# Title of Work

# Ration Distribution Management Using Block chain

# Ration Distribution Management Using Block chain

In existing systems, there are security available in public distribution system websites yet there are many number of nodes that could not be connected at the same time and also the major point is that several fraud activities occur on 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  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 testpc network, which runs on only one system and acts as a single node.

The world is changing incredibly fast, and we are not all aware of it. Block chain technology and crypto currencies are an irreversible advancement that is disrupting established industries and the ways in which we interact financially. For that reason, I believe understanding and being aware of this block chain wave is incredibly important. The existing systems work as centralized architecture in database system.

- Large data storage is required for decentralized data storage as well as information system.
- The different attack issues in centralized database architectures.
- There are no automatic attack recovery in central data architectures.
- The decentralized architecture provides the automatic data recovery from different attacks.

After the analysis of this system we move to develop the decentralized system architecture, and distributed computing provides parallel processing in distributed environment.

**Object:**

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 authorized s a server and does the transactions. The data transferred is placed in all the node’s database. The special property of this system is definitely the decentralized network and the POW(proof of work).

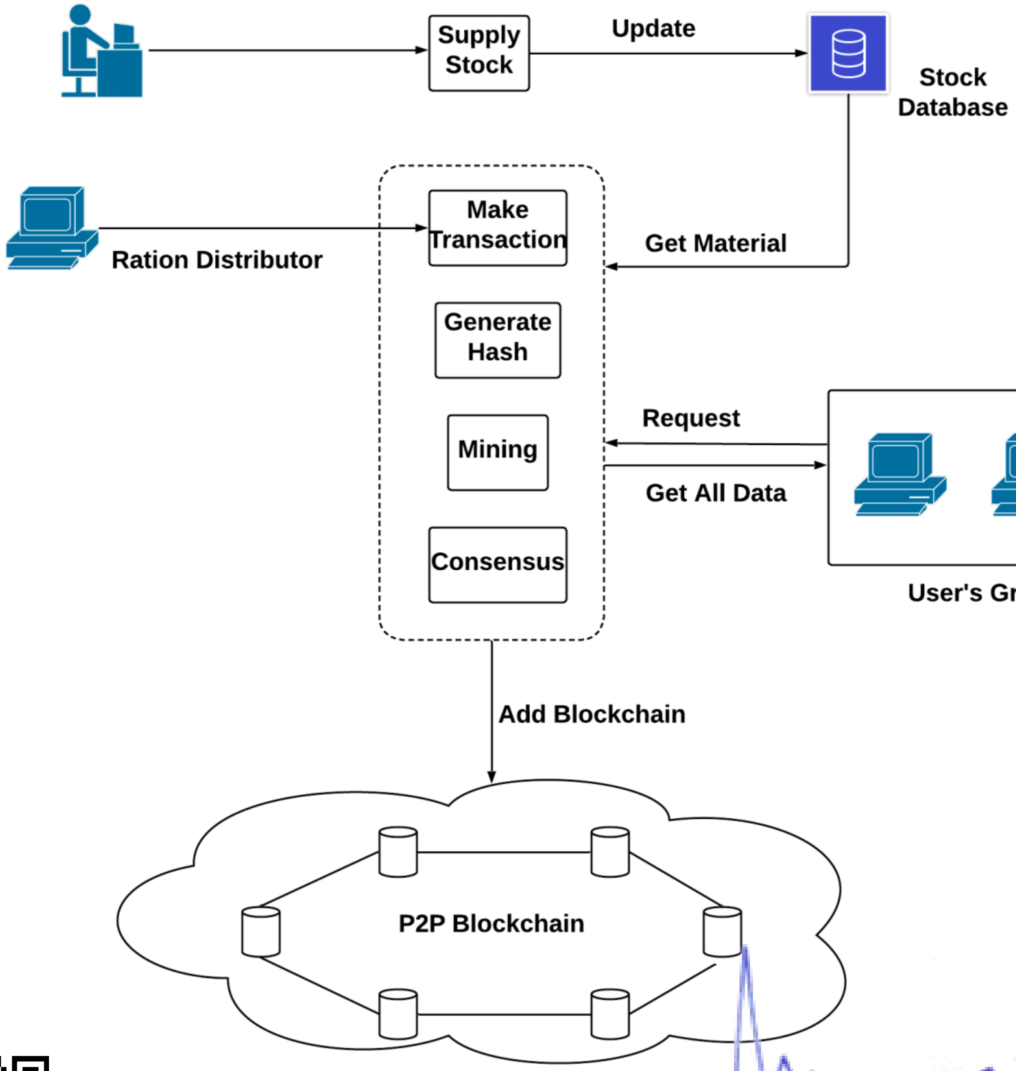
Merits of Proposed System

- 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.

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 has 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 hash 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 all the 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.



The supply stock will be updated by the administrator from government side. It will be added to the stock database. Now a ration distributor will update it’s requirement and try to access the amount of stock it would want from it’s side. Whenever a Ration distributor would want to have the supplies from the database, the complete cycle of blockchain will be performed and if the node is found to be a verified distributor then it will be added as a chain node.

**Innovativeness & Usefulness of project**

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.

**Current Status of Development**

- Objectives and problem statement finalization has done.
- Required tool set up has done on open source as well as windows environments.
- SHA 256 algorithm implementation has successfully done, for the generation of transaction hash for custom blockchain.

## Methodology of Evaluation

- The SHA-256 compression function operates on a 256-bit intermediate hash value.
- Automatic attack recovery by system.
- Quality assurance during the transaction.
- Immediate show of all historical transaction is single click, without any third partyinterface.

Algorithm 1 : Hash Generation

```
  Input : Genesis block, Previous hash, data d,
  Output : Generated hash H according to given data
  Step 1 :  Input data as d
  Step 2 : Apply SHA 256 from SHA family
  Step 3 :CurrentHash= SHA256(d)
  Step 4 : Return CurrentHash
```

Algorithm 2 : Protocol for Peer Verification

```
Input : User Transaction query, Current Node Chain CNode[chain], Other Remaining Nodes blockchain NodesChain[Nodeid] [chain],
Output : Recover if any chain is invalid else execute current query
Step 1 : User generate the any transaction DDL, DML or DCL query
Step 2 : Get current server blockchain
Cchain ← Cnode[Chain]
Step 3 : For each
    $NodesChain\ [Nodeid, Chain] \sum_{i=1}^{n} (GetChain)$
End for
Step 4 : Foreach (read I into NodeChain)
If (!.equals NodeChain[i] with (Cchain))
Flag 1
ue Commit query
Flag == 1)
```

```
Count = SimilaryNodesBlockchian()
Step 6 : Calculate the majority of server
Recover invalid block chain from specific node
Step 7: End if
End for
End for
```

## Mining Algorithm for valid hash creation

```
Input : Hash Validation Policy P[], Current Hash Values hash_Val
Output : Valid hash
Step 1 : System generate the hash_Val for ith transaction using Algorithm 1
Step 2 : if (hash_Val.valid with P[])
Valid hash
Flag =1
Else
Flag=0
Mine again randomly
Step 3 : Return valid hash when flag=1
```

## Methodology

- The central outline of the proposed algorithm is the implementation of ration distribution data storage using block chain.
- System creates the trustworthy communication between multiple parties without using any third party interface.
- We use the Hash generation algorithm and the Hash will be generated for the given string.
- Before executing any transaction, we use peer to peer verification to validate the data.
- If any chain is invalid then it will recover or update the current server blockchain.
- This will validate till the all nodes are verified and commit the query.
- ing algorithm is used for checking the hash generated for the query till the valid hash is erated.

- For experiment analysis to create multi peer nodes using Amazon EC2 public cloud environments.

Ration cards are an official document issued by state governments in India to households that are eligible to purchase subsidized food grain from the Public Distribution System (under the National Food Security Act). They also serve as a common form of identification for many Indians.

The main advantages of implementing the smart ration card are:

a. The ration items will be effectively delivered to the valid ration card holders who are below poverty line.

b. The main advantage here is that the customers get their rightful entitlement in terms of quantity. What's meant for them cannot be diverted to the open market because of maintaining the database correctly and generating bills properly.

c. Ration shops do not open every day. Nor do they keep regular hours. So to avoid discomfort to the customers a system generated message will be delivered to their mobile when the stock is available and the shop is opened so that it does not cause any trouble to the customer

d. A common practice is adopted by most people that run ration shops i.e., they charge people more than the mandated rates, and they often under-weigh the commodities. But using this technique they cannot do so because each and every item will be having its own code and the price will be generated from that code and hence no overcharge can be done.

e. The government services are reached to poor people effectively and also the corruption in PDS and FPS can be reduced or avoided to a great extent.

**Abstract Points**

- To design an approach for public ration distribution where system can stores all historical transactional data into block chain manner.
- To develop a custom blockchain for proposed public system, that end user can access and view entire data publically.
- To develop an own smart contract as well custom mining policy to achieve the efficiency into the system.
- To developed a consensus algorithm for proof of validation between P2P decentralized networks, for data security and eliminate different network attacks.
- To explore and validate how proposed system provides, beneficial influence than classical ration distribution system.