Secure Agro-Food Supply Chain Traceability using Block Chain And IPFS

Mr. A.Rajeshkumar , Dr. N. Sathyabalaji

Abstract— "To address several issues with traditional traceability systems, many blockchain initiatives have adopted the Inter Planetary File System (IPFS) for storing user data off-chain. These issues include centralized administration, ambiguous data, unreliable data, and the ease of creating information islands. In this study, to developed a monitoring system that leverages blockchain technology to record and inquire about product information within the Non-Perishable (NP) agro goods supply network. By harnessing the distributed, tamper-proof, and traceable properties of blockchain technology, to significantly enhance the transparency and trustworthiness of traceability data. To ensure efficient information retrieval without overloading the blockchain, established a storage structure that stores both public and private data using cryptography in both the blockchain and the Inter Planetary File System (IPFS). This approach not only helps trace the origin of food but also contributes to the development of reliable food supply chains and fosters trust between farmers and their customers. Additionally, it provides a secure repository for data, facilitating the adoption of data-driven farming techniques. Furthermore, by recording farm data in IPFS and storing encrypted IPFS file hashes in smart contracts; to address the issue of blockchain storage expansion. When combined with smart contracts, this setup enables instantaneous transactions between parties in response to changes in blockchain-stored data. In this paper also includes simulations that assess the implementation's performance. The results validate that our system enhances security for sensitive information; safeguards supply chain data, and meets the demands of real-world applications. Moreover, it improves throughput efficiency while reducing latency."

Keywords— Blockchain; IPFS; supply chain management; traceability; Ethereum

I. INTRODUCTION

Everyone is concerned about the nutritional value of the meal they are about to consume. The food supply chain is prevalent, with tedious processes prone to human errors [1]. A blockchain-based supply chain can offer visibility into the movement of commodities by making all transaction records accessible to all network nodes. End-to-end traceability is another feature of the blockchain-enabled food supply chain technology that is helpful in the case of a food investigation or recall. Supply chain management combines actions to transform raw materials into completed goods, increasing customer value and achieving a long-term competitive advantage. The supply chain generally encompasses people, things, initiatives, and organizations involved in transforming raw materials into finished goods, mainly and secondary to fulfilling customer orders. Although the government has developed national traceability requirements for significant products, fake and subpar interests are still common in the marketplace. Thus, several issues with food security have led to a crisis in consumer confidence, which is also a significant obstacle to national efforts to build a trustworthy society [2].

NP agro-food monitoring program can determine food origin and provide detailed information about food production and distribution. The farm-to-table process includes the production, processing, transportation, and sale of agricultural products. Any fraud in any of the connections above can result in potentially fatal threats to food safety. Therefore, various management solutions have arisen with IoT, automation, and different learnings. These systems can trace the complete procedure autonomously, but they must solve the problem of altered data and food poisoning. The reason for this is that in the conventional data storage procedure, there is always the risk of data being tampered with or lost. Researchers have been experimenting with blockchain technology to store data and protect data security by addressing the issues above [3]. It develops a blockchain-based system for storing agricultural product provenance data. Due to their linkage to IoT devices, agricultural items will automatically transmit whatever data they collect to a network.

Once again, the server will dynamically record the information onto the blockchain following data processing. In this instance, provenance data secure storage is implemented using blockchain technology. As a result, it successfully ensures the authenticity of provenance data. A lot of real-time monitoring data would be produced when many agro items joined the provenance monitoring platform. Blockchain was initially developed for transactions involving digital currencies; the volume of data generated is far less than that of real-time monitoring data. This makes it extremely difficult for the rate of block construction to stay consistent with storing traceability information. Thus, more than a direct application of blockchain technology is needed. We merge the IPFS and blockchain to offer a data storage and query method for a traceability solution for farm products. IPFS is a peer-to-peer decentralized file system with the ambitious goal of connecting all devices that use computers to a single, universal file system. It first suggests a data storage model based on

Mr. A. Rajeshkumar., Department of Computer Science and Engineering, JKK Munirajah College of technology, Erode, Tamilnadu 608 506, India (Email Id: rajeshak276@gmail.com)

Dr. N. Sathyabalaji M.E., M.I.S.T.E., Ph.D., Associate Professor, Department of Computer Science and Engineering, JKK Munirajah College of technology, Erode, Tamilnadu 608 506, India (Email Id : sathyabalajin@gmail.com)

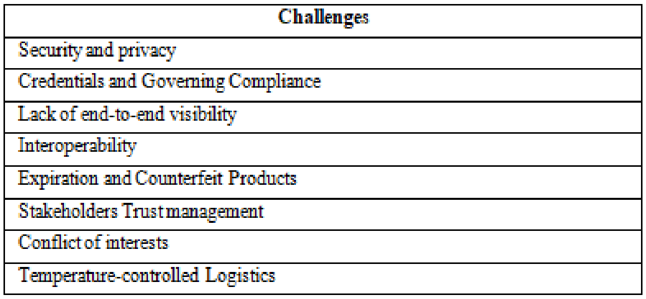
blockchain and IPFS [4]. The submitted video, picture, and sensor data are automatically encapsulated and parsed by this model. The above information is then sent to IPFS, and the blockchain is updated with the associated hash addresses. The blockchain transaction's hash values are then saved in the database. By requesting the authenticity database hash address of an item in IPFS, customers can access the provenance data using the transaction content from the blockchain.

The article is divided into the following sections: Section II provides a quick review of blockchain technology and terminology, stages, methods, and benefits of traceability. Section III also discusses previous initiatives to incorporate blockchain into provenance systems. Section IV describes a modeling approach that has been presented. Section V goes through the outcomes and performance. Section VI brings the paper to a conclusion.

II. BLOCKCHAIN FOR TRACEABILITY

Blockchain technology can offer improved tracking of agri-foods from the ranch to your dinner plate. Blockchain technology might greatly minimize the food safety concerns arising from deliberate deception, terrible organization, and being short of guidelines. [5] Blockchain technology will revolutionize how traceability is viewed by overcoming the challenges in Table I.

TABLE I. CHALLENGES IN TRACEABILITY SYSTEM



Challenges
Security and privacy
Credentials and Governing Compliance
Lack of end-to-end visibility
Interoperability
Expiration and Counterfeit Products
Stakeholders Trust management
Conflict of interests
Temperature-controlled Logistics

Merkle tree is called a leaf, a separate data item or record. A cryptographic hash function H (), is used for evaluating a leaf of X records which in turn has a 2X −1 inner node. A tree with X = 2y nodes has a complexity of y = log X. Also, a single unique root at height y = 0 is the source of the entire hierarchical tree. The claim that the root value Ŕ encapsulates the correctness of all the entries in the tree constitutes a statement made to the entirety of the tree. Conforming to each child n at height y', Z forms a collection of y'' systems on the whole hierarchy.

$Á = H(n, Z)$ (1)

where, HFt is a succession of y' hash function H(.)calculations. The entire Merkle hash tree is stored by an untrustworthy party to prove, whereas a verifier only stores the root Ŕ. The party attempting to verify the authenticity of node n provides Z for each node in the tree. Given,

$Á = Hf(m, Z)$ (2)

Eq. (2) concludes that statement n∈Ŕ, where n is the existing root. Knowing the present Ŕ, a steady improvement state occurs from Ŕ towards R = Hft (m', Zm) every time the current node m reorganized to m'.

Hashing

For a continuously increasing value, m=α0, α1, αn, a hash function h(.) is applied. This results from a declaration Ḡ called Gatherer Hash (GH) to the progression. The process to get nth hash gatherer Ḡn is given in eq. (3),

$0 = h(\, a0), \beta 1$

$= h(\beta \parallel a1) \ldots \beta n \,,$

A. *Functioning of Blockchain*

The digital register is a "link" of unique "blocks" information. As new data is added to the network, a new block is created and linked to the chain. To maintain consistency, all nodes (computers) must update their versions of the blockchain ledger. One of the elements that make blockchain so highly secure is the process of adding new blocks [6]. This is due to the requirement that a participating node verifies and validate the validity of new data well before a new node can be recorded to the blockchain. About crypto currencies, this can mean proving that brand-new transactions within a block are legitimate and that no coins have been spent more than once.

On the other hand, a single database or worksheet permits revisions to a single version without restriction. Once consensus is reached, the block is added to the ledger, and the underlying records are kept in the distributed ledger [7]. Blocks are safely joined together to form a secure digital chain that extends from the start of the log to the latest addition. Nodes are frequently given fresh amounts of the native currency of the blockchain in appreciation for their work confirming revisions to the linked data.

B. *Merkle Tree*

The Merkle binary hash tree of 1987[8] is an essential component of the Blockchain structure. Each node of the

$= h(\beta n - 1 \parallel an - 1)$(3)

Also, a cryptographic hash function's h () attribute assures that determining any sequence of numbers other than α0, α1... αn that yields the current GHβn is unfeasible.

C. *IPFS*

Despite multiple attempts to develop distributed file structures, IPFS has been the initial universal storage structure to achieve high throughput and autonomous delivery on a global scale and on the system level. Peer-to-peer (P2P) networks and blockchain technology allow secure information sharing without a central organization. Inter Planetary File System may replace HTTP (Hyper Text Transfer Protocol). IPFS is a persistent, open-source data storage system. It's used by many to exchange content efficiently. IPFS distributes files throughout the network and uses their cryptographic hashes to identify each item based on its content. IPFS stores file off-chain while referencing blockchain hashes [9]. While IPFS incorporates useful concepts from earlier peer-to-peer systems, its primary contribution is in streamlining, advancing, and integrating tried-and-true methodologies into a single coherent system that is more effective than the sum of its parts [10]. The IPFS constructs an algorithmically authorized data model on top of these, a Merkle Directed Acyclic Graph (DAG) of permanent objects, to aid in effectively disseminating files and file version control. Git13 is a popular system for managing file revisions and distribution. Content addressability, tamper resistance, and deduplication are all provided by the core IPFS principles [11]. Additionally, the IPFS implements the Inter Planetary Linked Data (IPLD) standards to produce more adaptable, flexible, decentralized data structures that are globally addressable and linkable for many types of data. The Interplanetary Way back is a persistent Web archive that distributes data files into the IPFS network [12]. The CDXJ index is built, and then IPFS is used to disperse the response records' headers and payloads independently. The method has the potential to speed up indexing generally.

III. RELATED STUDY

To solve the problem of the blockchain's lack of significant data storage, Yang et al. [13] employed Hyperledger as the provenance link that processes the database. Its disadvantages over IPFS data storage include expensive costs, a slow rate of data movement, inadequate privacy, and so on. Additionally, it needs a feedback feature for the customer, preventing retailers from initially accessing the information on product security and other factors. Liao and Xu [14] developed a blockchain monitoring system utilizing intelligent farming and sensor networks to manage tea quality and safety. Using hazard characteristics; they also developed technologies for culinary threat assessment and safety tracing. Xie et al. [15]'s ETH-based traceability of agricultural items used IoT technology to protect data from unauthorized tampering or damage. However, information is saved utilizing blockchain technology at the file storage layer; as a result, network overheads will increase as data volumes do. Bumblauskas et al. [16] integrated IoT and blockchain to track products in real time. Using a Midwestern company's egg supply chain as an example, blockchain technology was implemented from farm to consumer.

A provenance storage solution using blockchain technology would record food progress information in IPFS and analyze such data with the aid of an auxiliary database, claims a study by Hao et al. [17]. Yu and Huang [18] proposed the broiler chicken traceability method by fusing RFID and blockchain technology. The "inverted tooth" design of the chicken claw ring prevents it from being resold. The approach allows intelligent technologies to scan the ring's QR code and access the relevant details and data. Benet [8] advises using the InterPlanetary File System (IPFS) to link all related devices using a single file system. Using a content-addressed strategy, IPFS is a peer-to-peer dispersed file system that provides high-throughput storage space. There are other attempts as well that aim to establish a global file system. The AFS system is installed by Howard et al. [19] and can enhance the capability of cache validation, server process structure, and other things. Additionally, several sizable media file-sharing platforms like Napster, KaZaA, and BitTorrent are developed to hold enormous amounts of data.

IV. PROPOSED MODELLING

A. Non-Perishable (NP) Agro-food Supply Chain Traceability System

Poor server management and maintenance from distributed cloud storage providers or an extremely concentrated variety of cloud providers are the main causes of the present issues with cloud storage [20]. A backup file's hard disk position might match the original file's hard disk location if the cloud hard drives are centralized, even if both files are kept on the same cloud hard drive. As a result, in the event of a power failure or other issue, the servers malfunction and are unavailable from the outside; the only option is to wait for the servers to recover. Though it is unrestricted, IPFS is a more current Internet technology than the HTTP protocol. It is based on the idea that a file can be divided into numerous bits dispersed throughout the network and obtained from multiple servers consecutively using a P2P network (PPN). If some servers are unavailable, users from outside the network can still connect to the system and access data. Additionally, the network has many backups, even if some nodes' data is completely lost as a result of an error. Data loss, outdated infrastructure, and a lack of user feedback are just a few issues with the conventional centralized public cloud that can be addressed with IPFS's benefits.

High standards for transaction data backup are necessary to ensure the traceability of the supply chains for agricultural products. Since it divides a file into several pieces and disperses them across the network, the IPFS storage system has a more reliable backup capability than cloud storage. The openness of the information kept in IPFS may be ensured by blockchain technology, which is excellent for the supply chain traceability of agricultural products. In this section, we have used the blockchain to track and execute the interactions in the NP agro supply chain products to decrease trust in the central database. We can do this with the help of smart contracts and IPFS transaction records. We can do this by leveraging smart contracts and documenting transactions in IPFS.

B. System Model Overview

Numerous parties, including producers, manufacturers, distributors, retailers, logistics, and customers, are involved in the NP agri-food supply chain model. The regulatory framework that governs the traceability system is responsible for distributing both the public and the private keys to each participant.

It is possible to strengthen customers' confidence in the safety of NP agricultural products by providing consumers with complete information on agricultural products via a traceability system. This will allow for increased sales of NP agricultural products.In this article, the relationships between production, manufacture, distribution, retailing, logistics, and sales are disentangled to investigate agricultural goods' transparency. The NP agri-food is planted, transplanted, watered, fertilized, and harvested as part of the production link. Additionally, it requires recording essential data, including details on seedlings, planting techniques, environmental factors, and product transactions. NP commodities are categorized, weighed, packed, priced, and subjected to various operations in the manufacturing unit. It also includes keeping track of data on NP products, production processes, processing parameters, product transactions, and other essential facts. The distribution unit transports the full goods from one place to several others. When handling the delivery of items to the consumer, the shop takes great care. Transportation that is a part of IoT operations is used during production, manufacturing, distribution, and retail operations.

Law enforcement agencies can track down incidents involving how good and safe agricultural products are and identify the principal parties at fault. To certify the integrity and openness of provenance data in farm produce monitoring systems, traceability uses blockchain technology's decentralization, non-tampering, and tracking properties. The production, processing, transportation, and sales of agricultural products may all be monitored with the help of the blockchain-based NP agro products tracking system, which maintains growth data, processing data, logistics details, and sales data. Fig. 1 depicts the structural layout of the blockchain-based monitoring system for NP agro products. The regulator must approve the blockchain traceability scheme, including all parties. The approval follows registration. After registration is complete, the parties involved can transfer individual and NP product traceability data. If you want to check if the data on your chain of custody has been tampered with, you can use the provided a comparison tool to check for validity. Data analysis, a consensus mechanism, key management, smart contracts based on a user's reputation, and key authorization is all part of the system. The most fundamental applications of smart contracts are adding data to blockchains and the subsequent querying of that data. When a request is made, the smart contract immediately begins carrying it out. Businesses may input data in various links, customers can query traceability data, and regulators can keep tabs on it all through the system's platform, which is designed to accommodate a wide range of users. We store the data to IPFS in order to prevent blockchain data explosion. The IPFS hash value is kept in the blockchain once consensus has been reached.

C. IPFS Encrypted Storage

The blockchain traceability system's current storage option entails immediately writing the traceability data of each system of agricultural goods onto the blockchain. The burden on blockchain's storage grows as there are more nodes, resulting in more transaction data being collected [21]. Due to the blockchain‟s unique chain-type topology, users of a single blockchain community can view all the information on the blockchain even when query efficiency is extremely low. To address these issues, this article developed a solution integrating encrypted private data storage and hash storage for public data to enhance the storage style of a blockchain monitoring system for NP agro products. Traceability data for products is just one part of the supply chain's comprehensive dataset, including sensitive information authorized parties may only access. Data confidentiality is a significant concern for rival businesses. Public information may be about the producer, manufacturers, retailers, logistics and their reputation, product details, date of manufacture, price, and provenance. In this work, Algorithm 1 depicts the data entry to the blockchain in protecting traceable information, in which sensitive data is encrypted using a smart contract and then stored on the blockchain alongside the corresponding hash value of public data.

1) *Algorithm 1: Double Encryption*

```
Initialize Stakeholders ID, Public_data, Sensitive_info, Keys. Stakeholders ID → SID
If
Sensitive_info! = Null then do Generate a Random key (KA)
Sensitive_info →Encry (GCM (Sensitive_info, KA))
Encry_key→Encry(Key_Encryption_Method (KA, PuK))
(Sensitive_info + Public_data) → IPFS
Hash (Sensitive_info) + Hash (Public_data) → BC End If
If
Sensitive_info == Null then Hash (Public_data) → BC
End If End
    Result: The hash value stored in the blockchain.
```

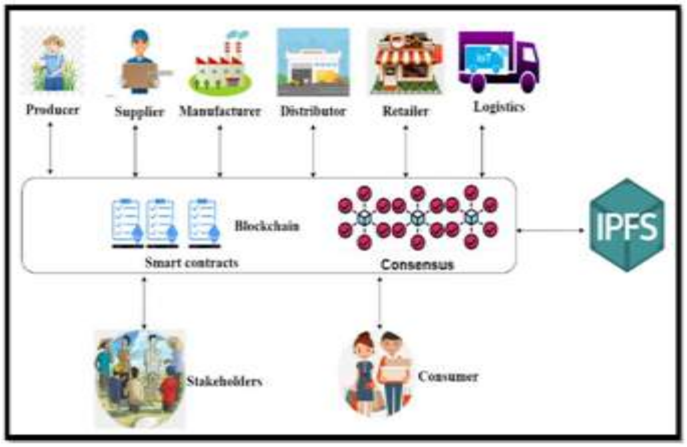


Fig. 1. Blockchain-oriented traceability mode.

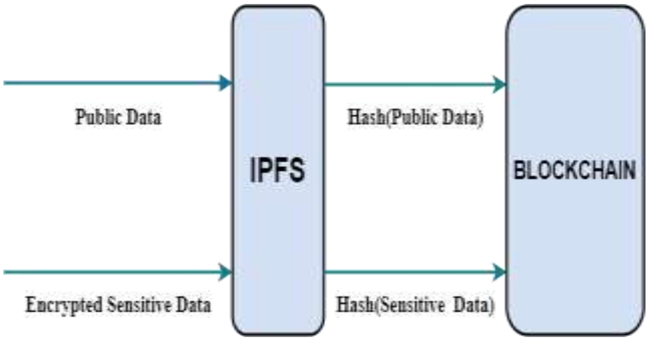


Fig. 2. Storage of public and sensitive data.

The AES encryption technique uses the Galois/Counter Mode (GCM) to encode sensitive data, „Senstive_Info‟. The necessary Key, „KA‟ is chosen at random by a random generator using the smart contract, which also creates as well as uploads encoded substitution cipher to the network. The Key is encrypted using the Key Encryption Method (ECC) to guarantee its security. The viewing node was approved by the encrypted Public Key, „PuK‟. Sensitive data as well as open data are transferred to IPFS. A pair of keys made up of the Encrypted Key and the Public Key of the Trusted Observing Nodes are kept in the current picture of the smart contract and sent to the ledger as IPFS hashes as shown in Fig. 2. The existing node's private key, „PiK„ is used to decipher the blockchain's encoded key in order to acquire the original Key, which is then used to decipher the sensitive data and sight it when the appropriate nodes access the private data.

V.RESULTS AND DISCUSSIONS

Ethereum is a blockchain open-source platform that is used for simulations. We create and test smart contracts using the Remix Integrated Development Environment (IDE), Ganache, Truffle, and Metamask. The smart contracts are used and tested on the Ethereum Ropsten test networks. The script was created using the Remix IDE and Solidity version 0.8.7. The system requirements include an x64-based processor, Win10 Pro, a 64-bit operating system, an Intel(R) Xeon(R) CPU E5-2630 v4 @ 2.20GHz, and IPFS version 0.8.0. Ganache does nevertheless distribute a certain amount of crypto currency to virtual accounts. After each transaction, the crypto currency is removed from the contract's designated account. In Ganache, every account has a unique address and private key. The truffle is the framework. Through the Metamask, a bridged browser plugin, Ganache, and the Remix IDE may communicate with one another.

Through IPFS, the file is uploaded to the blockchain. It displays a ledger with a number of records. The key that represents each transaction is used to identify each record. The record is a file's many hashes. Each entry starts with a key, then a record that includes the multi-hash value of the file, the ID of the network node reading the file, and the time stamp. Due to the network's addition of IPFS hash addresses, access to files on blockchains using IPFS is constrained. This restricts access to the IPFS system and its associated hash addresses to legitimate users only. This lowers the number of handlers who have admittance to the files. Also, lessen illegal admittance to

the file as well. Since user activity is not recorded on the IPFS network, users are free to view any files without fear of repercussions. This experiment places a barrier on unwanted access due to the immutable logging of user file access.

A. Consensus

The consensus mechanism assures blockchain nodes have the latest blocks. Popular ones include Proof of work, Proof of stake, Delegated Proof of Stake, and Practical Byzantine Fault Tolerance [22]. By facilitating competition between dispersed nodes in terms of computational power, POW increases data consistency and integrity, which is helpful in fending off Sybil attacks. The researchers created a POS approach that doesn't require processing resources and a DPOS mechanism to reduce power consumption. PBFT can reach a consensus with a few malicious nodes. Signatures, verification, and hashing prevent tampering, counterfeiting, and message repudiation and made BFT polynomial. PBFT's high consensus cost renders it unsuitable for public chains. Fewer-node consortiums or private chains operate better. The consortium chain is the core network, while PBFT is the consensus method.

B. Performance and Evaluation

Here, we measure how long it takes to verify a transaction by evaluating all the transaction data from the moment the validator first receives it until the transaction is authenticated. On the Ethereum Ropsten testbed, we assess the latency and throughput of our implementation. The approximate transaction validation time is given for all transaction types, including stakeholders.

Key extraction in ECC encryption is as simple as producing a random integer between two specified values. Any positive integer within the range is valid as an ECC secret key. It is possible to minimize the time spent waiting by taking two different approaches when computing keys throughout decryption and encryption. ECC provides less delay than the alternative by processing keys in two stages. Since the ECC key is shorter, it consumes less computing capacity while still providing secure protocols for authorized mutual authentication.

Some of these are reasonable despite the large additional operations required, such as validating signatures and hash data to and from IPFS, confirming permissions in the control list, and performing several other overheads. Transactions take the longest to complete since the qualifications of both the buyer and the vendor must be confirmed. The effectiveness of the blockchain network is examined in this section regarding various transaction rates. As a result, testing involved using transaction counts of 50, 100, 150, 200, 250, and 300 per second. By changing the number of transactions occurring, the impact of having numerous transactions active in a blockchain was examined.

Standard operations and query transactions were both put to the test in every situation. The number of total transactions has been adjusted to facilitate the development of a more comprehensive understanding of how the amount of all transactions influences the throughput and latency of the blockchain. Each transaction on the blockchain has its throughput and latency recorded and logged for future reference. This information is stored in a distributed ledger. Fig. 3 and 4 presents the calculations‟ results on the specifics of the delay and throughput measurements.

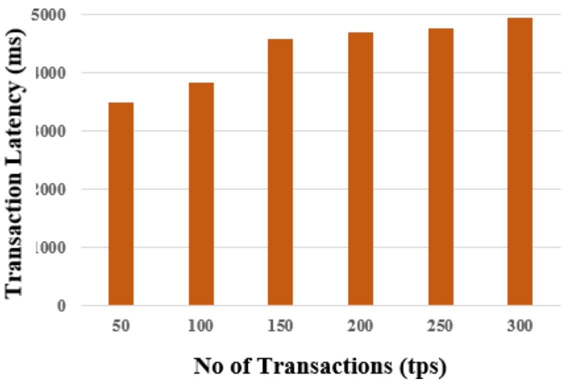
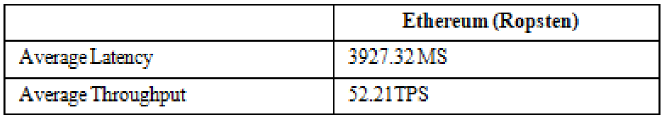


Fig. 3. Transaction throughput of the traceability system.

TABLE II. AVERAGE LATENCY AND THROUGHPUT OF THE TRACEABILITY SYSTEM



	Ethereum (Ropsten)
Average Latency	3927.32 MS
Average Throughput	52.21TPS

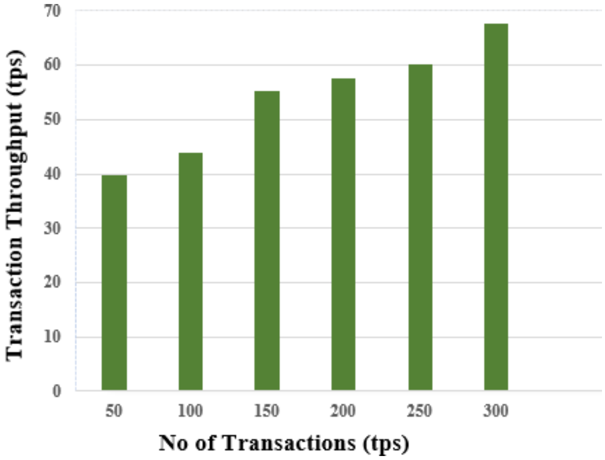


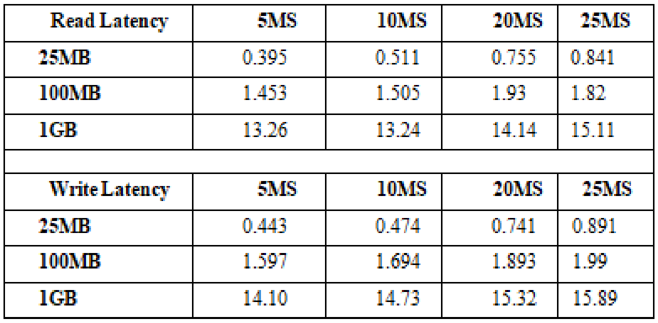
Fig. 4. Transaction latency of the traceability system.

Average delay and average throughput are determined from test results on the Ropsten test networks and are shown in Table II. Calculations are done for various transactions, including registration, the record of trace data, approvals, querying of recalls, etc.

C. IPFS Read Write Latency

While reading files over the network, IPFS reads them more quickly than it writes or adds them. A 0.256 MB file is typically received in around three seconds and written to a remote IPFS gateway in about five seconds. Because it caches the data locally after the initial transmission, IPFS is substantially faster when requesting the same file a second time. We also tested the performance of IPFS on its own to compare the outcomes of the combined systems. Files were sent between local workstations, and the server latency fluctuated. The impact of delays is more significant on smaller files than on bigger ones. The following is a performance analysis of scaling-out IPFS-attached storage. Table III displays their reading and writing results for different file sizes and latency.

TABLE III. IPFS READ WRITE LATENCY

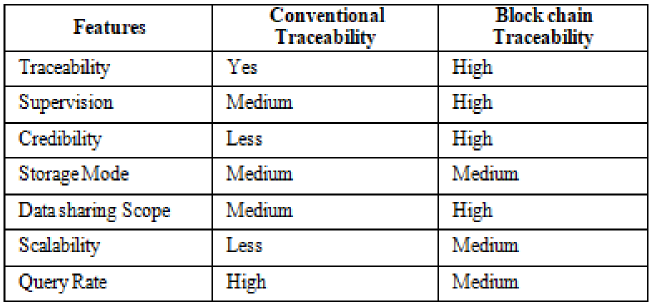


Read Latency	5MS	10MS	20MS	25MS
25MB	0.395	0.511	0.755	0.841
100MB	1.453	1.505	1.93	1.82
1GB	13.26	13.24	14.14	15.11
Write Latency	5MS	10MS	20MS	25MS
25MB	0.443	0.474	0.741	0.891
100MB	1.597	1.694	1.893	1.99
1GB	14.10	14.73	15.32	15.89

D. Comparisons

Our system has the following benefits: a better standard of decentralization; better network resilience; more integrity in data communication; and high reliability in data processing, according to the assessment of findings. The time-suggested technique enables more transactions to be added to the chain at the same rate, serving more users and enhancing overall scalability. We are evaluating our solution in comparison to several traceability systems.

TABLE IV. COMPARATIVE RESULTS



Features	Conventional Traceability	Block chain Traceability
Traceability	Yes	High
Supervision	Medium	High
Credibility	Less	High
Storage Mode	Medium	Medium
Data sharing Scope	Medium	High
Scalability	Less	Medium
Query Rate	High	Medium

Table IV contains comparable outcomes. The performance of the decentralized and blockchain-based traceability systems is lower than that of the proposed method. All designs can track data. The proposed system cannot be altered in any way, making it superior to centralized systems and other approaches. Our method is decentralized, scalable, and protects users' privacy at the same time. This method reduces the amount of data generated compared to conventional blockchain technology.

VI. CONCLUSIONS

In this study, we developed and assessed a system for tracking agricultural products using blockchain's tracing and anti-tampering features. We also examined the system's architecture for querying and storage. The problems of the blockchain traceability system's enormous data overload constraint and the lack of private security is addressed, and a suggestion for on-chain and off-chain file storage is made. The public data consumers see in the supply chain is stored in the IPFS, whose hash value is uploaded to the ledger system. For discussing with related firms, the blockchain maintains private data that has been encrypted using an encryption method. The storage approach described in this model integrates the existing scenario, considering the necessity for public scrutiny of supply chain public data and the requirement that private corporate information is encrypted, and minimizes the data burden on the chain. After the consumer scans the Tracking number for public database information, the system validates the information using the relevant block to verify if the product information has been updated. Blockchain technology is expected to develop in the direction of numerous test beds, platforms, and shading. We will continue looking into the technology tying together diverse platforms and a cutting-edge consensus mechanism suitable for traceability in future studies.

REFERENCES

[1]Lodovica Marchesi,Katiuscia Mannaro,Michele Marchesi and Roberto Tonelli, “Automatic Generation of Ethereum-Based smart contracts for agri-food Traceability system”, vol. 10, pp.3171045, May. 2022.

[2]C. Costa, F. Antonucci, F. Pallottino, J. Aguzzi, D. Sarriá, and P. Menesatti, ``A review on agri-food supply chain traceability by means of RFID technology," Food Bioprocess Technol., vol. 6, no. 2, pp. 353366, Feb. 2013.

[3]C. Dalvit, M. De Marchi, and M. Cassandro, ``Genetic traceability of livestock products: A review," Meat Sci., vol. 77, no. 4, pp. 437449,Dec. 2007.

[4]F. Antonucci, S. Figorilli, C. Costa, F. Pallottino, L. Raso, and P. Menesatti, ``A review on blockchain applications in the agri-food sector," J. Sci. Food Agricult., vol. 99, no. 14, pp. 61296138, Nov. 2019.

[5]F. Tian, ``A food traceability system based on blockchain and Radio Frequency Identification Technologies," in Proc. 13th Int. Conf. Service Syst.Service Manage. (ICSSSM), Jun. 2016, pp. 16.

[6]K. Demestichas, N. Peppes, T. Alexakis, and E. Adamopoulou,``Blockchain in agriculture traceability systems: A review," Appl. Sci.,vol. 10, no. 12, pp. 122, 2020.

[7]K. Sornalakshmi, S. Sindh, G. Sujatha, and D. Hemavathi, “An architectural framework of a Decision Support System (DSS) to increase the returns of small-scale farmers in Kanchipuram District, India,” EAI Endorsed Trans. Energy Web, Vol. 0, No. 0, 2018, pp. 163978, https://doi.org/10.4108/eai.13-7-2018.163978.

[8]L. Cocco, K. Mannaro, R. Tonelli, L. Mariani, M. B. Lodi, A. Melis, M. Simone, and A. Fanti, ``A blockchain-based traceability system in agrifood SME: Case study of a traditional bakery," IEEE Access, vol. 9, pp. 6289962915, 2021.

[9]L. Zhang, W. Zeng, Z. Jin, Y. Su and H Chen , "A Research on Traceability Technology of Agricultural Products Supply Chain Based on Blockchain and IPFS." Security and Communication Networks 2021, 2021, https://doi.org/10.1155/2021/3298514.

[10] L. Marchesi, K. Mannaro, and R. Porcu, ``Automatic generation of blockchain agri-food traceability systems," in Proc. IEEE/ACM 4th Int. Workshop Emerg. Trends Softw. Eng. Blockchain (WETSEB), May 2021, pp. 4148, doi: 10.1109/wetseb52558.2021.00013.

[11] M. M. Aung and Y. S. Chang, ``Traceability in a food supply chain: Safety and quality perspectives," Food Control, vol. 39,pp. 172184, May 2014. [Online].Available: https://www.sciencedirect.com / science / article / pii / S0956713513005811.

[12] F. Tian, “A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things,” in 2017 International Conference on Service Systems and Service Management, 2017, https://doi.org/10.1109/ICSSSM.2017.7996119.

[13] S. Balachander and A. Murugan, "Challenges and Opportunities in the Advancement of Privacy and Security of Blockchain Technology." Telematique, Vol. 21, No. 1, pp. 6651-6659, 2022.

[14] Shanthi and K. Venkatesh, “An analysis of various techniques in blockchain applications,” in 2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS), 2022, https://doi.org/10.1109/ICICCS53718.2022.9788137.

[15] X. Yang, M. Li, H. Yu, M. Wang, D. Xu, and C. Sun, “A trusted blockchain-based traceability system for fruit and vegetable agricultural products,” IEEE Access, Vol. 9, 2021, pp. 36282–36293, https://doi.org/10.1109/ACCESS.2021.3062845.

[16] Y. Liao and K. Xu, “Traceability system of agricultural product based on block-chain and application in tea quality safety management,” Journal of Physics: Conference Series, Vol. 1288, No. 1, 2019, pp. 012062, https://doi.org/10.1088/1742-6596/1288/1/012062.

[17] C. Xie, Y. Sun, and H. Luo, “Secured data storage scheme based on blockchain for agricultural products tracking,” in 2017 3rd International Conference on Big Data Computing and Communications (BIGCOM), 2017, https://doi.org/10.1109/BIGCOM.2017.43.

[18] D. Bumblauskas, A. Mann, B. Dugan and J. Rittmer, "A blockchain use case in food distribution: Do you know where your food has been?" International Journal of Information Management, Vol.52, 2020, pp.102008, https://doi.org/10.1016/j.ijinfomgt.2019.09.004.

[19] J. Hao, Y. Sun, and H. Luo, “A safe and efficient storage scheme based on blockchain and IPFS for agricultural products tracking,” Journal of Computers, Vol. 29,2018, pp.158–167, doi:10.3966/199115992018122906015.

[20] W. Yu and S. Huang, “Traceability of food safety based on blockchain and RFID technology,” in 2018 11th International Symposium on Computational Intelligence and Design (ISCID), 2018, DOI 10.1109/ISCID.2018.00083.

[21] J. H. Howard et al., “Scale and performance in a distributed file system,” ACM Trans. Computer Systems, Vol. 6, No. 1, 1988, pp. 51–81, https://doi.org/10.1145/35037.35059.

[22] K. Venkatesh, L. N. B. Srinivas, M. B. Mukesh Krishnan, and A. Shanthini, “QoS improvisation of delay sensitive communication using SDN based multipath routing for medical applications,” Future Generation Computer Systems, Vol. 93, 2019, pp. 256–265, https://doi.org/10.1016/j.future.2018.10.032.

[23] J. F. Galvez, C. Juan, and J. Mejuto, “Future challenges on the use of blockchain for food traceability analysis,” TrAC Trends in Analytical Chemistry, Vol. 107, 2018, pp.222–232, https://doi.org/10.1016/j.trac.2018.08.011.

[24] K. Harshini Poojaa and S. Ganesh Kumar, “Scalability Challenges and Solutions in Blockchain Technology,” in Inventive Computation and Information Technologies, Singapore: Springer Nature Singapore, 2022, pp. 595–606 , DOI: 10.1007/978-981-16-6723-7_44.