IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 6, June 2019

Implementing Blockchain in Public Distribution System

Asmath Fahima Famnaz[1], Dr.Sharmila Kumari[2]

M. Tech, Student Department of Computer Science & Engineering, P.A College of Engineering, Mangalore, India[1]

Head of Department, Department of Computer Science & Engineering, P.A College of Engineering, Mangalore, India[2]

Abstract: In this paper we will describe a blockchain technology-based prototype that can be used in a small website. There are presently many fraud activities and corruptions taking place in the food supply schemes present as it sometimes does not reach the poor or the other sections of the society. This paper focuses on developing blockchain prototype that is used to record all the transactions/records and log all these transactions. A simple end-to-end web based app of this kind of the blockchain prototype can be built that has most of the features and functionalities to carry out all kinds of the transactions between the central government, state government, the district office, ration shop/and the customers, are recorded in the system. The user of the system can view the transactions of any part of the public distribution system. The project have some features that is guaranteed to provide the most important aspect that is, the security using the concept of blockchain.

Keywords: Blockchain, Public Distribution System, Blocks, POW, Mining, Bitcoin

I. INTRODUCTION

In the present world is such a common word. It's surprising that the working behind the bitcoin i.e. was actually introduced after the bitcoin. word bitcoin consists of two parts that is," which refers to 1's and 0's and "coin" refers to currency. So it basically means currency in the digital world. is also called currency [5].

We know that for most of the applications, there exists three type of people namely producer consumer and a broker/middleman. Suppose that you wanted to sell a book in Amazon, you do it will have to pay 45%-50% fees to sell the book in the site. middleman is an important part of the producer's money.

To clearly understand how the bitcoin works is important to know why it is brought in the first place. It was actually brought to remove the middleman, your are sending money from India to a friend in UK. you will have to pay a certain fee in the bank. if your friend have to the money should also pay an amount to the bank. It is not only that the fee is a problem's also the problem for the data that is being stored. know that the banks store a lot of private information about their customers. banks have been hacked for over so many years. is also dangerous nowadays to store the amount in the banks. know that the bank has the capability to freeze 's accounts whenever they want. is can also say that banks have too much power and control over the population that use the bank. banks played a major role during the financial crisis in the year 2008. is said that its because of this reason why bitcoins where introduced [5].

The remedy was to build a system in which a central authority was not involved that is should be controlled. The is one such technology that can be used to implement these schemes which can help to eliminate frauds and corruption activities is done by recording and maintaining all the activities that take place and thus having a transparency to all the users involved in the system. The public distribution system is a food security and food supply system which have the right to control and distribute the food supply to the population. was brought by the government of India held under the Ministry of consumer affairs and the public distribution. is also jointly managed by the state govt of India. major commodities they supply rice, sugar etc through a large and wide network of the rations hop spread across India. The supply to is managed by the government For example, if a wants to sell the commodities supplied from the government to consumers, it must do a transaction looking into account the amount to be supplied and this food transfer transaction will be recorded into the . this way every food transfer will be recorded into the and anybody can verify whether a particular item was distributed in the system starting from the government is reaching the consumers. After all the transfers have taken place, the government can see any time all the transfers of . If a reports that he has sold a particular item, government can verify that by viewing the transactions recorded on the . Thus, this can help us to eliminate any fraud activities in the system[2].

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 8, Issue 6, June 2019

II. PROBLEM STATEMENT

The aim of this project is to build a blockchain which helps in managing the public distribution system. The prototype for public distribution system consists of a network of central government, state government, and customers nodes of blockchain network), all have the distributed identical blockchain database which has the records of all the transactions that have taken place between any levels. The blockchain stores the logs of all the commodity transfers and money transfers in the system. Commodity transfers include the supply of stock from the central government to the state government, food stock distribution to by the state government, and food supply to consumers by the . The money transfer blockchain stores transfers of money from the central government to the state government for the food stock received and the money transferred from the customers to the state government for the quantity of food products bought from the [1].

III. EXISTING SYSTEM

In existing systems, there are security available in public distribution system websites yet there are many number of nodes could not be connected at the same time and also the major point is that several fraud activities occur in these sites. It is mainly due to the reason that the exact transactions done by the lower levels (till the ration shops) cannot be viewed by the government. So, this drawback appears to as a chance for the frauds to manipulate the public distribution system.

In the paper “Blockchain prototype for E-governance”, the blockchain prototype built is currently deployed on the local testrpc network, which runs only one system and acts as a single node. This prototype can be modified to incorporates a network of nodes of the blockchain the consists of governments, fair price shops and customers acting as nodes, which can be used by the government. The concept of the blockchain network perspective, that is, the concept of miners that is used to mine all the transactions is not used in their system[1].

The central government has developed a website for the public distribution system .However this system is not free from its limitations. Large number of bogus cards are issues using which the middlemen and the fps owner sells the grains to the open market. This transactions are not recorded and this fraud activities cannot be viewed by the upper levels(central government, state government and district offices).There different cards issued for the people belonging to BPL and the people above the poverty line. Each person must get the allowable quantity as said by the government. However in the current system, people do not get the entitled amount of grains from the ration shops. All of these fraud activities are not transparent[11].

There exists public distribution systems like the “Agent Based Simulation model and unique Identification Based Empirical Model” introduced by N.Hitaswi and K.Chandrasekaran, had an insight into the problems of duplicate and bogus ration cards. However, it did not provide the central government to view all the transactions occurring in the lower levels[9].

S.Kalpanadevi, S.Sukumar, K.Gopinathan and P.Naveen kumar, had developed a public distribution system that used an embedded system technology where they provided fingerprint detection for security. It had limitations due to high cost and problems in data storage (which could be easily managed in our proposed system)[10].

IV. PROPOSED SYSTEM

The proposed application is of more security due to the use of blockchain technology. The data is transparent so that the government can see the transactions of money and commodities at anytime. This website can be used by several nodes at a time at any level. So basically ,each authorizes node acts as a server and does the transactions. The data transferred is place in all the node’s database. The special property of this system is definitely the decentralized network and the POW(proof of work).

Merits of Proposed System

- Can be used by many nodes at the same time.
- Provides high security from fraud and thefts.
- Saves time and cost compared to existing system.
- The government can anytime verify the money transfers and commodity transfers that took place..
- The data cannot be tampered. Even if somebody tries to tamper it, he would drain all his money and electricity and eventually give up.
- Uses the property of Proof-of-work
- Since it is decentralized, the system cannot fail if it shutdowns at a single point.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 6, June 2019

Let us see what a blockchain is.A blockchain is a chain of blocks that contains records of the transactions. It is managed by computers present in the networks and there is no central authority/server that controls. All the blocks in the blockchain are very much secured and is connected to each other using different cryptographic algorithms. The blockchain is a shared ledger that contains immutable data. So, the blockchain has the main property called transparency. Using which, the chain and the transactions can be seen by any person in the network. Suppose that you need to pass the data from A to B .Here the first party i.e., A creates a block. This block is distributed throughout the nodes present in the network. This block is verified by all the other nodes in the network. Once it is verified ,it is added to the chain. If a hacker/attacker tries to tamper any of the block present in the chain ,he will need to fix all the other blocks in the chain too. This is impossible.

We know that a chain consists of data blocks. Each block consists of the data/transactions. A block consists of several components. As shown in fig. 1 ,main components are as follows:

1. The hash of the previous block
2. The current block hash
3. The timestamp
4. The proof
5. The data

We know that chain is composed of blocks. Each block its own cryptographic hash calculated using the contents in it. This value is stored in the succeeding block .So each block will be having a hash of its own and the has of the previous one. This is the manner in which each of the block is connected to each other(similar to that in a linked list).This is the main component that helps in the connection between the blocks and also the chronology creation between every blocks. The proof is kind of a nonce that is stored in the block that is used during mining. The data present in the blocks can be any kind of transactions.

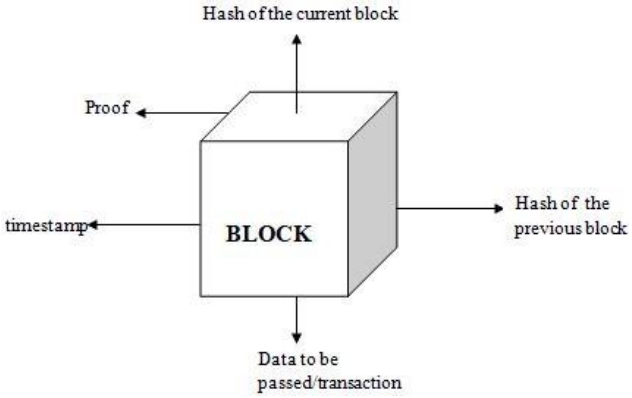

Fig. 1 A Block

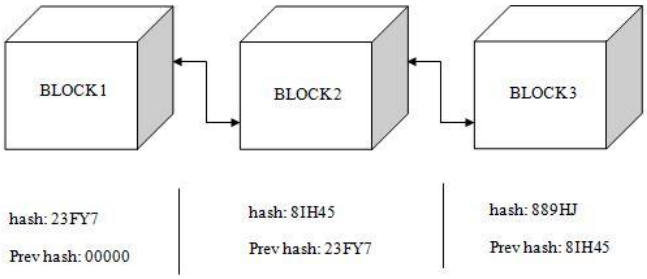

Fig. 2. A simple example of Blockchain

The blockchain of the blocks is demonstrated in the figure 2,where each of the block's hash is stored in the consecutive blocks. In this way, the blocks are linked together. POW is a protocol that is used for prevention from the denial-of-service attack(DDoS) that exists in the network. Due to this attack the network will be filled with many fake requests that will eventually lead to the exhaustion of the resources. This technique was existed before the introduction of bitcoin by Satoshi Nakamoto(identity not revealed).The important feature of this technique is that it allows trust less and distributed agreements[5].

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 8, Issue 6, June 2019

The POW actually consists of an expensive calculation called “mining”. The result from the mining decides whether to create a block and add it to the chain. Mining serves two purposes:

1. To check the validity of a transaction(or to avoid double-spending).
2. To create a new digital reward(or currency) providing those miners to performs the task.

The following is what actually happens during the transaction. Transactions/data are placed inside the blocks. Each block consists of index, timestamp, hash, hash of previous block and transactions. One of the node triggers a transaction. This node broadcasts the block to all the other nodes in the network. The nodes compete by trying to solve the mathematical problem/puzzle. One of the nodes succeeds and broadcasts the "End of mining" message to all other nodes. The nodes upon receiving the message, stops the mining. The nodes now verify whether the block is valid or not. If the block is valid, then it is added to the chain. The mathematical problem is such that it must be hard on the requesting side and must be easy to check for the network. This mechanism must be so difficult that one has to use a brute force method to find all the possible values. In our project, we have used a value called proof. The mining uses a random number multiplied to a predefined integer rather than an incremental value as a nonce. This makes the difficulty level high and prevents from flooding of blocks in network.

V. RESULTS AND DISCUSSIONS

As shown in the fig. 3, there exists four levels of nodes here, namely, the central nodes, state nodes, district nodes, and the ration shop nodes.

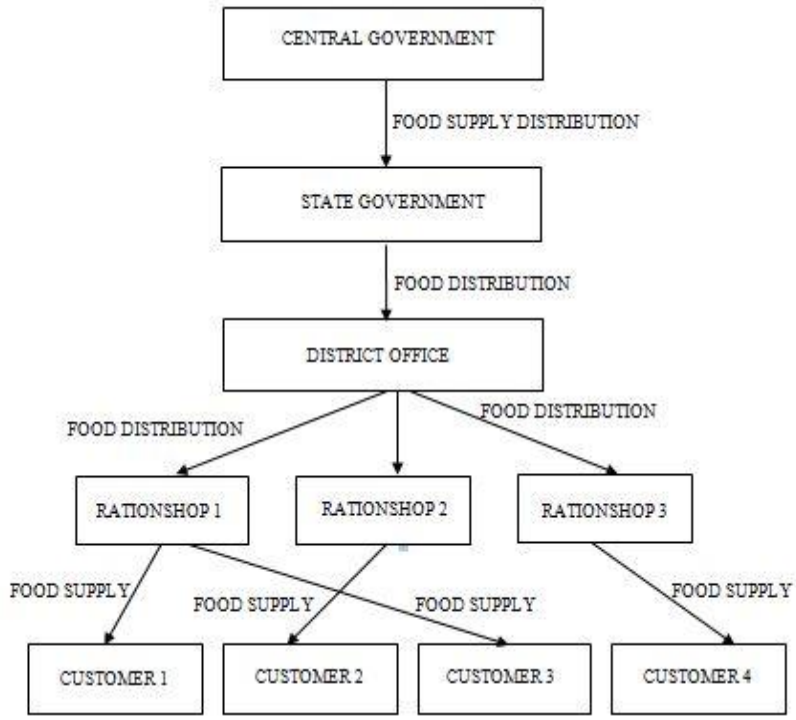

Fig. 3. Blockchain prototype of public distribution system

At each level of the prototype ,it is allowable to connect any number of nodes. These nodes are admins of the respective levels i.e., central government, state government, district office and ration shop. At each of the levels there is a blockchain created that shows the transactions. At the central government level, the admins logs on to the network and allocate the required food items to the state government. The transactions from all the admins are recorded and added to the blockchain and also the information is updated to the respective databases. At the district office level, the admins logs on to the network and allocate the required food items to the ration shops. The transactions from all the admins are recorded and added to the blockchain and also the information is updated to the respective databases. At the ration shop, the shopkeepers view the type of eligible cards the customers use. If the customer belongs to BPL (below poverty line),then they are supplied with the government fixed quantity of food item free of cost. If the customer possess the blue card, then they are supplied with food items as fixed by the government. They pay the required amount. All the transactions are recorded in a blockchain and the required databases are updated.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 8, Issue 6, June 2019

```
mineBlockallot(block)
{
this.blocks.push(block);
block.hash=block.hashValue();
console.log('Mined Successfully');
this.io.emit(actions.END_MINING_ALLOT_PUBLIC DISTRIBUTION SYSTEM,
{"newchain":this.toArray(),"block":block});

}

async newTransaction(transaction) {

this.currentTransactions.push(transaction);
if (this.currentTransactions.length === 1) {
console.info('Starting mining block...');
const previousBlock = this.lastBlock();
process.env.BREAK = false;

const block = new Block(previousBlock.getIndex() + 1, previousBlock.hashValue(), previousBlock.getProof(),
this.currentTransactions);

const { proof, dontMine } = await generateProof(previousBlock.getProof());

block.setProof(proof);
this.currentTransactions = [];
if (dontMine !== 'true') {
this.mineBlockallot(block);
}
}
}
```

The above code is the crucial part of this system. As we know there are a number of nodes present in the system and it is necessary to have mining operations. The nodes starts to mine the block. At each point of time the flag is checked to see if any node in the system has successfully completed the mining. In the generateProof method of the code, a proof similar to that of a nonce is created. But rather than just incrementing of the nonce, it is better to use a random number, so that the difficulty of mining is high.

As soon as a node completes the mining, it broadcasts the message to all the other nodes to stop mining. Each node now checks the block and upon verification, it is added to the chain.


```
{
    "index": 1,
    "proof": 3706889514.1633415,
    "timestamp": 1558138086347,
    "previousBlockHash": "a7e18a1bc82dfc9f907547df054c16730d342a9065e6992475e3a
    "transactions": [
        {
            "name": "Beena",
            "cardtype": "Blue card",
            "membercount": "5",
            "quantity": "10 ",
            "price": "100"
            "timestamp": 1558138086346
        }
    ],
    "hash": "00201bc93fd6c5c00ab3aae508bf9d624ce86d6e3b8763620ed451bc92b2997d"
},
```


Fig. 4(a). Blockchain created at the ration shop level

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 8, Issue 6, June 2019


```
{
    "index": 2,
    "proof": 4198617827.6871185,
    "timestamp": 1558138116297,
    "previousBlockHash": "00201bc93fd6c5c00ab3aae508bf9d624ce86d6e3b8763620ed45
    "transactions": [
        {

            "name": "Ram",
            "cardtype": "BPL card",
            "quantity": "25 ",
            "timestamp": 1558138086346
        }
    ],
    "hash": "f598cdd3cd49f0af2bfa5da151f3f380a81a7fc03f4cc61d938e42621be25384"
}
```


Fig. 4(b). Blockchain created at the ration shop level

In the similar way, each nodes in the central level, state level, district level & the ration shop level can add the transaction to the block. The recorded transaction at each level will have a blockchain similar to the figures 4(a) & 4(b).

VI. CONCLUSION

A blockchain prototype for the public distribution system is built using the help of node.js and blockchain functionality. The prototype for this public distribution system consists of the central government, the state government, the district office, the ration shops/public distribution system outlets and customers who are involved in the blockchain network in a decentralized way to interact with one another and carry out the required transactions of the food supply and the money transfers. The blockchain prototype will record each and every transaction that will happen in the system and it will maintain the entire history of the transactions from the initial transaction to the current time transaction. Hence it will help in the better security of the system and help to reduce fraud activities and corruption activities in the public distribution system.

REFERENCES

[1]. Prabhu, Shreekanth & Chauhan, Devendra & Ranjan, Ayushi. (2018). "Blockchain Prototype for E-Governance", CHAPTER-1. 10.13 140/RG.2.2.10710.14408.
[2]. Kamilaris, Andreas & Prenafeta Boldú, Francesc & Fonts, Agusti. (2018)." The Rise of the Blockchain Technology in Agriculture and Food Supply Chain".
[3]. G. Perboli, S. Musso and M. Rosano, "Blockchain in Logistics and Supply Chain: A Lean Approach for Designing Real-World Use Cases," in IEEE Access, vol. 6, pp. 62018-62028,2018.
[4]. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder," Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction"
[5]. CB Insights. (2017). How Blockchain Could Transform Food Safety. Retrieved from https://www.cbinsights.com/research/blockchain-grocery-supply-chain/
[6]. https://blockgeeks.com/guides/what-is-blockchain-technology/
[7]. https://dev.to/sadarshannaiynar/blockchain-using-nodejs-and-socketio-5gbe
[8]. https://medium.com/@pfedchen/how-blockchain-technology-will-transform-grocery-retail-7eaaf5fa405a