iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** IX **Month of publication:** September 2022

DOI: https://doi.org/10.22214/ijraset.2022.46572

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue IX Sep 2022- Available at www.ijraset.com

Blockchain Based Pubic Distribution System

Syeda Amira Hussaini[1], A. Thyagaraja Murthy[2]
[1]*MTech Student,* [2]*Assistant Professor, Department of Electronics and Communication, JSS Science and Technology University, Mysore, India*

Abstract: ***The Public Distribution System (PDS) is a digital scarcity management system that distributes food grains to low-income families at affordable prices. It began in the 1940s as a way to alleviate food scarcity caused by World War II. Illegal usage, overcrowding, inability to obtain materials at any time, processing speed, household selection, targeting of bogus cards, and ration card hijacking are some of the problems of the current PDS. To address this flaw, the suggested solution makes use of blockchain technology, which is a cutting-edge technology. Because the data is sensitive and critical, blockchain improves security, and it can substantially alter how your critical information is seen because it is a distributed ledger.***
Keywords: Blockchain, SHA Algorithms

I. INTRODUCTION

In the chapter, a brief introduction, problem statement, motivation, block diagram is dis- cussed along with the objectives of application and organization of report. In order to overcome the food shortage brought on by World War II, India's Public Distribu- tion System (PDS) was created in the 1940s.Due to its popularity, PDS evolved throughout the 1970s and 1990s into the focal point of the nation's food supply chain. The PDS system has been reintroduced under the Targeted PDS as a welfare programme for low-income families (TPDS).Since then, the Indian government has made various upgrades to PDS. Rice and wheat are essential foods (but states can give additional commodities if they wish).In accordance with ration cards, qualified households will be able to purchase sugar, kerosene, and fortified atta at the issued price, which is undertaken by the government and less cost than the market. The India Planning Commission's assessment of which households are qualified to receive TPDS subsidies depends on their level of poverty. The PDS has been essential in maintaining food price stability and ensuring the country's food and nutritional security. At MSP the Food Commission of India purchases the crops from the farmers. MSP is more costly than the market price. This will sup- port farmers financially and to promote increased agricultural output. This promotes local shopping anlowers the cost of travelling. To reach the necessary minimum . It also meets the immediate requirement for food grains during natural disasters and releases food grains on a weekly basis as part of the TPDS programme. The FCI must also distribute the food grains to the government stock- piles in each state. The state government is in charge of making deliveries to beneficiaries and Fair Price Shops (FPSs).this application uses blockchain technology and log product details. All food grains in each state will be trackable by the federal and state governments' depots, which will only have access to transactions. which happen there .The access of the State Level FPSs is further constrained so that they can only review transactions in their particular region. This will ensure that everything is open and honest To keep track of any irregularities, such as the theft of food grains, etc., the programme will notify the Central Government. In the event of catastrophes and disasters like floods, In the event of a food grain shortage, the State Government Depots and State Level FPSs may contact the Central Government. The amount of food available will be modified by the central government, grains that will be moved to other states in the event of such circumstances. In the follow- ing situations, such as when it purchases food grains from farmers, the Central Government gives food supplies to State Government Depots, which in turn receive food supplies from the Central Government. The State Government Depots then provide food supplies to the State Level FPSs, who in turn supply them to the State Level FPSs. Each transaction will be recorded for the relevant state chain in the blockchain.

II. LITERATURE SURVEY

PoS, PoW, and BFT are often used, either independently or in combination, through- out the organisational layers of the supply chain, according to Jabbar, S., Lloyd, and Ham- moudeh's presentation of blockchain technology.The development ecosystem for building Blockchain-based applications is made up of the type of Digital Ledger Technology (DLT), Integrated Development Environment (IDE), testing tools, libraries, programming language to create smart contracts, accessibility scope option, Blockchain platform, consensus algo- rithm, and related tools including storage applications. Furthermore, it was discovered that MOHBSChain, a cutting-edge framework for supply networks powered by Blockchain had enhanced the application. 2.

According to Ahmad, Mahmood, Habib, Jabbar, S., Faisal, and Sardar, M. B., M., the usage of smart contracts—basically blockchain-based programmes that are activated when specific circumstances are met—is helping to solve the trust problem in supply chains and improve the payment process. 3. Santiago Matalonga, Keshav Dahal, and Ravi Chandra Koirala assert that Ethereum has been the best option for three smart connections for third parties without any inter- mediary's involvement or time loss as evidence of our verification and validation efforts. Etheram simply creates using a peer-to-peer network to check the application code for smart contracts. The transactions on the blockchain are kept secure without the use of any third- party verification. As the demand for supply chains using smart connections grows in the future, Koirala, R. C., Dahal, and Matalonga explain how the same information is being delivered to all of the chains, from farmers to recipients of the crops to the fare pricing mer- chants that are supplied at the end. Three ethereum-powered smart contracts have been deployed as a result of the elements' transparency. 4. Sschain is a comprehensive sharding method for public blockchains without addi- tional data transfer cost proposed by Chen, H., and Wang, Y. They have used the database partitioning technique known as sharding to increase the scalability of blockchains so they can support higher trans- action values. They have proposed SSChain, a non-reshuffling topology for both state and transaction sharding that can accommodate a sizable volume of transactions. 5. The Chicago police's official webpage is where the crime statistics are taken from. It includes details on crimes, such as a description of the crime's scene, Latitude, longitude, date, and time, before the model was trained. After this feature, data preparation are carried out and explained in detail in paper. Scaling and selection will be carried out to ensure correctness. The categorization system K-Nearest Neighbor (KNN) will be evaluated. The data set will be shown using graphical methods. illustration of several instances. 6. A 5G enabled IOT in mobile edge computing is presented by the paper's authors, Jan- girala, S., Das, and A.V. Vasilakos. that can be used for bandwidth, which is a limitation for the supply chain of products. To address this, they used a lightweight RFID authentication protocol based on a blockchain called LBRAPS for the 5g supply chain. The cryptographic hashing procedure known as SHA is believed to be secure against a variety of threats. The only approach that works is encryption; decryption is impossible. 7. Ashraf, S., Zahid, B., Jabbar, S., Mahmood, S., and Shahid, M. R , Due to its incor- poration of several elements, including Peer-to-peer networking and decentralised systems use economic modelling, public key infrastructure, and cryptography. systems, blockchain is garnering interest from both academics and business. consensus to achieve distributed database synchronisation. A secure, decentralised sharing economy technique is one of the most recent applications of the blockchain. In this study, we suggest a share econ- omy paradigm based on blockchain. The concept of communication between the lender and renter is based on the Peer-to-peer networking and decentralised systems use economic modelling, public key infrastructure, and cryptography. The context for communication for the sharing economy leverages SE TP to provide reliable and effective data handling. Everyone has access to the information of every shared item as well. There is also a case study that backs up the suggestion. 8. Anoh, K., Jogunola, O., Adebisi, B., and HammoudehA key technology for preserv- ing international trade and economic rivalry is blockchain (BC).It is seen as a security and trust enabler As the sharing economy grows, In this paper, we show how BC can be used for energy exchange amongst peers (P2P) in smart grids. For a use case in energy P2P trade on the IBM platform, a smart contract for managing trust and transactions is built and implemented using Hyperledger Composer. Investigated and analysed are current problems that can result from using BC to safeguard energy P2P trading. 9. Q.H. Mahmoud and S.S. HazariA distributed ledger known as a blockchain, which establishes a worldwide consensus on a transactional history, is the core technology that the digital currency Bitcoin. Its uses go far beyond the financial industry. Transactions using cryptocurrencies must be verified far more thoroughly than those involving more es- tablished digital payment methods. The capacity to create a solution that offers a quicker Proof of Work is one way to increase scalability, or the rate at which transactions are han- dled. In this research, we propose a technique that parallel mining rather than solo mining to accelerate the Proof of Work procedure. The objective is to prevent more than two min- ers from exerting the equal amount of work to solve a single block. The suggested strategy includes a manager selection process, the task distribution, and a payment schedule. This approach has been evaluated using a range of case situations, changing the difficulty level and number of validators, in a test environment that has all the qualities required to carryout Proof of Work for Bitcoin. Evaluations of experimental results on a local and cloud -based basis were conducted, and the results indicate that the suggested technique is viable. 10. D. W. Kravitz In-depth study of the literature on blockchain- based applications across several industries is provided in this article. Analyzing the state of blockchain tech- nology today and its uses is the goal of this study, which also aims to show how some features of this disruptive technology have the potential to radically transform existing business practises. This overview includes a number of stories from the grey literature, as well as the theoretical foundations of many research papers that have been published in prestigious scientific journals over the last ten years. This helps us with our analysis and accurately captures how the blockchain sector is growing and evolving.

We propose a detailed classification of blockchain-enabled applications across several industries based on a thorough, organised assessment of the available literature and a thematic content analysis that takes into account data privacy, business, healthcare, IoT, and supply chain. We identify important subjects, recurring themes, and novel study directions. We also draw attention to the flaws that have been noted in the pertinent specifically the drawbacks of blockchain technology and how they affect various industries. Based on these findings, we suggest a number of gaps in knowledge and prospective directions for future exploration, which are anticipated to be very beneficial to both academics and practitioners.

III. PROPOSED SYSTEM

The application proposed will support a blockchain network to record transfers and control the conditions for transfers of food grains. The Central Government, State Government Depots and State Level FPSs are provided with logins so as to be able to view transactions that occur at different stages of food grain transfer. The Central Government officials will have complete access to view all transactions that take place in the blockchain network across all states.The State Government Depots will only have access to all transactions that take place in their respective state and will be able to track all food grains in that state. The access is further restricted for the State Level FPSs to view transactions only in their particular region.This will ensure transparency of the entire system. In case of any inconsistencies like the loss of food grains, etc., the application will issue an alert to the Central Government to track this inconsistency. In case of emergencies and calamities like floods where there may be a shortage of food grains, the State Government Depots and State Level FPSs can alert the Central Government about a shortage of food grains. The Central Government will have access to modify the amount of food grains that will be
distributed to different states in case of such emergencies. A transaction will be recorded in the following cases:

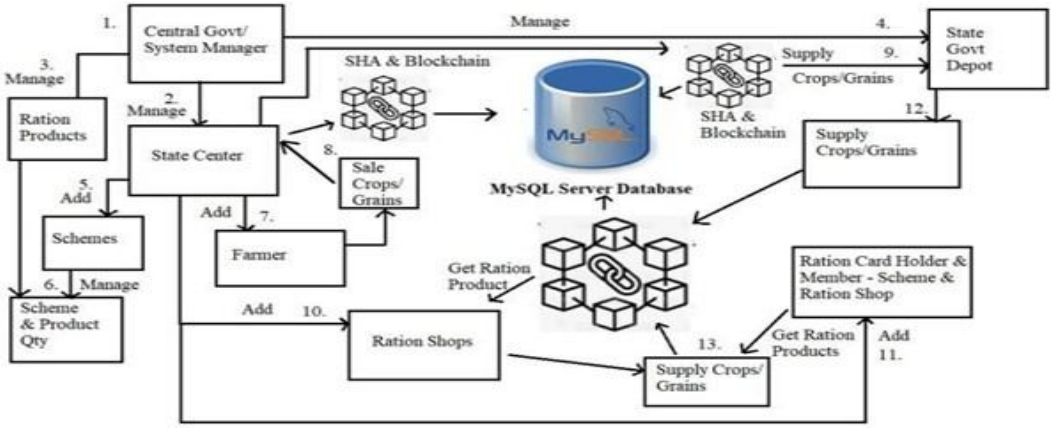


Fig 1: Proposed block diagram

1) The Central Government receives food grains from farmers
2) The Central Government sends food grains to State Government Depots
3) State Government Depots receive food grains from the Central Government State Government Depots sends food grains to the State Level FPSs
4) State Level FPSs receive food grains from the State Government Depots
5) State Level FPSs sell food grains to beneficiaries.

Each transaction will be recorded in the blockchain for the corresponding state chain.

A. Module Description

1) System Manager: Default Login Id and Password for Logging In Add state, add state name, add State wise Centers Staff's- Should add state centre name, state name, mobile number, email address, and address after which a special ID and password are produced based on this information. State-specific state government depots should be added. Passwords are then generated based on the state name, mobile number, email address, and address of each state government depot. Product addition: Must include ration products and price/kg View Transaction: Viewing the transaction and altering the product quantity are both possible.

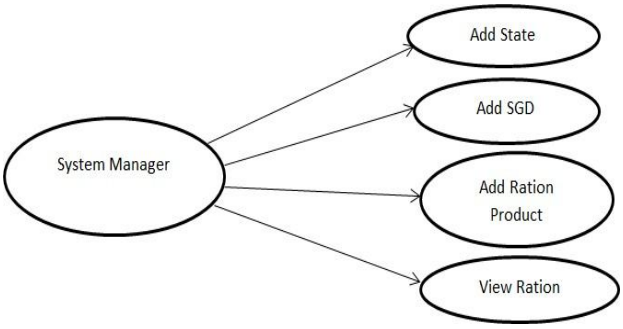


Fig 1.1: state manager flow diagram

2) *State Center:* Login: Create a code using a special ID and password. Insert Scheme: Ratio schemes are being added, including state names, scheme names, ranges, and descriptions. then, based on the schemes, we can add products and quantities while also viewing the schemes and products that allow us to change the quantities (2 members) Farmers should be included; details such name, state, phone number, and address should be added. Then, using the blockchain's established SHA algorithm, we will purchase crops from farmers by providing product specifications, farmer identification numbers, and quantity. Based on this, we can determine whether any tampering occurred with the crop transaction. additionally uses a tampering programme that allows us to alter transactions by inserting state and product information. comes with an option to edit; if chosen, the programme is altered. the crop transaction can then be retrieved from database 1 to database 2 FPS (RationShop) Staff should add the name of the city and any area names, such as the city and area names. We must add the city, area, name of the ration shop, mobile number, email address, and address based on the area. Adding a ration card holder by entering their address, phone number, city, state, neighbourhood, ration shop, and name of the family head. adding information on ration card holders, including their name, date of birth, gender, photograph, occupation, Aadhar card number, and mobile number (2 members) blockchain-based goods distribution to state government depots. therefore, product supply should be made. Add information such as the product (when we add the product, the available amount is displayed automatically), as well as the state government depots id. The state centre keeps track of these depot numbers; the information is gathered and a table is made in a SQL database. We can view transactions in sgd. By inputting information like the state and sgd ID and clicking on edit, it can also be altered here. However, it can be corrected by checking in view sgd and recovering it. viewing the transaction, or viewing it.

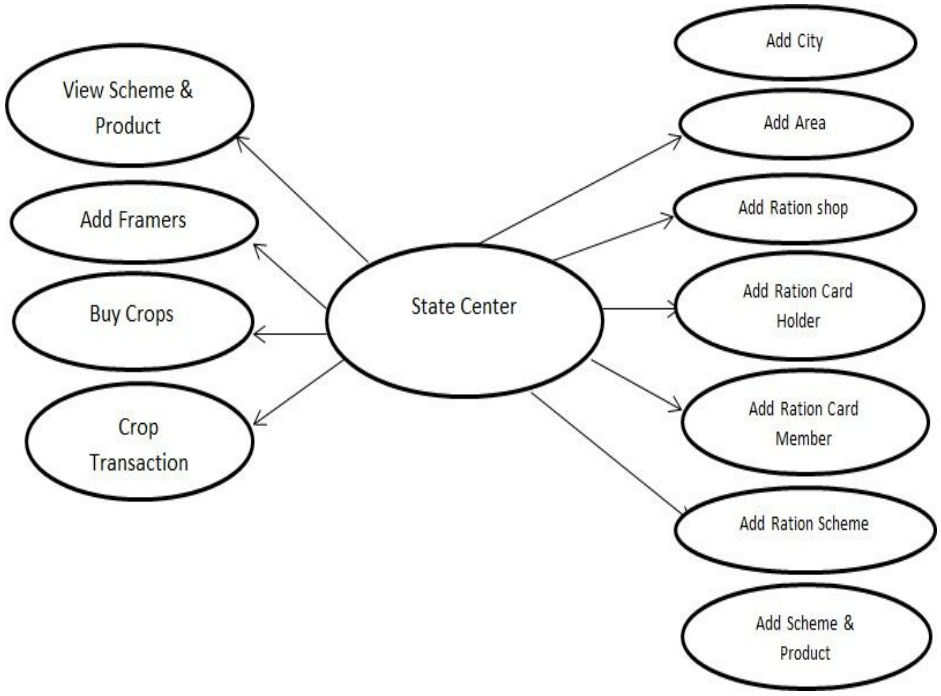


Fig 1.2: State center flow diagram

3) *State Government Depots:* Login: Enter your username and password to access the state government depots' main page after your credentials have been validated by the database. Product supply to FPSs: successful addition of the product, the product's quantity, the state, the city, the area, the ration store, and the supply's quantity in the database. In this instance, tampering is also possible by adding information like the state, city, area, or ration shop, then editing the quantity. To access the tampering part recovery option, log into FPS using your username and password and go to the product transaction page, where it will be clear that the item has been tampered with and may be fixed.

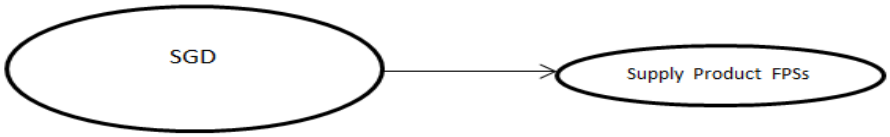


Fig 1.3: State government depots flow diagram

4) *Fair Price Shops:* Login with your master password and ration shop ID. Giving recipients items based on the APL/BPL scheme and SHA algorithm Ration card purchases, Ration card transactions, and FPS goods stocks all use blockchain technology. transaction involving products earlier Ration card id, scheme, product, amount, and price are the additional details for ration card product purchases. To successfully check the database, click Add Product, Verify Product and Quantity, Clear Purchase, and Generate Receipt. Even this can be changed by clicking the edit button and adding information like the state, city, area, or ration shop. A tampered with ration card product transaction can be recovered. FPS is another idea that exists. Product stock indicates how much of a given item is on hand both before and after transactions.

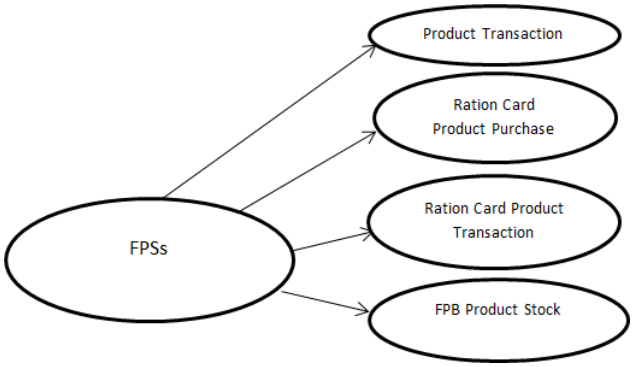


Fig 1.4: fair price shop flow diagram

B. Algorithms Used

1) *Blockchain Technology:* In essence, blockchain is a network of computer systems that repeats and disseminates a digital log of transactions. Each participant's ledger receives a copy of every new transaction that occurs on the blockchain, and each block in the chain consists of several transactions. Each ledger will contain data, a hash value, and a related hash of the preceding ledger.
2) SHA Algorithm:: Data security is a goal of the Secure Hash Algorithms (or SHA) family of cryptographic procedures.It works by modifying the data by using a hash function, an algorithm composed of bitwise operations, modular additions, and compression functions.

C. Cryptography Hash Function

A cryptographic hash function can be used to transform an information string into a fixed-length numeric string.The output of the hash function is the hash value. During our analysis, we employ a range of hashing techniques, including SHA1, SHA2, and SHA3. The most popular algorithm right now for routine tasks is SHA-256, which produces hashes with 256 cycles.

The SHA-2 cryptologic hash works include the SHA-256 cryptologic hash algorithm that is employed by the National Security Agency, and figure 3 depicts how it operates. 2. The hashing algorithm includes the following steps:

1) Text will be inputted and broken up into an assortment of ASCII character codes.
2) ASCII codes will be converted into binary codes.
3) Zero will be placed as padding in front of each code until it is 8 bits long.
4) The processed code will eventually be joined and will be associated with the number 1.
5) The binary message will continue to be extended with zeroes until it exceeds 512 mod 448.
6) The code in array format will be six characters long.
7) We must pad the message till the binary message is 64 characters long with 0's.
8) The previous binary message that was previously prepared will be appended with this message.
9) The aforementioned message will be divided into chunks of 512 characters.
10) These 512 character chunks will then be divided into sixteen 32 bit array "words."
11) An array of 16 32-bit 'words' will be looped over for each chunk, and this array will be expandedto an 80-word array.
12) After that, it needs to be initialised with a variable.
13) Bit-wise operations for variable reassignment will be performed for each chunk through looping.
14) The five resulting variables will now each be given a hexadecimal value.
15) Ultimately, the value will be returned after joining the two of them.

IV. RESULTS AND DISCUSSION

1) Home Page

When the application is opened first, it directs to start page also known as the Home page. It also acts as the content of the application. The Homepage is shown in figure 2

Fig 2.1 : Home page

2) Login Page

Login page: login details such as User id and Password

Fig 2.2:login page

3) Adding System Manager Details

System manager: Need to login for system manager to add details of the products

Fig 2.3: System manager details

4) Adding state Center Details

State center: After adding details to system manager, next comes the state center bylogging in by its login id and password.

Fig 2.4: Adding state center details

A. Adding Farmer Details

Adding details of the farmer: Adding farmer details such as farmers name, state name,mobile number and address.Here comes the blockchain concept into picture when buying crops from the farmer, where the third party can tamper the products which can be recovered is blockchain technology using SHA algorithm.

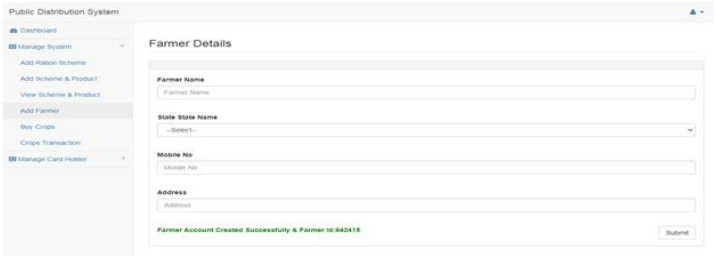


Fig 2.5: farmer details

Here comes the blockchain concept into picture when buying crops from the farmer, where the third party can tamper the products which can be recovered is blockchain tech- nology using SHA algorithm .

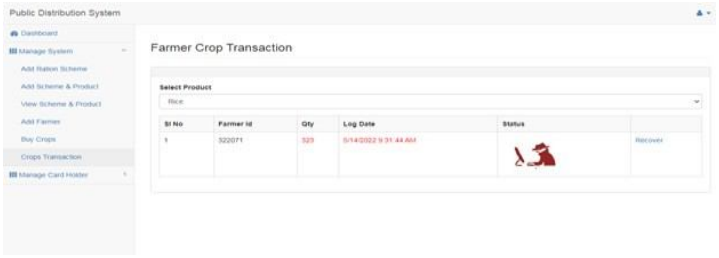


Fig 2.6: Tampered farmer

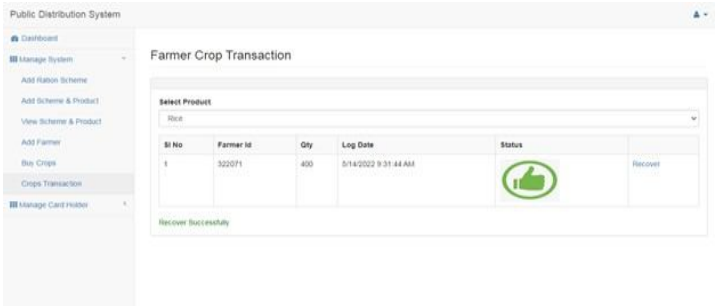


Fig 2.7: Recovered farmer

B. SQL Database

MySQLyog is used as a Database to store the data in this Project.

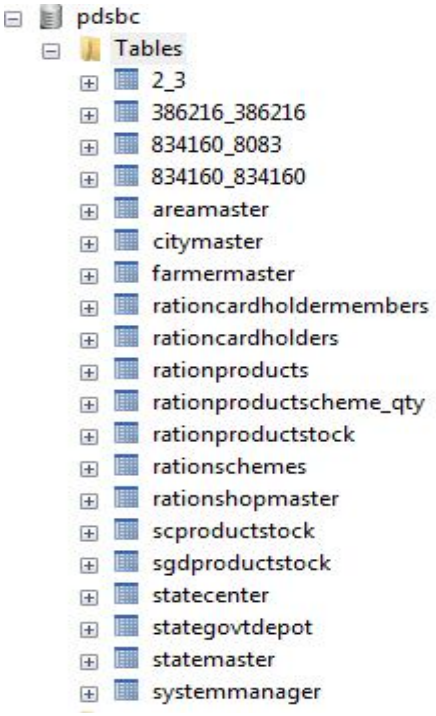


Fig 2.8: SQL database

C. Hash Value

Hash is used to authenticate messages transferred between the client and server.

PHV	CHV
000	7b42df23c024d6dd323dd4e2e4c6fc14b77a3960bbb981aef5f89b342fa3
(NULL)	(NULL)

Fig 3: Hash values

V. CONCLUSION AND FUTURE WORK

In conclusion, The authors of this system proposal have offered a sharded, scalable blockchain architecture for the TPDS. The adoption of the proposed system demonstrates the viability of a blockchain solution. Sensible strategy for enhancing the transparency of the TPDS in India. It explains food grain leakage, which is now the main problem with TPDS. Main- tainability, scalability, and reliability are ensured by utilising a single platform across all states. Beneficiaries can use it to assist them decide when to pick up their meals from their local FPSs. With little to no human intervention, the suggested A system that is scalable, transparent, and safe is provided by blockchain.

REFERENCES

[1] Jabbar, S., Lloyd, H., Hammoudeh, M. et al. Blockchain-enabled supply chain: analysis, challenges, and future directions. Multimedia Systems (2020).
[2] Habib, M. A., Sardar, M. B., Jabbar, S., Faisal, C. N., Mahmood, N., Ahmad, M.: Blockchain-based supply chain for the automation of transaction process: Case studybased validation, in: 2020 International Conference on Engineering and Emerging T echnologies (ICEET), IEEE, pp. 1–7 (2020).
[3] Koirala, R. C., Dahal, K., Matalonga, S.: Supply chain using smart contract: a blockchain enabled model with traceability and ownership management, in: 2019 9thInternational Conference on Cloud Computing, Data Science Engineering (Conflu- ence), IEEE, pp. 538–544 (2019).
[4] Chen, H., Wang, Y.: Sschain: A full sharding protocol for public blockchain with-out data migration overhead. Pervasive Mobile Comput. 59, 101055 (2019
[5] N. Hitwasi and K.Chandrasekaran. Agent Based Social Simulation Model and Unique Identification Based Empirical Model for Public Distribution System. In 2017International Conference on Recent Advances in Electronics and Communication Technology (ICRAECT), pages 324-328, 2017

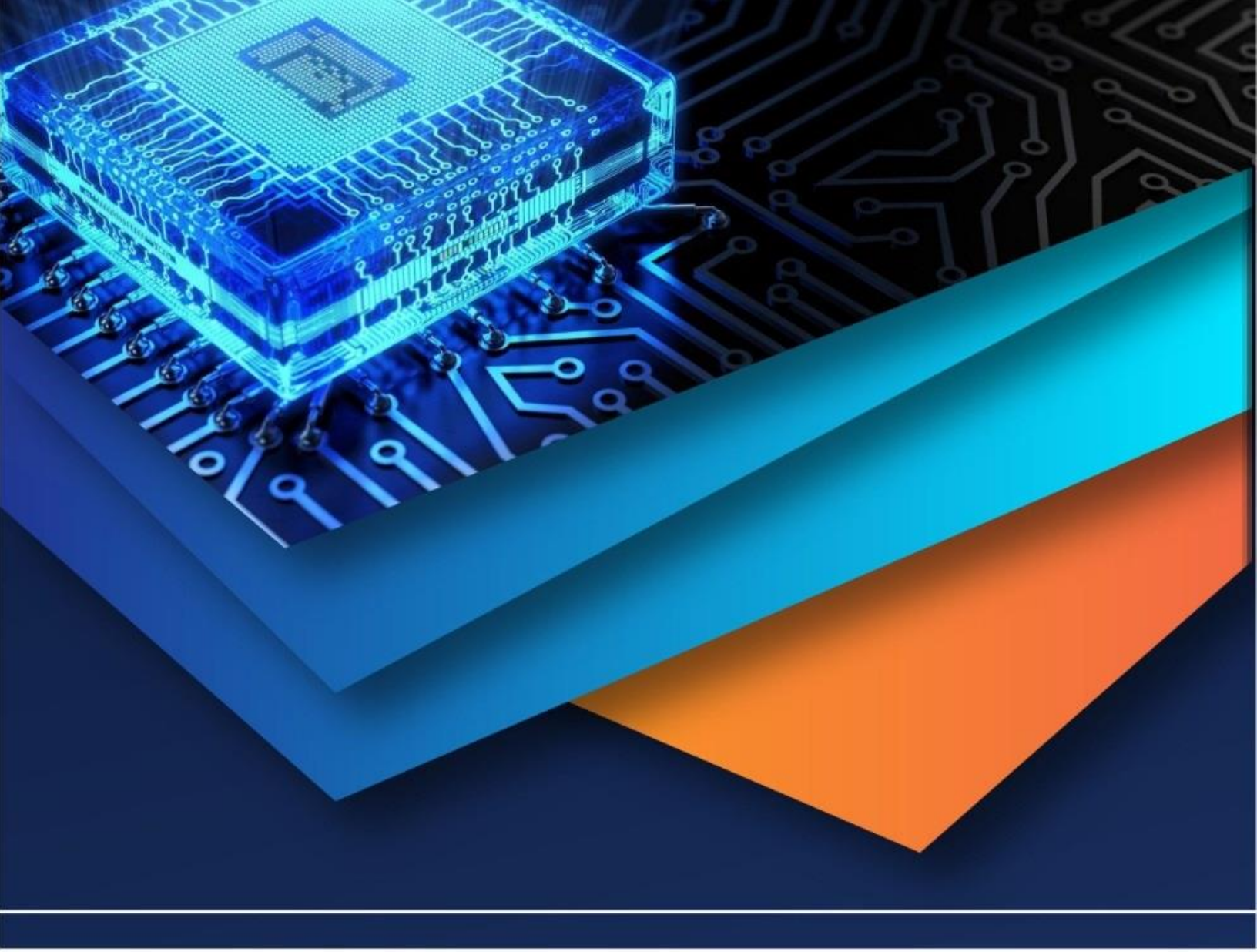
[6] Jangirala, S., Das, A.K., Vasilakos, A.V.:Designing secure lightweight blockchain-enabled rfd-based authentication protocol for supply chains in 5g mobileedge computing environment. IEEE T ransactions on Industrial Informatics (2019)

[7] Shahid, M. R., Mahmood, S., Hafeez, S., Zahid, B., Jabbar, S.,Ashraf, R.: Blockchain based share economy trust point: Case study basedvalidation, in: Pro-ceedings of t he 3rd International Conference on Future Networks and DistributedSystems, ACM , p. 41 , (2019).

[8] Jogunola, O., Hammoudeh, M., Adebisi, B., Anoh, K., Demonstrating blockchain-enabled peer-to-peer energy trading and sharing, in, : IEEE Canadian con-ference of electrical and computer engineering (CCECE). IEEE 2019, 1–4 (2019).

[9] Hazari, S.S., Mahmoud, Q.H., A parallel proof of work to improve transaction speed and scalability in blockchain systems, in, : IEEE 9th annual computing andcommunication workshop and conference (CCWC). IEEE2019, 0916–0921 (2019).

[10] Kravitz, D. W.: Transaction immutability and reputation traceability: Blockchain as a platform for access controlled iot and human interactivity, in: 2017 15th AnnualConference on Privacy, Security and T rust (PST), IEEE,pp.3–309(2017)



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY