IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Revue d'Intelligence Artificielle
Vol. 37, No. 2, April, 2023, pp. 267-274
Journal homepage: http://iieta.org/journals/ria

Blockchain and IPFS: A Permanent Fix for Tracking Farm Produce

Subashini Babu[1], Hemavathi Devarajan[1], Venkatesh Kaliamoorthy[2*]

[1] Department of Data Science and Business Systems, School of Computing, SRM Institute of Science and Technology, Kattankulathur 603203, Tamilnadu, India
[2] Department of Networking and Communications, School of Computing, SRM Institute of Science and Technology, Kattankulathur 603203, Tamilnadu, India

Corresponding Author Email: hemavatd@srmist.edu.in

https://doi.org/10.18280/ria.370203

Received: 6 December 2022
Accepted: 10 March 2023

Keywords:
blockchain, IPFS, supply chain management, traceability, Ethereum

ABSTRACT

Blockchains typically employ IPFS for off-chain storage of user information. Centralized management, muddled data, inaccurate data, and the simplicity of building information enclaves plague traditional traceability systems. In this research, blockchain technology is used to record and access data on Non-Perishable (NP) agricultural commodities in the distribution chain to solve the challenges above. The blockchain and IPFS both store public and private data encrypted. This lessens the burden on the blockchain and enhances information search. Blockchain technology enhances farmer-customer relationships and food supply chains by tracking food back to its source. Its secure data storage enables data-driven farming. By storing encrypted files IPFS hashes in smart contracts, IPFS secures agricultural data and addresses the blockchain storage problem. Being deployed in association with connects makes it possible for rapid financial transactions to occur with any changes made to the blockchain's data. This article analyses performance and simulates implementation in Ethereum testnets. The results show that our system protects sensitive data, supply chain data, and real-world applications by increasing the throughput and latency.

1. INTRODUCTION

The healthfulness of our food nowadays is a significant concern for everyone. Errors are commonplace in the food supply chain because of the monotony of the work involved [1]. All transactions in a blockchain-based supply chain are available to all network nodes, providing transparency into the flow of goods. Supply chain management coordinates the processes through which raw materials are transformed into finished products to maximize customer value and sustain a company's competitive edge over the long term. Raw materials are transformed into finished products by various people, objects, initiatives, and organizations that make up what is commonly referred to as the supply chain, whose primary and secondary function is to fulfill client orders. The government may have established national provenance criteria for significant products, yet fraudulent and inferior interests still need to be prevalent in the market. As a result of these concerns, consumer confidence is at a shallow level [2].

Food is grown, prepared, shipped, and sold from farm to table. Any dishonesty in the linkages above could compromise food safety. Different technologies and learning have produced numerous management solutions, which help track the entire process. Traditional data storage exposes data to loss or alteration risk. Researchers use blockchain technology to safeguard and store agricultural-related data [3]. IoT components in farm machinery automatically provide those data.

A large amount of real-time data would be created if many agricultural goods participated in the provenance monitoring program. Blockchain technology was developed specifically to handle digital currency transactions since they generate fewer data than real-time monitoring data. This makes it more challenging to track traceability data and block generation rates. So, a gateway is required for blockchain technology. To store and search for agricultural product traceability information, we employ IPFS and blockchain. A peer-to-peer decentralized file system called IPFS suggests connecting every machine to a single file system. We advise storing data on blockchains using IPFS [4]. IPFS updates the blockchain with hash addresses. The database keeps track of blockchain transaction hashes [5]. By requesting the IPFS authenticity database hash address, customers can use blockchain transaction content to discover an item's origin.

The primary contributions of this work include a decentralized storage system based on blockchain technology that permits trading transactions between participants involved.

2. TRACEABILITY AND BLOCKCHAIN TECHNOLOGY

Blockchain technology makes it possible to track the provenance of food items from the farm to the table with greater accuracy. The adoption of blockchain technology has the potential to significantly reduce the risks to food safety posed by fraud, disorganization, and a lack of norms. The advent of blockchain technology will fundamentally alter our understanding of and reliance on provenance. Traceability in the food industry refers to the process by which a product can be followed from its initial production location through the entire distribution chain to the final customer. Some of the challenges are discussed in Table 1.

Table 1. Challenges in traceability system

Challenges
• Complex supply chains;
• Lack of standardization;
• Data collection and management;
• Food fraud;
• Cost.

2.1 Blockchain preliminaries

Blockchain is public, immutable, anonymized, encrypted, and decentralized. A P2P distributed public ledger is maintained by all network participants using Merkle trees and secure hash techniques. Peer node records are kept on shared ledgers. Papers are grouped to produce a block that has been consensus-validated [6]—the digital ledger stores data as a collection of connected, separate chunks, as shown in Figure 1. A distinct block is generated and added to the chain whenever fresh information is uploaded to the system [7]. There can be no inconsistency if each computer (node) in the network does not regularly update its copy of the public blockchain.

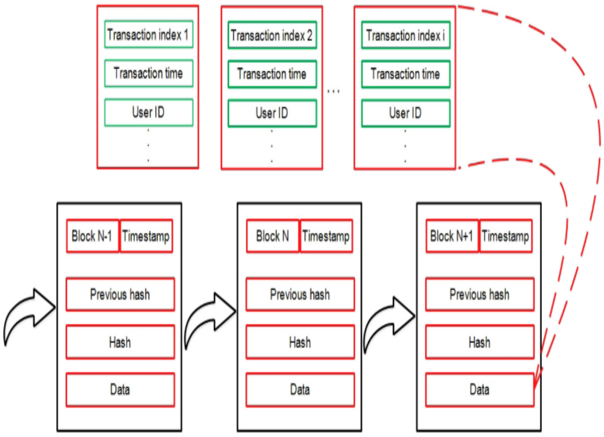

Figure 1. Structure of the blockchain

Adding new blocks is one of the fundamental characteristics of blockchain that contributes to its extraordinary security [8]. This is so that a new node can join the blockchain only after a participating node has confirmed and authenticated the accuracy of all pre-recorded data. This may entail proving that all freshly recorded transactions inside a block of digital currency exchanges are genuine and that no funds have been spent more than once. However, you can modify a single database or spreadsheet. The distributed ledger stores the block's records if everyone agrees [9]. For confirming data modifications, nodes receive new blockchain currency.

The Merkle binary hash tree was fundamental to the Blockchain's design, first introduced in 1987 [10]. Branches in a Merkle tree are known as leaves, and each leaf represents a unique piece of information. An *R*-record leaf with a *2R-1* inner node is evaluated with the help of the cryptographic hashing function *Has()*. The intricacy of a tree with *R = 2s* nodes is *s = log R*. Furthermore; the entire hierarchy may be traced back to a single, distinct root node located at height *s = 0*. Claiming that the tree can be summed up in the root value *Ś* is a claim on the validity of all its nodes and leaves. *T* is a set of *s'* units over the entire hierarchy, and it conforms to each descendant node *c* at depth *s'* in such a way that:

$$\acute{S} = Has\ F_t(c, T) \quad (1)$$

$$\acute{S} = Has\ f_t(d, T) \quad (2)$$

where, *HasF*$_t$ is a series of *s'* function *Has(.)* in (1). An adversary keeping a Cryptographic tree for proof stores the whole tree, while a validator supports the base node Ś. The verifier of node c in the tree gives the tokens T for all of the other tree's nodes. Considering this, it follows from (2) that the given expression *c∈Ś*, whose *c* would be the current root. With knowledge of the existing state Ś, each reorganization of the current node d to d' results in a gradual improvement state from Ś near *S = Has f*$_t$ *(d', Td)*.

A numerical set with a static output is converted to a group of dynamic inputs via hashing methods [11]. Hashing algorithms are used for data authentication, throughput comparison, and other purposes. They are frequently used to safeguard data.

3. RELATED STUDY

IPFS, a decentralized, peer-to-peer file-sharing protocol, stores and retrieves massive volumes of data. It can hold vast amounts of food traceability data, such as photographs, videos, and documents, that may be too large for a blockchain [12]. IPFS stores and retrieves data offline, which is advantageous in rural areas where agricultural operations are more popular and internet access is scarce. This guarantees data accessibility in low-connectivity areas. We evaluate the I/O performance of IPFS and compare it with HTTP to analyze their transmission efficiency. Moreover, we examine how the resolving and downloading operations affect the I/O performance of IPFS [13].

Many people rely on it to quickly and easily share information. By using cryptographic hashes, IPFS can uniquely identify files throughout the network. Off-chain file storage provided by IPFS is referenced via blockchain hashes [14]. For immutability and future verification, a hash of all data (including photos or videos) will be submitted to the public Ethereum blockchain. IPFS is a protocol for storing and sharing data on a distributed peer-to-peer file system [15]. IPFS borrows several good ideas from other peer-to-peer systems, but its real innovation lies in how it unifies and improves upon established practices to create a whole of its portions [16]. The IPFS foundational principles [17] ensure content addressability, tamper resistance, and deduplication. Several primary probes have proven that blockchain technology may be used for proof-of-origin in the supply chain business. Authors [18] created a solution based on the Ethereum blockchain and the IPFS [19] file storage system to guarantee precise product tracking across the healthcare supply chain. The Interplanetary Archive distributes data files into the Interplanetary File System (IPFS) [20] as a persistent Web archive.

Hyperledger was used as the provenance link that processed data in the database by Yang et al. [21] to address the issue of insufficient data storage provided by the blockchain. Its drawbacks to IPFS data storage include high prices, sluggish data transit speeds, inadequate privacy protections, etc. Retailers should only have access to the data on product security and other aspects once a customer satisfaction function is implemented. Liao and Xu [22] designed a blockchain-based monitoring system for tea quality and safety that uses smart farming and sensing networks. They also created tools for evaluating potential hazards in the kitchen and tracking down their sources. To prevent tampering or harm to the data, Xie et al. [23] utilized IoT technology in their ETH-based system to track agricultural products. Blockchain technology is used to store data at the file storage layer; nevertheless, this increases bandwidth overhead expenses as data volumes grow. Using IoT and blockchain, Bumblauskas et al. [24] were able to keep track of inventory in real time. As one example, a Midwestern company has incorporated blockchain technology throughout its whole egg supply chain, from farm to customer.

A blockchain-based traceability storage solution would use IPFS to store data on the development of food [25]. Yu and Huang [26] demonstrated a system for tracking broiler chickens that combines RFID and blockchain technology. The chicken claw ring's "inverted teeth" design prevents it from being sold again. Using this technique, smart devices may retrieve the relevant data from the QR code on the ring. Benet [16] advises using the InterPlanetary File System (IPFS) as the universal file system to link all devices. IPFS is a peer-to-peer distributed file system with content addresses that offers quick data transfer rates. Blockchain is swiftly gaining traction as a viable solution to prevent food corruption and forgeries and to provide trustworthy, transparent, and shareable data throughout the agri-food supply chain. To better manage the distribution of a classic Italian food item—Carasau bread—these findings suggest a paradigm shift toward the use of smart contracts, the Interplanetary File System, and the Internet of Things [27].

4. PROPOSED MODELLING FOR NON-PERISHABLE FOOD (NPF) TRACEABILITY SYSTEM

The lack of adequate system administration and administration on the side of decentralized cloud services and a severely constrained selection of cloud suppliers are the most critical elements leading to the current issues with cloud storage [28]. The challenging disc position of a backup file may match the hard disc position of the source file even when both files are stored on the same cloud storage device if the cloud storage devices are centrally located. In the occurrence of a blackout or other disruption, the systems would fail by becoming inaccessible externally, leaving users with little choice but to delay till normal service is restored. Internet Protocol File System (IPFS) is a more modern Internet protocol than the more traditional Hypertext Transfer Protocol (HTTP), despite its lack of restrictions. It operates on the principle that data in a file can be split up into smaller pieces and then retrieved in order from different servers over a P2P network.

Clients from beyond the connection can still join the network and get data even if specific servers are out. And even if specific nodes' data is lost forever due to an error, the network has multiple backups. Conventional centralized public clouds have several drawbacks that IPFS can help fix, such as a higher risk of data loss, older technology, and a need for more customer feedback. To keep the capacity to trace the provenance of agricultural products, backup transaction data must be protected with strict security measures. IPFS, a distributed file storage technology, provides more reliable recovery than cloud storage by dividing a file into multiple portions and dispersing them over the network.

Monitoring in the food supply chain is greatly aided by blockchain technology since it ensures the transparency of the data kept in IPFS. In this section, we use the blockchain to keep tabs on and execute the transactions associated with the NPF supply chain items, thereby reducing reliance on a centralized database. We can accomplish this using smart contracts and IPFS system logs. This is possible with the use of smart contracts and the IPFS ledger.

4.1 System model overview

The NPF supply chain includes consumers, distributors, retailers, manufacturers, and logistical service providers among its participants. The system's governing design distributes the traceability system's keys among all users. Consumers trust in the safety of non-perishable agricultural goods can be increased by giving them detailed information about farm commodities via a traceability system. In order to transparency of agricultural goods, the linkages between produce, manufacturing, marketing, commerce, transportation, and selling are detached in this article.

To complete the supplied link, the non-perishable agri-food must first be cultivated, transferred, irrigated, fertilized, and harvested. In addition, it necessitates essential recording data, such as specifics on seedlings, planting methods, climate changes, and goods transactions. In the production plant, NPF products are categorized, weighed, packaged, marketed, and exposed to various other procedures. Additionally, it entails maintaining records of information regarding NPF products, manufacturing procedures, process criteria, product trades, and further crucial details. The dispersion unit moves the entire cargo from one location to several others. The company takes considerable care while handling item delivery to the customer. Producing, processing, distributing, and retail all involve the utilization of transit.

Bureaus of law regulations can investigate occurrences regarding the quality and safety of agricultural products and pinpoint the primary persons responsible for the misdeeds. Blockchain's distributed, unchangeable, and trackable nature is put to use in the process of traceability. This allows for validating the authenticity of provenance information in agriculture product control systems. The NPF goods tracking system, built on the blockchain, stores information about agricultural product cultivation, processing, transportation, and sales. Figure 2 depicts the architectural plan for the blockchain-based NP agro products monitoring system. Any consensus-based blockchain tracing system worth its salt will need the blessing of the appropriate authorities. After signing up, you'll be given the go-ahead. Once everyone has registered, they can share information about the provenance of individual and NP products. A comparison tool is available to see if the news on your line of possession has been altered.

The system has critical authentication, contracts that consumers, access control rate, and data analysis. Adding data to blockchains and accessing that data is the most fundamental use case for smart contracts. Smart contracts are capable of immediately commencing executing a transaction. The platform's flexible enough to accept data from various sources, allow clients to query provenance information, and satisfy the needs of regulators. To avoid a blockchain storage explosion, we save everything on IPFS. After a consensus is obtained, the IPFS hash value is stored in the ledger.

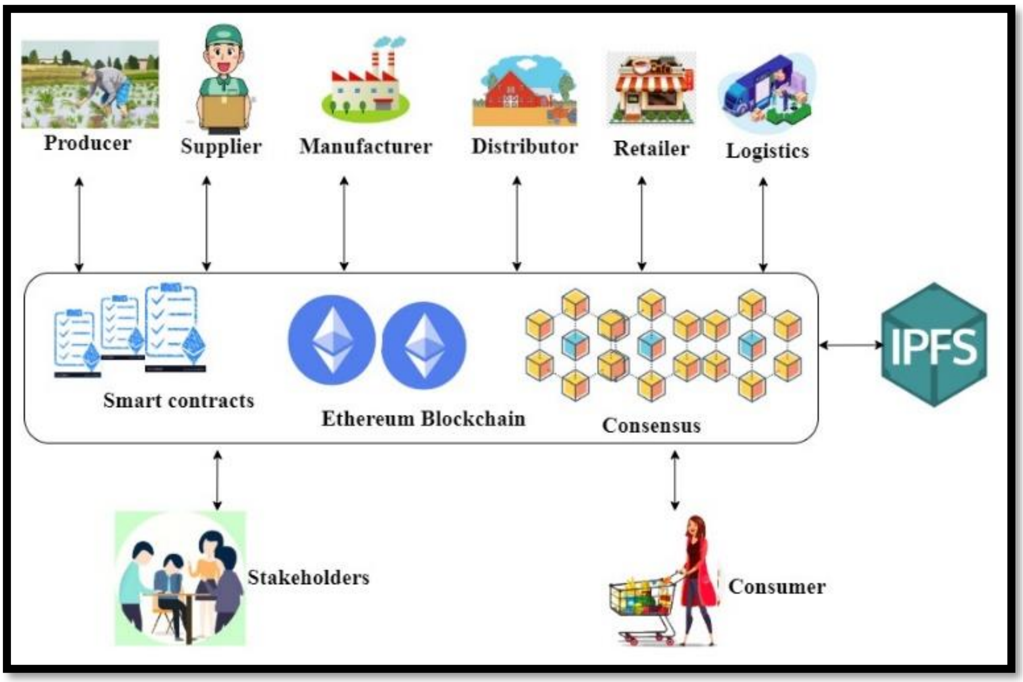

Figure 2. Tracking system based on the blockchain

4.2 Protected data storage with IPFS

The current approach for storing information in the blockchain provenance system is an instant recording of the tracing data for each method of producing agricultural goods onto the blockchain. When there are more nodes in a blockchain, there are more transactions that need to be saved [29]. This means that more space will be required to keep them. Because of the unique structure of the blockchain, users that are part of the same blockchain community have access to all of the blockchain's data. This is true regardless of how effective the users' queries are.

This article presents a way for a blockchain tracking system for NP agricultural items that combines secured personal data storage with hash caching for public data. The goal of the paper is to find a solution to the challenges that have been identified. Data on the origin of products is just one component of the vast dataset about the supply chain. This dataset also contains critical information only available to parties with the appropriate authorization.

Concerns regarding protecting customers' data are frequent among companies competing with one another. Details on the product itself, its manufacturer, retailer, and logistics providers, as well as its price, date of manufacturing, and provenance, may be among the information available to the public. In the context of this article, Algorithm 1 illustrates the process of data entry into the blockchain to safeguard the information that can be traced back to its source. The information that is considered to be the most critical is first encrypted with the assistance of a smart contract. After that, the relevant hash code of publicly available data is appended to the ledger, permanently recording the transaction.

The Authenticated Encryption Mode(AEM) of the Advanced Encryption Standard (AES) is used to secure the vital data set "In_data". The required Key, "Key_{Ran}," is randomly selected through a smart contract, which generates and sends an encrypted substitution cipher to the network. Elliptic Curve Cryptography is used to encrypt the Key to ensure its security. The encrypted Public Key, or "P_K," approved the watching defer of data to IPFS, including critical and open data. As shown in Figure 3, the current iteration of the smart contract keeps a pair of credentials, the Private Key and Public Keys of the Verified Monitoring Endpoints, transmitted to the blockchain as IPFS hashes. Once the correct nodes have access to the secret information, the source Key decodes the data so it can be viewed. To decrypt the ledger key encryption, the current station uses its private key, called "Pi_K".

Algorithm 1
Input: Players ID, Out_data, In_data, Public Key, Private Key.
Output: The hash value kept in the distributed ledger.

```
Players ID → PID
If
In_data! = Null then
Randomly generate a key ($Key_{Ran}$)
In_data → Enc (AEM (In_data, $Key_{Ran}$))
Enc_key→Enc (ECC ($Key_{Ran}$, $P_K$))
Overall (In_data + Out_data) → IPFS
Hash (In_data) + Hash (Out_data) → DL
End If
If
In_data == Null then
Hash (Out_data) → DL
End If
To receive the information by querying
If
Data to be retrieved
Dec_key→Dec (ECC ($Key_{Ran}$, $Pi_K$))
DL → Trace_Data
End
End
```

A rise in transmission costs and a possible increase in the likelihood of data leakage are both possible outcomes of the widespread use of delegated decryption keys. The size of the encrypted message is also taken into consideration, as it has a direct bearing on storage fees. Many essential assignment techniques make use of previously-classified files to produce decryption keys. When a new file format is added to the server, it's necessary to adjust the categories in which the files are stored. A user can also modify the criteria used to classify items. It is impossible to modify key accumulation encryption to fit the new requirements. In some cases, the size of the ciphertext and the corresponding decryption keys may be predetermined by our encryption method. Also, because our system permits regular file upgrades, this doesn't affect how the files are organized.

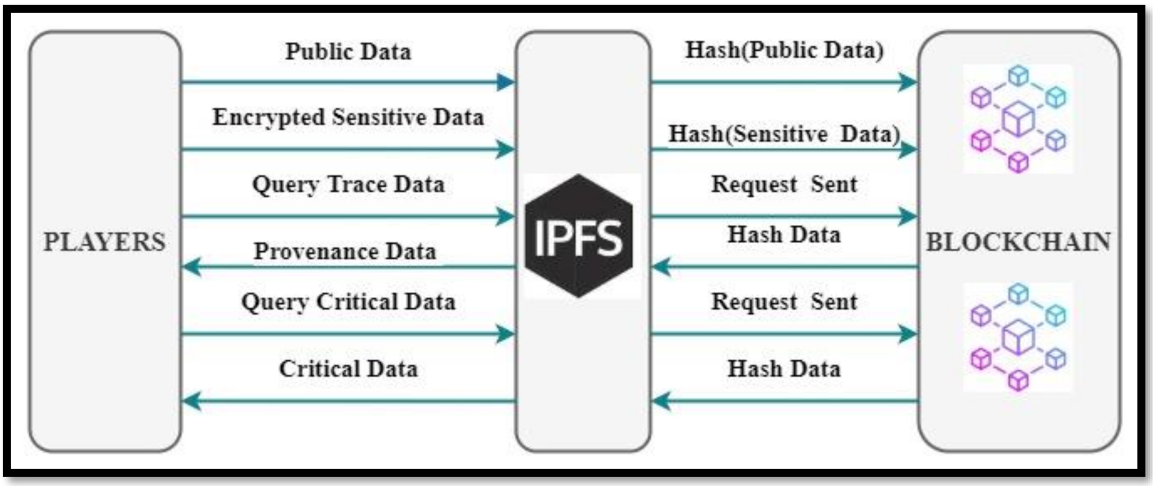

Figure 3. Storage of public and critical data

5. OUTCOMES

Ethereum is a no-cost blockchain development environment. We use the Remix Integrated Development Environment to create and verify smart contracts. Also, Metamask, Ganache framework with truffle is used. The Ethereum Sepolia test networks are employed and tested for smart contracts. The writing was written in Solidity. You only need a 64-bit operating system, an Intel(R) Core (TM) i7-12700 2.10 GHz, an x64-based processor, and IPFS version 0.8.0. Yet, Ganache provides some coins to digital wallets that are removed after each transaction.

IPFS is used to upload the file to the blockchain. An entry-filled ledger is displayed. The key that represents each operation allows easy access to data records. The file's multiple hashes constitute the log. The hash identifies the entry and is accompanied by a document containing the file's multi-hash values, the device's identifier connected to retrieve the file, and the time stamp. Blockchains that employ IPFS have limited access control since the network has added IPFS hash addresses to their nodes. Only authorized users can enter the IPFS network and its corresponding hash values. Because of this, fewer handlers will be able to access the data. Reduce unauthorized access to the record as well. Users can safely access any file on the IPFS system without worrying about their actions being tracked. With the permanent recording of user data files, this research creates a barricade against unauthorized entry.

5.1 Consensus

"Proof of Work," "Proof of Stake," "Delegated Proof of Stake," and "Practical Byzantine Fault Tolerance" are popular consensus in use [30]. POW increases data's reliability and truthfulness and protects against Sybil attacks by encouraging remote nodes to compete in processing power. A Proof of Work (POW) consensus mechanism supports Bitcoin's network. When it comes to Proof-of-Work, miners' effort is for trim. Many PoW methods permit reusing previous work, which helps mitigate the damage. Proof of Stake requires substantially less processing power than Proof of Work (PoW). In this context, PoS miners are responsible for ensuring the security of monetary transactions. Theory suggests that those with more coins are less likely to engage in malicious network activity. Byzantine fault tolerance (PBFT) is a replication mechanism [31].

Researchers created a processing-free POS method and a DPOS mechanism to reduce power grid strain. PoS, a direct democracy, differs from DPOS, a representative democracy. When nodes intentionally weaken the network, PBFT can help reach a consensus. Signatures, hashing, and verification prevent message tampering, forging, and denial. PBFT's pricey consensus makes it unsuitable for distributed databases. Fewer nodes improve private and public networks. The network's brain is the PBFT consensus process and consortium chains. The comparative results of the discussed consensus are given in Table 2.

Table 2. Relative results

Features	PoW	PoS	PBFT	DPOS
Node identification	Open	Open	Permissioned	Open
Power consumption	Bad	Limited	Good	Limited
Approved attack power	Less than 25%	Less than 51%	Less than 33%	Less than 51%

5.2 Performance and Evaluation

To compute the time needed to validate a transaction, we consider all related information, beginning with when the validator receives it and ending when the transaction is verified. We use the Ethereum Sepolia test platform to measure the performance and delay of our system for all sorts of transactions and all parties involved are given an estimated time for verification. Despite the substantial extra work involved, some are acceptable; for example, validation of IPFS users and their data hashes, authentication checks against the master database, and completing a few additional administrative tasks. Closing a deal takes the most time because both parties' credentials must be verified. This section looks at different transaction rates and analyzes the blockchain network's efficiency.

Various transaction rates (50, 100, 150, 200, 250, 300, and 350 per second) were utilized to put the system through its paces. By manipulating the transaction volume, we could examine the effects of a blockchain with high throughput. All routines and inquiry transactions were discussed. The total number of transactions was altered to examine the impact on the blockchain's throughput and latency. The speeds and delays of all blockchain-based transactions have been measured and recorded. Figures 4 and 5 depict the finer points of the throughput and latency measurements, respectively.

Table 3. Aggregate delay and efficiency

	Ethereum (Sepolia)
Average Latency	4729.27 ms
Average Throughput	57.12 tps

Based on the results of the Sepolia test networks, the mean latency and performance are listed in Table 3. Calculations are necessary for many processes, including registration, data tracing, approvals, and recall queries.

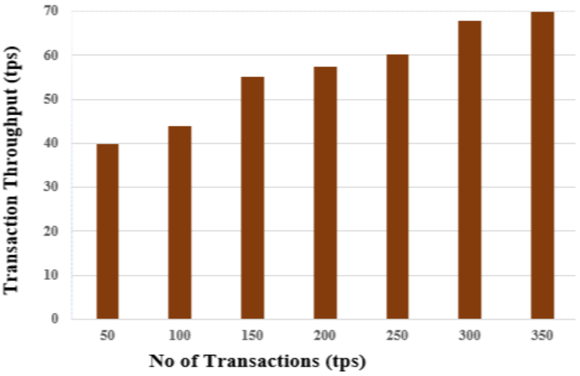

Figure 4. Traceability system's transactional rate

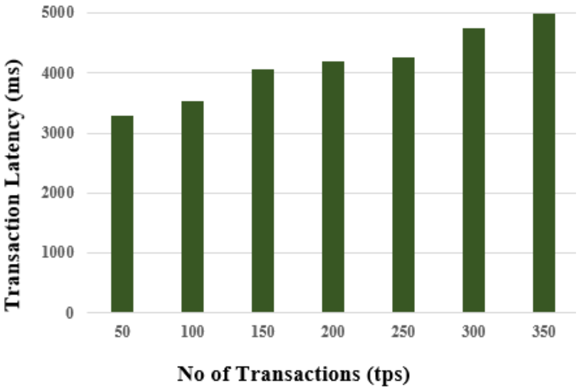

Figure 5. Traceability system's operation latency

Table 4. Transfer time delay in IPFS

RL / WL	25MB	100MB	1GB
5MS	0.236/0.332 L	1.361/1.479 L	12.11/13.90 L
10MS	0.465/0.382 L	1.461/1.549 L	12.42/13.31 L
20MS	0.732/0.689 L	1.828/1.730 L	13.44/14.23 L
25MS	0.759/0.798 L	1.71/1.87 L	15.51/15.22 L

RL - Read Latency WL - Write Latency L = RL / WL

5.3 Latencies in reading and writing to IPFS

IPFS reads network data faster than it publishes it. A remote IPFS portal receives a 0.5 MB file in four seconds and sends it in five. IPFS stores initial transfer data to speed up later file requests. We compared our IPFS testing with our combined system tests to determine the systems' overall effectiveness. When the server was delayed, workstations transferred files locally. Smaller files cause more delays than larger ones. IPFS-attached storage is scaled here. Various file sizes and delay circumstances are shown in Table 4.

5.4 Comparison

According to the results, our system offers several advantages. These include a high degree of decentralized standard, increased system durability, more secure data transfer, and strong calculation accuracy rates. Since more customers can be serviced at once with the then-proposed method, scalability is improved. Inferring from these, we find that our approach outperforms other traceability methods. Data monitoring and recording capabilities are built into every system. Instead of centralized systems and other processes, ours cannot be manipulated. The privacy of our consumers is safeguarded without compromising the scalability or decentralization of our approach. The amount of data created by this approach is lower than that produced by traditional blockchain technology.

6. CONCLUSIONS

We built and evaluated a blockchain-based food supply chain monitoring system. We looked at both the querying structure and the storing structure. The blockchain traceability system lacks private security and limited data storage capacity. Both on-chain and off-chain file storage have been recommended to address these issues. A hash value representing the public IPFS data from the supply chain is transmitted to the ledger system. A distributed ledger called the blockchain allows participating companies to exchange information securely. To reduce the volume of data the supply chain must process, this model's storage solution considers the need for open procurement monitoring and data protecting personal corporate data. The system will immediately check the Tracking number against a public database if the product's details have changed since the client last did so. It's feasible that test networks, platforms, and sharding will emerge as blockchain technology advances. Future studies will concentrate on platforms that connect various platforms and a new method of tracking consensus.

ACKNOWLEDGMENTS

The authors are grateful to all who supported us in producing this article and to those who contributed to this study.

REFERENCES

[1] Sornalakshmi, K., Sindh, S., Sujatha, G., Hemavathi, D. (2020). An architectural framework of a Decision Support System (DSS) to increase the returns of small-scale farmers in Kanchipuram District, India. EAI Endorsed Transactions on Energy Web, 7(29): e2-e2. https://doi.org/10.4108/eai.13-7-2018.163978

[2] Zhang, L., Zeng, W., Jin, Z., Su, Y., Chen, H. (2021). A research on traceability technology of agricultural products supply chain based on blockchain and IPFS. Security and Communication Networks, 2021: 3298514. https://doi.org/10.1155/2021/3298514

[3] Tian, F. (2017). 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, IEEE, Dalian, pp. 1-6. https://doi.org/10.1109/ICSSSM.2017.7996119.

[4] Pawar, M.K., Patil, P., Hiremath, P.S. (2021). A study on blockchain scalability. In ICT Systems and Sustainability, Springer, Singapore, pp. 307-316. https://doi.org/10.1007/978-981-15-8289-9_29

[5] Balachander, S., Murugan, A., (2022). Assessing the feasibility of blockchain technology in automotive industry. In 2022 IEEE 9th Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON), Prayagraj, India, pp. 1-6. https://doi.org/10.1109/UPCON56432.2022.9986381

[6] Xiong, Z., Zhang, Y., Luong, N.C., Niyato, D., Wang, P., Guizani, N., (2020). The best of both worlds: A general architecture for data management in blockchain-enabled Internet-of-Things. IEEE Network, 34(1): 166-173. http://dx.doi.org/10.1109/MNET.001.1900095

[7] Berdik, D., Otoum, S., Schmidt, N., Porter, D., Jararweh, Y., (2021). A survey on blockchain for information systems management and security. Information Processing & Management, 58(1): 102397. http://dx.doi.org/10.1016/j.ipm.2020.102397

[8] Shanthi, P., Venkatesh, K. (2022, May). An analysis of various techniques in blockchain applications. In 2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, pp. 857-860. https://doi.org/10.1109/ICICCS53718.2022.9788137

[9] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review, 21260. (White paper). https://doi.org/10.2139/ssrn.3440802

[10] Merkle, R.C. (1988). A digital signature based on a conventional encryption function. In Advances in Cryptology—CRYPTO’87: Proceedings 7, pp. 369-378, Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-48184-2_32

[11] Wang, F., Chen, Y., Wang, R., Francis, A.O., Emmanuel, B., Zheng, W., Chen, J. (2019). An experimental investigation into the hash functions used in blockchains. IEEE Transactions on Engineering Management, 67(4): 1404-1424. https://doi.org/10.1109/TEM.2019.2932202.

[12] Khan, M.A., Hossain, M.E., Shahaab, A., Khan, I. (2022). ShrimpChain: A blockchain-based transparent and traceable framework to enhance the export potentiality of Bangladeshi shrimp. Smart Agricultural Technology, 2: 100041. https://doi.org/10.1016/j.atech.2022.100041

[13] Doan, T.V., Bajpai, V., Psaras, Y., Ott, J. (2022). Towards decentralised cloud storage with IPFS: Opportunities, challenges, and future directions. arXiv preprint arXiv:2202.06315. https://doi.org/10.48550/arXiv.2202.06315

[14] Politou, E., Casino, F., Alepis, E., Patsakis, C. (2019). Blockchain mutability: Challenges and proposed solutions. IEEE Transactions on Emerging Topics in Computing, 9(4): 1972-1986. https://doi.org/10.1109/TETC.2019.2949510.

[15] Nishi, F.K., Shams-E-Mofiz, M., Khan, M.M., Alsufyani, A., Bourouis, S., Gupta, P., Saini, D.K., (2022). Electronic healthcare data record security using blockchain and smart contract. Journal of Sensors, 2022: 1-22. https://doi.org/10.1155/2022/7299185

[16] Benet, J. (2014). Ipfs-content addressed, versioned, p2p file system. arXiv preprint arXiv:1407.3561. https://doi.org/10.48550/arXiv.1407.3561.

[17] Patsakis, C., Casino, F. (2019). Hydras and IPFS: a decentralised playground for malware. International Journal of Information Security, 18(6): 787-799. https://doi.org/10.1007/s10207-019-00443-0.

[18] Musamih, A., Salah, K., Jayaraman, R., Arshad, J., Debe, M., Al-Hammadi, Y., Ellahham, S. (2021). A blockchain-based approach for drug traceability in healthcare supply chain. IEEE Access, 9: 9728-9743. https://doi.org/10.1109/ACCESS.2021.3049920.

[19] Abdulkader, O., Bamhdi, A.M., Thayananthan, V., Elbouraey, F. (2019). IBMSDC: Intelligent blockchain based management system for protecting digital currencies transactions. In 2019 Third World Conference on Smart Trends in Systems Security and Sustainablity (WorldS4), London, UK, pp. 363-367. https://doi.org/10.1109/WorldS4.2019.8904003

[20] Alam, S., Kelly, M., Nelson, M.L. (2016). Interplanetary wayback: The permanent web archive. In Proceedings of the 16th ACM/IEEE-CS on Joint Conference on Digital Libraries, Newark, NJ, USA, pp. 273-274. https://doi.org/10.1145/2910896.2925467

[21] Yang, X., Li, M., Yu, H., Wang, M., Xu, D., Sun, C. (2021). A trusted blockchain-based traceability system for fruit and vegetable agricultural products. IEEE Access, 9: 36282-36293.

https://doi.org/10.1109/ACCESS.2021.3062845.

[22] Liao, Y., Xu, K. (2019). Traceability system of agricultural product based on block-chain and application in tea quality safety management. Journal of Physics: Conference Series, 1288(1): 012062. https://doi.org/10.1088/1742-6596/1288/1/012062.

[23] Xie, C., Sun, Y., Luo, H. (2017). Secured data storage scheme based on block chain for agricultural products tracking. In 2017 3rd International Conference on Big Data Computing and Communications (BIGCOM), Chengdu, China, pp. 45-50. https://doi.org/10.1109/BIGCOM.2017.43.

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

[25] Hao, J., Sun, Y., Luo, H. (2018). A safe and efficient storage scheme based on blockchain and IPFS for agricultural products tracking. Journal of Computers, 29(6): 158-167. https://doi.org/10.3966/199115992018122906015

[26] Yu, W., Huang, S. (2018). Traceability of food safety based on block chain and RFID technology. In 2018 11th International Symposium on Computational Intelligence and Design (ISCID), 1: 339-342. https://doi.org/10.1109/ISCID.2018.00083

[27] Howard, J.H., Kazar, M.L., Menees, S.G., Nichols, D.A., Satyanarayanan, M., Sidebotham, R.N., West, M.J. (1988). Scale and performance in a distributed file system. ACM Transactions on Computer Systems (TOCS), 6(1): 51-81. https://doi.org/10.1145/35037.35059

[28] Venkatesh, K., Srinivas, L.N.B., Krishnan, M.M., Shanthini, A. (2019). QoS improvisation of delay sensitive communication using SDN based multipath routing for medical applications. Future Generation Computer Systems, 93: 256-265. https://doi.org/10.1016/j.future.2018.10.032

[29] Galvez, J.F., Mejuto, J.C., Simal-Gandara, J. (2018). Future challenges on the use of blockchain for food traceability analysis. TrAC Trends in Analytical Chemistry, 107: 222-232. https://doi.org/10.1016/j.trac.2018.08.011

[30] Harshini Poojaa, K., Ganesh Kumar, S. (2022). Scalability challenges and solutions in blockchain technology. In Inventive Computation and Information Technologies: Proceedings of ICICIT 2021, pp. 595-606, Singapore: Springer Nature, Singapore. https://doi.org/10.1007/978-981-16-6723-7_44

[31] Distler, T., Cachin, C., Kapitza, R. (2015). Resource-efficient Byzantine fault tolerance. IEEE Transactions on Computers, 65(9): 2807-2819. https://doi.org/10.1109/TC.2015.249521