International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 6, June 2020 ||

Supply Chain Management System Using Blockchain Technology

Krushna Bharat Pise, Prof. S. M. Shinde

Department of Computer Science &Engineering, SVERI's College of Engineering, Pandharpur, Maharastra, India

Asst. Professor, Department of Computer Science & Engineering, SVERIS's College of Engineering, Pandharpur, Maharastra, India

ABSTRACT: Blockchains assume an imperative job in everybody lives to track and follow the source of nourishment items in nourishment inventory network. Store network Management (SCM) is a fundamental business process in all circles of the economy. SCM makes use of specific tactics to attach from producer to consumer requirement through a chain. In Blockchain technology primarily based system, "statistics are immutable and trusted, and also eliminate the requirement of thired parties to be involved. Block-chain is a disruptive technology that can provide an innovative solution for product traceability in agriculture and supply chain management. 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. Our fundamental intend to accomplish these objectives by building up this application where everybody will makes a worth chain of trustworthiness from ranch to fork by utilizing BCT.

KEYWORDS*:* Blockchain, supply chain management, traceability, security, immutable, reliable.

I.INTRODUCTION

The block-chain was invented in 2008 by a person or group of persons called Satoshi Nakamoto. Till date, no one knows who Satoshi Nakamoto is, and whether he is a person or whether the name represents a group of people. Block-chain has evolved into something very powerful since then. "The block-chain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value."

Block-chain is a decentralized, distributed database that maintains a continuously growing list of secure data records. It first emerged in the context of Bitcoin, where it serves as a decentralized, distributed digital ledger recording all Bitcoin transactions. Bitcoin is a currency that is controlled by the network of users instead of by centralized banks. Through the use of Bitcoin, money can be transferred directly. In the traditional banking system, when money is transferred through banks, they are notified to transfer the money; the bank(s) will send notification and update accounts appropriately. The relevant data is stored in a database owned by the bank (or in multiple databases owned by banks), and users only have partial access to that data. Users must trust third parties. This has two implications. First, the bank has to make a profit, so in the aggregate; this means less for the other participants. In addition, if some third party or the bank itself manipulates the data or commits fraud, it might be challenging for all participants to quickly and efficiently detect this. On the other hand, the Bitcoin database is decentralized and distributed, so that everyone has the entire database on his or her own device. These are not copies of some original database – they are the database itself, and each device syncs with all others. Thus, if a specific device is hacked, or imports incorrect data, the network will not accept this, and will correct the data using other databases. Unless a single entity controls more than half of the devices on the network, it is almost impossible to delete or edit data. In block-chain, data is stored in blocks of data that are linked to the previous blocks. On average, every ten minutes Bitcoin creates a block of data and all user devices will permanently store that data. Each block references the previous blocks, so if someone wants to change data in a block, he must change all previous blocks as well, which is almost impossible.

Block-chain technology is built using peer-to-peer networking. Anyone can join the network and there is no central authority to manage it. It is operated by people, called miners, who lend their computing power to the network in order to solve complex algorithms. Machines run by miners perform the necessary functions to solve the algorithms, and for that they are rewarded with a fee. In a block-chain, each block stores the data of the transaction, its hash code and the previous

block's hash code. So whenever a new block is created, it is validated by a majority of the peers or miners on that network. If anyone tries to change the data in one block, the entire block-chain will be invalidated; so it's nearly impossible for an individual to change all other attached blocks and that's how a block-chain remains secure and managed. Also, all the data is encrypted for security purposes.

1.1 Motivation

Supply Chain Management increases customer satisfaction. It is responsible for the efficient production and supply of products from the farm level to the consumers to meet consumers' requirements reliably in terms of quantity, quality and price.

II.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 Blockchain supply chain Management.

In this paper, the author research used an advancement of the theory of mindfulness to assess the use of blockchain technologies in the context of logistics and supply chain management. The five discussed case studies suggested different engagement and understanding of the new technology and the problems it is supposed to solve. Several implications, both on the theoretical and on the managerial levels, can be deduced from the case study discussion. [1]

This paper provides, through its methodology, a detailed analysis of the blockchain fit in the supply chain industry. It defines the specific elements of blockchain that affect supply chain such as scalability, performance, consensus mechanism, privacy considerations, location proof and cost, and details on the impact that blockchains will have in disrupting the supply chain industry. Discussing the tradeoff between consensus cost, throughput and validation time it proceeds with a suggested high-level architectural approach, and concludes as a result with a discussion on changes needed and challenges faced for an in-vivo deployment of blockchains in the supply chain industry. [2]

In this paper, author proposed an innovative blockchain-based IoT architecture to help build a more secure and reliable IoT system. By analyzing the shortcomings of the existing IoT architecture and the advantages of the Blockchain technology. We decompose and reorganize the original IoT architecture to form a new, multi-center, partially decentralized architecture. Then, we introduce some relative security technologies to improve and optimize the new architecture. Thus, the proposed architecture represents a significant improvement of the original architecture, which provides a new direction for the IoT development. [3]

In this paper, the author propose a blockchain-enabled efficient data collection and secure sharing scheme combining Ethereum blockchain and deep reinforcement learning (DRL) to create a reliable and safe environment. In this scheme, DRL is used to achieve the maximum amount of collected data, and the blockchain technology is used to ensure security and reliability of data sharing. Extensive simulation results demonstrate that the proposed scheme can provide higher security level and stronger resistance to attack than a traditional databasebased data sharing scheme for different levels/types of attacks. [4]

This paper presents a systematic mapping study in order to map out all relevant research on SCM based on BCT. Guided by a set of research questions, the main motivation for this work was to identify research trends, open subjects, and gaps for improvement in this discipline. The rest of the papers treat 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. The large part of selected studies is concentrating on proposing solutions of currents SCM challenges by designing new blockchain based frameworks. Nevertheless, many of the proposed frameworks-based solutions lack real performance evaluation on the industrial context. [5]

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 6, June 2020 ||

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. [6]
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. [7]
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. [8]

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. [9]

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. [10]

III.PROBLEM STATEMENT

In current supply chain management there is problem that, the Farmer and end customer had a loss because the Farmer sells the product to the third party customer purchase it from third party, so customer needs to pay more money to purchase it.
This problem will be solved and supply chain will be managed easily due to this proposed system.

IV.PROPOSED METHOD

The 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 the proposed work we find the solution of the above problem (i.e implemented in chapter 1) by using block-chain technology in supply chain management. So that there is transparency between the owner and the customer, also customer & owner gains profit because we remove intermediate (i.e. dealer) from owner & customer.
The new system will provide transparency throughout the supply chain. It reduces the operating cost and save lot of time. It also increases the trust level among consumers as well as vendors as they know what they are buying.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 6, June 2020 ||

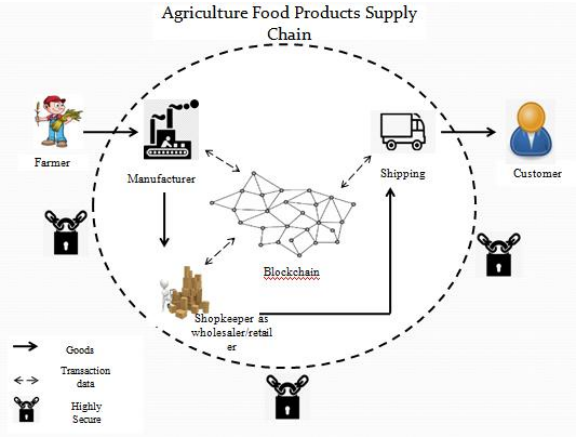

Fig.1 System Architecture

1. **Algorithm:**

Hybrid Approach:

In this we are going to increase the security and timeefficiency by using algorithms i.e. Blockchain Algorithm(Cryptography algorithm).

The main purpose of using public-key cryptography forthe blockchain is to create a secure digital reference aboutthe identity of a user. Secure digital references about who iswho, and who owns what,are the basis for P2P transactions.Public-key cryptography allows proving one's identity with aset of cryptographic keys: a private key and a public key.

Advanced Encryption Standard:

The more popular and widely adopted symmetricencryption algorithm likely to be encountered nowadays is theAdvanced Encryption Standard (AES). It is found at least sixtimes faster than triple DES.

A replacement for DES was needed as its key size wastoo small. With increasing computing power, it was consideredvulnerable against exhaustive key search attack. Triple DESwas designed to overcome this drawback but it was foundslow.

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 seriesof linked operations, some of which involve replacing inputsby specific outputs (substitutions) and others involve shufflingbits around (permutations).Interestingly, AES performs all its computations on bytesrather than bits. Hence, AES treats the 128 bits of a plaintextblock as 16 bytes. These 16 bytes are arranged in fourcolumns and four rows for processing as a matrix.

Unlike DES, the number of rounds in AES is variable anddepends on the length of the key. AES uses 10 rounds for128-bit keys, 12 rounds for 192-bit keys and 14 rounds for256-bit keys. Each of these rounds uses a different 128-bitround 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)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 6, June 2020 ||

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)

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.

VI. MATHEMATICAL MODEL

The algorithm implemented in this project is describe as:
Initialization: password,key,time,salt:string
time ⟵get time
input ⟵(password)
key ⟵salt + time
Encryption:
Ciphertext ⟵AESEncrypt(password; key)
output(ciphertext)
Decryption:
key ⟵salt ⟵time
forasmuchtolerancegiventime
ifkey = get time
key ⟵salt + time
plaintext ⟵AESDecrypt(ciphertext; key)
endif
endfor
output(plaintext)

VII. RESULTS

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.

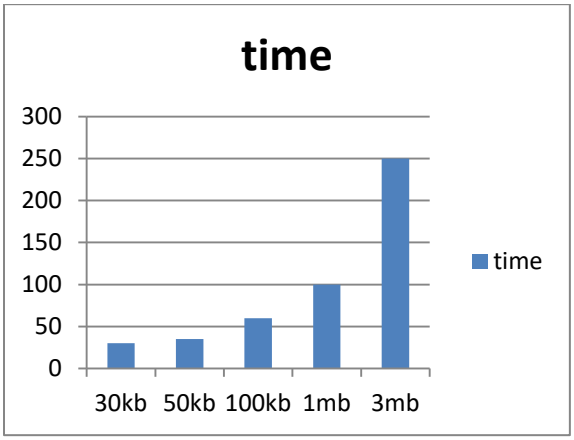

Fig.2Shows file size on X axis and time (ms) to upload on Y-axis

Explanation: Graph shows size of file and time to upload that file after performing fragment and t-coloring .As size of file increases the time will increase.

ID	File size	Time to upload (ms)
1	30kb	30
2	50kb	35
3	100kb	60
4	1mb	100
5	3mb	250

Table 01: Time to upload file

Above table 01 gives the information of uploading time for 30kb, 50kb, 100kb, 1mb and 3mb file size.

VIII.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. Further we are trying to trace the counterfeit agricultural products by using the QR code concept.

REFERENCES

[1] Peter Verhoeven, Florian Sinn, Tino T. Herden, “Logistics and Supply Chain Management: Exploring the Mindful Use of a New Technology”, MDPI September 2018.
[2] Antonios Litke, Dimosthenis Anagnostopoulos, Theodora Varvarigou, “Blockchains for Supply Chain Management: Architectural Elements and Challenges towards a Global Scale Deployment”, MDPI January 2019.
[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 Volume: 15, June 2019.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 6, June 2020 ||

[4] Chi Harold Liu, Senior Member, IEEE, Qiuxia Lin, Shilin Wen. "Blockchain-enabled Data Collection and Sharing for Industrial IoT with Deep Reinforcement Learning", IEEE Transactions on Industrial Informatics Volume: 15, Issue: 6 , June 2019

[5] Youness Tribis, Abdelali El Bouchti, Houssine Bouayad1, "Supply Chain Management based on Blockchain: A Systematic Mapping Study", MATEC Web of Conferences (2018).

[6] 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.

[7] K. Salah, N. Nizamuddin, R. Jayaraman, M. Omar, "Blockchain-based Soybean Traceability in Agricultural Supply Chain", IEEE Access.

[8] Feng Tian, "A Supply Chain Traceability System for Food Safety Based on HACCP, Blockchain & Internet of Things", IEEE 2017 International Conference on Service Systems and Service Management.

[9] Yunchuan Zhang, Ting Zou, "A Review of Food Traceability in Food Supply Chain", IMECS 2017.

[10] 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.