International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 03 | Mar 2021 www.irjet.net p-ISSN: 2395-0072

BLOCK CHAIN TECHNOLOGY IN PUBLIC RATION DISTRIBUTION

Prof. Sagar Dhanake[1], Shubham Desale[2], Prashant Pawar[3], Gaurav Patil [4], Sahil Shende[5]

[1]Assistant Professor, Dept. of Computer Engineering, DYPIET,SPPU, Pune, Maharashtra, India

[2,3,4,5]Student, Dept. of Computer Engineering, DYPIET,SPPU, Pune, Maharashtra, India

---

Abstract - *In this project 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 project 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.*

Key Words: *Public ration distribution, Block chain, SHA 256 AES, java, etc.*

1.INTRODUCTION

An increasing demand in society for greater information about food reflects the need for more transparency and the lack of trust. One of the most frequently used words in India, corruption signifies a range of things. In 2005, Transparency International, and Delhi-based Centre for Media Studies, a research firm, undertook the India Corruption Study. The survey covered 4,405 respondents over 20 states. The results, published in the same year, said that Indians pay about 21,069 crore as bribes while availing one of 11 public services. The study remains the most recent and most comprehensive report on corruption in India. Here we cover corruption in Indias public distribution system (PDS), the chain of ration shops that provide supplies to just under 10% of the country's population (the government claims 16%) as well as Corruption in Education. Corruption in PDS Bulk users are from the rural hinterland (7.6 crore). Pointers to how rampant is corruption in a sphere where the government has promised subsidized food for all through the PDS are: 1.5 crore households have admittedly paid bribe during the past year; States with a higher poverty index have registered higher corruption (up to 67%); 60% households using PDS confirmed unavailability of rations; In high poverty incidence states, out-of-stock" scenarios were as high as 80%; 34% of those visiting ration offices had to make four or more visits before their voice could be heard and suitable action taken; and Nearly 50% paid bribe for obtaining a new, perfectly legitimate ration card While the Fair Price Owner is accused of cheating and being corrupt, he has his constraints which include: Low margins leading to low profitability, especially post launch of targeted public distribution system (TPDS); credit provided is so low that they cannot lift stock from government godowns; they have no control over quality of grains; they too may have to pay bribe to ration officials to get their quota of supplies from the Food Corporation of India (FCI); supplies from FCI are erratic and late in coming.

1.1 Motivation

The last three years have seen an explosion of interest in Blockchain Technology (BCT) with a great many companies and research institutions focusing on potential applications of this technology across a range of financial, industrial and social sectors. However, the technology has also been surrounded by a great deal of exaggeration and hype resulting in misplaced expectations and misunderstandings. BCT is still in an early stage of development, with considerable potential for real-life commercial applications. Innovation in blockchain architectures, applications and business concepts is happening at a fast pace; it is often characterised by decentralised, open source development, and it is perceived as being disruptive to traditional players in many industries.

1.2 Project Scope and Limitations

Project will be developed as a prototype model using JSP and servlet technology. It will run as a local host. System will be communicate through wireless local area network. System

communication will be limited in the wireless local area network, but in future if we will host the project using WAN , it can communicate world wide.

2. PROBLEM DEFINITION AND OBJECTIVES

2.1 Problem Definition

To develop a prototype model for PDS using BCT which will developed as a web based protype model using JSP & servlet technology in java with MySQL as a database where SHA 256 will be used for block chain generation.

2.2 Objectives

1. To implement a java based web application.
2. To implement visual cryptography.
3. To learn and understand block chain technology.
4. To learn and understand distributed database system using WLAN.

2.3 Methodologies of Problem Solving

BCT PDS are the foundation of the peoples survival, and the quality of PDS has always been the focus of attention of society and the government; the original PDS traceability system is too difficult to tamper with data due to the excessive concentration of data storage, it faces the challenge of fraudulent data tracing, and it is difficult for citizens to trust such traceability results. Moreover, the centralized storage method is not conducive to the centralized management of traceable data from many enterprises, and there will be problems of low traceability and difficulty in government supervision. The emergence of blockchain technology provides a new solution for data security problems of food traceability, its decentralization, anti-tampering and other characteristics and data encryption technology improve the difficulty of data fraud and ensure data security. If the blockchain is combined with the traceability of PDS , the safety of traceable data and the tampering of data can be guaranteed to the greatest extent, the authoritity's behavior can be regulated, and consumers confidence in ration quality can be improved. This project mainly proposes a framework of PDS traceability system based on blockchain technology, it uses MySQL to store the traceability data of PDS safely, and proposes a traceability model of PDS, which can cover the entire PDS chain and citizens can query the authentic source of traceability of PDS.

3. LITERATURE REVIEW

[1] RFID Based Exam Hall Maintenance System Seating Arrangement of students during examinations is distributed. Students face difficulties as they have to scrounge for their examination hall numbers and seating arrangement while they are wits end. An innovation which could aid the students in finding their exam halls and seats would be welcoming and very rewarding. This paper RFID BASED EXAM HALL MAINTENANCE SYSTEM , presents a modernized method of examination hall management. It is possible for a student to identify the particular exam hall from any other hall, when they swipe RFID card in a card reader located there. This helps them to identify the floor or get directions to their respective halls without delays. The card reader is provided at the entrance of the building, if the students enters wrongly a buzzer alarm sets off, otherwise the room number is displayed on the LCD, connected to controller.

[2] Online Ration Card System by using RFID and Biometrics In this paper, we have developed a smart ration card using Radio Frequency Identification (RFID) technique to prevent the ration forgery as there are chances that the shopkeeper may sell the material to someone else and take the profit and put some false amount in their records. In this system, a RFID tag is used that carries the family member details and the customer needs to show this tag to the RFID reader. The microcontroller connected to the reader will checks for the user authentication. If the user is found authentic then the quantity of ration to be given to the customer according to the total number of family members will be displayed on display device. This smart ration card is free from theft as the information about the delivered ration will be send directly to the government without manual feeding using Global system for Mobile Communication (GSM) technique.

[3] Design of an Intelligent SMS based Remote Metering System Electrical distribution utilities are facing problems due to high energy losses that amount to 8The problem is mainly associated with sub-transmission and distribution networks. This paper presents a unique solution to devise a unit which is tamper proof, cost effective, fast, accurate and remote metering at any level of the distribution system. The system helps to access accurate and sufficient data from metering devices to measure the electrical parameters, eliminating the use of energy meters and human intervention. The software application provides a real time parameter like line voltage, line current, power factor, true power, apparent power and reactive power from remote

substations. Remote metering system is implemented using microcontroller based mixed signal circuitry.

[4] Implementation of ZigBee GSM based home security monitoring and remote control system As technology becomes more advanced and modernized; more features are added to the existing system for the purpose of satisfying the increasing security needs of the people. Deploying wireless technologies for security and control in home offers attractive benefits along with user friendly interface. In this paper we present a smart security system comprises of Zigbee, GSM, Sensors and Smartphone for Security monitoring and control, when the user is at remote premises. Three sensors namely P. IR, vibration and door sensor are installed at windows and doors. Whenever there is a security breach the sensors sends the signal to the Pic microcontroller. The Max 232 converter provides serial interface between the microcontroller and the zigbee. The Zigbee end device then transmits the signal to the Zigbee coordinator. The ZC at the control console communicates with MCU using max 232 converters. MCU would in turn access and control the GSM module via AT commands and automatically sends SMS to the owners mobile phone informing him about the security breach. On receiving the SMS, user can make a video call using Skype account; Smartphone installed at home will feed us with a live video. On viewing the video the user can know whether an intruder has entered or not. Then accordingly faint gas valve and door lock can be controlled by the user. Thus whenever there is an intrusion, our system lets the user to monitor and control his premises from any part of the world.

[5] The Pros and Cons of RFID in Supply Chain Management This paper presents the pros and cons of using radio-frequency identification (RFID) in supply chain management (SCM). While RFID has a greater number of benefits than its predecessor, the bar code, it currently comes at a price that many businesses still consider prohibitive. On the one hand, RFID is advantageous because it does not require line of sight scanning, it acts to reduce labor levels, enhances visibility, and improves inventory management. On the other hand, RFID is presently a costly solution, lacking standardization, it has a small number of suppliers developing end to end solutions, suffers from some adverse deployment issues, and is clouded by privacy concerns. Irrespective of these factors, the ultimate aim of RFID in SCM is to see the establishment of item level tracking which should act to revolutionize SCM practices introducing another level of efficiencies never before seen.

4. PROPOSED SYSTEM

An automatic ration material distribution system is implemented using GSM (Global System for Mobile) and RFID (Radio Frequency Identification) technology. This system replaces the ration cards by RFID tags. Stock availability in the ration shop will be intimated to the customer by sending a message through GSM. To get the materials in ration shops, one need to show the RFID tag into the RFID reader, then controller checks the customer's code and asks for the password. After verification, the customer is asked to enter the required materials and quantity by using selection keys. Based on the type of material, the motor or solenoid valve is open. After receiving materials controller sends the information to the Government through GSM technology. In addition to this some features has been implemented such as, Fire alarming system that gives an alert in case of fire accidents. For fire detection, temperature sensor DR25 is used. It senses the heat and passes the signal through multi vibrator to controller. The other feature is tampering detector system that detects in case of theft. In this, Probe sensors are used which detect the connectivity between two probes and generate the signal to the controller accordingly. If connectivity is missed it passes the signal to the controller. In both the cases the controller switches the alarm and sends the alert message to the government.

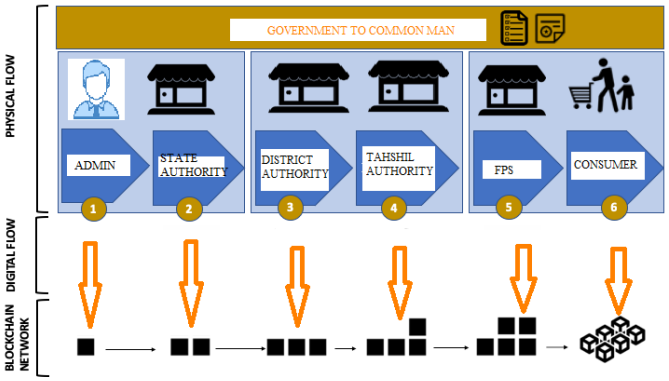

Fig -1: System Architecture

Whenever any transaction will occur in the system , the record of that transaction is maintained in the form of hash value in a block. Each next block will get attached to the previous block and in this way a virtual block chain will occur. The hash value of a current block is generated using the data of a current block and the hash of the previous block. In this way if any of the block is tempered the subsequent all the blocks hash must be changed . Such multiple copies are maintained at different servers , which

will assure the data security and confidentiality. As everything is through application interface, it will maintain the transparency in the PDS.

5. MATHEMATICAL MODEL AND ALGORITHMS

5.1 Mathematical Model

Let
S be Closed system defined as, S = Ip, Op, Ss, Su, Fi, A
To select the input from the system and perform various actions from the set
of actions A so that Su state can be attained.
S=Ip, Op, Ss ,Su, Fi, A
Where,
IP1=Username, Password, image
Set of actions=A=F1,F2,F3,F4
Where
F1= Send Mail
F2= Merge Images
F3= Encrypt Database
F4= Generate Hash
S=Set of users
Ss=rest state, registration state, login state
Su- success state is successful analysis
Fi- failure state
Objects:
1) Input1: Ip1 = Username, Password
2) Input2 : Ip2= image from mail
1) Output1 : Op1 = Transaction Record
2) Output2 : Op2 = Encrypted Database
3) Output3 : Op3 = Hash Codes.

5.2 Algorithms

AES:
AES is used to encrypt the database. The encryption process uses a set of specially derived keys called round keys. These are applied, along with other operations, on an array of data that holds exactly one block of data, the data to be encrypted. This array we call the state array.

Steps:
1. Derive the set of round keys from the cipher key.
2. Initialize the state array with the block data (plaintext).
3. Add the initial round key to the starting state array.
4. Perform nine rounds of state manipulation.
5. Perform the tenth and final round of state manipulation
6. Copy the final state array out as the encrypted data (ciphertext).

SHA 256:Hash Function

SHA-256 (secure hash algorithm, FIPS 182-2) is a cryptographic hash function with digest length of 256 bits. It is a keyless hash function; that is, an MDC (Manipulation Detection Code). A message is processed by blocks of 512 = 16 32 bits, each block requiring 64 rounds A cryptographic hash (sometimes called digest) is a kind of signature for a text or a data file. SHA-256 generates an almost-unique 256-bit (32-byte) signature for a text. A hash is not encryption it cannot be decrypted back to the original text (it is a one-way cryptographic function, and is a fixed size for any size of source text). This makes it suitable when it is appropriate to compare hashed versions of texts, as opposed to decrypting the text to obtain the original version.

6. CONCLUSIONS

Thus we are going to implement a prototype web based software application in Java for application of BCT in PDS . We have will implement block chain features such as:
1. Decentralization
2. Visual Cryptography
3. Hash Algorithm
4.Encrypted Database.
using java programming language. Thus it is possible to track PDS supply chain and so that ration will reach the common man without any corruption.

ACKNOWLEDGEMENT

The completion of our project brings with it a sense of satisfaction, but it is never complete without them those people who made it possible and whose constant support has crowned our efforts with success. One cannot even imagine our completion of the project without guidance and neither can we succeed without acknowledging it. It is the great pleasure that we acknowledge the enormous assistance and excellent co-operation to us by the respected personalities.

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 Bold, 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-grocerysupplychain.

[6] A. Abbas, S. Khan, A review on the state-of-the-art privacy preserving approaches in e-health clouds", IEEE Journal of Biomedical Health Informatics, 2014.

[7] J. Yang, J. Li, Y. Niu, A hybrid solution for privacy preserving medical data sharing in the cloud environment , Future Generation Computer Systems, 2015.