BLOCKCHAIN-BASED AGRI-FOOD SUPPLY CHAIN: A COMPLETE SOLUTION

Ruturaj R. Varne, Dept. of Computer Engineering, Zeal College of Engineering & Research, Pune, MH.
Aishwarya M. Shinde, Dept. of Computer Engineering, Zeal College of Engineering & Research, Pune, MH.
Swapnil N. Wakale, Dept. of Computer Engineering, Zeal College of Engineering & Research, Pune, MH.
Prof. Pravin S. Patil, Project Guide, Dept. of Computer Engineering, Zeal College of Engineering & Research, Pune, MH.

***Abstract*—**Supply chains are evolving into automated and highly complex networks and are becoming an important source of potential Benets in the modern world. At the same time, consumers are now more interested in food product quality. However, it is challenging to track the provenance of data and maintain its traceability throughout the supply chain network. The traditional supply chains are centralized and they depend on a third party for trading. These centralized systems lack transparency, accountability and auditability. In our proposed solution, we have presented a complete solution for blockchain-based Agriculture and Food (Agri-Food) supply chain. It leverages the key features of blockchain and smart contracts, deployed over ethereum blockchain network. Although blockchain provides immutability of data and records in the network, it still fails to solve some major problems in supply chain management like credibility of the involved entities, accountability of the trading process and traceability of the products. Therefore, there is a need of a reliable system that ensures traceability, trust and delivery mechanism in Agri-Food supply chain. In the proposed system, all transactions are written to blockchain which ultimately uploads the data to Interplanetary File Storage System (IPFS). The storage system returns a hash of the data which is stored on blockchain and ensures efficient, secure and reliable solution. Our system provides smart contracts along with their algorithms to show interaction of entities in the system. Furthermore, simulations and evaluation of smart contracts along with the security and vulnerability analyses are also presented in this work.

Keywords*— *Accountability, blockchain, credibility, reputation, supply chain, traceability, trust.

I. INTRODUCTION

Traceability plays a vital role in food quality and safety management. Tracing products and processes across complex supply chain networks has become an integral part of current supply chain management. At the same time, consumers are now more interested in food product quality. Block Chain Technology: A block-chain is a database that is shared across a network of computers. Once a record has been added to the chain it is very difficult to change. The records that the network accepted are added to a block. Each block contains a unique code called a hash. It also contains the hash of the previous block in the chain. The term "block-chain technology" typically refers to the transparent, trustless, publicly accessible ledger that allows us to securely transfer the ownership of units of value using public key encryption and proof of work methods. The technology uses decentralized consensus to maintain the network, which means it is not centrally controlled by a bank, corporation, or government. In fact, the larger the network grows and becomes increasingly decentralized, the more secure it becomes. A block-chain is a decentralized, distributed and public digital

ledger that is used to record transactions across many computers so that any involved record cannot be altered retroactively, without the alteration of all subsequent blocks. Crowd- sourcing is a sourcing model in which individuals or organizations obtain goods and services, including ideas and finances, from a large, relatively open and often rapidly-evolving group of internet users; it divides work between participants to achieve a cumulative result. Blockchain technology is defined as the technology that plays as a role of distributed ledger in which transactions are made in digital manner and at the same time these transactions are recorded, verified, and validated throughout the network of nodes without the approval of central authority. The most important feature is the decentralization, which ensures that there is no individual resource that controls the whole system. All participating nodes of the system can use all their resources to prevent the many-to-one traffic, which eventually succeed in dealing with problem raised to single point failure and decreases the delay. The decentralized system makes sure that the system is robust and scalable.

1.1 Motivation

Block-chain is an emerging technology for distributed and important data sharing across a large network of un-trusted participants. In today's day in healthcare is growing fast also as well as the data need to store securely. It allows new forms of distributed software architectures.

1.2 Problem Definition

Now a days agri supply chain system is growing fast also as well as the data need to store securely. Some data might be sensitive that the users does not want to move to the cloud unless the data confidentiality and query privacy are guaranteed.

1.3 Project Scope

1. Useful for multi keyword search on encrypted data.
2. Improve security using block chain technology.
3. Useful for agri applications.

II. RELATED WORK

[1] New directions in cryptography" Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems of long standing.

[2] An efficient protocol for authenticated key agreement" This paper proposes an efficient two-pass protocol for authenticated key agreement in the asymmetric (public-key) setting. The protocol is based on Diffe-Hellman key agreement and can be modified to work in an arbitrary finite group and, in particular, elliptic curve groups. Two modifications of this protocol are also presented: a one-pass authenticated key agreement protocol suitable for environments where only one entity is on-line, and a three-pass protocol in which key confirmation is additionally provided. Variants of these protocols have been standardized in IEEE P1363

[17], ANSI X9.42 [2], ANSI X9.63 [4] and ISO 15496-3, and are currently under consideration for standardization and by the U.S. government's National Institute for Standards and Technology.

[3] Identity-based fault-tolerant conference key agreement" Lots of conference key agreement protocols have been suggested to secure computer network conference. Most of them operate only when all conferees are honest, but do not work when some conferees are malicious and attempt to delay or destruct the conference. Recently, Tzeng proposed a conference key agreement protocol with fault tolerance in terms that a common secret conference key among honest conferees can be established even if malicious conferees exist. In the case where a conferee can broadcast different messages in different subnetworks, Tzeng's protocol is vulnerable to a different key attack" from malicious conferees. In addition, Tzeng's protocol requires each conferee to broadcast to the rest of the group and receive n 1 messages in a single round (where n stands for the number of conferees). Moreover, it has to handle n simultaneous broadcasts in one round. In this paper, we propose a novel fault-tolerant conference key agreement protocol, in which each conferee only needs to send one message to a semitrusted" conference bridge and receive one broadcast message. Our protocol is an identity-based key agreement, built on elliptic curve cryptography. It is resistant to the different key attack from malicious conferees and needs less communication cost than Tzeng's protocol.

[4] Identity-based key agreement protocol employing a symmetric balanced incomplete block design" Key agreement protocol is a fundamental protocol in cryptography whereby two or more participants can agree on a common conference key in order to communicate securely among themselves. In this situation, the participants can securely send and receive messages with each other. An adversary not having access to the conference key will not be able to decrypt the messages. In this paper, we propose a novel identity-based authenticated multi user key agreement protocol employing a symmetric balanced incomplete block design. Our protocol is built on elliptic curve cryptography and takes advantage of a kind of bilinear map called Weil pairing. The protocol presented can provide an identification (ID)- based authentication service and resist different key attacks. Furthermore, our protocol is efficient and needs only two rounds for generating a common conference key. It is worth noting that the communication cost for generating a conference key in our protocol is only O (n n) and the computation cost is only O nm2, where n implies the number of participants and m denotes the extension degree of the finite field Fpm. In addition, in order to resist the different key attack from malicious participants, our protocol can be further extended to provide the fault tolerant property.

III. PROPOSED SYSTEM

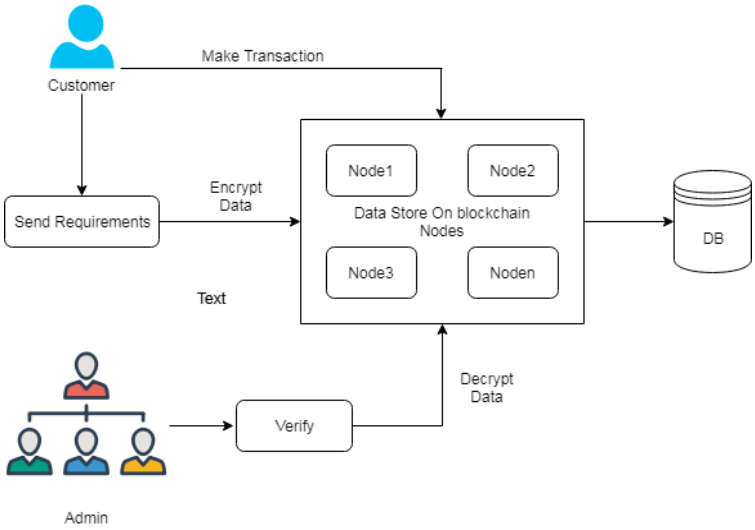

Fig 1: System Architecture

IV. SPECIFICATIONS

1. Hardware Specifications

- Processor - I3,I5
- Speed - 3.8 GHz
- RAM - 4GB
- Hard Disk - 1 TB
- Key Board - Standard Windows Keyboard
- Mouse - Two or Three Button Mouse
- Monitor - LCD(Liquid Crystal Display)

2. Software Specifications

- Operating System: Windows 10
- Programming Language: JAVA
- Backend: Mysql 5.0
- IDE : Eclipse Oxygen
- Tool: Apache Framework

V. MODULE SPECIFICATION

User Modules:
1. User Registration and login
2. Search file.
3. Enter Keyword.
4. View Requirements.
5. Request for key.
6. Send Requirements.

Admin Modules:
1. Admin login.
2. Admin view all users.
3. Upload food Dataset.
4. View Graph.

VI.CONCLUSION

Using blockchain, supply chain industry has gained numerous benefits to grow and move towards decentralization and achieve a trustless environment for all processes. However, despite the trustless nature of blockchain, it is hard to fully maintain trust between the seller and buyer of the product. This is because the entities may act maliciously and the buyer can doubt their credibility. Moreover, supply chain involves multiple processes and sub-processes that need to be carried out in a decentralized manner in order to achieve traceability, accountability and security. In this paper, we have proposed an end to end solution for blockchain-based Agri Food supply chain. We have provided detailed information of proposed solution in terms of traceability, trading, delivery and reputation. We have evaluated and carefully analyzed the performance of smart contracts in order to ensure that the proposed solution is efficient and robust. The reputation system is proposed to maintain the credibility of the Agri-Food supply chain entities and quality ratings of the products. Moreover, it also maintains the immutability and integrity of the transactions as these transactions are based on blockchain.

APPLICATIONS

- We implement agri food Data Security System.
- Improve security using block chain technology.
- Search reports using keyword search.
- Reduce data loss and hacking major issues.

REFERENCES

1. F. Chen, T. Xiang, Y. Yang, and S. S. M. Chow, \Secure cloud storage meets with secure network coding," in IEEE INFOCOM, 2014, pp. 673{681.

2. D. He, S. Zeadally, and L. Wu, \Certificate less public auditing scheme for cloud-assisted wireless body area networks," IEEE Systems Journal, pp. 1{10, 2015.

3. W. Di_e and M. E. Hellman, \New directions in cryptography," IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644{654, 1976.

4. J. Shen, H. Tan, S. Moh, I. Chung, and J. Wang, \An efficient authentication protocol providing strong privacy and security," Journal of Internet Technology, vol. 17, no. 3, p. 2, 2016.