model.*

DESIGN MODULES

The design of this system consists of various modules or parts that has to be integrated together to complete the system. This involves the creation of:

- DApp
- Quality Check module
- Block creation module
- Database definition and manipulation module
- Cloud integration module

DApp is essential for any user to interact with the system. It's present in the presentation layer in the system. There are various frameworks available for the creation and deployment of DApps. The end consumer who gets the finished product can trace the flow of its birth to the end state by scanning the QR Code or RFID tag present in the object. This should redirect to the DApp and give the necessary information to the user. Embark is a framework that allows the design and deployment of DApps. There are various other ethereum development tools available such as Remix, Ethfiddle and Ganache.

The quality check module is highly subjective and depends on the item which is being supplied. It could range from simple Quantity evaluation or texture evaluation by hands to really complex lab tests performed elsewhere in the country. However, the results of the tests are processed into a transaction object by software that can be created from programming languages like python, Java etc. The module is integrated to the DApp which has many pages and shows only those pages to the authorized people in the supply chain. The data collected is further stored in the ledger using querying languages like NodeJS or mySQL. Block creation module can be developed in IDEs like Ethereum, hyperledger or R3 Corda. Ethereum is coded in a language called Solidity and is one of the earliest platforms for blockchain ledger development. Hyperledger can be coded in languages like python, C etc. R3 Corda is one of the recent IDE that is complex but provides various features. Database can be created in MongoDB. It is a cross platform document oriented database program. Classified as a NoSQL database program, MongoDB uses JSON-like documents

with schema.

Supply chain is a vast chain that can contains nodes in various parts of the world. It can also be a small one where all processing from raw material state to the finished state happens in one factory itself. However, in many such cases, ingredients mixed with them are processed elsewhere. This makes cloud computing an essential and integral part of the proposed system. The goal of cloud integration is to connect the disparate elements of various cloud and local resources into a single, ubiquitous environment that allows administrators or peers to seamlessly access and manage applications, data, services and systems. IBM App connects and Microsoft Azure is two cloud services that can be used.

Apart from the above mentioned modules, the finished product will have a unique ID either in the form of a bar code or a QR code. This code can be scanned by the end consumer. For this, there are third party apps that support QR code scanning. For RFID scanning, which is only feasible for an organization, one will have to purchase an RFID Scanner.

CONCLUSION AND FUTURE WORK

The idea to implement Blockchain in Food Supply Chain will not only change the way of how the industry manages the supply chain but also help in managing significant wastage and proper management of rice. If there is an event where the authority finds out that a particular product is found to be contaminated which could hamper the health of an individual by consuming it. Through this study we were aware about the transfer proof feature of the blockchain and how this technology avoids the fraud attacks and errors. Blockchain technology reduces the cost that we needed and the interruption of third parties. With the proposed blockchain framework the entire operational efficiency of the system can be improved. By this we can see the processing journey of the products from its raw state to final state. If needed the raw material from that specific production site or batch can be recalled rapidly. Also, the consumer will be benefited in getting good quality products. The system will provide a tracking facility in which we can see all the activities that happened in between initial state to final state. Here all the activities have transparency and fight towards the fraud attacks. Making an unchangeable and permanent history in the decentralized digital platform will make the entire system more efficient. This technology brings Security to Real Estate transactions because there is no central point of failure. From Security point of view the ledger is distributed among many computers so attacker needs to attack 51 percentage of network which is not feasible with the current CPU technology.

In this research attempt, we have focused on how Blockchain technology brings security to transactions associated with food supply chain because of its transparency and no central involvement. Thus, our future work would be to extend the use of Blockchain Technology to facilitate an accessible, stream-lined supply chain that comprises almost all ingredients that’s involved, making it a large scale supply web. It is more efficient and effective by employing faster or simpler working methods. Current system of this project is able to do Registration and Transfer using Public Ethereum Blockchain of the item and is also not able to view the flow of journey. Future enhancements include being able to trace the path of the constituents used in the products as well. In Future Proof-of-Authority (PoA) can also be used so that the details can only be viewed by the authorized person and not by anyone else.

REFERENCES

1. Lin Q., Wang H., Pei X., Wang J. *Blockchain and more - Algorithm*

driven food traceability. State Key Laboratory of ASIC and System, Fudan University, Shanghai. China, 4, 201-203p, 2017.

2. Creydt M., Fischer M. *Blockchain and more - Algorithm driven food traceability.* Hamburg School of Food Science, Institute of Food Chemistry, University of Hamburg, Grindelallee 117, 20146, Hamburg, Germany. 2019
3. Zheng Z., Xie S., Dai H., *et al. An overview of blockchain technology: Architecture, consensus, and future trends.* 2017 IEEE international congress on big data (BigData congress). 557–564p. https://doi.org/10.1109/BigDataCongress.2017.85
4. Burkhardt D., Werling M., Lasi H. *Distributed ledger*. 2018 IEEE international conference on engineering, technology and innovation (ICE/ITMC). https://doi.org/10.1109/ICE.2018.8436299
5. Nofer M., Gomber P., Hinz O., Schiereck D. *Blockchain.* BISE, 59(3), 183–187p, 2017. https://doi.org/10.1007/s12599- 017-0467-3.
6. Yiannas F. *A new era of food transparency powered by blockchain*. Innovations: Technology, Governance, Globalization, 12(1–2), 46–56p, 2018. https://doi.org/10.1162/inov$_{a0}$0266.
7. Schelm S., Haase I., Fischer C., Fischer M. *Development of a multiplex real- time PCR for determination of apricot in marzipan using the plexor system*. Journal of Agricultural and Food Chemistry, 65(2), 516–522p, 2017. https://doi.org/10.1021/acs.jafc.6b04457.
8. Popov S. *The tangle*. 2016. http://www.tangleblog.com/wp-content/uploads/2016/11/IOTA$_{W}$hitepaper.pdf, Accessed date: 4 March 2019.
9. Abad E., Palacio F., Nuin M., *et al. RFID smart tag for traceability and cold chain monitoring of foods: Demonstration in an intercontinental fresh fish logistic chain.* Journal of Food Engineering, 93(4), 394–399p, 2009. https://doi.org/10.1016/j.jfoodeng.2009.02.004.
   Anderson R. *The eternity service*. Proceedings of Pragocrypt, 96, 242–252p, 1996.
10. Sylvester G. *E-agriculture in action blockchain for agriculture opportunities and challenges.* The food and agriculture organization of united nation, 2019
11. Qi Tao,Xiaohui Cui, Xiaofang Huang, Angella M. Leigh, Hehe Gu. *E-agriculture in action blockchain for agriculture opportunities and challenges*. The food and agriculture organization of united nation, 2019.
12. Nakamoto S. *Bitcoin: A Peer-to-Peer Electronic Cash System*. www.bitcoin.org.
13. Liang K. *Ruggedness of 2D code printed on grain tracers for implementing a prospective grain traceability system to the bulk grain delivery system*. Food Control, 33(2), 359–365p, 2013. https://doi.org/10.1016/j.foodcont.2013.03.029
14. Kuswandi B., Wicaksono Y., Jayus A.A., *et al. Smart packaging: Sensors for monitoring of food quality and safety.* Sensing and Instrumentation for Food Quality and Safety, 5(3), 137–146p, 2011.
15. Kakkar A., Ruchi. *A Blockchain Technology Solution to Enhance Operational Efficiency of Rice Supply Chain for Food Corporation of India*. ICSCN 2019, LNDECT 39, 24–31p, 2019.
16. Tian F. *A Supply Chain Traceability System for Food Safety Based on*

HACCP, Blockchain Internet of Things. 2017.
17. Ganeshan R., Terry H.P. *An introduction to supply chain management*. Department of Management Sciences and Information Systems. 21(1/2), 71–77p, 2001.
18. Lee H.L., Billington C. *The evolution of supply-chain- management models and practice at Hewlett Packard*. Interfaces, 25, 42–63p, 1995.
19. Christopher M. *Logistics and supply chain management: strategies for reducing costs and improving services*. Interfaces, 25, 42–63p, 1995.
20. Nir K. *Exploring blockchain technology and its potential applications for education*. Int. J. Manag., 2018.
21. Kumar A., Rao T., Nagpal S. *Using Strong, Acquaintance and Weak Tie Strengths for Modeling Relationships in Facebook Network.* Proceedings of the 5th International Conference on Contemporary Computing. 2012.
22. Guo G., Zhang J., Thalmann D. *Merging trust in collaborative filtering to alleviate data sparsity and cold start.* Knowledge- Based Systems, 2014.
23. Xiao Shen, Haixia Long, and Cuihua Ma. *Incorporating Trust Relationships in Collaborative Filtering Recommender System*. IEEE SNPD, 2015.
24. Adomavicius G., Tuzhilin A. *Toward the next generation of Rss: A survey of the state- of-the-art and possible extensions*. IEEE Transactions on Knowledge and Data Engineering, 2005.
25. Bedi P., Kaur H., Marwaha S. *Trust based recommender system for semantic web*. In IJCAI207: Proceedings of International Joint Conferences on Artificial Intelligence, 2677-2682p, 2007.
26. Peng Yu. *Recommendation method for mobile network based on user characteristics and user trust relationship*. IEEE International Conference on Big Data Analysis (ICBDA), 2016.
27. Kahanda I., Neville J. *Using transactional information to predict link strength in OSNs*. Proceedings of the 3rd International Conference on weblogs and social media, 2009.
28. Gilbert E., Karahalios. *Predicting tie strength with social media*. Proceedings of the 27th International Conference on Human Factors in Computing Systems, 2009.
29. Xiang R., Neville J., Rogati M. *Modeling Relationship Strength in Online Social Network.* Proceedings of the 19th International Conference on World Wide Web, 2010.
30. Adali S., Escriva R., Goldberg M.K., *et al. Measuring Behavioral Trust in Social Networks.* Proceedings of International Conference on Intelligence and Security Informatics, 2010.
31. Katz Y., Golbeck J. *Social network-based trust in prioritized default logic.* Proceedings of the 21st International Conference on Artificial Intelligence, 2006.
32. Tian F. *Agri-food supply chain traceability system for China based on RFID & blockchain technology.* 13th International Conference on Service Systems and Service Management, 2016.