iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** VII **Month of publication:** July 2020

DOI: https://doi.org/10.22214/ijraset.2020.30340

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VII July 2020- Available at www.ijraset.com

Implementation of Blockchain Technology in Food Supply Chain to Determine Authenticity

Dr. R. Sumathi[1], S. Akash[2], R. Amruth Shogul[3], Anirvan Vinod[4], R. Varssni[5]
[1]*Professor & Head Information Technology, Saranathan College of Engineering, Trichy, India*
[2, 3, 4, 5]*Information Technology, Saranathan College of Engineering, Trichy, India*

Abstract: ***The food supply chain is the most complex and fragmented of all supply chains. The production is found all over the world both on land and in water. A lot of the producers and intermediaries are difficult to identify and track. For all the participants in the production chain this creates uncertainty and risk. Mitigating this uncertainty comes at a cost, and the outcome may still be insufficient. Examples of problems that have been difficult or impossible to solve with current technologies include establishing reliable provenance and preventing fraud and counterfeiting. These issues can have knock-on effects on public health and the environment, and reduce financial costs of unnecessary recalls of food products. Due to the growing need of authenticity and transparency, we propose a Blockchain inspired architecture for creating a transparent food supply chain (FSC) which would assist the customers in validating the authenticity of a particular product which they intend to buy. The Blockchain architecture makes use of a proof-of-object based authentication protocol, which is completely analogous to the proof-of-work protocol in the Cryptocurrency genre. We will be making use of the sensor data from different RFID sensors, QR codes gathering the sensor data and feeding it to the Blockchain. The sensor would be integrated on the physical layer of the particular product. RFID and QR provides us with the unique identification of the product data. The Blockchain architecture aids in creating a tamper-proof environment which would contain the database of the food packages at each instance. We hope to implement this on a variety of food products which are available in the market and hope to reduce any kind of intentional or unintentional damages caused to the product before reaching the hands of the customer.***

Index Terms: Blockchain, QR, RFID, Supply Chain

I. INTRODUCTION

Blockchain has huge potential to impact global Medical Product supply chain (MPSC) by increasing productivity in terms of supply chain performance. Among many challenges the United States Centre for Diseases Control (CDC) estimates that 48 million people get sick from expired medical product usage, 128,000 are seriously hospitalized, and 3,000 die each year in the U.S. alone.

Apart from illness, economically and criminally motivated Medical Product adulteration is also a growing concern due to globalization and wide growing supply chain networks. Real-time monitoring of the medical product quality and visibility of that quality index would prevent outbreak of food-borne illnesses, economically motivated adulteration, contamination, food wastage due to misconception of the labelled expiry dates, and losses due to spoilage, which have broad impacts on the medical product security. In order to improve safety and prevent wastage, modern Blockchain based technologies are required to monitor the Medical product quality and increase the visibility level of the monitored data. There are a number of Block Chain based tracking and tracing infrastructures such as Electronic Article Surveillance (EAS), Radio Frequency Identification (RFID), and QR codes which are primarily targeted for automatic package level tracking. However, the role of these technologies is limited in identifying the medical product package and does not provide any information pertaining to the state of the Medical product quality. This limitation prevents quick removal of a defective product from reaching higher levels of the MPSC. For example, when a quality control lapse is identified along the MPSC, the company is forced to recall all the Medical products within a certain time frame leading to a huge economic loss, which can be mitigated with the availability of individual Medical Product package quality information resulting in targeted recalls. In literature, a number of sensing techniques compatible with existing tracking and tracing infrastructure are proposed for monitoring the various kinds of medical products. Also, the medical products can be invasive or non-invasive in monitoring the physical or chemical properties of medical products such as pH, conductivity, and permittivity or the packaging environment such as temperature, humidity, moisture or aroma. In general, these are aimed to prevent defective products from reaching the consumers. Furthermore, these sensors help in identifying key bottlenecks in the MPSC to improve the overall efficiency. Currently, little work has been done in integrating these to the tracking and tracing infrastructures. Moreover, the collected tracking as well as sensing data is more centralized and selectively used by specific entities of the MPSC.

©IJRASET: All Rights are Reserved

The consumers have to trust the quality of the product based on the printed expiry date without any additional knowledge of its current quality. To move beyond a "traceability-centric" or "income-centric" to a "value-centric" supply chain, a more decentralized approach is needed in terms of data sharing. However, a trade off exists between providing sufficient information to the consumer about an individual product and at the same time safe guarding the operational privacy of the MPSC. Blockchain has emerged as a decentralized public consensus system that maintains and records transactions of events that are immutable and cannot be falsified. Blockchain technology has attracted attention beyond crypto currency due to its ability to provide transparent, secure, and trustworthy data in both private and public domains. The technology is based on a distributed ledger, which is not owned or controlled by a single entity. Data in the public ledger is visible publicly and any authorized entities can submit a transaction, which is added to the Blockchain upon validation. The advantage of Blockchain technology can be applied in MPSC to improve the digital data integrity which is obtained as the product passes through different entities of the MPSC. The complete medical product visibility across different entities of the supply chain can become a reality with the integration of sensor based Blockchain technology data management systems. The key benefits of applying Blockchain technology in MPSC are: real time tracking and sensing of Medical products throughout the MPSC, and allowing identification of key bottlenecks; Discouraging adulteration of Medical products, and identifying weak links on occurrence; determining the shelf life of Medical products leading to reduced waste; providing end to end information to the consumer; and allowing specific and targeted recalls. A test prototype of the Unique ID is integrated are demonstrated experimentally in this work. The Unique ID integrated can be attached to a food package to extract information regarding the package along MPSC.

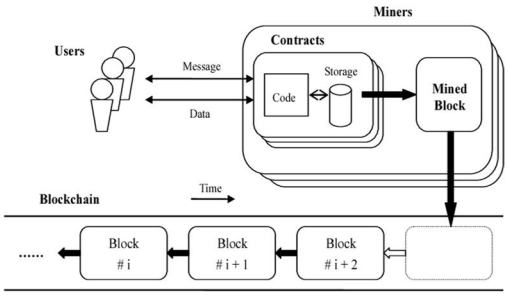


Fig. 1 Mechanism of Blockchain

II. CHARACTERISTICS OF BLOCKCHAIN TECHNOLOGY

The analysis of public blockchains has become increasingly important with the popularity of bitcoin, Ethereum, Litecoin and other cryptocurrencies. A blockchain, if it is public, provides anyone who wants access to observe and analyse the chain data, given one has the know-how. The process of understanding and accessing the flow of crypto has been an issue for many cryptocurrencies, crypto-exchanges and banks. The reason for this is accusations of blockchain enabled cryptocurrencies enabling illicit dark market trade of drugs, weapons, money laundering etc. A common belief has been that cryptocurrency is private and untraceable, thus leading many actors to use it for illegal purposes. This is changing and now specialised tech-companies provide blockchain tracking services, making crypto exchanges, law-enforcement and banks more aware of what is happening with crypto funds and fiat crypto exchanges. The development, some argue, has led criminals to prioritise use of new cryptos such as Monero. The question is about public accessibility of blockchain data and the personal privacy of the very same data. It is a key debate in cryptocurrency and ultimately in blockchain.

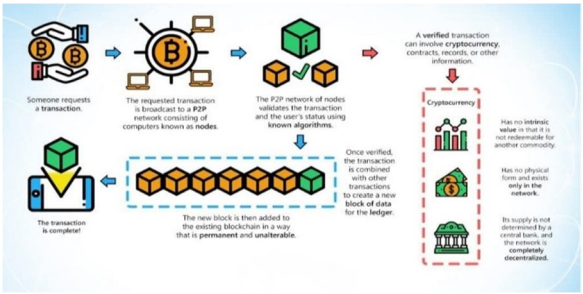


Fig. 2 Blockchain in Cryptocurrency

©IJRASET: All Rights are Reserved

A. Blocks

Blocks hold batches of valid transactions that are hashed and encoded into a Merkle tree. Each block includes the cryptographic hash of the prior block in the blockchain, linking the two. The linked blocks form a chain. This iterative process confirms the integrity of the previous block, all the way back to the original genesis block. Sometimes separate blocks can be produced concurrently, creating a temporary fork. In addition to a secure hash-based history, any Blockchain has a specified algorithm for scoring different versions of the history so that one with a higher score can be selected over others. Blocks not selected for inclusion in the chain are called orphan blocks. Peers supporting the database have different versions of the history from time to time. They keep only the highest-scoring version of the database known to them. Whenever a peer receives a higher-scoring version (usually the old version with a single new block added) they extend or overwrite their own database and retransmit the improvement to their peers. There is never an absolute guarantee that any particular entry will remain in the best version of the history forever. Block chains are typically built to add the score of new blocks onto old blocks and are given incentives to extend with new blocks rather than overwrite old blocks. Therefore, the probability of an entry becoming superseded decreases exponentially as more blocks are built on top of it, eventually becoming very low. For example, bitcoin uses a proof-of-work system, where the chain with the most cumulative proof-of-work is considered the valid one by the network. There are a number of methods that can be used to demonstrate a sufficient level of computation. Within a blockchain the computation is carried out redundantly rather than in the traditional segregated and parallel manner.

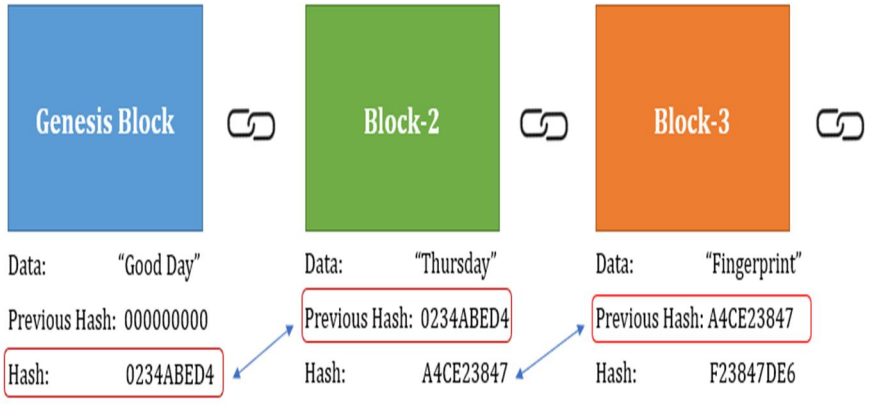


Fig. 3 Blocks

B. Decentralization

Storing data across its peer-to-peer network, the blockchain eliminates a number of risks that come with data being held centrally. The decentralized blockchain may use ad hoc message passing and distributed networking. Peer-to-peer blockchain networks lack centralized points of vulnerability that computer crackers can exploit; likewise, it has no central point of failure. Blockchain security methods include the use of public-key cryptography. A public key (a long, random-looking string of numbers) is an address on the blockchain. Value tokens sent across the network are recorded as belonging to that address. A private key is like a password that gives its owner access to their digital assets or the means to otherwise interact with the various capabilities that blockchains now support. Data stored on the blockchain is generally considered incorruptible.

Every node in a decentralized system has a copy of the blockchain. Data quality is maintained by massive database replication and computational trust. No centralized "official" copy exists and no user is "trusted" more than any other. Transactions are broadcast to the network using software. Messages are delivered on a best-effort basis. Mining nodes validate transactions, add them to the block they are building, and then broadcast the completed block to other nodes. Blockchains use various time-stamping schemes, such as proof-of-work, to serialize changes. Alternative consensus methods include proof-of-stake. Growth of a decentralized blockchain is accompanied by the risk of centralization because the computer resources required to process larger amounts of data become more expensive.

©IJRASET: All Rights are Reserved

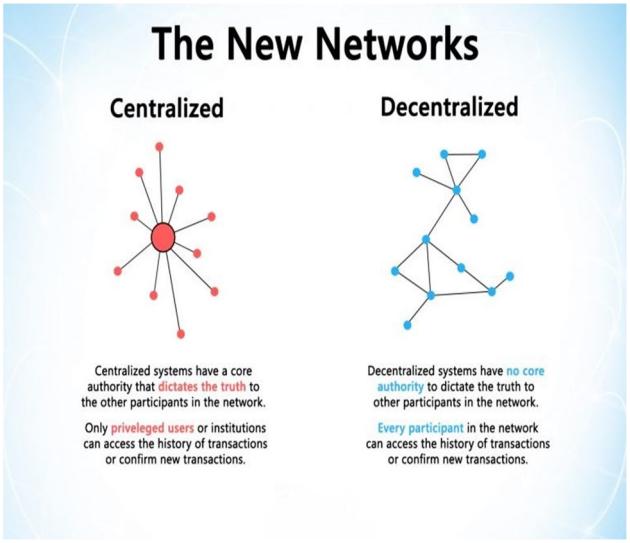


Fig. 4 Decentralization

C. Openness

Open blockchains are more user-friendly than some traditional ownership records, which, while open to the public, still require physical access to view. Because all early blockchains were permission less, controversy has arisen over the blockchain definition. An issue in this ongoing debate is whether a private system with verifiers tasked and authorized (permissioned) by a central authority should be considered a blockchain. Proponents of permissioned or private chains argue that the term "blockchain" may be applied to any data structure that batches data into time-stamped blocks. These blockchains serve as a distributed version of multiversion concurrency control (MVCC) in databases. Just as MVCC prevents two transactions from concurrently modifying a single object in a database, blockchains prevent two transactions from spending the same single output in a blockchain. Opponents say that permissioned systems resemble traditional corporate databases, not supporting decentralized data verification, and that such systems are not hardened against operator tampering and revision. Nikolai Hampton of Computerworld said that "many in-house blockchain solutions will be nothing more than cumbersome databases," and "without a clear security model, proprietary blockchains should be eyed with suspicion."

D. Permission Less

The great advantage to an open, permission less, or public, blockchain network is that guarding against bad actors is not required and no access control is needed. This means that applications can be added to the network without the approval or trust of others, using the blockchain as a transport layer. Bitcoin and other cryptocurrencies currently secure their blockchain by requiring new entries to include a proof of work. To prolong the blockchain, we need to understand that bitcoin makes use of Hashcash puzzles. While Hashcash was designed in 1997 by Adam Back, the original idea was actually first proposed by software engineers Cynthia Dwork and Moni Naor and Eli Ponyatovski in their 1992 paper "Pricing via Processing or Combatting Junk Mail".

III. EXISTING SYSTEM

With regard to the various engineers and developers in the food supply chain industry and the various authors who have developed the architecture for the existing Food Supply chain management system is totally based on the web-based architecture of the products where all the details of the food products are based on the cloud architecture with a centralised middleman server to regulate and authenticate the various operations to be performed. The cloud enabled Food Supply Chain Management System is also not very secure since it cannot promise the consumers an end to end security because various middlemen are involved. In supply chain management, FSC is considered complex and complicated due to its environmentally sensitive nature and the presence of shelf life. Supply chain interested parties and end customers pay close attention to information regarding products, shipment information, and environmental monitoring, to minimize the processing and transportation of unsafe and poor-quality products. This can reduce impact from adverse publicity, liability, and recalls. Therefore, traceability systems play a crucial role with significant values in the FSC. To establish a Food product traceability system, TRUs should be well defined for building a complex traceability

©IJRASET: All Rights are Reserved

tree. There are three major components for system implementation: identification of TRUs, attributes of TRUs, and documentation of transformations. The identification of TRUs and transformations in traceability systems require further improvements. Therefore, reliability, information accuracy, and traceability efficiency can be further secured and enhanced, and decision support in FSC can be obtained beyond monitoring and data management. To improve Food product traceability systems, Block chain technology is deemed promising for interconnecting products, shipment journeys, order information, and environmental control.

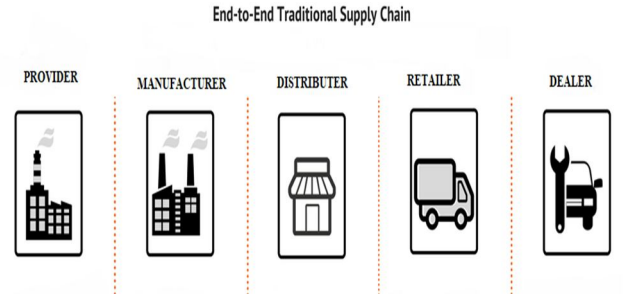


Fig. 5 Traditional Supply Chain

A. Disadvantages

It has a great lack in digitalization and weak supporting systems also including the lack of connectivity, particularly with upstream suppliers. Coordinating process and digital transformation across multiple, disbursed, and often disconnected supply chain actors. Onerous and costly data reconciliation. Ineffective solutions for handling large amounts of disparate and potentially inconsistent data.

IV. PROPOSED SYSTEM

While keeping in mind the various efforts of the developers of the traditional food supply chain unit, we have to understand that they might not have fully considered the possibility of taken into account the need for transparency of the transactions performed between the various parties involved in the food supply chain unit. We have also identified a few modules which make use of the blockchain technology. The blockchain is a new set of tools for digitization. The reason blockchain technology is interesting is that there are certain functions that are very valuable for the digital world that hasn't been invented before the blockchain. We also make use of the IOT and the Blockchain by the data collecting and processing node, that scans a secret code is termed as a 'terminal'. The common network shared by all the terminals is termed as 'shared network'. The scan of a secret ID by a terminal and enlisting the data is termed as a 'transaction'. Once a transaction is validated based on the consensus of participating terminals, the transaction is converted into a 'block' and included in the Blockchain. Apart from terminals, there exists another type of node, a 'manager', that is responsible for policy making and processing requests based on consensus with other nodes. Finally, there exists a third type of node, called 'agent', that requests information about a secret ID from the blockchain by providing a proper cyber address. 'Address collision' is referred to the existence of a minimum of two identical cyber or physical addresses. A typical Food product-based supply chain is each packaged food product with an embedded secret ID travels through multiple stages of transactions at different terminals starting from packaging through transportation, storage and finally to a consumer for purchase. A data block is created containing the information about the package at each valid transaction. Once the transaction is verified, the transaction of the secret ID is converted into a block of information and appended to its pre-existing data blocks thus forming a chain of information blocks and thus a Blockchain.

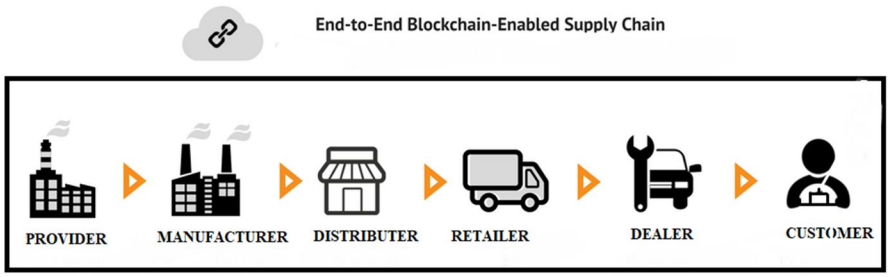


Fig. 6 Blockchain Supply Chain

©IJRASET: All Rights are Reserved

A. Advantages

1) Faster locating stock
2) Lower labour requirement
3) Reduction of out-of-stock
4) Decrease in lost stock
5) Faster locating stock
6) Lower labour requirement
7) Reduction of out-of-stock
8) Low safety stock level
9) Low barriers to entry
10) Low safety stock level
11) Low barriers to entry
12) Digital units impossible to copy
13) Digital files that can't be manipulated

V. SYSTEM ARCHITECTURE

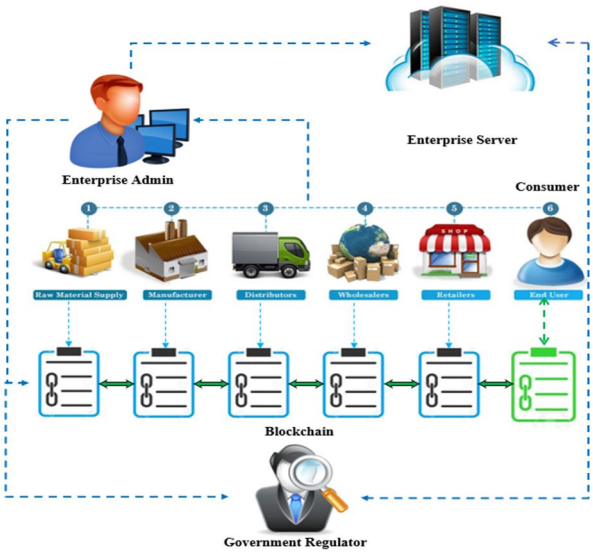


Fig. 7 System Architecture

From the proposed system and the system architecture given above, we have identified a few modules which can form the basis of the enterprise solution we are developing which can be of help to the various organizations in the food supply chain industry. The main needs of enterprises in the food data shared supply chain are: 1) the specific accessibility of them on the blockchain must be assured to prevent the leakage of sensitive information and to provide confidentiality. 2) The maintenance cost of blockchain system should be appropriately controlled. Only by satisfying the above needs will this system truly benefits enterprises.

A. Consumer

For consumers, the most basic and essential requirement of the system is to provide traceability for the product they purchased. The characteristic of data according to the demand of consumer ought to be tamper-proof as well as confidential. Additionally, the system needs to be available for the public by the concise and low-cost design.

B. Government Regulator

As for the demand of government regulators, we should provide highest accessibility to them to monitor all data on the traceability system in order that they can pinpoint the culpable sector as soon as possible once the food safety event occurs. Also, they should have capability to ensure that all data uploaded by the enterprise is legal and verified.

©IJRASET: All Rights are Reserved

VI. INFORMATION CAPTURE MODULES

This module is designed to collect key traceability information brought forth by the process of production, storage, circulation of food. It can work automatically and manually to identify and create detailed event information from the circulation of food in the supply chain.

A. Information Extraction Module

This module is primarily devised for extracting information that needs to be uploaded on blockchain from the traceability information database as well as preparing the data for the uploading.

B. Blockchain Module

Blockchain module has two functions. One is the data interaction including the upload of key traceability information on blockchain, the request of on-chain information and the verification of event information. The other is to provide options for users to be the full blockchain node or the light-weight blockchain node i.e. to decide whether or not to participate in the maintenance of the blockchain.

C. Interaction Authority Management Module

This module is in charge of the verification of enterprise identity when there is any event information interaction i.e. to determine whether the requester who initiates the request for event information is in this supply chain.

D. Consumer Traceability Client

1) *Blockchain Module:* This module is designed for the link between the client and system, through which it can request information on the blockchain and verify the legitimacy of the information. A light node is chosen for this module to lower user's maintenance cost.

VII. CONCLUSION

A Blockchain based FSC monitoring architecture has been proposed in this work. Sensing modality was integrated with identification with a small footprint for tracking and quality monitoring of the Food product packages. When the Food Product packages are scanned at different retailers, logistics or storage stage within the supply chain, the real time sensor data is updated in a blockchain providing a tamper-proof digital history. Any consumer or retailer can check the public ledger to obtain information regarding the specific Food product packages. The information helps in updating the shelf life, identifying key bottlenecks in the FSC, implementing targeted recalls and moreover increasing visibility. A single secret ID integration was demonstrated in this work. The proposed architecture takes consensus from participating terminals in the network before updating the blockchain data. The broader participation of all the nodes helps to keep the network decentralized. The security analysis showed that the validation of a fake block drops with a higher number of node participation in the network and multiple consensus stages.

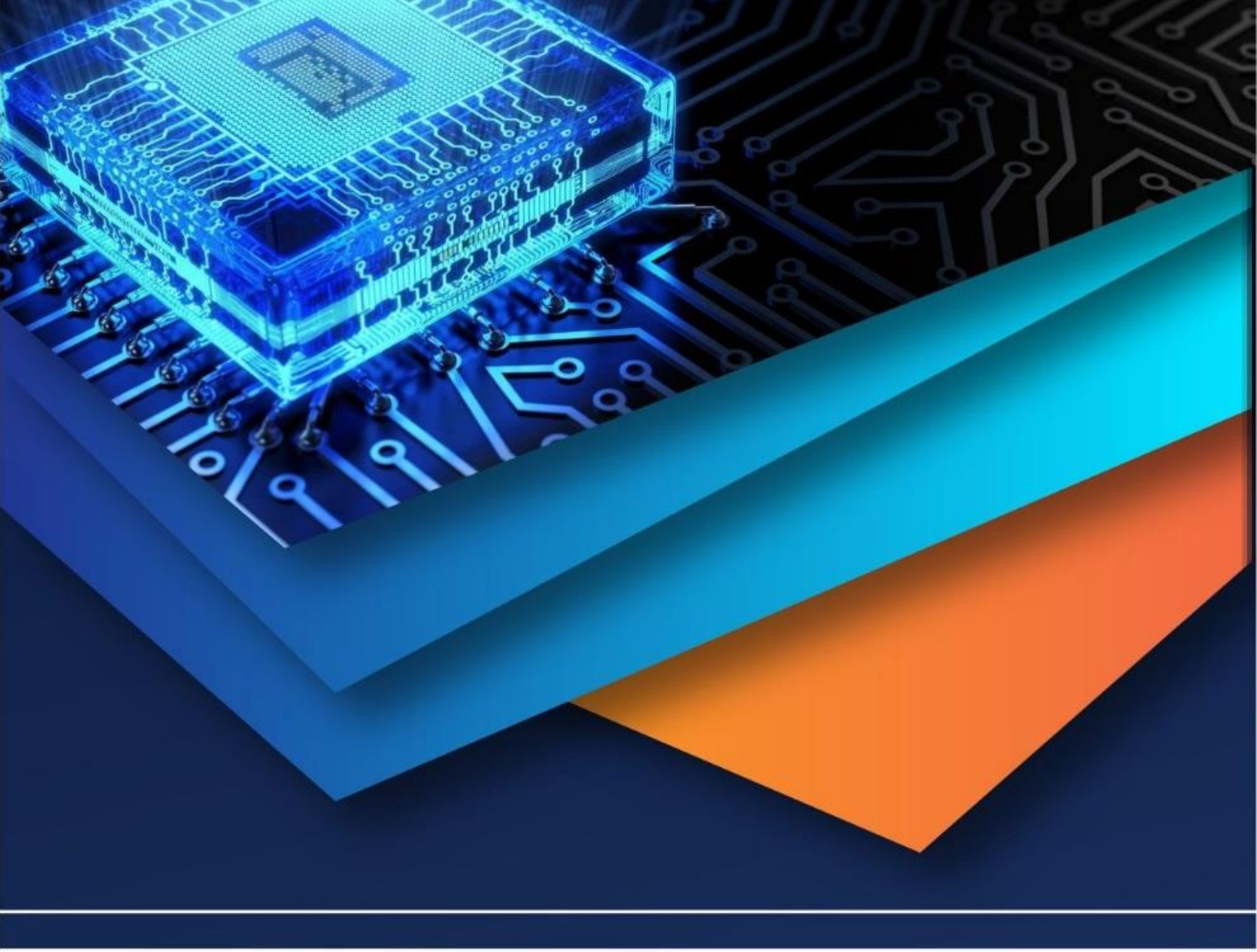
REFERENCES

[1] M. M. Aung and Y. S. Chang, ``Traceability in a food supply chain: Safety and quality perspectives," *Food Control*, vol. 39, pp. 172_184, May 2014.
[2] T. Bosona and G. Gebresenbet, ``Food traceability as an integral part of logistics management in food and agricultural supply chain," *Food Control*, vol. 33, no. 2, pp. 32_48, 2013.
[3] J. Hobbs, ``Liability and traceability in agri-food supply chains," in *Quan- tifying the Agri-Food Supply Chain*. Springer, 2006, pp. 87_102.
[4] D. Mao, Z. Hao, F. Wang, and H. Li, ``Novel automatic food trading system using consortium blockchain," *Arabian J. Sci. Eng.*, vol. 44, no. 4, pp. 3439_3455, Apr. 2018.
[5] L. U. Opara and F. Mazaud, ``Food traceability from _eld to plate," *Outlook Agricult.*, vol. 30, no. 2, pp. 239_247, 2001.
[6] F. Dabbene and P. Gay, ``Food traceability systems: Performance evaluation and optimization," *Comput. Electron. Agricult.*, vol. 75, no. 2, pp. 139_146, 2011.
[7] J. Storoy, M. Thakur, and P. Olsen, ``The TraceFood framework_ Principles and guidelines for implementing traceability in food value chain," *J. Food Eng.*, vol. 115, no. 2, pp. 41_48, 2013.
[8] M. A. Khan and K. Salah, ``IoT security: Review, blockchain solutions, and open challenges," *Future Gener. Comput. Syst.*, vol. 82, pp. 395_411, May 2018.
[9] L. Lucas. Financial Times. (2018). *From Farm to Plate, Blockchain Dishes Up Simple Food Tracking*. Accessed: Jun. 12, 2018. [Online]. Available: https://www.ft.com/content/225d32bc-4dfa-11e8-97e4-13afc22d86d4
[10] A. Bogner, M. Chanson, and A. Meeuw, ``A decentralised sharing app running a smart contract on the Ethereum blockchain," in *Proc. 6th Int. Conf. Internet Things*, 2016, pp. 177_178.
[11] K. Salah, M. Rehman, N. Nizamuddin, and A. Al-Fuqaha, ``Blockchain for AI: Review and open research challenges," *IEEE Access*, vol. 7, pp. 10127_10149, 2019.

©IJRASET: All Rights are Reserved

[12] H. Hasan and K. Salah, ``Combating deepfake videos using blockchain and smart contracts," *IEEE Access*, vol. 7, no. 1, pp. 41596_41606, Dec. 2019.
[13] R. Beck, J. S. Czepluch, N. Lollike, and S. Malone, ``Blockchain-the gateway to trust-free cryptographic transactions," in *Proc. ECIS*, May 2016, p. 153.
[14] M. E. Peck, ``Blockchains: How they work and why they'll change the world," *IEEE Spectr.*, vol. 54, no. 2, pp. 26_35, Sep. 2017.
[15] https://www.semanticscholar.org/paper/A-supply-chain-traceability-system-for-food-safety-Tian/304083f2a7b00d07d7c33883e2e74ac0fd8245c5
[16] https://blockgeeks.com/guides/what-is-blockchain-technology/
[17] https://medium.com/swlh/blockchain-characteristics-and-its-suitability-as-a-technical-solution-bd65fc2c1ad1
[18] https://blockgeeks.com/guides/what-is-blockchain-technology/
[19] https://blog.futurefoundry.in/a-use-case-on-blockchain-enabled-supply-chain-79615efce6e0

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)