**Ration Distribution Management Using Blockchain Technology: An Overview**

**Abstract:** Recently, the Public Ration Distribution System structure is one of the prime government commercial schemes. Low economical group and people below scarcity line use these amenities provided by the government. Due to deception appear in a chain; such amenities do not reach to the needy people. This happens because in the existing system all the work is done physically. To computerize or automate this physical job there is not any specific unreasonable technology or tools involved. Due to this, the system facing two problems firstly weight of the material that is given to the people may be inaccurate or imprecise, and secondly, at the end of the illegal wrong entries in the inventory of the shop about the amount of the material given to the consumers. In this work, we will describe a blockchain technology-based prototype that can be used on a small website. There are presently many fraud activities and corruption 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 a blockchain prototype that is used to record all the transactions 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 transactions between the central government, state government, the district office, ration shop 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 has some features that are guaranteed to provide the most important aspect that is, security using the concept of blockchain.

**Keywords:** blockchain technology. E-ration distribution, P2P, consensus algorithm, smart contract, mining, hash generation

**Introduction**

In existing systems, there is security available in public distribution system websites yet there are several nodes that 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 as a chance for the frauds to manipulate the public distribution system. In the Blockchain prototype for E-governance", the blockchain prototype built is currently deployed on the local test 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 are used to mine all the transactions is not used in their system. The central government has developed a website for the public distribution system .However this system is not free from its limitations. A large number of bogus cards are issues using which the middlemen and the fps owner sell the grains to the open market. These transactions are not recorded, and these 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.

The definition of the block header is given in the above figure 1.1. the block header and the frame are the contents of the block

1. version: indicates which set of rules to follow for block validation

2. root hash: All blocks hash value

3. nBits: goal block hash threshold.

4. Nonce:: a 4-byte field that usually starts at 0 and increases the calculation for each hash

5. Parent hash key: a hash value of 256-bit pointing to the previous block.

6. Timestamp: present standard time as seconds

Key Characteristics of Blockchain

**Decentralization** Payment must be checked through the central trusted entity (e.g. the central bank) in traditional hierarchical transaction structures, ultimately resulting in the cost and performance bottlenecks on the central servers. In comparison to the hierarchical model, blockchain no longer requires third parties. Consensus algorithms in blockchain are used in the distributed network to preserve data integrity.

**Persistency** Transactions can be easily checked and honest miners would not accept fraudulent transactions. Once they are included in the blockchain, it is almost impossible to delete or rollback transactions. Blocks containing invalid transactions could be automatically discovered

**Anonymity** Each user must communicate with a created address with the blockchain, which does not disclose the user’s real identity. Because of the inherent constraint, blockchain can not guarantee total security.

**Literature Survey**

Smart Contracts [1] also called crypto-contract, is a computer program used for transferring the property or digital currents in specific parties. It does not only determine the terms and conditions but may also implement that policy. These smart contracts are stored on block-chain and BC is an ideal technology to store these contracts due to ambiguity and security. Whenever a transaction is considered, the smart-contract determines where the transaction should be transferred/returned or since the transaction actually happened.

Currently, the CSIRRO team has proposed a new approach to integrating Block On IOT with [2]. In its initial endeavor, he uses smart-home technology to understand how IOT can be blocked. Block-wheels are especially used to provide access control systems for Smart-Devices Transactions located on Smart-Home. Introducing BC technology in IoT, this search again provides some additional security features; however, every mainstream BC technology must have a concept that does not include the concept of comprehensive algorithms. Moreover, this technology can not provide a general form of a block-chain solution in case of IoT usage.

According to Ilya Sukhodolski. Et. Al [3] system presents a prototype of a multi-user system for access control over datasets stored in incredible cloud environments. Like other unreliable environments, cloud storage requires the ability to share information securely. Our approach provides access control over data stored in the cloud without the provider's investment. Access Control Mechanism The main tool is the dynamic feature-based encryption scheme, which has dynamic features. Using BlockChain based decentralized badgers; Our systems provide an irrevocable log for accessibility requests for all meaningful security incidents like large financing, access policy assignment, alteration, or cancellation.

According to Huehuangenet. Al [4] offers a blockchain and a MedRec-based approach by enabling encryption and attribute-based authentication to enable secure sharing of healthcare data. By applying this approach: 1) The fragmented EHR fragment of all patients can be seen as a complete record and can be safely stored against tampering; 2) The authenticity of patients EHR can be verified; 3) Flexible and finer access control can be provided and 4) it is possible to maintain a cleared audit trail.

According to Vipul Goyal et. Al [5] develops new cryptosystems to share encrypted data properly, which we call key-policy attribute-based encryption (KPABE).In our cryptosystem, exits labeled with a set of properties and controls that it connects to private key access configurations that a user can decrypt the encryption. We display the utility of our product to share audit log information and broadcast encryption.

Hao Wang et Mate Al [6] offers a secure electronic health record (EHR) system based on special-based Cryptococcus and blockchain technology. In our system, we use attribute-based encryption (ABE) and identity-based encryption (IBE) to encrypt medical data and to use identity- based signature (IBS) to apply digital signatures.

According to Yan Michalevsky et. Al [7] system introduces the first practical decentralized ABE scheme with proof of policy-hiding. Our creation is based on the basic encryption of decentralized internal product, which is an encryption strategy launched in this paper. This ABB scheme supports results, disputes, and threshold policies, which protect the access policies of those parties that are not authorized to decrypt the content. In addition, we handle the receiver's privacy issue.

System [8] they successfully address these issues by offering a cleared policy feature-based data sharing

plan with direct cancellation and keyword searches. In the proposed scheme, the non-terminated users' private key is not required to be updated during the cancellation of the direct revocation of features. In addition, a keyword search has been realized in our plan, and the search is stable with the increase in time features. Specifically, the policy is hidden in our plan, and therefore, the privacy of users is preserved. Our security and performance analysis shows that the proposed plan can deal with security and efficiency concerns in cloud computing.

According to Sarmadullah Khan et. Al [9] embedded power transactions in blockchain are based on their defined characteristics through the signature of many manufacturers. These signatures have been verified and customers are satisfied with the features that do not open any information that meets those features. The public and private key manufacturers have been created for these customers and using this key ensures that the support process is authorized by customers. There is no central authority required in this perspective.

According to Ruuguet. Al [10] To guarantee the validity of the EHR surrounding the block channel, he has submitted a special-based signature scheme with multiple officials, in which the patient supports the message according to the specifications, but there is no evidence that he does not have any other information. In addition, there are many officers without generating a reliable individual or a central person in order to generate and deliver a public key, which avoids the escrow problem and adapt to the mode of data storage distributed in the Block.

**Research Methodology**

System execution which carried out custom blockchain implementation. This research basically describes the data security approach in the blockchain environment with various consensus algorithms. The first phase system deals with a graphical user interface (GUI) where end-user uploads some data or information. Each uploading event considered as a transaction for each block, we carried open Smart contract for custom blockchain. SHA-256 hash generation algorithm and use to generate a hash of transactional data. Mining policy validates the transaction with the combination of current has as well as previous hash. For the first transaction system considered this block as a Genesis block and defined threshold value considered as the previous hash. ones the mining policy has to fulfill the system commit the transaction with an entire number of data nodes. P2P network executive various consensus algorithms to validate respect to the transaction in entire data nodes. we propose PoS, PoS, LPoS, and PoET consensus algorithm during the execution.

**Outcomes**

* Transactional clarity to end-user.
* Provide data security as well as automated data recovery without any third-party resource.
* Entire transactional process in the blockchain.

**Advantages**

* The single authority can’t change once any transaction has done.
* End-user can view all supply and well as distribution on a single click where the system generates the transactional clarity.
* It can easily eliminate different network attacks.

**Disadvantages**

* Required multiple database resources to create a large peer to peer network
* Much expensive

**Conclusion**

The proposed survey investigates blockchain usage in cloud computing and its effectiveness for secure data storage. A good consensus algorithm means efficiency, safety, and convenience, recently a number of endeavors had been made to improve consensus algorithms in the blockchain. Despite the great potential of blockchain, it faces numerous challenges that limit the performance and usage of blockchain. Blockchain cannot guarantee transactional privacy since the values of all transactions publicly visible.

**References**

[1] Smart Contracts," http://searchcompliance.techtarget.com definition smart-contract, 2017, [Online; accessed 4-Dec- 2017]

[2] A. Dorri, S. S. Kanhere, and R. Jurdak, Blockchain in the internet of things: Challenges and Solutions, "arXiv:1608.05187 [cs], 2016. [Online]. Available:http://arxiv.org/abs/1608.05187

[3] Sukhodolskiy, Ilya, and Sergey Zapechnikov. "A blockchain-based access control system for cloud storage." Young Researchers in Electrical and Electronic Engineering (EIConRus), 2018 IEEE Conference of Russian. IEEE, 2018.

[4] Yang, Huihui, and Bian Yang. "A Blockchain-based Approach to the Secure Sharing of Health-care Data." Proceedings of the Norwegian Information Security Conference. 2017.

[5] Goyal, Vipul, et al. "Attribute-based encryption for fine-grained access control of encrypted data." Proceedings of the 13th ACM conference on Computer and communications security. Acm, 2006.

[6] Wang, Hao, and Yujiao Song. "Secure cloud-based EHR system using attribute-based cryptosystem and blockchain." Journal of medical systems 42.8 (2018): 152.

[7] Michalevsky Y, Joye M. Decentralized Policy-Hiding Attribute-Based Encryption with Receiver Privacy.

[8] Wu, Axin, et al. "Hidden policy attribute-based data sharing with direct revocation and keyword search in cloud computing." Sensors 18.7 (2018): 2158.

[9] Khan S, Khan R. Multiple authorities attribute-based verification mechanism for Blockchain microgrid transactions. Energies. 2018 May;11(5):1154.

[10] Guo, Rui, et al. "Secure attribute-based signature scheme with multiple authorities for Blockchain in electronic health records systems." IEEE Access 776.99 (2018): 1-12.