NOLEGEIN Journal of
Corporate & Business Laws

ISSN: 2581-7779
Volume 6, Issue 1, 2023
DOI (Journal): 10.37591/NJCBL

http://mbajournals.in/index.php/JoCBL/index

Review NJCBL

Blockchain-based Cheating Prevention System in Fair Price Shops

Mahammad Ashfaq Sasalatti[1,*], Akshata Kumbar[1], Trupti Chandanshiv[1], Shravan Kumar Dhangi[1], Varun P. Sarvade[2]

Abstract

The existing public distribution system (PDS), commonly known as the ration system, is marred by rampant fraudulent activities, leading to a lack of efficient distribution of subsidized essentials to the deserving beneficiaries. This paper introduces a novel approach to address this issue by leveraging blockchain technology to create an alternative solution for the traditional ration distribution system in India. The proposed prototype harnesses the inherent benefits of blockchain to establish an accountable and transparent distribution framework. Our study involves the development of a robust blockchain prototype tailored specifically for recording and safeguarding every transaction that takes place during ration distribution. This immutable ledger ensures that all recorded data remains tamper-proof and resistant to unauthorized alterations. Operating through a user-friendly end-to-end web interface, the system mirrors the features and functionalities of the conventional distribution system, ensuring seamless user adoption. Central to the proposed system is the capability for users to access transaction records effortlessly from the public distribution system. By utilizing blockchain technology, the vulnerability of data pertaining to user and distributor registrations, as well as transaction histories, is significantly reduced. The integration of blockchain not only bolsters the security aspect but also drastically minimizes the possibility of data breaches and manipulations. The outcome of this endeavor is a fully operational, tamper-proof blockchain-driven platform poised to revolutionize the traditional ration distribution system. This innovative solution has the potential to curb fraudulent activities and foster equitable distribution, reinstating faith in the welfare system. As the technology matures and gains wider acceptance, it holds the promise of transforming the landscape of public welfare distribution systems beyond the confines of India, heralding a new era of transparency and accountability.

Keywords: Blockchain, public distribution system, ration, smart contracts, cybersecurity

***Author for Correspondence**
Mahammad Ashfaq Sasalatti
E-mail: ashfaqsasalatti123@gmail.com

[1]Student, Department of Computer Science and Engineering, Biluru Gurubasava Mahaswamiji Institute of Technology (BGMIT), Mudhol, Karnataka, India
[2]Assistant Professor, Department of Computer Science and Engineering, Biluru Gurubasava Mahaswamiji Institute of Technology (BGMIT), Mudhol, Karnataka, India

Received Date: July 26, 2023
Accepted Date: August 15, 2023
Published Date: August 30, 2023

Citation: Mahammad Ashfaq Sasalatti, Akshata Kumbar, Trupti Chandanshiv, Shravan Kumar Dhangi, Varun P. Sarvade. Blockchain-based Cheating Prevention System in Fair Price Shops. NOLEGEIN Journal of Corporate & Business Laws. 2023; 6(1): 42–54p.

INTRODUCTION

Background

- *Public distribution system*: The public distribution system (PDS) is an Indian food security system that provides low-cost food and non-food goods to the country's underprivileged. The Indian government founded it in 1997. The items given to beneficiaries include food grains like wheat, sugar, and rice and fuels like kerosene. The distribution occurs at fair price shops (ration shops) situated throughout India [1].
- PDS is chastised for failing to successfully serve the needy. This is due to large corruption that occurs due to lack of supervision [2].

- Currently, E-PoS (electronic point of sale) machines are used in fair price shops to carry out distribution. These provide authentication through biometrics (fingerprint) and OTP (one time password) generation [3].

Motivation

The introduction of ePOS contributes to enhancing food security and controlling malpractices. However, all the transactions are stored in the state PDS server, which can be manipulated by fraudsters using attacks such as SQL injection attack.

Other flaws of ePoS machines include the need for regular maintenance, high cost, and no fault tolerance, so once the link goes down then no operations can be performed [4].

The graph in Figure 1 shows financial losses incurred in the public distribution system due to various fraud activities in the past decade, as mentioned by various news articles. The money loss is represented in terms of crores.

Objective

Our objective is to create a blockchain technology-based prototype that will act as an alternative to the traditional PDS. It will be a web application to replace existing food supply schemes using blockchain technology that has similar features and functionalities involved in the PDS, and thus mitigate the corruption taking place in it.

Paper Organization

The rest of this paper is structured as follows: The second section provides a synopsis of the associated works. The third section explains blockchain technology and the mathematics behind it. The fourth section gives an overview of the algorithm that depicts the process involved in our system. The approach is discussed in the fifth section, and the system deployment is outlined in the sixth section. The penultimate section presents the results, while the final section concludes the study.

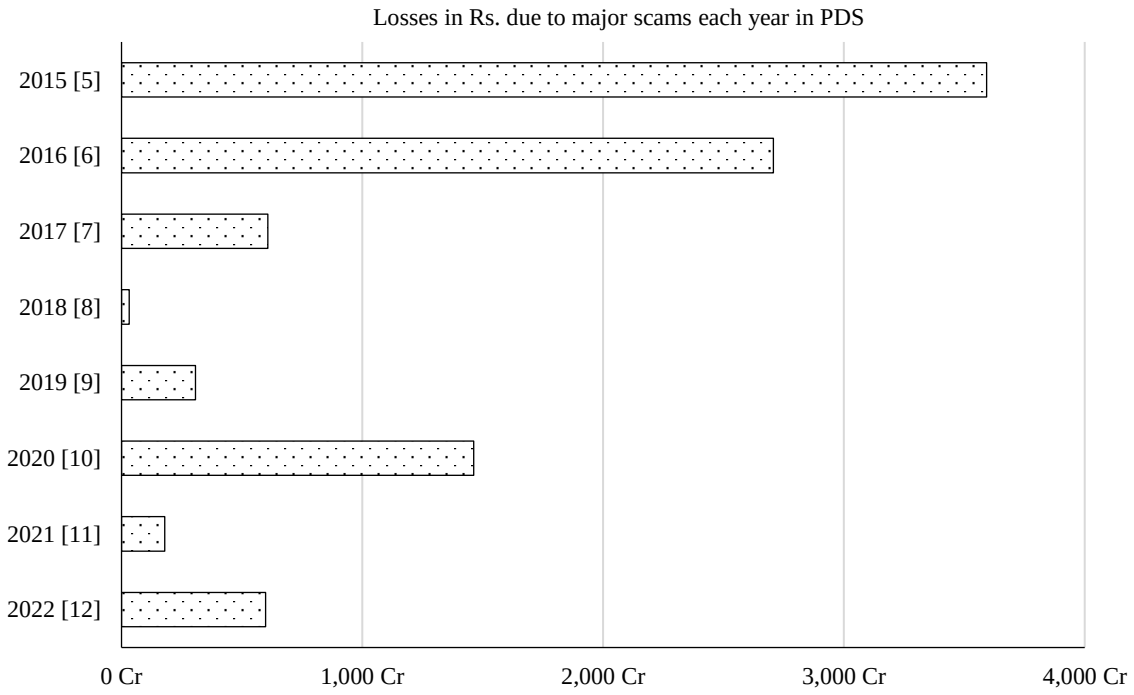

Figure 1. Loss due to major public distribution system (PDS) scams.

LITERATURE SURVEY

A blockchain-based prototype for usage in a small website. This paper proposes a system that distributes materials automatically through GSM (global system for mobiles) and RFID (radio frequency identification) technology. RFID tags are being utilized to replace conventional ration cards. Available stock is sent as a messageto the customer through GSM. After verification through RFID tags, the customer can enter the required materials through selection keys, and they will be provided [5]. GSM is then utilized to send information to the government. Transactions are recorded as hash values in blocks and each subsequent block maintains a copy of the previous block, making them devoid of tampering and assuring data security and confidentiality. In addition to this, the prototype also provides fire alarms and tampering detectors using sensors.

An Android-based automatic ration system has been developed to solve the problem in traditional ration systems [6]. Traditionally, the handling and distribution of commodities in ration shops are manual,which can lead to illegal usage of goods. The authors have designed an Android app into which users can log in and check the transactions. The data is saved on a cloud-based web server. The system uses a microcontroller that controls the operation at all parameters and uses smart cards instead of RFID cards for authentication. Smart cards are used to store the details of the user (UID). GSM module and WiFi module are used to send messages to mobile and to provide connectivity to the system respectively. Overall, this system can reduce the limitations of the conventional rationing system effectively.

Another study reports an automated public food distribution system that uses a smart contract written in solidity language and compiled, deployed, and run in Remix IDE [7]. This system contains the majority of the characteristics and functions of a ration store. It is currently deployed in the browser using Java virtualmachine (JVM) and the authors plan to make it into an interactive web application.

This framework has typical benefits of being provided by blockchain technology, that is, transparency, and data protection, and is also time and cost-effective.

A mechanism that utilizes smart contract-based transactions and internet of things (IoT) technology for asset tracking to ensure transparency andavoid malpractice during transportation is developed. Google speech engine was also used to develop interfaces in local languages. The planned blockchain network's performance is analyzed and reported on. The response time of the system was around 130 ms, making it suitable for real-time application and the system was 100% immutable. The article suggests that this system could improve the PDS by providing more transparency and access to all transactions while preventing corruption [8].

A system based on blockchain that can act as an alternative to electronic health records (EHRs) has been developed. Because of its security, privacy, secrecy, and decentralization, blockchain technology has enormous potential in the healthcare sector. This study offers a blockchain-based system that may be used as an alternative to EHRs. The authors state that EHRs have the potential to improve care quality. decrease expenses and improve efficiency in healthcare systems. However, there are several challenges associated with EHRs, such as security, interoperability, and patient control over their health data. Blockchain can improve the security and privacy of EHRs by providing a decentralized, tamper-proof system that allows patients to control access to their health data [9]. Additionally, blockchain can improve interoperability by providing a standardized system for exchanging health data between different healthcare providers. The authors also discuss the potential benefits of blockchain-based EHRs, such as increased efficiency, improved patient outcomes, and reduced healthcare costs. The paper also discusses some of the challenges associated with implementing blockchain-based EHR systems, such as scalability and regulatory issues. The authors point out that various technological and regulatory hurdles must be overcome before blockchain-based EHR systems can be extensively implemented.

A detailed description of an IoT-based smart ration system that uses biometrics to authenticate beneficiaries and ensure transparency in the distribution process. The proposed system uses a fingerprint scanner and an iris scanner to identify beneficiaries andauthenticate their transactions. It also uses IoT devices such as sensors and cameras to monitor the distribution process and ensure transparency. The authors also present a detailed analysis of the advantages of the proposed system, which are reduced fraud and improved targeting of beneficiaries. Furthermore, the paper highlights the potential impact of theproposed system in improving the efficiency and transparency of the Indian PDS. The authors argue that the proposed system can help to reduce leakages. However, there is no consideration of the difficulties that may arise during the implementation of the suggested system. For example, the cost of implementing such a system could be a significant barrier to its adoption, and the authors do not provide an estimate of the cost of the proposed system. Furthermore, the report does not address the various technical and operational issues that may occur during system deployment.

BLOCKCHAIN

Blockchain was designed by Nakamoto [10] for his cryptocurrency Bitcoin. It is similar to a distributed ledger in that it is made up of blocks (records) that are securely linked together using cryptographic hashes. Each block includes transaction data, a timestamp, and the preceding block's hash. The blockchain transactions are immutable in that, data in each block cannot be altered without subsequently changing the subsequent blocks.

Smart Contract

A smart contract is a piece of code that executes a certain function on the blockchain. The code executes by itself when the user performs a transaction and certain conditions are met. As they are stored in blockchain, they are tamper-proof. Solidity is now the most common language for creating smart contracts.

Mathematical Model

The mathematical model of blockchain can be defined using the hash functions, the Merkle tree, and the elliptical curve. These are discussed below.

Hash Functions

A hash function is a mathematical function that creates a unique output from an input message or data, known as a hash value. Hash functions are similar to digital fingerprints and are used to verify the authenticity and integrity of data. It is extremely difficult to find two different inputs that generate the same output, making hash functions very useful in ensuring data security. SHA256 is a widely known hash function that converts a message into a 256-bit binary number, which is sometimes represented as a 64-digit hexadecimal number. An example of a hash value is given below [11].

SHA256:
625da44e4eaf58d61cf048d168aa6f5e492dea166d8bb54ec06 c30de07db57e1

Merkle Tree

A Merkle tree is a type of data structure that allows for the efficient storing of vast quantities of data while maintaining data integrity [12]. Each tree leaf node represents a single data piece, whereas each non-leaf node represents the hash value of its offspring nodes. Data d is shown in Equation 1 below.

$$d = \{L1, L2, L3, \ldots, Ln\} \quad (1)$$

The leaves of the tree in this case are h(L1), h(L2), and soon where h is a hash function.

To construct the tree, we take the hash values of the adjacent nodes in the previous layer and add them to form the next layer until a single root node is formed [13]. The root node represents the hash

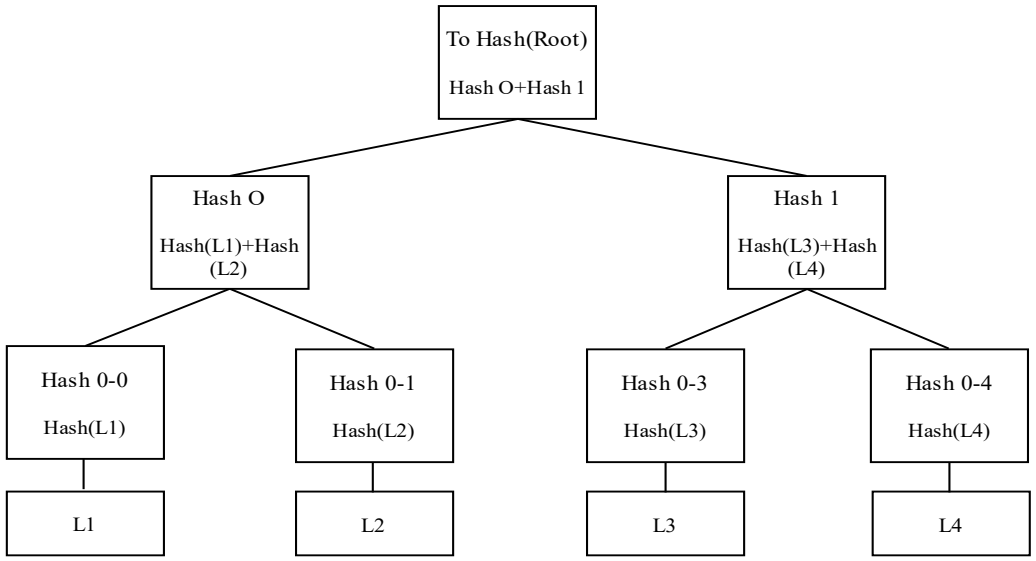

Figure 2. Merkle tree.

value of all the data in the tree, andchanges if any change is made to that data. As a result, the data's integrity may be easily checked. The use of Merkle trees is widespread in various applications such as cryptocurrencies,file sharing, and data synchronization.

Figure 2 depicts the Merkle tree for D = {L1, L2, L3, L4}.

Elliptic Curve

Elliptic curve cryptography (ECC) is a popular method used in blockchain to generate public and private keys for digital signatures. The challenge of ECC is to solve the discrete logarithm problem over elliptic curves to assure system security.

The elliptic curve equation used in the blockchain istypically in the form of

$$y^2 = x^3 + ax + b \quad (2)$$

The elliptic curve algorithm generates a public key by multiplying a private key by a fixed point on the curve. The public key can then be used to verify digital signatures and ensure the authenticity and integrity of blockchain transactions.

Elliptic curves provide a high level of security while using smaller key sizes than other cryptographic methods, making them well-suited for use in blockchain technology.

ALGORITHM

Below is the algorithm for the operation of distributing items to the customers.

1. Customer registers using the web application.
2. Data is saved on the blockchain, and the customer is assigned a unique identifier. The government adds employees (distributors) and a list of food items that are stored in the blockchain.
3. To distribute the items, we need to provide the unique ID of the user to the system.
4. If that ID is present in the list of beneficiaries, the system will generate OTP which is sent to the registered customer’s mobile number.
5. The distributor inputs the OTP into the system.
6. After verification of OTP, the distributor can give the items to the customer, and the transaction is saved in the blockchain.

METHODOLOGY

Method Behavior

The distributor can register a beneficiary to the system through the 'register' webpage. Here, we must put beneficiary details, that is, their name, identification number, Aadhar number, and phone number. Distributors also have options to add and delete members to an existing card and to delete a card. The phone number and Aadhar numbers are required for OTP authentication. The unique ID is the address of the beneficiary's valet. All the data inserted is saved in the blockchain (Figure 3).

The government sets the required number of items that must be given to each beneficiary. It can also add or delete new shops and distributors in it. From user registration details to issue details, all data is saved in the blockchain server. It can be accessed at any time.

The distributor fetches data from the blockchain server to issue materials. An OTP server sends a six-digit OTP to the beneficiary's registered mobile number. It fetches the number from the blockchain.

DEPLOYMENT

Use Cases

Figure 4 shows the actors and the operations / functions they have access to in the system.

We can see that the distributor and customer are both involved in the registration process as the customer must give their information to the distributor. Sequence diagrams for registration and distribution processes are given in Figures 5 and 6, respectively.

Front End

The front end is created using HTML, CSS, and Bootstrap. The web pages provide the user with all of the necessary information. Users can input the data and submitit through the webpage. The website contains the following pages:

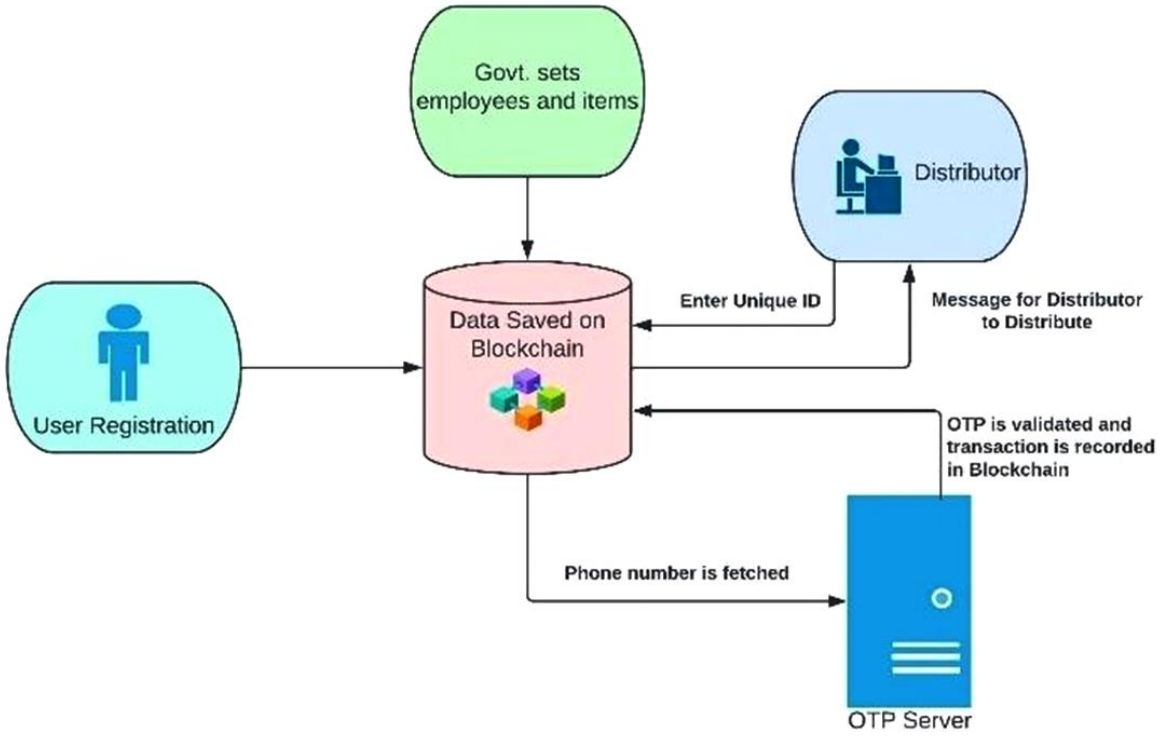

Figure 3. Block diagram of the system.

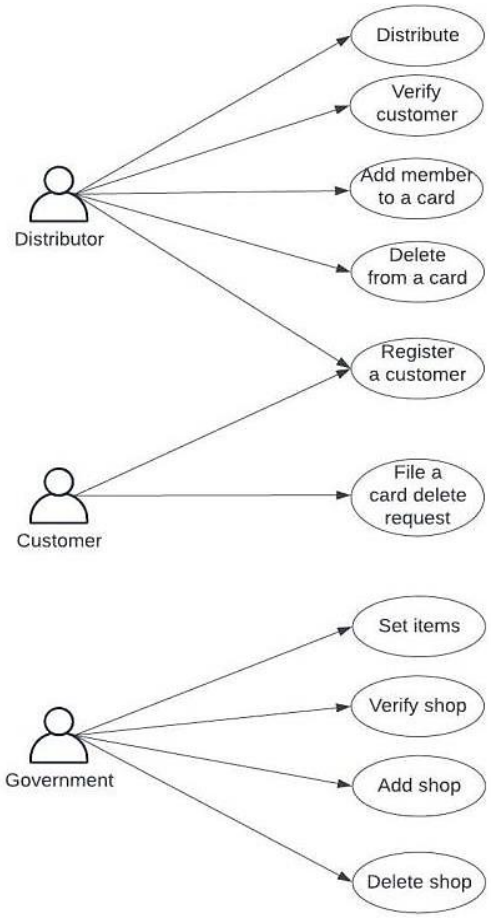

Figure 4. Use cases.

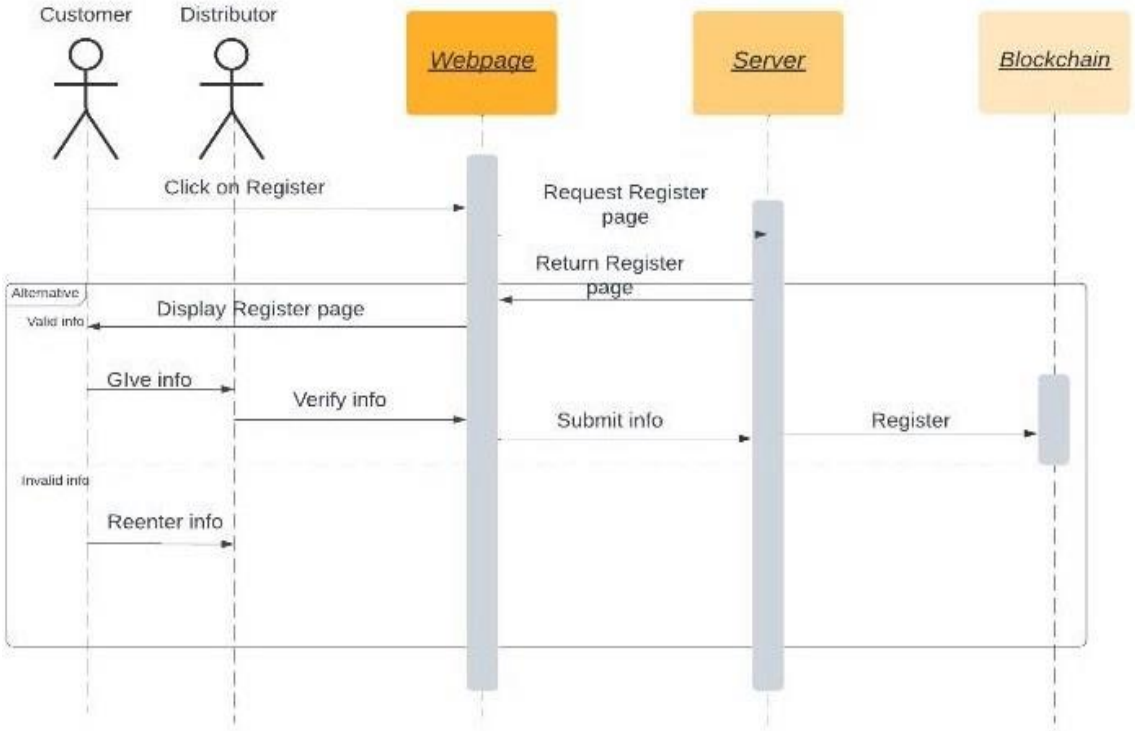

Figure 5. Sequence diagram for registration.

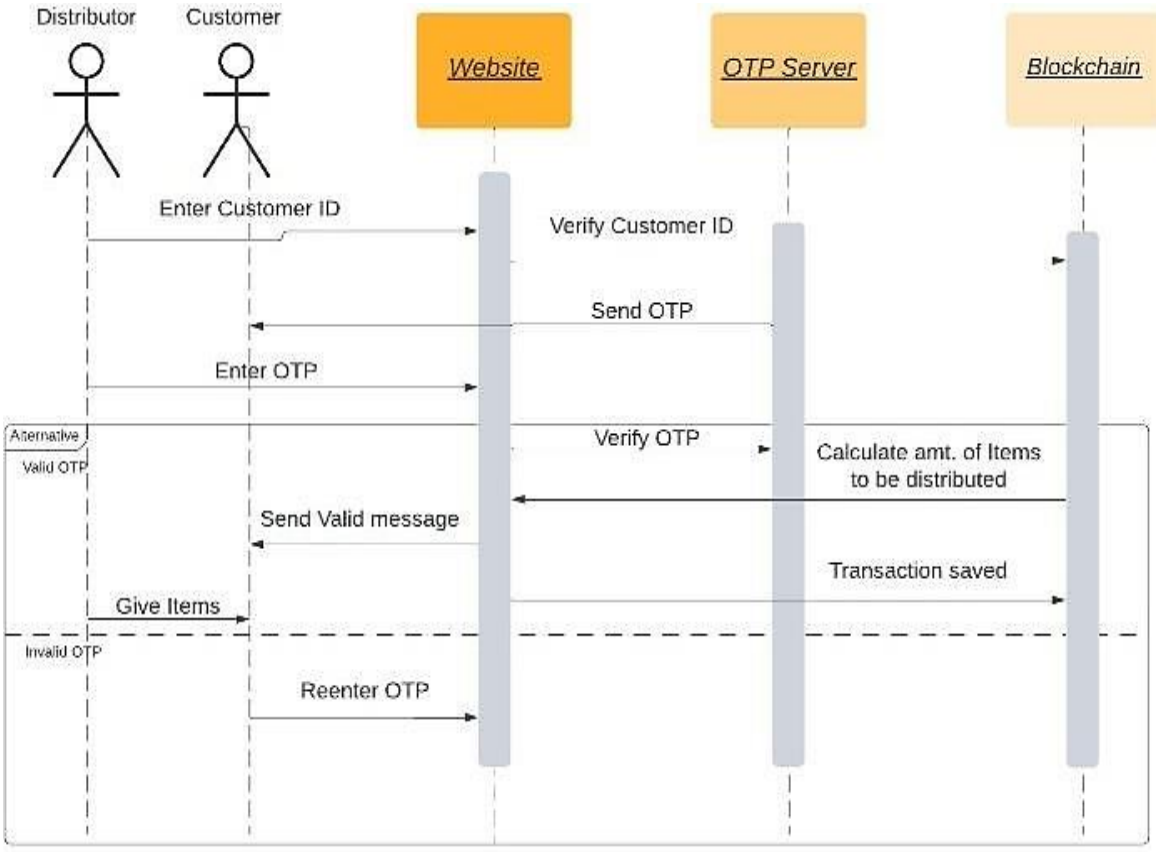

Figure 6. Sequence diagram for distribution.

1. *Home:* Provides information about the project.
2. *Issue goods:* Here, the distributor can issue items tothe customer. The customer has to log in through their ID, the page asks for the OTP that is sent to the customer, and after OTP authentication, the items can be given. Distributors can also verify newly registered customers and delete customers based on the request of the customer.
3. *Register:* This page is for registering new customers. Italso contains options to add new members to an existing Ration card or delete one from the card. Customers can also file a request to delete their card.
4. *Government-related:* This page involves government related work, that is, modifying items and the number of items to be given to a beneficiary, adding and deleting a shop and the employees in it.
5. *Reports:* Contains all prior transactions that have occurred.

Backend

The following are the technologies used in backend development:

1. *Node.js:* Node.js is a popular runtime environment for developing server-side JavaScript applications. Node.js offers a rich library of built-in modules and packages that simplify the development of web servers, APIs (application programming interfaces), and other network applications.
2. *Ether.js:* Ether.js is a JavaScript library that provides that you can use to interact with the Ethereumblockchain. We used it here to interact with our Smart contract.
3. *Remix IDE:* It is a web-based integrated development environment (IDE) for developing smart contracts onthe Ethereum blockchain
4. *Metamask:* Metamask is a wallet with which users can interact with the apps and the Ethereum blockchain.

Metamask is available as a browser extension forChrome, Firefox, Opera, and Brave browsers.

Nodejs and Etherjs are used on the backend. Etherjs is used to communicate with smart contracts that have been put on a specific blockchain. The smart contract is developed in Solidity and deployed on the Goerli test network using Remix IDE. Customers will have to connect their cryptocurrency wallet as every transaction cost a certain amount of cryptocurrency, a phenomenon known as gas. Luckily, customers can make use of Metamask to manage their wallets and every transaction needs confirmation by the wallet owners.

RESULTS

Results for each use case are obtained as follows.

User Registration

As seen in the Figures 7–9, customer details are submitted to the Register page. Once the details are submitted, a transaction is triggered, and the system asks forconfirmation through the Metamask wallet. After approval of the transaction from the user, the customer is registered, and their details and the transaction are stored in the blockchain.

Each transaction costs a certain amount of the crypto currency (known as gas) which will be deducted fromthe wallet holder. Before the transaction takes place, the Metamask wallet asks for confirmation from the user, as shown in Figure 8.

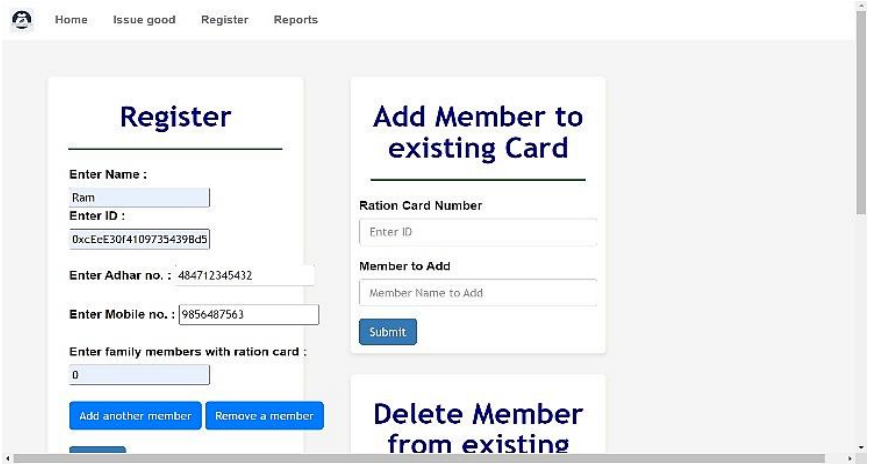

Figure 7. Screenshot showing customer details being entered intothe Register page.

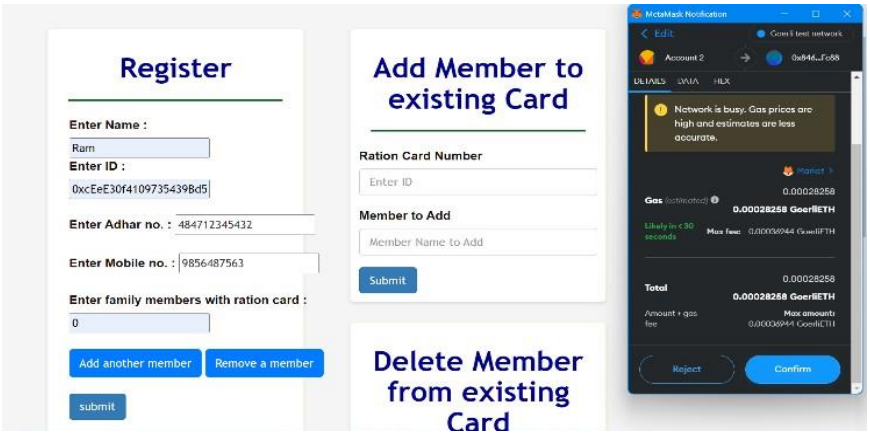

Figure 8. Screenshot of the system asking for confirmation of thetransaction.

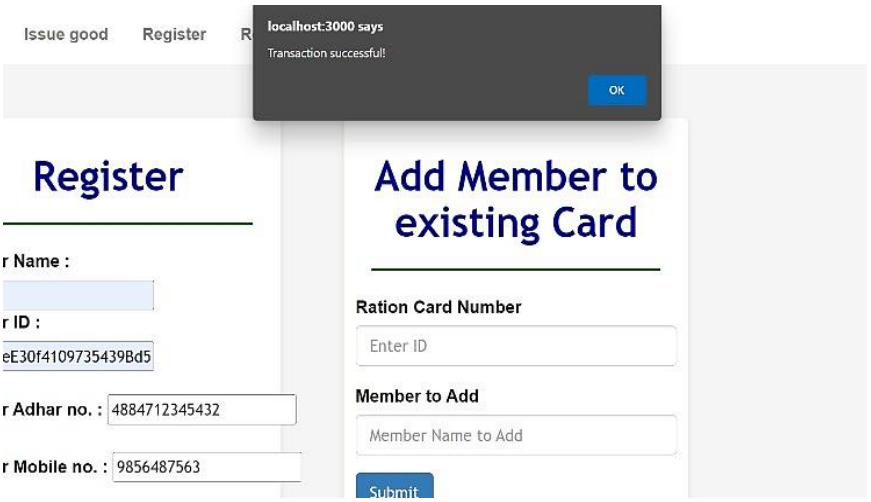

Figure 9. Screenshot of transaction being successful, and thedetails being saved.

Allocating the Number of Items

Government allocates the number of items needed to be givento the customers. Just as before the system asks for transaction confirmation and the details are stored after that (Figures 10–12).

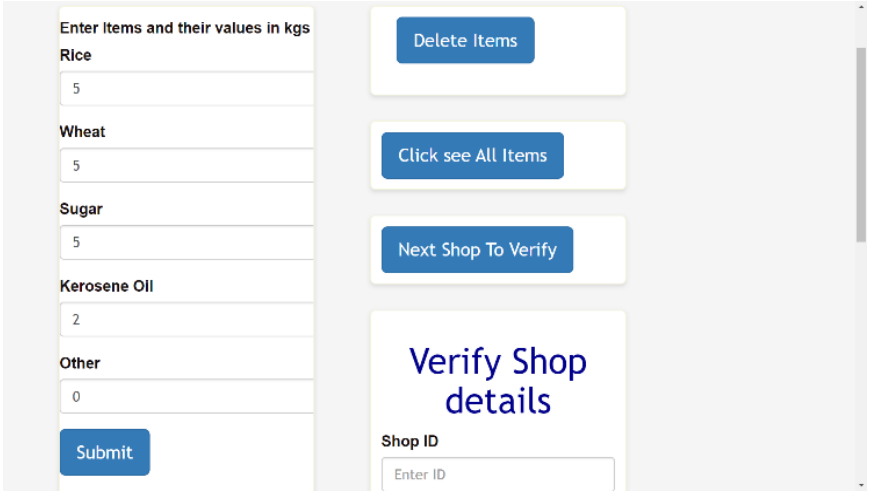

Figure 10. Screenshot of the number of items being modified.

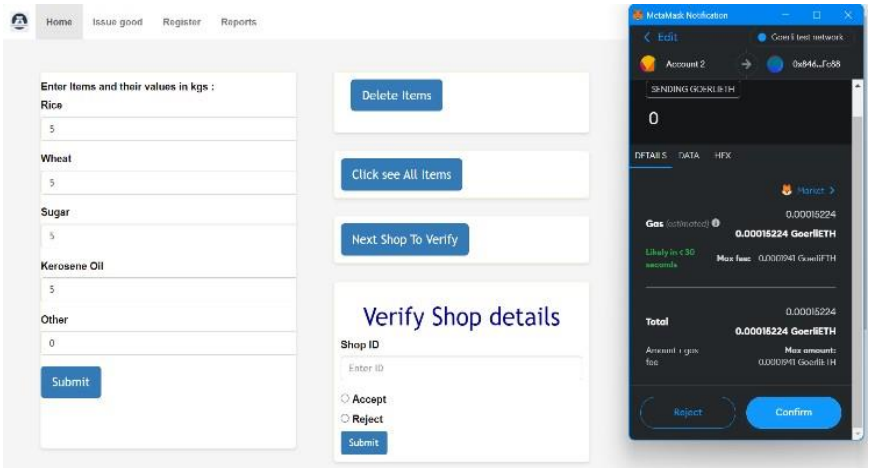

Figure 11. Screenshot of the system asking for confirmation of thetransaction.

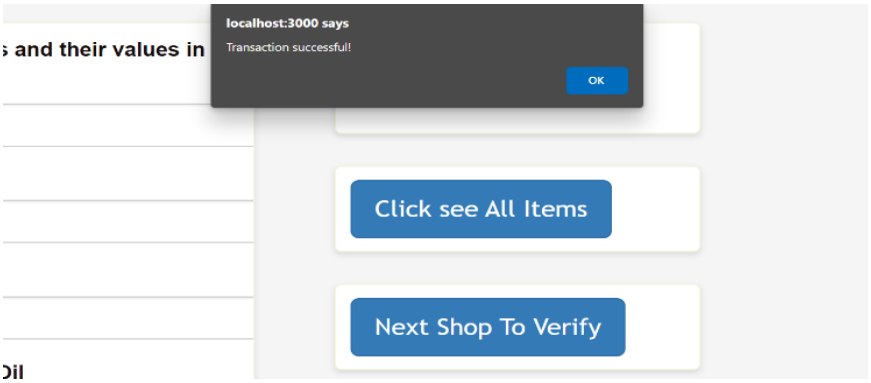

Figure 12. Screenshot of the transaction being successful.

Item Distribution

The distributor enters the customer ID to log in. The system tells the consumer of the quantity of things to be supplied to them. The distributor enters the OTP that is sent to the customer, If OTP is valid, the transaction is successful, and the distributor can hand out the items. This process is shown in Figures 13–16.

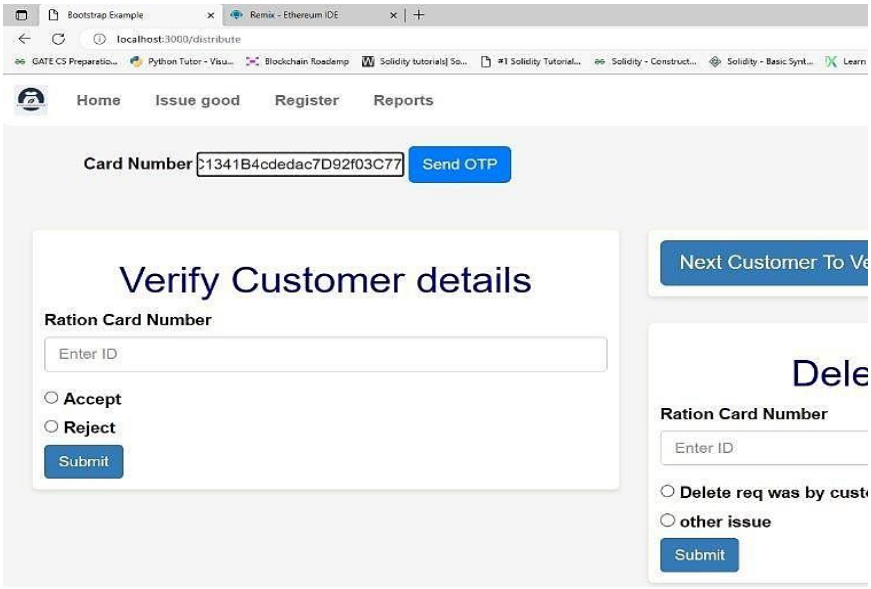

Figure 13. Screenshot of customer logging in.

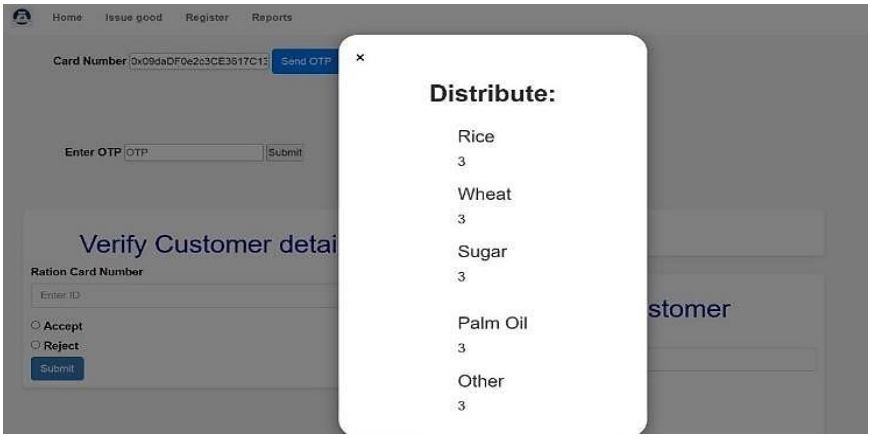

Figure 14. Screenshot of system instructing the distributor todistribute items to the customer.

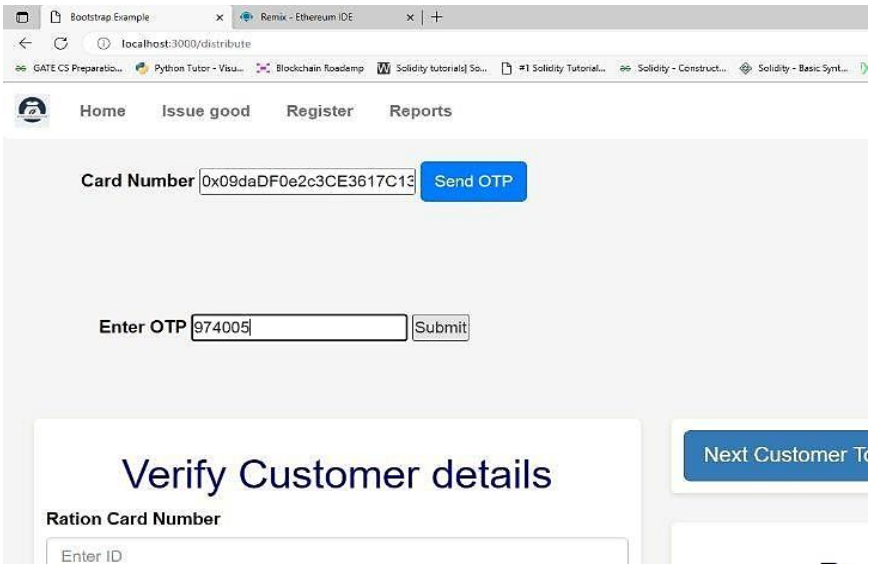

Figure 15. Screenshot of distributor entering the one time password (OTP) sent to thecustomer.

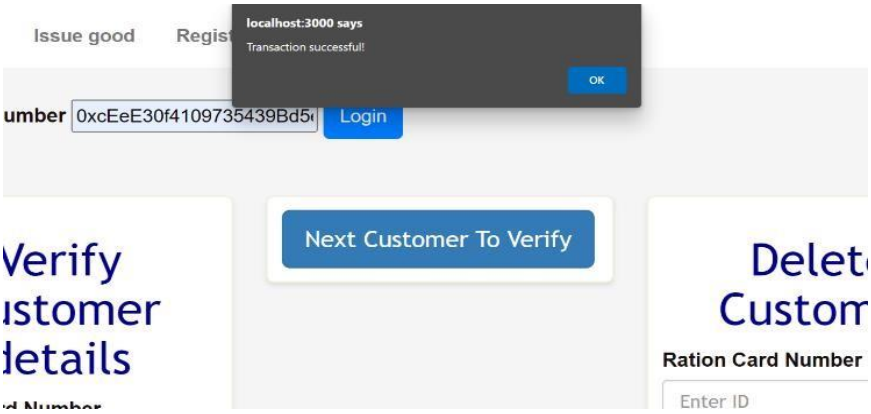

Figure 16. Screenshot of the transaction being successful.

The system instructs the number and amount of items to be distributed to the customer.

Discussion of Results

The results show a fully working system with user-friendly and easily accessible user interface. Storing data in blockchain improves security makes it almost impossible to tamper or manipulate the user data and using account or wallet addresses as ration card number helps reduce fraud using bogus ration cards and issue of forgetting password taken care by wallet that is being used in our case Metamask. Scanning the fingerprints (being used in current implementation of ePOS system) of workers such as laborers and masons can be challenging as their fingerprints may become erased due to the nature of their work and most of the beneficiaries of ePOS are from this class of people.Therefore, using an OTP would be more practical and convenient for delivering goods to beneficiaries compared to a fingerprint-based system.

The proposed system is resistant to attacks that were possible on traditional databases such SQLi attack (a well-known attack on database to gather and manipulate the data stored).

CONCLUSION AND FUTURE WORK

A blockchain-based architecture can significantly improve security and ensure better distribution of food items to ration card holders. The transactions are immutable and hence cannot be modified by

fraudsters. Moreover, they are transparent to everyone. The OTP system also provides further security through two-step authentications. Overall, it proves to be a much better alternative to the existing system.This system can be further improved by bringing the blockchain application directly into EPoS machines instead of being a web application.

REFERENCES

1. Balani S. Functioning of the Public Distribution System. New Delhi, India: PRS Legislative Research; 2013.
2. Overbeck D. Leakage and corruption in India's public distribution system. [Online]. December 2016. Available at https://www.isid.ac.in/~epu/acegd2016/papers/DanielOverbeck.pdf
3. Pradeep A. Impact of e-PoS enabled public distribution system with special reference to Kattapana Municipality. Int J Adv Eng Manage. 2022; 4 (2): 1208–1212.
4. Mishra B. Agriculture, industry and mining in Orissa in the post-liberalisation era: an inter-district and inter-state panel analysis. Econ Polit Wkly. 2010; 46 (20): 49–68.
5. Sebastian T. A 'Chennai' in every city of the world: the lethal mix of the water crisis, climate change, and governance indifference. Law Technol Humans. 2022; 4 (1): 79–101.
6. Mettler M. Blockchain technology in healthcare: The revolution starts here. 2016 IEEE 18th International Conference on e-health Networking, Applications and Services (Healthcom). Munich, Germany. 2016, Sep 14-16. IEEE. (pp. 1-3).
7. Yangchen Lhamu K. State, NGOs and Tribal Development: Study in Doors Region of West Bengal with Special Reference to the Role of the Non-governmental Organisations since 1991. Doctoral dissertation. Siliguri, India: University of North Bengal; 2018.
8. Dhanake S, Desale S, Pawar P, Patil G, Shende S. Blockchain technology in public ration distribution. Int Res J Eng Technol. 2021; 8 (3): 732–736.
9. Nagpure T, Kumbhar A. Android based automatic rationing system. Int J Innov Eng Res Technol. 2021; March: 1-6.
10. Ducrée J. Satoshi Nakamoto and the Origins of Bitcoin--A story in names, data and numbers. arXiv preprint arXiv:2206.10257. Jun 2022
11. Devi Parameswari C, Mandadi V. Public distribution system based on blockchain using Solidity. In: Raj JS, Iliyasu AM, Bestak R, Baig ZA, editors. Innovative Data Communication Technologies and Application. Lecture Notes on Data Engineering and Communications Technologies, vol 59. Singapore: Springer; 2021. Pp. 175–183.
12. Malathi D, Ponnusamy V, Saravanan S, Deepa D, Ahanger TA. A design framework for smart ration shop using blockchain and IoT technologies. Intell Automation Soft Comput. 2022; 32 (1): 605–619.
13. Shahnaz A, Qamar U, Khalid A. Using blockchain for electronic health records. IEEE Access. 2019; 7: 147782–147795.

