Smart Contract: Data Provenance In Rice Supply Chain

Amrita Jyoti, R. K. Chauhan

Abstract: ***Before the invention of the various technologies, managing various activities and actions over the internet was achieved through a centralized server to guarantee valid data. With the expanding measure of accessible storage space and the quickening of data stream incited by the internet, a developing enthusiasm for data about the creation procedure and sources of information has developed. While this wide scope of use territories would profit by provenance data, the kind of provenance information, manipulation and querying facilities required vary from application to application. In this way, to discover the distinctions and similitudes between the different application and information model provenance needs and present a general plan for the arrangement of provenance. By characterizing this plan and applying it to existing work we plan to uncover open inquiries in the region of information provenance In this paper we survey the blockchain and provenance of the data in rice supplychain. We implement our proposed approach using smart contract which is to be deploy on ethereum blockchain network in rice supplychain to show the security and provenance of the data . We can track the progress of rice batch after each stage in blockchain and also discussed the need of provenance of assets in supplychain as it increase the trust of the customer***

Keywords: data provenance; blockchain technology; supply chain; smart contract, ethereum

I. INTRODUCTION

Data provenance is a historical record for any bit of information. Data provenance frameworks track changes that are made to information, where information starts and moves to, and who makes changes to it after some time. In other words, data provenance is "indicating work" in a database. This verifiable record of data would then be able to be trusted for information approval and review purposes. In this paper we are concern about the data provenance in supply chain. The automated tracking and storage of provenance data promises to be a significant preferred position of logical work process frameworks [1]. Data provenance can be thought of as metadata that monitors the beginning of an information object, who is the proprietor of the record and what tasks performed on that information object. Lately, as the measure of information that is created has developed exponentially - the need for tracking and storing provenance information to distinguish blunders, fraud and malicious attacks.

Revised Manuscript Received on January 15, 2020

Amrita Jyoti (Phd scholar, Kurukshetra University), Computer Science & Engineering, ABES Engineering College, Ghaziabad, India

Dr. R. K Chauhan , Professor, Department of Computer Science and Appliaction , Kurukshetra University, Kurukshetra, India

II. PROBLEM STATEMENT

To create a sustainable sourcing, the data provenance need traceability, transparency and tamper-proof data. If each connection in the supply chain network can believe the individuals who went before it and conveys what can be trusted by those to who come after it can the entire chain be trusted. This requires coordination of information from every one of the phases in the profitable procedure: extraction, handling, transport, storage, creation, and utilization. Distributed records (blockchains) are the ideal instrument for accomplishing these results. Blockchain innovation is intended to be secure. The information it conveys is adequately changeless yet can be made open to all. It is equipped for making a chain of provenance that is completely reliable. The extension that will be actualized in this project will use the blockchain innovation to store the provenance data in supply chain using smart contract and synchronize it with the work process definition and the outcomes from the executed work process.

-To conceive an effective method to transfer data provenance from the framework into blockchain.

-To devise an efficient system to store the information on the blockchain, so it will be easy to check for indications of tampering.

III. BLOCKCHAIN

A blockchain can be seen as a distributed ledger: a chronological chain of ‘blocks’ where every block contains a record of the valid network activity since the last block was added to the chain. For developing a secure block chain based data provenance in supply chain using smart contract the following papers are surveyed. Several existing methods are prone to attacks from malicious sources questioning the security of data on the blockchain. Also traditional methods are less efficient in handling resources and consumes more energy and cost. The data traceability is a major issue in the blockchain networks. Hence periodical updates regarding the status of the material should be stored in the blockchain. This section presents a review of several papers in which blockchain based transactions are done in various fields such as agriculture, IoT, marketing etc. From the problems discussed in the existing methods, a solution must be formulated for providing secure data provenance in the near future. Formulation of codes for processing in smart contract is vital since the code developed must not be accessed by the third user in the network. The secure transmission of data or product from the producer to the supplier has to be ensured such

that provenance is achieved at the end. Yet another aspect of the blockchain is it must be tamper resistant when subjected to several attacks in the transaction. While invoking smart contacts, mining is done for the creation of subsequent blocks. Several types of mining are done to establish blocks in the blockchin.

Saqib *et al.* [4] provides a secure data provenance method for cloud centric Internet of Things (IoT) networks with the use of block chain smart contracts. In the first step, the data extracted from these devices are sent to the gateway node, which consist of registry manager and key generator. Then, a unique id is developed for of each devices in the IoT network by means of Elliptic Curve DiffieHellman (ECDH) key generator. Next, the registry manager maps this unique id to the Domain Name System (DNS), which is the individual name of the devices in the IoT network..

Tien *et al*. [5] suggests a benchmarking method for effective data provenance by means of smart contract in block chain. In this method, there are four layers such as consensus, data model, execution engine and application layer. Each block bench layer consists of workloads for finding the concert of the layer individually. At the first consensus layer a DoNothing workload is given, and the smart contract accept it as the input and without performing any operations it returns the value. The consensus layer is responsible for finding the overall performance of the BLOCKBENCH. In the second layer called as the data layer, the Analytics workload is given and here the total transaction values are computed between two different blocks.

Nour *et al.*[6] suggests a method that uses the blockchain technology and decentralized autonomous organization (DAO) for attaining better performance in e-government system in case of issuing contracts. Initially, the basic set of rules are framed by implementing the general requirements of the contract in a smart contract. There are four major divisions by which the processes are done such as contract preparation and submission, bidding and selection, contract execution and monitoring, and finally auditing. At each step of execution, the satisfaction of requirements by the parties are checked. In the first step, the contracts are changed into smart contract and is digitally signed by the contract issuer. Then it is sent to the eGov-DAO to make it accessible to the public. In the second step, the interested contractors creates a proposal and makes a digital signature then submits it to the eGov-DAO.

Oscar Novo [7] provides a method based on distributed access control system for IoT networks using blockchain. At first public keys are generated for every IoT devices present in the wireless sensor network using cryptographic technologies. Then in the next step, the managers grant access control permissions to the devices and without the consent of the manager no device can participate in the blockchain

Ali *et al.* [8] proposes a blockchain based method for maintaining privacy and security of smart vehicles. Initially the privacy information of the vehicles such as location and maintenance history are stored in in-vehicle storage. The vehicle produces a signature with the signed hash for the stored data in the storage of in-vehicle. This hash is directed to the Overlay Block Manager (OBM) and then it is stored in blockchain. The OBM verifies the transaction by checking the signature of the participant with the public key and also it verifies the details of the before transactions in the blockchain.

Esther *et al.* [9] suggests a method for marketing of energy resources using distributed information and communication technology of block chain. Initially, the market phenomenon is written in a smart contract and a unique address is given to every agents in the chain. Then these address are connected to the checking account, which enables the payment and withdrawal of money. Then the agents requests for orders by means of Application Program Interface (API) and their money is kept locked until the transactions are finished. Finally, at the destination of each period, all the buy and sell orders are checked to be complete and the update is made for any balances in the accounts.

IV. DATA PROVENANCE

Data provenance refers to the record of the systems, entities, inputs, and processes that influences data of interest, providing a historical record of the data and its origins. A provenance management framework can record different data about each source data item. A source could be signified as the original data, metadata connected to the source, the source hierarchy structure. Transformations provenance is data about the transformation that were included in the production of a data item. A transformations is not constrained to be a programmed process, however might be a manual procedure or a self-loader process with client association. The transformation provenance of a data could incorporate metadata like creator of the transformation, the client who executed the transformation and the whole execution time.A provenance model is partly significant to model the data in world level, whichever be closed or open. In a closed world model the provenance framework controls transformations and data item. Opposite in an open world model the provenance framework has no or just constrained command over the executed changes and information items [5]. Many information models have an explicit or implicit leveled structure. This chain of command in blend with a key property or worth equivalence could be utilized to distinguish a data item.

A. *Query and manipulation functionalities*

To be helpful for a certifiable application, a provenance framework ought to give offices to manipulate and query provenance data [2]. If a provenance framework handles transformations at different degrees of detail, it should provenance components for merging different transformations into one transformations and split an unpredictable change into an arrangement of less complex changes. In Figure 1.2. Shows the overview of Query and manipulation functionality.

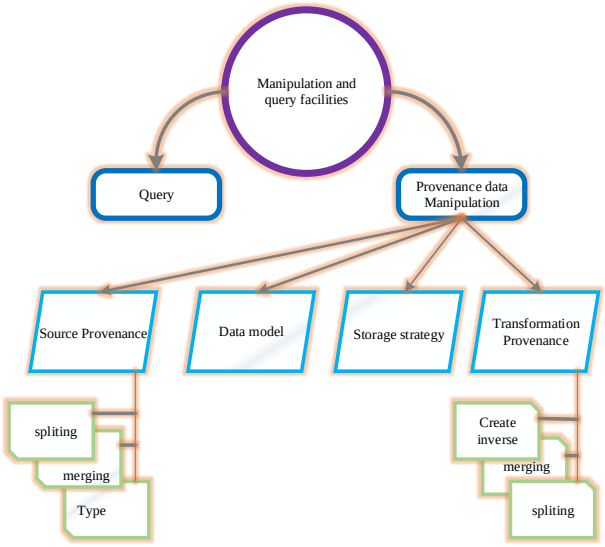

Fig. 1 Query and manipulation functionality model.

Split and merge activities could likewise be applied to the data item measurement. Split partitions a more elevated level data item into its lower-level parts and merge consolidates lower-level data item into a more significant level. A provenance framework that records provenance data for various information models ought to give offices to changing over the portrayal of a data model structure to another [3]. If a provenance framework can figure the opposite of a transformations at that point the reversal can be used to reproduce source data item from the resultant data items.

V. PROPOSED METHODOLOGY FOR PROVENANCE IN RICE SUPPLY CHAIN

Fig 1 shows the proposed architecture for the provenance of the assets in the blockchain. Raw material's information, manufacturing details, retailer and product information and inventory update information will save in blockchain using smart contract in solidity on Ethernet network which is public blockchain . For testing purpose we will use any testing network like Robstan Testing Network or Rinkyby Testing Network.

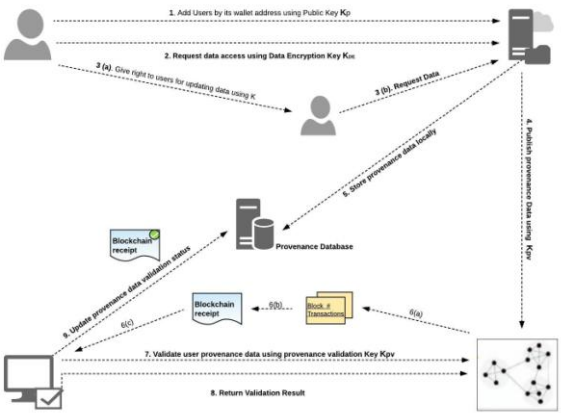

Fig.2. Proposed architecture for data Provenance in Supply chain

Figure 2 shows the proposed architecture for the provenance of the assets in the blockchain. Steps for provenance data in supply chain

1. Admin add different actors or users by its wallet address using Public Key Kp on Server
2. Admin Request Data on Server access using encryption Key KDE
3. (a) Admin right to actors for updating the data for provenance as per their role
   (b) Actors update the data on server using their encryption Key KDE
4. Publish Provenance data Using KPV
5. Store Provence data Locally
6. (a) Create the Block Hash (# value)
   (b) Create block of transaction
   (c) Blockchain Reciept
7. Validate user Provenance data using provenance validation key KPV
8. Return Validate Result
9. Update Provence data Validation status (local server)

We used smart contract on ethereum blockchain for the provenance of the information in rice supply chain. Ethereum is a decentralized global software platform, and it empowers one to compose codes to control cash and construct applications that can be accessed from anywhere around the world that depends on the blockchain technology. The principle of Ethereum is that it enables designers to construct and deploy on decentralized applications. Ethereum is one of the efficient and well-developed platform that designs the decentralizing applications (Dapps). Ethereum assists designers with making tasks dependent on their needs, which implies developers to process on a huge number of various applications. In spite of the fact, that the toolset you need will differ depending upon the particular blockchain, and most of the tools are compatible with Ethereum, and thus we investigate the different improvement devices utilized on the Ethereum platform.

A. *Smart contract*

A smart contract is a computer program that builds on the block chain technology receives much attention in the field of business and scientific community. These are lines of code that has details and permissions which are automatically executed when the encoded terms and condition are met. For instance, the smart contract is just like a vending machine, where your needed document, driving license, your escrow or whatever will added into your account. The contract encrypts the set of rules in its programming code that executes the code when certain types of events occur. The benefit of smart contract technology include that the transactions are consistently executed by a network of mutually distrusting nodes and thus exclude the involvement of third parties [10]. This is applied in wide range of applications include decentralized gambling, financial services, healthcare services and governance applications. The smart contract are executed with the transactions via crypto currencies which have the interfaces to manage the input from the participants. At the time of execution on block chain, the smart contract act as autonomous entity perform actions when conditions are met. This is because they are executed as program code, without any possibility of censorship, fraud or third party

dependence. There are certain block chain platforms utilized to create the smart contracts in which Ethereum is the commonly used due to its unlimited processing capability [11].

B. *Rice Supply chain*

Here we are using scenario of rice supply chain include different stages of rice supply chain and making it verifiable by all stakeholdres in supply chain using proposed approach. In this scenario we are using six stages with respect to six actor :

1. Admin
2. Farmer
3. Harvester
4. Exporter
5. Importer
6. Company

Admin : Admin creates new batch which is initial stage of rice batch.

Farmer : Farmer are responsible for inspecting rice farms and updating the information like rice family, type of seed and fertilizers used for growing rice.

Harvester : Harvesters conducting plucking, hulling , polishing , grading and sorting activities, further updating the information of crop variety, temperature used and humidity maintained during the process.

Exporter : Exporters are the organization who exports rice throughout the world. Exporter adds quantity, destination address, ship name, ship number, estimated date and time and exporter id.

Importer : Importers imports the rice from rice suppliers and updates quantity, ship name, ship number , transporters information, warehouse name, warehouse address and the importer's address.

Company : Company are the organizations who makes it ready for packaging and to sale into markets. Company adds the information like quantity, temperature , internal batch number , packaging date time, processor name and processor address.

C. *Object model diagram*

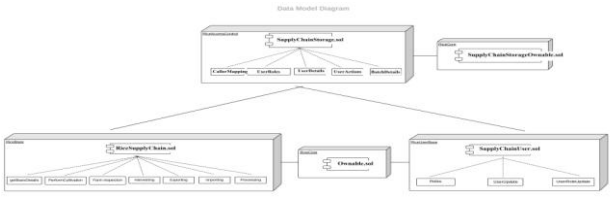

Figure 3 Object Model diagram for rice supply chain

Data Model diagram shows the number of smart contract we are using this rice supply chain. Figure 3 shows the main three smart contract SupplyChainStoage.sol, RiceSupplyChain.sol and SupplyChainUser.sol. Here .sol is the extension of the solidity code in smart contract. SupplyChainStorage.sol contract used for caller mapping, user roles, user details, user actions and batch details of rice. RiceSupplyChain.sol used for perform cultivation, farm inspection, harvesting exporting, importing and processing. SupplyChainUser.sol contract used roles, user updates and roles updates activities.

VI. RESULT ANALYSIS

Provenience of the data in the rice supply chain is our main concern but as well as cost is also involve in this process. The creation of Ethereum contracts and the interaction with these contracts consume gas and have to be paid by the admin who deploy the smart contract and every actors who involved in the rice supply chain.

A. *Deployment costs*

According to the gas costs spreadsheet published in the Solidity documentation, the main costs for deploying a contract are the costs associated with storing the contract code (\CREATEDATA") with costs of 200 gas per byte and the costs for storing additional data on the storage of the contract (\STORAGEADD") with 20000 gas per 256 bit word. Further, in addition to the 21000 gas for a normal contract transaction, 32000 gas have to be paid for a transaction that creates a contract [13]. The absolute deployment costs for a contract dependent heavily on the size of the contract code and the amount of bytes that it assigns to the storage in its constructor. Deployment costs in gas can be estimated using the equation (1).

$$Cgas = (53000 + 200 * Nbytes + 20000 * Nwords) \quad (1)$$

Where Cgas are the total transaction costs in gas, Nbytes is the contract size in bytes and Nwords is the number of 256 bit words that are initialized in the constructor. To calculate the deployment price in US-Dollar, the gas usage has to be multiplied with the the gasprice Pgas and the US-Dollar exchange rate for the ether Pexchange using equation(2).

$$Cdollar = Cgas * Pgas * Pexchange * 10^{-18} \quad (2)$$

Table 1 Gas used and cost of deploying Smart Contract

Smart Contract Name	Used gas	Total gas for deploying
SupplyChainStorage	5200413	0.10400826 ETH
RiceSupplyChain	4989063	0.09978126 ETH
SupplyChainUser	1495102	0.02990204 ETH

The actual deployment costs in gas for the Supply ChainStorage.js , RiceSupplyChain.js and SupplyChainUser contracts are shown in Table1.

B,Security

This section discusses the most important security aspects including the security of Ethereum accounts and the security of transactions. Accounts can either be managed remotely on the server running the Ethereum client. This method should only be used for testing purposes since it involves unlocking the account on the Ethereum client and sending the wallet password over the network in plain text. When using the WalletAccountService the local wallet file is decrypted using the password provided by the user and the credentials are used

by the RawTransactionManager to sign every transaction with the private key belonging to the account. Using the WalletAccountService provides protection against eavesdropping because the wallet password is never sent to the Ethereum client.

C. Privacy of personal user data

All profile information including the prole images are stored on the internal storage of the Distributed application. This will prevent that other applications on the device can access this data. However, it does not provide protection against an attacker that has physical access to a non-encrypted file system or against an attacker that has root access on the operating system [14].

D. Provenance

In this rice supply chain with the help of QR code we can view the provenance of every batch of rice. As soon as different actors like farmer, harvester, importer and exporter do their activity or perform their role they feed the information for the particular rice batch in the rice supply chain and block created as per the transaction and after the mining the block, it add in the blockchain of rice supply chain. In this way, we can track the progress of rice batch after each stage in blockchain. We used IPFS, is a point-to-point protocol in which each node stores a collection of hash files. A client that wants to recover one of these files has access to a nice level of abstraction where it is sufficient to call the hash of the desired file. IPFS then passes through the nodes and provides the client. It's a distributed way to archive and reference files, but it gives you more control and refers to files using the hash, which allows much richer programmatic interactions [15]The stages which are yet not updated in blockchain are denoted using cross sign and the stages which are completed are denoted by right tick sign. You can also find out the name, address and contact information of user who updated the particular stage in rice supply chain.

VII. CONCLUSION

We described and evaluating assets provenance in the rice supply chain using smart contract on ethereum blockchain. Smart contract are PC conventions that encourage, confirm, or implement the arrangement or execution of an agreement, or that forestall the requirement for an authoritative statement. Smart contract for the most part additionally have a user interface and regularly imitate the rationale of authoritative provisions. Defenders of smart contracts guarantee that numerous sorts of legally binding provisos may along these lines be made halfway or completely self-executing, self-authorizing, or both. Smart contracts mean to give security better than customary smart contract and to decrease other exchange costs related with contracting .In particular, as blockchain technology develops, as more business models conceived that hold it and as well as more researchers explore research opportunities with its use, we believe that the smart contract for data province can make a contribution to the growth of blockchain. Supply chain requires coordination of information from every one of the phases in the profitable procedure: extraction, handling, transport, storage, creation, and utilization. Distributed records (blockchains) are the ideal instrument for accomplishing these results.

REFERENCES

1. Bates A, Pohly DJ, Butler KR. Secure and Trustworthy Provenance Collection for Digital Forensics. InDigital Fingerprinting 2016 (pp. 141-176). Springer, New York, NY.
2. Jamil HM, Sadri F. Crowd enabled curation and querying of large and noisy text mined protein interaction data. Distributed and Parallel Databases. 2018 Mar 1;36(1):9-45.
3. Morabito V. Managing change for big data driven innovation. InBig Data and Analytics 2015 (pp. 125-153). Springer, Cham.
4. Ali S, Wang G, Bhuiyan MZ, Jiang H. Secure Data Provenance in Cloud-Centric Internet of Things via Blockchain Smart Contracts. In2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI) 2018 Oct 8 (pp. 991-998). IEEE.
5. Dinh TT, Liu R, Zhang M, Chen G, Ooi BC, Wang J. Untangling blockchain: A data processing view of blockchain systems. IEEE Transactions on Knowledge and Data Engineering. 2018 Jan 4;30(7):1366-85.
6. Diallo N, Shi W, Xu L, Gao Z, Chen L, Lu Y, Shah N, Carranco L, Le TC, Surez AB, Turner G. eGov-DAO: A better government using blockchain based decentralized autonomous organization. In2018 International Conference on eDemocracy & eGovernment (ICEDEG) 2018 Apr 4 (pp. 166-171). IEEE.
7. Novo O. Blockchain meets IoT: An architecture for scalable access management in IoT. IEEE Internet of Things Journal. 2018 Mar 5;5(2):1184-95.
8. Dorri A, Steger M, Kanhere SS, Jurdak R. Blockchain: A distributed solution to automotive security and privacy. IEEE Communications Magazine. 2017 Dec 13;55(12):119-25.
9. Mengelkamp E, Notheisen B, Beer C, Dauer D, Weinhardt C. A blockchain-based smart grid: towards sustainable local energy markets. Computer Science-Research and Development. 2018 Feb 1;33(1-2):207-14.
10. Luu L, Chu DH, Olickel H, Saxena P, Hobor A. Making smart contracts smarter. InProceedings of the 2016 ACM SIGSAC conference on computer and communications security 2016 Oct 24 (pp. 254-269). ACM.
11. Alharby M, van Moorsel A. Blockchain-based smart contracts: A systematic mapping study. arXiv preprint arXiv:1710.06372. 2017 Oct 17.
12. Nguyen HT, Cano A, Tam V, Dinh TN. Blocking Self-avoiding Walks Stops Cyber-epidemics: A Scalable GPU-based Approach. IEEE Transactions on Knowledge and Data Engineering. 2019 Mar 13.
13. Ethereum, Gas costs. URL:https://docs.google.com/spreadsheets/ d/1m89CVujrQe5LAFJ8-YAUCcNK950dUzMQPMJBxRtGCqs/edit #gi 0, Last visited July 27, 2017.Android, Security Tipps. URL:https://developer.android.com/training/ articles/securitytips.html, Last visited July 31, 2017
14. 108. Xu X, Weber I, Staples M. Cost. InArchitecture for Blockchain Applications 2019 (pp. 175-195). Springer, Cham.

AUTHORS PROFILE

Amrita Jyoti ,Ph.D. research scholar Kurukshetra University, Kurukshetra India and presently working as Associate professor in ABES Engineering College, Ghaziabad Uttar Pradesh, India. She received her B.Tech. degree in Information Technology from Kurukshetra University, India in 2003 and M.Tech. in Computer Science & Engineering from the Dr. A. P. J. Abdul Kalam Technical University, Uttar Pradesh, Lucknow, India in 2011. In 2005, she joined the Department of Computer Science & Engineering, ABES Engineering College, Uttar Pradesh, India as a lecturer and became an associate professor in 2015. She is the author of a Book ‘‘Title: Data compression’’ which has covered all the techniques of compression in text, audio and video. Her current research area include software Engineering, software testing, data compression, data structure, JAVA , cloud computing and Blockchain. She published many research paper in National and International Journals and presented many papers in various National and International Conferences.

Dr. R.K Chauhan is the oldest founder faculty member as well as senior most professors in the deptt of computer science & applications in Kurukshetra University, Kurukshetra. He obtained the doctor of philosophy in computer science from the Kurukshetra university. Under his supervision, fourteen scholars have been awarded Ph.D. degree on different areas of computer science and applications and three scholars are pursuing their research work. He has also guided more than fifty M.Tech desertion. He has affended and participated in numerous professional conferences meetings and has published more than hundred research papers in national and International journals. He was awarded 6 merit certificate for best research paper in Dec 1998 by Institution of engineers(India). He held the position of chairman of Deptt of Comp. Sci and Applications from Dec 2007 to Dec 2010. His research area include Advance Database, Data Mining & Warehousing, Mobile Computing, Ad-hoc Networks and Software Engineering. He has been the member of various academic and administrative bodies of Kurukshetra University and other University.

.