Analysis of Agricultural Supply Chain Management for Traceability of Food Products using Blockchain-Ethereum Technology

Pooja S
Dept of CSE
M S Ramaiah Institute of Technology
Bangalore, India

Meeradevi
Dept of CSE
M S Ramaiah Institute of Technology
Bangalore, India

Monica R Mundada
Dept of CSE
M S Ramaiah Institute of Technology
Bangalore, India

Abstract

The current agricultural supply chain is a centralized system that has many issues related to integrity, tracking, organizing the transactions. There is lack of trust and transparency in the supply chain. There are many irregularities in the implementation of schemes. The consumers doubt the quality of the food supplied to them. The farmers, wholesalers are affected from the payment frauds by the middlemen. Blockchain helps us solve these issues by keeping track of all the different stages of food. The public blockchain being transparent, open, immutable, trackable helps in reducing the irregularities, frauds. This paper proposes the agricultural supply chain system model that uses the Ethereum platform. The smart contracts are developed for different stages of the supply chain. These contracts ensure that all the pre-decided conditions are satisfied before proceeding with the transactions. This system ensures security, reliability, trust, openness. It eases the transactions, administrative processes. It gives a fair chance to farmers to quote a price using smart contracts.

Keywords: Blockchain, Ethereum, consensus, smart contract, Bidding, Traceability

I. INTRODUCTION

The Agricultural Supply Chain is the chain of the stakeholders who carry out various processes involved in transforming seeds into grown crops, transporting them and making it available in the retail stores. Some of the issues related to the agriculture and food supply chain are lack of transparency, reliability, security, trust. There is no proper way to identify the quality of food, to track the transportation of crops. Farmers face crop loss and are being exploited by middlemen. They don't get fair price value for the crop. They also lack the knowledge of financial aids provided by government. The centralization of data results in wastage of food between different stages of food. Blockchain being immutable, transparent provides solution for many of the issues listed above. It was first used as a public ledger for the transactions made in bitcoin. In 2014, the blockchain technology was isolated from currency and all started exploring it as a separate entity. Blockchain is the chain of blocks/records that grows continuously. These blocks are linked to each other. The information of every phase right from the stage of planting (the fertilizers used, the nutrients that support the growth) to selling the commodity to consumers, all the details are stored in the blockchain. The quality of the food can be determined with the help of stored data. The list of records of food continuously grows as the food passes from one phase to another.

The blocks in blockchain data structure are arranged in the chronological order of transactions. The node/machine that run Ethereum blockchain form the decentralized network. The people involved in the supply chain digitally sign transactions for authentication. The smart contracts help in reducing the complexity and automating the activities involved in the supply chain [1]. These contracts are the software programs that are executed on blockchain nodes to check the pre-coded conditions, to carry out specified transactions. A node is a machine that has the smart contracts and the required software to use Ethereum blockchain platform. There are various options available for developers in building a dApp (decentralized Application) with Ethereum blockchain platform. There are different softwares available that helps to setup the blockchain system. That includes Node Package Manager, Truffle, Ganache, Remix and Visual Studio code. The combination of these tools helps in developing applications with the Ethereum. The blockchain transactions are enabled by triggers. To improve trading among different organizations the activities should not rely on centralized server. It should be

978-1-7281-9885-9/20/$31.00 ©2020 IEEE

a decentralized network where all nodes can view all transactions and participate in bidding. All the peers enter into an agreement by deciding on the terms and conditions that are made by considering the views of all the actors involved in the network. When a node wants to join the network, it is displayed as a pending transaction to all the other nodes. The new node can join the network only if all the other nodes validate the transaction. Once it joins the network it can download the full blockchain to its system and view all the transactions. A new block is added to the chain whenever a change needs to be updated. The data is converted into hash using hashing algorithm and the output is stored in the blockchain. The transactions are digitally signed using private and public keys. The 256 bits private key is generated randomly, the public key is generated using an algorithm. This platform prevents tampering of data since users can only add data, they cannot edit the old blocks. The blockchain technology strengthens the information connection among the different entities of the agricultural supply chain, enhances the cooperation among the peers and brings the consistency in tracing the information quickly [2].

II. PROBLEM STATEMENT

There is reliability, security, transparency issues in agricultural supply chain. The farmers suffer due to these issues. They don't have accurate information about weather conditions, their agricultural land soil conditions, crop demands. Some blindly start growing the crop without knowing all the details of crop. There is no proper systematic analysis done on crops data. The involvement of middlemen worsens the situation and the farmers end up selling the crops at lower price whereas consumer pays high price for the crop.

III. RELATED WORK

Blockchain eases real time and dependable information sharing. It's an immutable chain that contains the blocks in the chronological order. This paper [1] gives the framework that helps in the pharmaceutical supply chain management, it has different smart contracts for supply management, Stock purchase, raw materials purchase etc. The quality is checked using quality checking contracts while the drugs are exchanged between two entities. This framework achieves user privacy using pseudo identity, transparency of the supplied drug as all users can view all the data store in the blockchain, tracking of drugs using pseudo identity, continuous and good quality of service, demand supply management by collecting the demand data from distributors. In [2] the authors have proposed different smart contracts for food grain supply namely food grain supply, bidding, trading and utilization, which are deployed on Ethereum blockchain for the decentralized trading of food grains. It uses Vickrey-Clarkegrove (Vickrey auction) method that also considers the second highest bidding for payoffs. It helps in the incentivized trading between farmers and end users. In paper [3] they propose a model that has central authority, Producer, Distributor, Wholesaler, Retailor, Consumer. They have implemented this model using three smart contracts – Provenance, Bidding, Tracking on an Ethereum platform. The Provenance contract helps the nodes to get the producer details, product details. The Bidding contract contains the conditions that are checked before deciding the winning bidder. The tracking contract contains the functions that tracks the item received with the serial number. In [4], the design integrates different platforms for information service in supply chain. The system contains administrator, Producer, Processor, Logistics, Distributor nodes. The system consists of four partitions. They are – Application Layer that contains Web User Interface, Internet of Things equipment, Service Layer that contains Node.js, Contract layer that contains smart contracts, Data Layer that contains Ethereum Blockchain Data and MySQL Database. It explains tracing process, reputation management, timestamp dependence.

This [5] investigates the Ethereum blockchain support for online Supply Chain systems and its feasibility in Business-to-Consumer (B2C) business model. They propose Consumer Ordering Consensus Protocol (COCP) for B2C online retail stores to securely and efficiently process orders. They compare three different systems-Retail Store outlet, Online Retail Store, Smart Contract based Online Retail Store based on order requests. They have developed an application to demonstrate smart contracts in the B2C Supply Chain system. They discuss the role of smart contracts in executing order transactions, from placing an order to receiving the shipment. In [6] discusses the various options available for developers in building anApp with Ethereum blockchain platform. It discusses the installation of different softwares that are helpful in blockchain system setup. That includes Node Package Manager, Truffle, Ganache, Remix and Visual Studio code. It gives the possible combination of tools required to easily develop applications with the Ethereum. In [7], the comparison of different blockchain technologies in the network is given. It explains the blockchain recording mechanism, blockchain transaction process in detail. The various applications of blockchain in different fields are discussed. The basic framework that contains Item, Store, Carrier, Insurance, Importer, Wholesaler and Retailer, Customer is proposed. Blockchain helps merchants at advancing their industry procedures that results in the growth of organization.

IV. METHODOLGY

Many entities, firms, actors are involved in the agriculture and food supply chain. Every entity adds value to the whole process of making the commodity available in the market. The proposed system model as shown in fig 1 includes:

FARMING: It involves planting the seeds, nurturing plants and keeping them away from diseases.

STORAGE: It's the post-harvest phase. The crops have to be stored at the required level of moisture, temperature and oxygen content.

MARKETING: It involves organizing, handling of agricultural produce, deciding on its price and making it available for consumer.

Figure 1: System Model

The actors who make entries in the ledger of the supply chain are:

Seed Company - The one who provides raw materials like seeds, chemicals, fertilizers for the growth of crop. The details of the quantity of seeds, the chemicals and fertilizers used are entered.

Farmer - The one who grows the crop. It involves nurturing the plant by keeping it free from diseases and pests. The name, type, quantity of crop required for the purchase are entered.

Wholesaler - The wholesaler buys the crop directly from farmer and sells it to the retailor. All the purchase and selling details are entered. This stage also involves the proper storage and cleaning of crop.

Retailor - It involves the responsibility of delivering the product to end users. The retailor buys the product from wholesalers. The purchased price, the sold price and all commodity related details are entered.

Customer – The one who buys the end product. The history of the product can be traced by scanning the bar code.

The Central Authority (CA) gives the unique address (also known as Ethereum address) to all nodes. The nodes carry out the transactions using the address provided. With the help of blockchain we can track all transactions, we can check whether the transaction adheres to the rules and regulations. If any issue arises it can be resolved quickly with the help of traceability. But some issues need to be addressed offline like removing or adding an entity to the network or taking some important management decisions. Central Authority is responsible for handling issues offline.

V. ETHEREUM BASED BLOCKCHAIN FOR AGRICULTURE AND FOOD SUPPLY CHAIN

Ethereum is the public blockchain that is open source, distributed. It also acts as an operating system where the decentralized Applications (dApps), games are developed. It's going to change the way internet works. An internet where everything is open, people own their data, earn from their data. Everyone can see other's data. The transactions in Ethereum platform is controlled by smart contract not by any government, organization, person. Ether is the cryptocurrency of Ethereum. This platform can be used in financial transactions as a digital wallet, a digital asset. The transactions are cryptographically signed. Ethereum provides a decentralized virtual machine, the Ethereum Virtual Machine (EVM) that execute scripts in a public network of nodes. The dApps are developed using Solidity language, these dApps don't run on any traditional server, it runs only on Ethereum blockchain.

The Ethereum smart contract runs on the public network of large number of nodes as shown in Fig 2. These nodes share blockchain database that contains the crop and product details. All these nodes can communicate with each other. The details that are entered is stored across the entire network of nodes. The information is validated through consensus mechanism before storing in blockchain. According to the consensus, more than half of the nodes must agree about the information before saving in blockchain. It's impossible to hack this kind of system since it's difficult to take control of more than half of system and possess that enormous computational power. An Ethereum block consists of timestamp, transaction hashes, the array of uncle hashes, block reward, address of miner, gas used, hash, parent hash, Nonce, sha3Uncles, block serial number, size, difficulty, transactions root. The mining process generates the new block with fellow miners by running smart contract. The miners are rewarded with Ether for performing the computation. In our system model every participant has an account associated with their identity. It has Ethereum Address (EA), which is given by central authority (CA). Every account has a certain amount of gas(fuel) associated with it. The gas is the crypto fuel that the node should possess to execute the code on EVM. After validation, the transactions are committed. All the contracts are run by everyone on the mining nodes, the decisions are taken collectively. A mining node can be any computing machine. The nodes that are distributed all over the network store the data related to the transaction in a ledger.

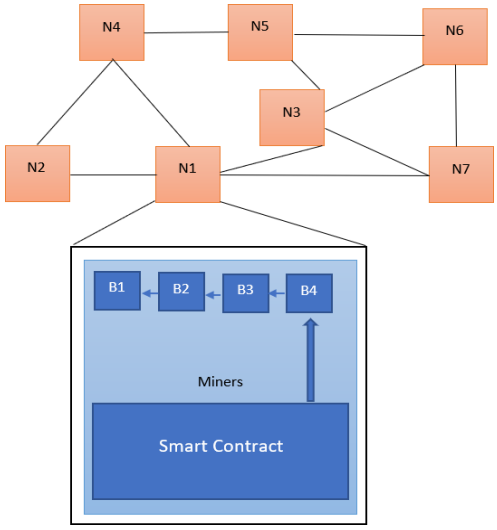

Figure 2: The Ethereum Architecture

All these nodes are synchronized. The Ethereum smart contracts are written in solidity language. Some of the advantages of using hash are the speed of retrieval of data is constant all over disk, the hash uses less memory comparatively and it increases security. One of the unique features of hash is for every input we get completely different output.

The system uses Ethereum Blockchain which is ideal for B2C transactions since users don't need permission to participate in the transactions. The Ethereum platform allows all the nodes to participate in the transaction. This platform provides a way to trade with untrusted parties. Also, it has its own crypto currency that facilitates the easy execution of transactions. The system is farmer friendly because the farmer is given the right to quote the price. The system tries to remove the involvement of middleman. The limitations are high latency and the system being open is not suitable for confidential transactions. Now we are going to illustrate how Ethereum smart contracts are used to carry out the transactions at different stages of agricultural supply chain. The transactions between them are successful only if the smart contract conditions are met. These conditions are pre-decided by the parties involved:

1. The Central Authority (CA) gives the unique address to all nodes. All the nodes carry out transaction using that address.
2. The seed company runs the seed details contract. The name, type, quantity of the seed is entered. Then the seed purchase smart contract is executed and the price x1 for seeds is fixed.
3. The Farmers respond to it and shows interest in buying seeds. The name, type, quantity of seed is checked by farmer. The account balance of farmer is checked by seed company. The payment transaction is initiated with the seed purchase smart contract.
4. The farmer plants the seed and nurtures it. The crop is sold with the help of the crop purchase smart contract. He fixes the price x2 for the crop. The wholesalers participate in bidding. The winning bidder gets the crop at the price decided during bidding.
5. The wholesaler runs the commodity sales smart contract. All the retailers participate in the bidding. The winning bidder purchases the commodity. The retailor is responsible for delivering the commodity to the end user.
6. The quantity checks happen at every level. The payment is held by the smart contract until the receiver confirms successful delivery.
7. The carrier is also selected through bidding to avoid unnecessary problems. The seller pays for the carrier.
8. The customer is the end user of the product who buys it. The bar code on the commodity is scanned to get the details of it.

All the transactions are committed only if it's validated by all nodes in the network. The seed company enters the seed details using seed details smart contract. The name, type, quantity details of the seed are entered. They are responsible for initializing the seed purchase by executing seed purchase contract. All the farmers get the notification for seed purchase. Then the farmer checks the name, type, quantity of seeds and sends the message with details showing his interest in buying it. The entities are authorized using entity authorization contract. The authorization details of entities can be checked using the authorized attribute. If the farmer purchases it, the details of the purchased seeds are entered. Next the crop details are added using crop details smart contract and crop sales are initiated by executing crop purchase smart contract. The farmer fixes the price 'x2' for the crop. All the wholesalers get the message of the initiation of crop sales. The wholesaler checks the crop, price details and responds. If more than one wholesaler is interested in buying, the bidding contract is executed and the crop is sold to the winning bidder. There are three types of bidding- Overbidding (bidding price greater than x2), underbidding, (bidding price lesser than x2), truthful bidding (bidding price equal to x2). The one who bids highest amount wins the bid. If all the wholesalers bid a price lesser than the price fixed by farmer, the farmer decides how to proceed with it. He has 3 options- the first one is selling the crop for lesser price to wholesaler, second one is to sell to government at a price fixed by government and the third one is cancelling the initiation of crop sales.

The entities can negotiate through online messages using the app messaging feature. The wholesalers collect demand data from the retailors regularly. They purchase the required quantity of crop based on demand. Then the payment is initiated between farmer and wholesaler. The wholesaler stores, processes the crop. It involves grinding, cleaning, washing, packaging and processing of crop to produce end product. The commodity sales smart contract is executed and the commodity is sold to the retailor. The carrier bidding contract is initiated if needed. All retailors get the notification. The interested retailors take part in bidding. The crop

is sold to the winning retailor. The retailor makes the commodity be available at retail stores for the consumers at a fixed price. The sale of commodities is recorded as and when it purchased by the customer. The tracking contract is used to get all the details associated with the commodity. Using tracking contract, the hash, quantity, location, timestamp is verified when the commodity is delivered. If there is any discrepancy the payment transaction is not initiated.

a. Pseudocode for Seed details smart contract

```
function get_seed(string identity_no) returns
(address, string, string, uint[], uint, uint)
{
 return (seeds[identity_no].entity,
seeds[identity_no].name, seeds[identity_no].type,
seeds[identity_no].location,
seeds[identity_no].timeStamp,
seeds[identity_no].quantity);
}
```

b. Pseudocode Crop purchase smart contract

```
function crop_purchase(string identity_no)
{
function send_croppurchase_info(string
identity_no);
function payment (address_farmer,
address_wholesaler, string identity_no);
}
function send_croppurchase_info(string
identity_no) returns (address, uint[], uint, uint)
{
return (crops[identity_no].entity, crops
[identity_no].location,
crops[identity_no].timeStamp,
crop[identity_no].quantity);
}
function payment(address_farmer,
address_wholesaler, string identity_no){
If(wholesaler[address_wholesaler]account_balance
>= x2){
whoelsaler[address_wholesaler]account_balance=
wholesaler[address_wholesaler]account_balance-
x2; crop[identity_no]quantity=
crop[identity_no]quantityy2;
farmer[address_farmer]account_balance=
farmer[address_farmer]account_balance+x2;} }
```

c. Pseudocode Entity authorization smart contract

```
function entity_authorization(address _entity) returns
(bool success)
{
entity [_entity].authorized = true; return true; }
function Find_entity(address _entity) constant returns
(string, uint, string, bool)
{ return (entity[_entity].name, entity[_entity].contactno,
entity[_entity].city, entity[_entity].authorized); }
// Get crop details
function Find_Crop(string identity_no) constant returns
(address, uint[], uint)
{ return (crops[identity_no].entity,
crops[identity_no].location, crops[identity_no]
.timeStamp); }
```

d. Pseudocode Bidding smart contract

```
function supply_chain_bidding() {
require(present <= Closetiming, "The Bidding time is
over");
require(entity.value > fixedBid, "Bid amount is lesser than
the fixed bid price");
require(entity[identity_no].authorized,"Unauthorized
entity");
require(entity[identity_no].reputationfactor>10,"enti ty
does not have the required reputation factor"); //After the
winner is decided
winner = entity[identity_no]; fixedBid = entity.value;
BiddingValueIncreased(entity[identity_no], entity.value);
}
```

e. Pseudocode tracking contract

```
function receive_info (string transaction_no, uint
block_timestamp, string block_commodity, uint
block_quantity, uint[] block_locData) returns (bool
success)
{
if(sha3(deliveries[transaction_no].commodity) ==
sha3(block_commodity)
{
Success('successful', transaction_no, block_timestamp,
entity[identity_no]);
if (block_timestamp <=
deliveries[transaction_no].timeStamp +
contractLeadTime && block_loc[0] == contractLoc[0]
&& block_loc[1] == contractLoc[1] && block_quantity
==deliveries[transaction_no].quantity) {
sendToken(deliveries[transaction_no].entity,
entity[identity_no], ca, contractPayment); }
else
{
Failure('Payment not initiated as conditions are not
satisfied');}
return true; }
else {Failure('crop/quantity error'); return false;}}
```

Some of the key factors that need to be considered are

1) Tracing process: The verifiable digital signature is stored in blockchain. The participants sign during information registration. The database stores original information and the blockchain store the digital signatures.

2) Reputation management: We can design specific evaluation methods based on the needs. It calculates the reputation value regularly and updates. We must consider few factors while designing the valuation system. Some of them are non-overlapping, extensive indicators, non-overlapping and easy evaluation.

3) Timestamp dependence: The time error is the time margin between verification and generation of an Ethereum block. The results might be unstable if it is based on timestamps accuracy. The malicious nodes might try to manipulate the execution results using timestamp value. We have to define the timestamp dependence prior to avoid transaction validation problems.

VI. CONCLUSION

The smart contracts and the blockchain technology help to develop an immutable, secured, efficient and traceable supply chain. The transactions are made transparent and open. The details of originality of commodity are possible. This improves security and helps in reducing losses from forged and grey market. All the supply chain processes are automatized to ensure trust, transparency, flexibility. This paper has proposed a blockchain enabled system model for agricultural supply chain. The systems that have implemented smart contracts based on Ethereum blockchain are surveyed. The system model and the network among different entities are shown. The details, bidding, tracking smart contracts are designed for agricultural supply chain. The future work includes the practical implementation of smart contracts, the study of agricultural insurance, agricultural loans, automating the entry of details using sensors.

REFERENCES

[1] Sandip Jangir, Alok Jaiswal, Sheetal Chandel, "A Novel Framework for Pharmaceutical Supply Chain Management using Distributed Ledger and Smart Contracts", *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, Kanpur, India, 2019, pp. 1-7, doi: 10.1109/ICCCNT45670.2019.8944829.

[2] Alok Jaiswal, Sheetal Chandel, Ajit Muzumdar, Madhu G M, Chirag Modi, C. Vyjayanthi, "A Conceptual Framework for Trustworthy and Incentivized Trading of Food Grains using Distributed Ledger and Smart Contracts ", *2019 IEEE 16th India Council International Conference (INDICON)*, Rajkot, India, 2019, pp. 1-4, doi: 10.1109/INDICON47234.2019.9030290

[3] Ravi Chandra Koirala, Keshav Dahal, Santiago Matalonga, "Supply Chain using Smart Contract: A Blockchain enabled model with Traceability and Ownership Management ", 9th International Conference on Cloud Computing, Data Science & Engineering (Confluece 2019)

[4] Zhijun Xu, Yichen Liu, Jun Zhang, Zhaoxiong Song, Jun Li, Jihua Zhou, "Manufacturing Industry Supply Chain Management Based on the Ethereum Blockchain", *2019 IEEE International Conferences on Ubiquitous Computing & Communications (IUCC) and Data Science and Computational Intelligence (DSCI) and Smart Computing, Networking and Services (SmartCNS)*, Shenyang, China, 2019, pp. 592-596, doi: 10.1109/IUCC/DSCI/SmartCNS.2019.00124.

[5] Feiyang Qu1, Hisham Haddad1, Hossain Shahriar2, "Smart Contract-based Secured Business-to-Consumer Supply Chain Systems", *2019 IEEE International Conference on Blockchain (Blockchain)*, Atlanta, GA, USA, 2019, pp. 580-585, doi: 10.1109/Blockchain.2019.00084

[6] RuhiTaş, ÖmerÖzgürTanrıöver, "Building A Decentralized Application on the Ethereum Blockchain ", *2019 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*, Ankara, Turkey, 2019, pp. 1-4, doi: 10.1109/ISMSIT.2019.8932806

[7] Rana M. Amir Latif, Samar Iqbal, Osama Rizwan, Syed Umair Aslam Shah, Muhammad Farhan, Farah Ijaz "Blockchain transforms the Retail Level by using a supply chain Rules and Regulation", *2019 2nd International Conference on Communication, Computing and Digital systems (C-CODE)*, Islamabad, Pakistan, 2019, pp. 264-269, doi: 10.1109/C-CODE.2019.8681027