Traceability of Agricultural food products in supply chain through Blockchain

Dhawale Asmita,Datir Tejashri,Lande Shradha.

BE Students, Department of Computer Engineering, H.S.B.P.V.T.Kashti

Suryavanshi P.M.

Professor, Department of Computer Engineering, H.S.B.P.V.T.Kashti

Abstract

The globalized production and the distribution of agriculture production bring a renewed focus on the safety, quality, and the validation of several important criteria in agriculture and food supply chains. The growing number of issues related to food safety and contamination risks has established an immense need for effective traceability solution that acts as an essential quality management tool ensuring adequate safety of products in the agricultural supply chain. Block-chain is a disruptive technology that can provide an innovative solution for product traceability in agriculture and food supply chains. Our proposed solution eliminates the need for a trusted centralized authority, intermediaries and provides transactions records, enhancing efficiency and safety with high integrity, reliability, and security. All transactions are recorded and stored in the block-chain immutable ledger with links to a decentralized file system and thus providing to all a high level of transparency and traceability into the supply chain ecosystem in a secure, trusted, reliable, and efficient manner.

Keywords: Traceability, Blockchain, Supply chain management, e-Commerce, agriculture sector, food safety.

Introduction

Monitoring the development of agricultural products and efficient logistics management in food and agricultural supply chain is critical to ensure product safety. The growing concerns about food safety and contamination risks have renewed the focus for enhanced traceability across the supply chain. In addition agricultural products being traded across several countries require precise tracking and conformance to country specific regulations. Traceability of products in agricultural supply chain requires collection, communication and management of critical information by precisely identifying the origin, various information exchanges in the supply chain. The dynamic nature of information in the agricultural/food supply chain where products are produced, processed and sent via several intermediaries makes it difficult to track and trace. Product contamination and its implications to public health strongly emphasize traceability as necessary policy tool towards monitoring food quality and safety. The current practice of traceability in agriculture supply chain largely suffers from data fragmentation and centralized controls which prove vulnerable to both data modification and management. Individual stages in food supply chains often have good traceability but exchange of information between stages proves to be difficult and time consuming. Recent technology developments through the application of blockchain technology can provide a meaningful and practical solution ensuring traceability of agricultural produce and eliminates the need for a trusted centralized authority. Blockchain technology has gained immense popularity among supply chain and logistics community due transparency and immutability of transactions, enhances trust among participating stakeholders. Due to its tamperproof, trusted, secure and traceable nature, blockchain can be deployed effectively in the agriculture and food supply chain management. The overall structure and functioning of food supply chain is vast and complex involving multiple stakeholders ranging from farmers, manufacturers, processors, and consumers. Food and agricultural supply chain is getting a lot of attention from the research community due to problematic long supply chain, from raw materials to the end consumer makes it extremely hard and time-consuming in tracking back the origin of a product. Hence, there is a need to create a secure framework for tracking details about the origin, farming methods adopted, and safety of the food product throughout the supply chain cycle without a third party or centralized control.

The blockchain is basically an immutable and decentralized, shared public ledger of transactions which allows participants to keep track of transactions without central record keeping. Blockchain is a shared distributed ledger composed of add-on blocks that include details of all transactions data, execution outcomes and is traceable. Each block is hashed and linked to the next block, making it a secure chain of immutable and tamper-proof records. The overarching objective of this paper is to demonstrate how blockchain can efficiently trace and track and enable flawless integration of business transactions and workflows in the agricultural supply chain. We propose, implement, and analyze a blockchain framework to provide traceability and visibility in the food supply chains.

Motivation

- Increase transparency between all the participants in the supply chain.
- Increase food safety.
- Trace food products in supply chain in order to obtain higher level of efficiency and information sharing.

Related Work

Literature survey is the most important step in any kind of research. Before start developing we need to study the previous papers of our domain which we are working and on the basis of study we can predict or generate the drawback and start working with the reference of previous papers.

In this section, we briefly review the related work on Traceability of the agriculture food products and their different techniques.

In this paper, the author implements FTSs well, traceability activities can be integrated with food logistics; the communication among partners should be strengthened; effective and efficient traceability technologies ought to be developed. In addition, more attention from society, government agencies and researchers should be given to FTSs. Future research can be focus on how to integrate traceability and logistics well and how to use big data in food traceability systems. [1]

Cooperatives play an important role in high standard agricultural production and commercialization processes. Because they function as both social and economic networks, also creating both horizontal and vertical relationships, they function as an integral part of net-chains within complex food-supply chains.By approaching complex supply chains and the inherent challenges of traceability systems, net-chain analysis is useful, particularly when coupled with organizational structures such as cooperatives, which inherently function as net-chains. Future research includes deepening the understanding of the net-chains that should be extended in scope and space as an effect of globalization. [2]

The author propose an innovative blockchain-based IIoT architecture to help build a more secure and reliable IIoT system. By analyzing the shortcomings of the existing IIoT architecture and the advantages of the Blockchain technology. We decompose and reorganize the original IIoT architecture to form a new, multi-center, partially decentralized architecture. Thus, the proposed architecture represents a significant improvement of the original architecture, which provides a new direction for the IIoT development. [3]

In this paper, the author proposed a novel blockchain-based product ownership management system (POMS) for the post supply chain, which makes the efforts of counterfeiters to clone genuine tags redundant since they cannot prove the possession of products on this system. In this they implemented a proof-of-concept experimental system employing a blockchain-based decentralized application platform and evaluated its cost performance. [4]

This paper presents a systematic mapping study in order to map out all relevant research on SCM based on BCT. The paper took a survey on other blockchain applications in SCM that need additional investigation, such as agricultural supply chain, security of additive manufacturing, product ownership management, common-pool resource management, purchasing and supply management, supply chain quality management, supply chain performance measurements. Nevertheless, many of the proposed frameworks-based solutions lack real performance evaluation on the industrial context. [5]

In this paper, the author gives a survey on the concepts of supply chain management and traceability in agriculture, and highlight the technological challenges in implementing traceable agricultural supply chains. Development of appropriate measurement tools for food product labeling and identification, activity/process characterization, information systems for data capture, analysis, storage and communication, and the integration of the overall traceable supply chain are essential for success. [6]

In this article, the author examines the impact of blockchain technology in agriculture and food supply chain, presents existing ongoing projects and initiatives, and discusses overall implications, challenges and potential, with a critical view over the maturity of these projects. The conclusion indicate that blockchain is a promising technology towards a transparent supply chain of food, with many ongoing initiatives in various food products and food-related issues, but many barriers and challenges still exist, which hinder its wider popularity among farmers and systems. These challenges involve technical aspects, education, policies and regulatory frameworks. [7]

In this article, the author proposed a generic framework leveraging blockchain to trace, track, and perform business transactions removing intermediaries and central point of processing for soybean traceability across agricultural supply chain. The details are generic enough and can be applied to provide trusted and decentralized traceability to any crop or produce in the agricultural supply chain. To date, blockchain technology still faces key challenges related to scalability, governance, identity registration, privacy, standards, and regulations. As a future work, we plan to look at addressing some of these key challenges and develop solutions addressing them. [8]

This paper proposes a food trade mechanism based on an alliance chain that helps to eliminate information asymmetry and guarantee market fairness. The proposed system is shown to be effective for the food trade field. According to the Sustainable Food Trade Association, a highly reputed agricultural sustainable development organization, the organic sector must integrate environmentally sound, socially just business practices using a systems-based approach to reach its full potential. This paper provides an effective technical means to achieve the above requirements. As computational costs of the on-chain matching algorithm depend on the amount of supply and demand information and cannot be determined in advance, a fair mechanism for the allocation of these costs has to be determined.[9]

In this article, we proposed a new decentralized traceability system based on internet of things and blockchain technology, and explored the challenges in scaling blockchain in general. This system will deliver real-time information to all supply chain members on the safety status of food products, extremely reduce the risk of centralized information systems, and bring more secure, distributed, transparent, and collaborative. However, to date, nearly all of these systems are centralized which are monopolistic, asymmetric and opaque that could result in the trust problem, such as fraud, corruption, tampering and falsifying information. [10]

Problem Statement

Imagine an online portal where farmers and end consumers directly exchange money and a promise to have produce delivered to them. A portal which reduced the cost of vegetables for the consumer and gives back more to the farmer. That is the idea behind the e-marketplace model for which the Department of Agriculture and Farmer Welfare sought solutions and wastage of food management.

Proposed Method

This system proposes, implement, and analyze a block-chain framework to provide traceability and visibility in the agricultural food products supply chain. We present, implement, and test algorithms that govern and ensure the proper interactions among key stakeholders in the agriculture supply chain. Our solution eliminates the need a trusted centralized authority and provides transactions and records for food supply chain management and safety with high integrity, reliability, and security. In this system we are going to add an NGO authority for saving the wastage of food.

Architecture

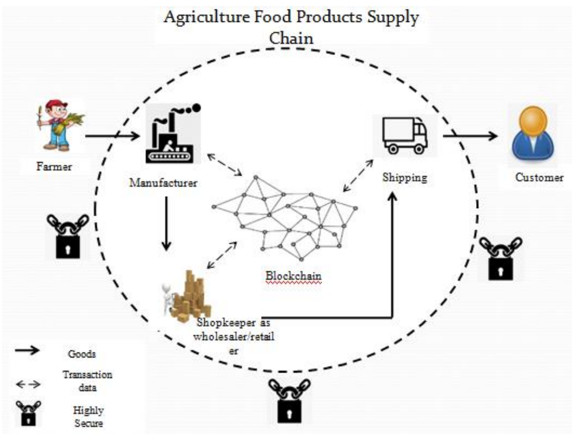

Fig 1.System Architecture

Algorithm

Hybrid Approach:

In this we are going to increase the security and time efficiency by using algorithms i.e. Blockchain Algorithm (Cryptography algorithm). The main purpose of using public-key cryptography for the blockchain is to create a secure digital reference about the identity of a user. Secure digital references about who is who, and who owns what, are the basis for P2P transactions. Public-key cryptography allows proving one's identity with a set of cryptographic keys: a private key and a public key.

1. **Advanced Encryption Standard:**

The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the dvanced Encryption Standard (AES). It is found at least six time faster than triple DES. A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow.

The features of AES are as follows:

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java

Operation of AES:

AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations). Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix.Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

1. Input:
2. 128 bit /192 bit/256 bit input(0,1)
3. Secret key (128 bit)+plain text(128 bit).
4. Process:
5. 10/12/14-rounds for-128 bit /192 bit/256 bit input
6. Xor state block (i/p)
7. Final round:10,12,14
8. Each round consists: sub byte, shift byte, mix columns, add round key.
9. Output:
10. cipher text(128 bit)

2. SHA-1(Secure Hash Algorithm)

Secure Hashing Algorithms, also known as SHA, are a family of cryptographic functions designed to keep data secured. It works by transforming the data using a hash_function: an algorithm that consists of bitwise operations, modular additions, and compression functions. The hash function then produces a fixed size string that looks nothing like the original. These algorithms are designed to be one-way functions, meaning that once they're transformed into their respective hash values, it's virtually impossible to transform them back into the original data. A common application of SHA is to encrypting passwords, as the server side only needs to keep track of specific user's hash value, rather than the actual password.

Steps are followed:

1. Sender feeds a plaintext message into SHA-l algorithm and obtains a 160-bit SHA-l hash.
2. Sender then signs the hash with his RSA private key and sends both the plaintext message and the signed hash to the receiver.
3. After receiving the message, the receiver computes the SHA-l hash himself and also applies the sender's public key to the signed hash to obtain the original hash H.

Mathematical Model

Mathematical equation:

The algorithm implemented in this project is described as:

Initialization: password, key, time, salt: string

time $\leftarrow$ get time

input $\leftarrow$ (password)

key $\leftarrow$ salt + time

Encryption:

Ciphertext $\leftarrow$ AESEncrypt(password; key)

output(ciphertext)

Decryption:

key $\leftarrow$ salt - time

forasmuchtolerancegiventime

ifkey = get time

key $\leftarrow$ salt + time

plaintext $\leftarrow$ AESDecrypt(ciphertext; key)

endif

endfor

output(plaintext)

Result and Discussion

Experiments are done by a personal computer with a configuration: Intel (R) Core (TM) i5-6700HQ CPU @ 2.60GHz, 16GB memory, Windows 7, MySQl Server 5.1 and Jdk 1.8.

In our system, We compared the proposed and existing system. The overall accuracy of proposed technique is enhanced as compared to existing techniques. So our proposed system accuracy is better than existing system. So this works gives better results as compare to existing method.

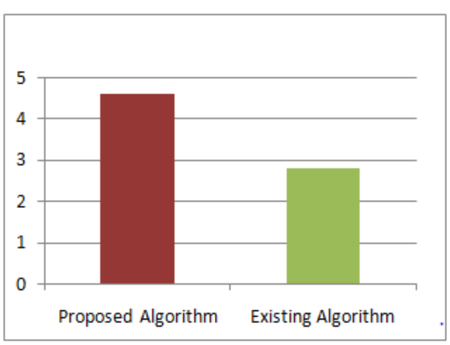

Fig 2. Algorithms Comparison

Conclusion

In summary, blockchain technology can help us to build a trusted, self-organized, open and ecological smart agriculture system, which involves all parties in the ecosystem; even they may not trust each other. To the best of our knowledge, this is the first work that applying blockchain technology on traditional agriculture ecosystem to solve the food safety issues. The proposed work implements the methods that govern and ensure the proper interactions among key stakeholders in the agriculture supply chain. In this system we are going to add an NGO authority for saving the wastage of food.

References

1. Yunchuan Zhang, Ting Zou, “ A Review of Food Traceability in Food Supply Chain”, IMECS 2017.

2. Cynthia Giagnocavo, Fernando Bienvenido,Li Ming,Zhao Yurong, Jorge Antonio Sanchez-Molina, Yang Xinting, “Agricultural cooperatives and the role of organisational models in new intelligent traceability systems and big data analysis”, IJABE,2017.

3. Jiafu Wan, Jiapeng Li, Muhammad Imran, Di Li, Fazal-e-Amin, “A Blockchain-Based Solution for Enhancing Security and Privacy in Smart Factory”, IEEE Transactions on Industrial Informatics, June 2019.

4. K. Toyoda, P. T. Mathiopoulos, I. Sasase, and T. Ohtsuki, "A novel blockchain based product ownership management system (POMS) for anti-counterfeits in the post supply chain”, IEEE Access, 2017.

5. Youness Tribis, Abdelali El Bouchti, Houssine Bouayad, “Supply Chain Management based on Blockchain: A Systematic Mapping Study”, MATEC Web of Conferences (2018).

6. Linus U. Opara, “Traceability in agriculture and food supply chain: A review of basic concepts, technological implications, and future prospects”, WFL Publisher Science and Technology Food, Agriculture & Environment,2003.

7. Andreas Kamilaris, Agusti Fonts and Francesc X. Prenafeta-Bold, “The Rise of Blockchain Technology in Agriculture and Food Supply Chains ”, Elsevier Trends in Food Science & Technology Volume 91, 2019.

8. K. Salah, N. Nizamuddin, R. Jayaraman, M. Omar, “Blockchain-based Soybean Traceability in Agricultural Supply Chain”, IEEE Access.

9. Dianhui Mao, Zhihao Hao, Fan Wang, Haisheng Li, “Innovative Blockchain-Based Approach for Sustainable and Credible Environment in Food Trade”, MDPI 2018.

10. Feng Tian, “A Supply Chain Traceability System for Food Safety Based on HACCP, Blockchain & Internet of Things”, IEEE 2017 International Conference On Service Management.