Traceability Of Agri-Food Supply Chain Management Using Blockchain Technology

Mohammed Abdul Waheed[1], Halima Anam[2*], Zohara Begum[3]

[1]Associate Professor, Dept. of Computer Science & Engineering, VTU, CPGS, Kalaburagi, Karnataka, India
prof.mawaheed@gmail.com
[2*]Student, Dept. of Computer Science & Engineering, VTU, CPGS, Kalaburagi, Karnataka, India,
halimaanam119@gmail.com
[3]Assistant Professor, Dept. of E&CE, FENT, KBN, University, Kalaburagi, Karnataka, India, zohra1@kbn.university

[*]**Corresponding Author:** Halima Anam
[*]Student, Dept. of Computer Science & Engineering, VTU, CPGS, Kalaburagi, Karnataka, India,
halimaanam119@gmail.com

Abstract
Traceability is the capacity to track down a certain item. The capacity to trace the origin, current location, or intended use of an object via official records is one possible interpretation. Small-scale farmers, primary processors, dealers, product makers, distributors, retailers, & consumers are just few of many participants in agri-food supply chain. Block-chain is distributed ledger operating with no centralized authority & allows generation of a decentralized, immutable, & verifiable record of transactions. These distinct characteristics have prompted its investigation into a wide range of potential uses, most notably in the financial industry. So, the aim of this project is utilising blockchain technology to provide trackable supply chains for agricultural products.

Keywords: Agri-food, Block-chain, farmers, processors, retailers, consumers

INTRODUCTION
Blockchain is a method of preventing manipulation of data by the use of cryptographically linked records among participants into peer-to-peer network. Bitcoin transactions are what inspired the creation of the blockchain [12]. A "block" has a timestamp, a hash code, and a collection of validated records or transactions. Hash code is a combination of the data in the current block and the data in the preceding block in the chain. Major nodes in network should agree that the block is effective before it can be added to chain. Prover (or miner) demonstrates to the verifiers, for instance, that they have expended computing effort for a certain goal (Proof-of-Work). For a survey of other consensus procedures, see [13]. These include PoA & PoAss. A few examples of blockchain parts include [9], [14], [15]:
•Cryptography: Super secure code that can only be accessed by authorized entities;
•Ledger: Data storage that is both communal and decentralized;
•Consensus: An anti-tampering technique for small nodes;
•Smart Contract: When this condition is satisfied, the relevant rules, fines, and actions will be implemented immediately.
Some of blockchain's most defining qualities and traits are: [3], [13], [14], [16]:
•Decentralization: P2P networks eliminate the requirement for a trusted third party by having participants (nodes) handle and evaluate data collectively;
•Trust-less: Participants need not be acquainted with one another to take part.;
•Anonymity: Each participant may have their own unique virtual identification code that can be used for communication;
•Permission-less: There's no constraint of participants;
•Autonomy: Transactions between nodes are secure and independent of any other parties.
•Ownership & uniqueness: In addition to the transactions that have occurred, a block also contains the block's owner & hash code;
•Irreversibly & Persistency: After block has been added to a blockchain, it is difficult to reverse a transaction.;
•Immutability: Controls & timestamps prevent tampering with saved information.;
•Transparency: Participants may see & track historical information;
•Auditability: Blockchain technology makes it possible to verify & trace transactions with greater security;
•Provenance: Every product now comes with its own unique digital fingerprint that verifies its legitimacy & provenance;
•Censorship resistant: Since a network has no central authority, it is impossible to restrict financial transactions;
•Open source: Everyone in the network has equal and unrestricted access to the original data. Not every quality is preferable. Because any user may initiate a transaction, the permission-less nature of the system opens the door to potential security risks. Who proves and validates blocks, who has access to the system, the degree of security and efficiency, the design methodologies, and the blockchain authority are all factors that might vary from one blockchain implementation

to the next [13]. With these options, we may categorize blockchains as public, private, or consortium (sometimes called permissioned or hybrid) blockchains.

AGRI-FOOD SUPPLY CHAIN AND TRACEABILITY:

The "activities from production through distribution that convey agricultural or horticultural goods from the field to the table" [2] constitute what is known as the "agri-food supply chain. "With so many different people and organizations involved, the agri-food supply chain is notoriously tough to manage. The storage life of agricultural goods is short. Time and surroundings, such weather and transportation, have an impact on the quality and safety of food. At any point, contamination is possible. Food recalls and the examination of food-borne diseases become more difficult as a consequence of the longer food chains brought forth by food globalization. Because of this complexity, we must work more effectively and with our partners. Concerns about transparency and trust may arise from the fact that traditional food supply chains sometimes depend on a third party to maintain information. For instance, a business may selectively provide information that would help them. Customers may not be able to independently verify many of the company's advertised food attributes. Because of the information gap that exists between the public and food producers in the wake of a food safety disaster, consumers may have less favorable opinions of the affected brands . As a solution to problems in food supply chain, traceability solutions are becoming more popular. Traceability is defined differently for different types of food, but according to ISO 22005:2007[19], it is " the capacity to track a feed or food item as it travels through a defined production, processing, & distribution chain." Even if the definitions are somewhat different, understanding the flow and stages of manufacturing might help with the recall of tainted goods, reassuring customers. Multiple stakeholders and their respective traceability needs allow for a systematic breakdown of the traceability into several categories. There might be only one stakeholder involved in the traceability (at the intra-company or internal level) or there could be several (at the supply chain or external level). Food safety and quality are the primary goals of voluntary traceability, whereas financial gain is the primary goal of mandatory traceability. Both required and voluntary traceability procedures are necessary for trustworthy and comprehensive traceability. The voluntary system is complicated with a large diversity of gathered data. This is because each stakeholder has different standards and tracking techniques. When designing a traceability system, considering four main questions: which data to gather, who owns the data, how to acquire the data, and how to make the data accessible and intelligible. The supply chain (at an external level) is the primary emphasis of this research. In particular, we're curious in the best practices for data collection and dissemination, both of which have an impact on and stand to gain from enhanced user interface design.

BLOCKCHAIN BASED AGRIFOOD TRACEABILITY:

Many academic institutions are beginning to use blockchain technology to improve traceability. It is believed that the blockchain would "provide transparency, boost information validity, as well as speed up food recall [9]". Dutta et al. [3] include 178 references in their analysis of the blockchain's use in the agricultural and food industries, demonstrating the technology's promise.traceability in agricultural or food supply chains using blockchain technology is also the subject of this article. Here, we analyze the existing literature reviews in field. Also, unlike previous reviews, we emphasize UI (i.e., how to collect data & how to render the data visible & intelligible).

RELATED WORK

M Iansiti and K. R. Lakhani [1]. Contracts, transactions, & documentation thereof are backbone of our economic system, yet they remain unchanged to match the digitization of world. They're like rush hour traffic snarling a Formula 1 racing car.

M. Blockchain technology may be the answer to this issue. Blockchain, the underlying technology of bitcoin, is a distributed, public ledger that verifies and records transactions quickly, reliably, and without human intervention. With blockchain, stock transfers, which may now take up to a week, might occur in seconds. The revolutionary potential of blockchain technology lies in its potential to reduce transaction costs and do away with middlemen like attorneys and banks. However, much like the widespread adoption of other internet technologies, blockchain adoption will take years and need extensive coordination. The authors of this piece lay out the future for blockchain technology and discuss how businesses should approach blockchain investments.

N. O. Ahumada & J. R. Villalobos[2], A lot of people have been thinking about the agricultural supply chain recently because of public health concerns. It is becoming clear that in the not-too-distant future, the planning and management of agricultural supply chains, especially those involving foods for human consumption, will be subject to stricter laws and tighter monitoring. In light of this, it's possible that established methods in the supply chain may need to evolve. The planning operations carried out in supply chains of agricultural goods are one facet that may be subject to extensive scrutiny. In this work, we sum up the most significant advances in the study of logistics for agriculturally based food production and delivery. The models that have already been effectively implemented are given special attention. Relevant characteristics are utilized to categorize models, including optimization techniques, crop types considered, and the breadth of plans. Based on our review of existing literature, we identify some of impending needs for modeling the agri-food supply chain.

P. Dutta, T.-M. Choi, S. Somani, & R. Butala [3], The secure, transparent, and auditable nature of the network is achieved through the collaborative functioning of blockchain's decentralized architecture, distributed ledger as well as storage mechanism, & asymmetric encryption. Blockchain technology has the potential to significantly transform supply chain (SC) services, ranging from enhancing provenance as well as restructuring company procedures to improving security

measures. There has been an increase in the quantity of scholarly articles examining the potential application of blockchain technology in supply chains. This study examines a total of 178 publications and conducts a comprehensive analysis of the extant literature pertaining to the integration of blockchain technology in supply chain operations. Our attention is directed towards the correlated opportunities, potential societal impacts, state-of-the-art technology, as well as significant trends and challenges. This study examines the potential of blockchain-based technologies to enhance transparency and facilitate efficient business process management across diverse sectors such as shipping, manufacturing, automotive, aviation, food, e-commerce, and education etc. In this paper, we create a future study agenda that will serve as a rock-solid basis for future studies in this promising new field of inquiry.
H. Feng, X. Wang, Y. Duan, J. Zhang, and X. Zhang [4], The role of traceability is of utmost importance in the management of food quality and safety. Conventional traceability systems within the realm of IoT offer viable solutions for monitoring traceability & quality of food supply chains. Nevertheless, the majority of IoT solutions heavily depend on the centralized server-client paradigm, which poses challenges for consumers in terms of obtaining comprehensive transaction information and effectively tracing the origins of products. The blockchain technology is an innovative and advanced solution that holds significant promise in enhancing the performance of traceability systems through its ability to ensure security and facilitate complete transparency. Nevertheless, the existing literature has not thoroughly examined the advantages, difficulties, and approaches to developing food traceability systems based on blockchain technology. Hence, the primary objective of this study is to examine the characteristics and functionalities of blockchain technology, ascertain the utilization of blockchain-based solutions in addressing concerns related to food traceability, emphasize the advantages and challenges associated with implementing traceability systems based on blockchain technology, and provide a framework for architecture design and an analysis flowchart to assist researchers and practitioners in the application of blockchain technology for food traceability systems. The findings of this research enhance comprehension and insight into enhancing food traceability through the development and implementation of traceability systems based on blockchain technology. This paper offers significant insights for both researchers and practitioners regarding the implementation of blockchain-based systems for managing food traceability. It demonstrates the positive impact of such systems on enhancing food sustainability.

PROPOSED SYSTEM

From the manufacturer's vantage point, the usage of blockchain technology aids in building brand loyalty and customer trust by making product details easily accessible and auditable. Businesses will be more successful if they are able to maximize the profit potential of their goods. This would make it more difficult for dishonest or low-quality producers to remain competitive, and it would put pressure on all producers throughout the agricultural and food industries to raise the bar on product quality. The blockchain provides consumers with accurate and trustworthy data on the production and exchange of food. It's useful for placating shoppers who fret about whether or not the food they buy is healthy for them and the planet. Since customers may have a more convenient and in-depth understanding of the food production process via the usage of blockchain, this opens up the prospect of interaction between consumers and producers. By lowering trade barriers, it helps customers feel more secure in the products they buy and the integrity of food supply chain. From standpoint of regulatory authorities, blockchain facilitates the availability of trustworthy and accurate data necessary for the effective implementation of well-informed legislation.From its initial production location to its final retail destination, blockchain technology can capture all of the relevant data about a product. It's a safe and permanent place to save information gathered at the beginning of the distribution chain, including the DNA traces of pesticides on grains and vegetables. Any participant in the product's supply chain has access to this data and may use it to verify the product's authenticity. It might be quite expensive to collect such information for all items, but it is possible to do so on samples. Blockchain technology has enabled a number of suggested solutions to increase the transparency of agricultural supply chains.

METHODOLOGY

The steps involved in getting food from farms to tables are as follows:
(i) Agricultural Bureau. To guarantee reliable information, this organization maintains tabs on farmers, seeds, plots, and harvests. the information is kept in IPFS (IPFS is a file sharing system that may be used to store and distribute huge files more effectively. Using cryptographic hashes which may be conveniently recorded on a blockchain, it achieves its aims. However, IPFS does not provide user-selected file sharing (and the blockchain stores just the hash value).
(ii) Farmer. He oversees the planting of crops and records data from sensors about the water, air, sunshine, and soil quality that affect their development. During the cultivation of crops, the farmer records his observations in IPFS. The farmer also has the added duty of creating smart contracts and maintaining hashes of IPFS data.
(iii) Processor. After harvesting, farmers sell their grain to processors, who turn it into finished goods for consumers while keeping track of production details in IPFS. A data hash is generated and added to the blockchain, while a data label is printed and attached to the product's packaging.
(iv) Quality Supervision Bureau. Its primary function is to inspect and regulate production facilities to ensure quality. All of these responsibilities contribute to upholding quality and standards laws and enforcing penalties for rule breakers.
(v) Distributor. The final product may pass through multiple channels of distribution before it reaches the store. The distributor is responsible for the bulk distribution of agriculturally processed goods to merchants. IPFS stores a variety of data, including company information, product sales timings, and pricing. Like the quality supervision bureau, hash value is recorded in blockchain so that data that follows cannot be altered.

(vi) Retailer. He buys in bulk from wholesalers and then sells merchandise to individuals. IPFS uses the blockchain to record some of the store's fundamental statistics. It keeps track of things like when things were sold, how many were sold, and a hash value.

(vii) Consumers. Consumers and eaters benefit from improved food monitoring since they can access comprehensive supply chain data simply by scanning a barcode, RFID tag, or QR code located upon product packaging.

Hash Function:

A hash is function which may encrypt data to required standards. Since hashes are always the same length, it is very difficult for an attacker to predict a hash and hence hack a blockchain. When hashing same data, the result is always the same. Among of mainstays of the blockchain infrastructure are hashes. Cryptographic hash function MD5 accepts a message of arbitrary length as input and outputs a message of fixed length (16 bytes). Message-digest algorithm, or MD5, is acronym for what it does. The goal of developing MD5 was to enhance security measures beyond those of MD4. MD5 always produces a 128-bit digest as its output.

MD5 algorithm follows as:

1. Append Padding Bits: First, we make sure the original message is a multiple of 512 by adding padding bits such that the final length is 64 bits less than 512.

Let's pretend someone has handed us a 1000-bit message to decipher. The original message needs some padding bits added. In this case, we need to pad original message by 472 bits. With the padding bits included, the first-step output message will have a size of 1472, or 64 less bits over a precise multiple of 512 (i.e. 512*3=1536).

Length (original message + padding bits) = 512 * i–64 wherein i=1,2,3…

2. Append Length Bits: To ensure final number of bits is exact multiple of 512, we now add the length bit from the first step's output. In this case, we simply increase the length bit in the first step's output to 64 bits.

i.e. 1st step output=512*n-64

length bits=64.

512 * n = exactly 512, hence the sum of the two is a multiple of 512.

3. Initialize MD buffer: In this case, we use a total of four buffers (J, K, L, and M). Every buffer is 32 bits in size.

- J = 0x67425301
- K = 0xEDFCBA45
- L = 0x98CBADFE
- M = 0x13DCE476

4. Processing Every 512-bit Block: MD5 algorithm relies on this stage to its greatest effect. In this case, there are a total of 64 procedures, spread throughout 4 iterations. It is planned to do 16 procedures in 1st round, 16 procedures in the second round, 16 procedures in the third round, and 16 procedures in the fourth round. The first round sees the application of F function, the second of the G function, the third of the H function, and the fourth of I function.

For mathematical purposes, we use the logical gates of OR, AND, XOR, and NOT. We use a total of three buffers—K, L, and M—for each operation.

- F(K,L,M) = (K AND L) OR (NOT K AND M)
- G(K,L,M) = (K AND L) OR (L AND NOT M)
- H(K,L,M) = K XOR L XOR M
- I(K,L,M) = L XOR (K OR NOT M)

After function has been applied, a further step is taken for each block. Operations need addition modulo 232.

M[i] – 32-bit message.

K[i] – 32-bit constant.

<<<n – Left shift by n bits.

\

Here we use J, K, L, and M as input to initialize the MD buffer. K's output will go into L, then M, and finally J. The next step is to do some calculations to get J's final result.

The first step is to take the results of executing K, L, and M & apply function F to them. For the output, we'll use J's modulo 232 addition.

We then combine the results of the first step with the M[i] bit message in the second.

Then, to the result of the second step, add a 32-bit constant, K[i].

Lastly, we do addition modulo 232 & left shift operation by n (where n is an arbitrary positive integer).

In the end, K will get the output from J. All three functions (G, H, and I) will now follow the exact identical procedure. In order to acquire our message digest, we need to do 64 separate procedures.

Output:

Once all iterations are complete, MD5 output begins at lowest bit J & ends with the highest bit M in the buffers J, K, L, and M.

System Architecture

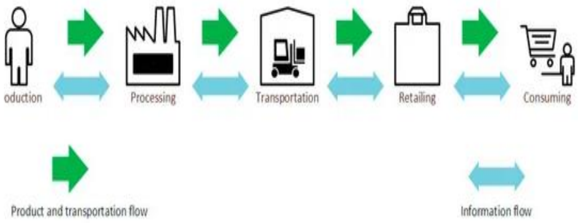

Figure 1: System Architecture

Implementation

Figure 2: Main Screen

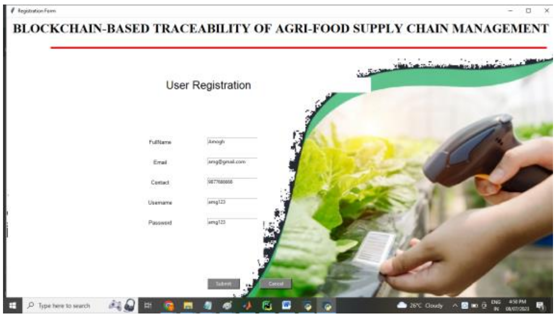

Figure 3

Figure 4 Add Batch

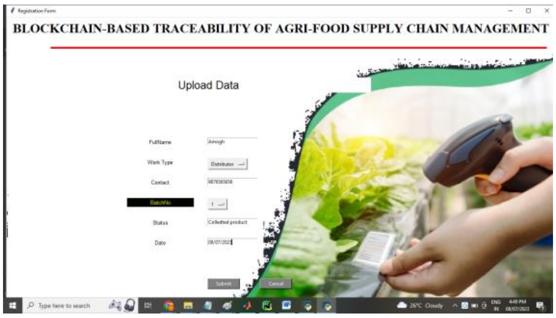

Figure 5: Upload data by Distributor

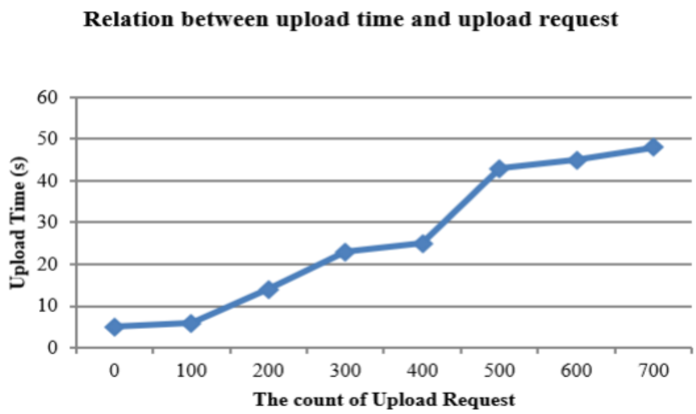

Figure 6: The Relation between Upload time and upload request

CONCLUSION

The capacity to track and identify a product of manufacturing or processing as it moves through the supply chain is what we mean when we talk about food traceability. Traceability refers to a product's ability to show its origins, such as the ingredients used in its creation or the steps it went through to get to the consumer's hands.

"Food Traceability is process of determining a product's provenance, application of components, and point of production."

REFERENCE

1. M. Iansiti and K. R. Lakhani. (2017). The Truth About Blockchain. [Online]. Available: https://hbr.org/2017/01/the-truth-about-blockchain
2. Ahumada and J. R. Villalobos, ''Application of planning models in the agri-food supply chain: A review,'' Eur. J. Oper. Res., vol. 196, no. 1, pp. 1–20, Jul. 2009. [Online]. Available: https://www.sciencedirect. com/science/article/pii/S0377221708001987
3. Dutta, T.-M. Choi, S. Somani, and R. Butala, ''Blockchain technology in supply chain operations: Applications, challenges and research opportunities,'' Transp. Res. E, Logistics Transp. Rev., vol. 142, Oct. 2020, Art. no. 102067.
4. H. Feng, X. Wang, Y. Duan, J. Zhang, and X. Zhang, ''Applying blockchain technology to improve Agri-food traceability: A review of development methods, benefits and challenges,'' J. Cleaner Prod., vol. 260, Jul. 2020, Art. no. 121031.
5. K. Demestichas, N. Peppes, T. Alexakis, and E. Adamopoulou, ''Blockchain in agriculture traceability systems: A review,'' Appl. Sci., vol. 10, no. 12, pp. 1–22, 2020.
6. Kamilaris, A. Fonts, and F. X. Prenafeta-Boldú, ''The rise of blockchain technology in agriculture and food supply chains,'' Trends Food Sci. Technol., vol. 91, pp. 640–652, Sep. 2019.
7. G. Zhao, S. Liu, C. Lopez, H. Lu, S. Elgueta, H. Chen, and B. M. Boshkoska, ''Blockchain technology in Agri-food value chain management: A synthesis of applications, challenges and future research directions,'' Comput. Ind., vol. 109, pp. 83–99, Aug. 2019.
8. J. F. Galvez, J. C. Mejuto, and J. Simal-Gandara, ''Future challenges on the use of blockchain for food traceability analysis,'' TrAC Trends Anal. Chem., vol. 107, pp. 222–232, Oct. 2018.
9. J. Duan, C. Zhang, Y. Gong, S. Brown, and Z. Li, ''A content-analysis based literature review in blockchain adoption within food supply chain,'' Int. J. Environ. Res. Public Health, vol. 17, no. 5, p. 1784, Mar. 2020.
10. C. Elsden, A. Manohar, J. Briggs, M. Harding, C. Speed, and J. Vines, ''Making sense of blockchain applications: A typology for HCI,'' in Proc. CHI Conf. Hum. Factors Comput. Syst., Apr. 2018, pp. 1–14, doi: 10.1145/3173574.3174032.
11. M. Foth, ''The promise of blockchain technology for interaction design,'' in Proc. 29th Austral. Conf. Comput.-Hum. Interact., Nov. 2017, pp. 513–517, doi: 10.1145/3152771.3156168.
12. C. S. Wright. (2019). Bitcoin: A Peer-to-Peer Electronic Cash System. [Online]. Available: https://bitcoin.org/bitcoin.pdf
13. Mistry, S. Tanwar, S. Tyagi, and N. Kumar, ''Blockchain for 5Genabled IoT for industrial automation: A systematic review, solutions, and challenges,'' Mech. Syst. Signal Process., vol. 135, Jan. 2020, Art. no. 106382.
14. M. Singh, A. Singh, and S. Kim, ''Blockchain: A game changer for securing IoT data,'' in Proc. IEEE 4th World Forum Internet Things (WFIoT), Feb. 2018, pp. 51–55.
15. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, ''Blockchain and IoT integration: A systematic survey,'' Sensors, vol. 18, no. 8, p. 2575, Aug. 2018.
16. M. Torky and A. E. Hassanein, ''Integrating blockchain and the Internet of Things in precision agriculture: Analysis, opportunities, and challenges,'' Comput. Electron. Agricult., vol. 178, Nov. 2020, Art. no. 105476.