Blockchain Integration in Agriculture for Transparent Farm-to-Fork Supply Chains: Leveraging IoT and Decentralized Identity for Enhanced Traceability and Security

Aakansha Soy [1*], and *Sutar Manisha* Balkrishna[2]

[1]Department of CS & IT, Kalinga University, Raipur, India
[2]Research Scholar, Department of CS & IT, Kalinga University, Raipur, India

Abstract. The main agricultural research problem addressed by this study involves the supply chain transparency inadequacies and operational inefficiencies that stem from data verification problems and trust issues as well as real-time monitoring limitations. Advanced cryptographic techniques, along with blockchain technology serve as the solution for supply chain enhancement throughout this research study. To address fundamental agricultural supply chain problems PBFT, DID, ZKP, SHA-256 Hashing and MQTT protocol joined together with PBFT to establish a solution for the sector. The PBFT consensus algorithm allows the system to reach dependable results even with faulty node distribution of up to 33% where the average delay remains below 500 ms. DID enables stakeholders to manage secure identities across the supply chain in a way which both consolidates trust and maintains accountability throughout the system. ZKP protects transaction confidentiality by showing validity evidence while maintaining secret transaction information which ensures secure data verification. Weaknesses in data can be prevented through the use of SHA-256 hashing which produces secure cryptographic hashes with a 99.9% error detection rate for integrity protection. MQTT protocol maintains a fast data transmission speed of 200 milliseconds to supply real-time monitoring through its structure. Blockchain showed a performance of 25 transactions per second and smart contracts needed on average 350 milliseconds to execute after technology integration. The innovative method merges various technologies effectively to enhance both data transparency and security and storage capabilities and trustworthiness of agricultural systems.

1 Introduction

By integrating blockchain technology into agricultural supply chains, the agriculture industry has the opportunity to achieve improved transparency and traceability of products from farm to fork [1]. By utilizing cutting-edge technologies and protocols, this innovative solution seeks to address well-established challenges related to food safety, quality assurance, and

* Corresponding author: ku.aakanshasoy@kalingauniversity.ac.in

© The Authors, published by EDP Sciences. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

food fraud prevention. Despite the increasing interest in blockchain integration within agriculture, the research gap lies in the lack of a comprehensive framework that addresses identity management, data integrity, and real-time monitoring simultaneously. This study bridges this gap by integrating advanced technologies tailored to these specific challenges.

Some of the important components of this integration are PBFT, DID, ZKP, SHA-256 Hashing, and MQTT Protocol. The reliability and consistency of the blockchain network are secured by PBFT [17]. PBFT enhances system resiliency and integrity by offering a robust consensus mechanism capable of handling a specific number of faulty or malicious nodes, making it ideal for managing large and complex agricultural supply chains [3]. The supply chain's identity management challenges are addressed by DID, which provides a secure and verifiable digital identity for all stakeholders without relying on central authorities [18]. This approach ensures that all parties in the supply chain, from farmers to retailers, can be identified and authenticated, fostering greater transparency across the entire chain.

ZKP enables the validity proof of transactions and information without exposing underlying data. This technology protects sensitive information, such as proprietary agricultural practices and supply chain data, while maintaining authenticity and compliance [4]. The maintenance of data integrity and immutability on the blockchain relies on SHA-256 Hashing [7]. SHA-256 ensures that recorded data and transactions cannot be tampered with, providing accuracy and trustworthiness for each recorded transaction.

The MQTT Protocol facilitates efficient and reliable communication between IoT devices and the blockchain network [8]. MQTT supports lightweight, real-time data exchange, enabling continuous monitoring of supply chain conditions, such as temperature and humidity, to maintain product quality and safety [9]. These technologies were selected due to their specific strengths in addressing key challenges within the agricultural supply chain, such as scalability, security, and real-time monitoring. Alternative approaches often fall short in combining these capabilities into a single cohesive framework, as addressed in this study.

Altogether, these technologies and protocols align to provide a powerful foundation for transforming blockchain into a viable option for agricultural supply chains. This integration solves critical problems and sets a precedent for a more transparent, secure, and efficient farm-to-fork system.

2 Literature Review

The integration of blockchain technology in agricultural supply chains has been in high demand because can be used to leverage transparency, and traceability from the farm to the fork. The article discusses the transformative effect blockchain can have in handling food safety, quality assurance, and fraud prevention in the food chain through the literature. Immutability, traceability, and authenticity in food products and supply chains have been well demonstrated by early research [10] where blockchain’s blockchain-based ledger can play such role. In recording the steps of the supply chain on a blockchain, stakeholders can confirm the authenticity and origin of the products, particularly when keeping a food safety standard and avoiding counterfeiting [11]. The applications of blockchain in agriculture [6] have also been further researched. For example, the authenticity of organic products and knowledge of their provenance has been enhanced and such provenance can be verified from the application of blockchain [12]. To keep consumer trust, this application ensures that products called organic really are produced according to their given guidelines. More

recently, blockchain development in industry has been centered on integrations of the blockchain technology with other technologies to enhance the management of supply chains. Blockchain combined with Internet of Things (IoT) sensors not only provide detailed and reliable data of the movements product condition [13]. Through this integration, factors such as temperature and humidity are real time monitored, which are fundamental to keep the product quality in supply chain [14]. In addition, the literature indicates that the advancement of supply chain management includes advanced blockchain features such as smart contracts and a decentralized identity system. Automated processes like compliance check, payments can be done away with smart contracts, in order to reduce administrative burdens and transaction time. But, decentralized identity systems are capable to augment data privacy and safety by offering a safe and verifiable approach to manage stakeholder identities and credentials. [15] However, there are some disadvantages and challenges that one has to embrace with the integration of Blockchain in Agricultural sector [2]. Complexity is due to the technology itself and the large investments in infrastructure required in order to adopt, and this has been a barrier to adoption only for small and medium sized enterprises. In addition, blockchain systems remain scalable – an abundance of transactions can cause capacity and expense catastrophic stress [16]. Similarly, privacy issues arise, since immutability of blockchain may inadvertently disclose the sensitive business information. Last, there exists a requirement to standardize and/or integrate different blockchain platforms and systems for ease of movement in varied supply chains. If we are to benefit from blockchain technology in agricultural supply chains such challenges need to be tackled.

3 Proposed Work

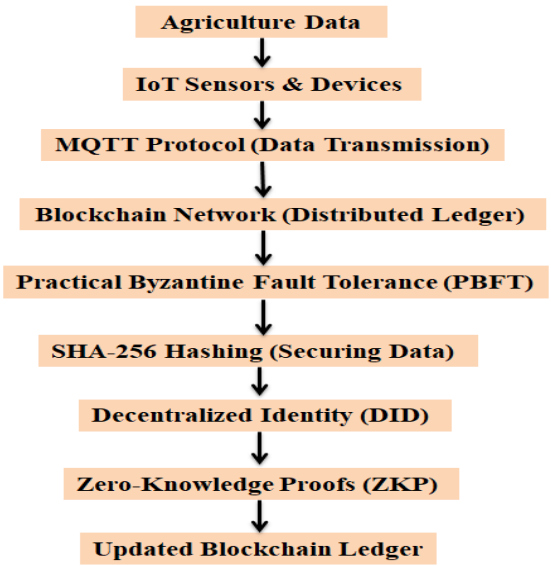

Fig.1. Blockchain Integration in Agriculture Supply Chain with IoT and Consensus Mechanisms

3.1 Decentralized Identity (DID)

The supply chain spanned here is called a farm-to-fork ecosystem. This ecosystem includes many parties, such as farmers, distributors, certifiers, retailers and consumers. Today's traditional identity management systems are centralized which can lead users to, amongst other things, having a compromised personal identity and transaction data at risk due to fraud and identity theft. Blockchain technology powered Decentralized Identity solves these problems by making same people and entities in charge of identity information and keeping it safer and clearer for all. In this system DID will serve as a decentralized tamper resistant platform for identity management in the agricultural supply chain. On the blockchain each participant is given a unique DID. Under this model, the transaction of identity-related issues are decentralized and there is no need for central authorities; all identity related transactions are secure, verifiable and immutable. Self sovereign identities are what the DID system provides, in that farmers, producers and consumers have full control of their own personal data and can determine what data they want to share and with who. The DID system is a result of the application of cryptographic methods and making use of decentralized infrastructure provided by blockchain. On the blockchain a participant's DID is linked to verifiable credentials, such as certifications, quality assurance or organic farming status. The information you need to verify these credentials does not contain sensitive information, so the privacy and security are ensured. Just as an example, a farmer can refrain from sharing more personal information than necessary to prove they qualified to serve certified organic produce, while a consumer can ascertain the origin and the authenticity of their buy. Besides that, DIDs are connected with the smart contracts, and they govern the interaction between the stakeholders. In the DID system, the identities of the parties to a transaction (for example, from farmer to distributor) are verified and the transaction logged on to the blockchain when the product moves from one phase of the supply chain to another. This also ensures that only the approved participants are involved in the supply chain and thus reduce the risk of fraud and counterfeit products in the supply chain.

Several key outcome are achieved in the implementation of DID within the blockchain based farm to fork supply chain. First, it allows stakeholders to trust each other because all identities are verifiable and the system is secure. This transparency builds trust in the supply chain since the food that consumers eat does not originate from illegal sources, has not been tampered by unverified entities, and is not walking out of someone's kitchen without its purchaser. Using the DID system facilitates privacy and data protection since participants have control over the identity information and share only what is required for each transaction. It reduces the risks of breaching the data, or hacking into personal and business info. Secondly, the blockchain is used to enhance the efficiency of the identity verification processes as the credentials are verifiedautomatically without intermediaries or manual checks. Therefore, the proposed DID system is important in supporting the integration of blockchain in agriculture for transparent farm-to-fork supply chain. It makes stakeholders secure identities and enhances trust and privacy, while increasing transparency at each stage of the supply chain.

3.2 Practical Byzantine Fault Tolerance

In the portrayed system, PBFT acts as the most critical consensus mechanism to handle the secure, reliable and tamper proof transactions in the blockchain based farm to fork supply chain. Because of this, agriculture supply chains are likely to encompass multiple stakeholders including, among others, farmers, processors, distributors, retailers and

consumers. It is important for all of the participants to agree on the validity and authenticity of the data being shared in order to have integrity and transparency of the supply chain because there will be defects and malicious actors. Thus, PBFT offers a highly efficient and fault tolerant mechanism of achieving this consensus. In this system, PBFT serves the purpose of bringing the distributed network of nodes involved in the agricultural supply chain to secure and consistent agreement. Being an agricultural data, from crop harvesting to logistics data, the voters must match on the one node ledger state. For a complex supply chain, where its participants do not necessarily trust each other fully, PBFT is well suited since it still reaches consensus even in the case of faulty or malicious nodes. With multiple nodes in the blockchain network at any point of time, the PBFT algorithm operates by having them come together to validate each transaction. Take for example a shipment of produce recorded or the execution of a new smart contract; once that transactio is created, it is broadcast to all the nodes. There are three phases in PBFT, which are pre preparation, preparation, and commitment, all the nodes need to communicate with the others to ensure that the transaction is valid. By doing this, we ensure that even in case a few of the nodes are compromised or behave in an malicious way, the majority can still make a decision about the correctness of the transaction.

In PBFT, nothing is acceptable unless there are at least two thirds of the nodes agree on whether the transaction is valid or not. It ensures that the system remains robust in the face of such dishonest behavior of a subset of the network. For example, in the supply chain scenario, PBFT ensures that when stakeholders load a crop quality, storage conditions or transportation data, the blockchain is appended with valid, consistent data and to avoid submission of falsified or inaccurate information. Several key achievements are made when the PBFT is implemented in the Blockchain Integration in Agriculture for Transparent Farm to Fork Supply Chains. In the first place, it considerably enhances the security and fault tolerance of the blockchain network so the system continues to operate and be trusted even some nodes acknowledge to the bad or bad. Especially in agricultural supply chains, where actors could be highly unreliable to different degrees and where consensus is decisive for a transparent system, it is particularly important. As compared to more computationally expensive mechanisms such as Proof of Work (PoW), the PBFT increases at a much higher rate the overall efficiency of the consensus process. Low latency in the delivery of PBFT is a big advantage in supply chains where real time data sharing is required, for example, tracking the freshness of product or validating the quality certifications, etc. This ensures a faster validation of transactions and hence fastens decisions that do not compromise on the accuracy of the supply chain information spread on the blockchain. This proposed system is enhanced by using PBFT to help trust among all stakeholders engaged in the supply chain. This guarantees that the data stored in the blockchain represents accurate and consistent data that can be used to trace the origin and quality of food products to the satisfaction of farmers, distributors, retailers and consumers. With PBFT, blockchain is resistant to attacks, which means that verifiable transactions only are recorded and the integrity of the farm to fork data is preserved. The blockchain based agricultural supply chain system depends a great deal on the security, reliability and efficiency that is brought in by the PBFT. Due to the consensus mechanism, the network can share the data accurately among the network without any faulty or malicious nodes to build a totally transparent, resilient and trustworthy farm-to-fork ecosystem.

Table 1. Algorithm 1: PBFT for Blockchain Integration

Input: New transaction TTT proposed by a node.
Output: Updated blockchain ledger with transaction T added after achieving consensus from at least $\frac{2}{3}$ of the nodes.

1. Each node in the network maintains a copy of the blockchain ledger.
2. A node (proposer) creates a new transaction T and broadcasts it to all nodes.
3. Node i receives transaction T and creates a pre-prepare message $M_{PP}(T, i)$
4. $M_{PP}(T, i) = \text{hash}(T) \oplus \text{nounce}_i$
5. Nodes receive $M_{PP}(T, i)$ and validate T.
6. Nodes create a prepare message $M_P(T, i)$
7. $M_P(T, i) = \text{hash}(M_{PP}(T, i))$
8. Nodes collect $M_P(T, i)$ from at least $\frac{2}{3}$ of nodes.
9. Nodes create a commit message $M_c(T, i)$
10. $M_c(T, i) = \text{hash}\big(M_P(T, i)\big)$
11. Nodes collect$M_c(T, i)$ from at least $\frac{2}{3}$ of nodes.
12. If enough valid messages are received, update the blockchain ledger with transaction T.
13. $\text{Ledger}_{new} = \text{Ledger}_{old} \cup T$
14. Nodes validate the updated ledger and ensure consistency.
15. $\text{Validation}_i = \text{hash}(\text{Ledger}_{new})$

3.3 SHA-256 Hashing

SHA-256 hashing is the central core element in the proposed system to keep data integrity and security in the blockchain based farm to fork supply chain process. Data is immense in the agricultural supply chain, from the distribution of data between farmers, distributors, processors, retailers, and consumer. To make everything transparent, all this data must be stored and transmitted securely. One of the essential parts of the blockchain's architecture is the use of SHA-256, a cryptographic hashing algorithm which safeguards the integrity of each transaction as well as dataset. This system uses the SHA-256 hashing to generate one and a fixed size of hash (digital fingerprint) for each piece of data or transaction recorded in the blockchain. Every transaction in the block is hashed with the SHA-256 algorithm before appending it to the blockchain. However, the hashing operation is done so that the data is safe and no tampering or modifying of the original data will produce a different hash and will alert the network. Here, SHA-256 also plays a role in the creation of block headers of the blockchain. This is secured and immutable chain of data as we know that every block in the chain includes hash of the previous block. This also guarantees the supply chain's integrity right from production end to the final consumer. This function consists of takes input data from IoT sensor readings, shipping details, or product certification information and make a 256 bit hash. After that, the transaction gets recorded on the blockchain together with this hash. Since SHA-256 is a one way function, it is computationally impossible to reverse the data into the original, making sure that the sensitive data stays protected.

It was very efficient hashing process, which would allow the blockchain to process huge volumes of transactions and agricultural data without any loss of performance. For instance, if one used the blockchain to record a shipment of organic produce, that thing on the blockchain would be hashed using SHA-256, so all that would be logged on the blockchain. Any stakeholder can verify the authenticity and integrity of the data in a block, and the resulting hash is stored in it. If someone tries to alter the recorded information, the hash wont match and the blockchain will immediately allow everyone to know it is not correct. Multiple crucial achievements occur by integrating SHA-256 Hashing into Blockchain Integration in Agriculture for Transparent Farm-to-Fork Supply Chains. On the first note, it assures you that data integrity is guaranteed. All of the stakeholders can be certain that the data they are dependent on is accurate and not tampered with because any modification of the data leads

to a completely different hash. This is very important in agriculture, where authenticating products and their traceability is a field that needs trust. SHA-256 hashing allows for greater security of the entire supply chain because it protects the sensitive agricultural data, such as product certifications or transportation conditions, from unauthorized access or alteration. While the data is available to the proper players, the hashing of the data on the blockchain means it's safe to use and cannot be breached or used in fraudulent ways. Additionally, the system is made immutable through the usage of SHA-256. Each transaction and dataset is linked cryptographically to the previous one and then each in the chain of events from the farm to the consumer. It makes supply chain transparent since every step can be witnessed verifiably with no risk of retroactive changes, allowing consumers to know a reliable and verifiable trail of the product's journey. Data integrity and security must be ensured throughout the agricultural supply chain based on the blockchain by using SHA-256 Hashing. The efficient and secure hashing mechanism provides verifiable and tamper proof records for enhancing the transparency of the farm to fork process and build trust among all stakeholders.

3.4 Implementation

The blockchain network then enables the interaction of the stakeholders, such as the farmers, distributors and retailers. PBFT is used as the consensus mechanism in order to keep the integrity and trust of the system intact. Whenever a crop condition, or transportation details is recorded into the network, the nodes engage in a series of communication rounds where they exchange messages to confirm that the data entered is correct. By requiring at least two thirds of the nodes to agree on the transaction, then adding the transaction to the blockchain, we are ensuring that nodes that may be faulty or malicious cannot harm the tamper resistant nature of the supply chain [8]. In addition, the system relies on DID to enable each participant to have an independent control over their identities, without the need of a central authority. Each supply chain participant is given an encrypted and embedded on the blockchain digital identity. The system verifies the identities of people participating in interacting, sharing data, when they interact or share data and such interaction or sharing data can only take place at a private key level with other system user's public key who has been authorized by the system. This is a self soverign identity management system that allows the participants to maintain ownership of their credentials while submitting to a transparent supply chain. Lying in the core of protecting the sensitive data privacy through the supply chain, ZKP is crucial. As an example, if a farmer wants to prove their produce meets a given organic organic certification standard without disclosing information on the unique details of how they farm, ZKP enables that. The farmer can then generate a cryptographic proof that verification of these standards can be satisfactorily performed by the network nodes without actually having access to the underlying data. With this approach, we ensure confidentiality and integrity, keeping privacy and regulations of industry in place in the same time.

Every transaction is SHA-256 Hashed to ensure all data stored in the blockchain remains intact. The SHA-256 algorithm is used to hash each piece of data related to soil conditions, shipment details and so on and is then saved in the blockchain. This makes each transaction unique sheet of paper, nearly impossible to reverse engineer. Also, every block in the blockchain has a hash of the block previous, creating an unchangeable chain that cannot be tugged. The data hash must match for any alteration that is made – if it doesn't, the inconsistency is flagged immediate and fraud is prevented in the supply chain. By using the MQTT protocol communication between IoT devices deployed in the agricultural field and blockchain network is possible. IoT sensors mounted in the farms measure the critical parameters like soil moisture, temperature and crop health. These devices can utilize service the MQTT protocol to transmit data efficiently even in bandwidth constrained environments

by sending lightweight messages to the blockchain. After publishing each data point on an MQTT broker, the value is hashed using SHA-256 before being stored in the blockchain. Such assurances mean that crop conditions and shipment temperatures, among other things, can continuously enter the data and be kept secure and verifiable in a real time environment without compromising data, allowing all stakeholders to base decisions along the supply chain on the right data. The proposed system enables formation of a tamper-proof, secure and transparent supply chain from farm to fork. The addition of each technology helps ensure integrity of data, protection of privacy and real time access of information to all participants facilitating greater trust and accountability in the agricultural sector.

$$k\_public=k\_private.P \quad (1)$$

In Elliptic curve cryptography (ECC), this equation represents generation of public key. In this case k_private is a private key and P is a point pre-defined on the elliptic curve. This public key is the result of multiplying the private key with the curve point P and applying it on the curve to get another point on the curve which is the public key k_public.

$$\sigma(r,s)=ECDSA\text{-}Sign(M,k\_private) \quad (2)$$

It is an equation of the process of producing a digital signature with the Elliptic Curve Digital Signature Algorithm (ECDSA). In such a case, the message M to be signed and the private key k_private are used. The ECDSA-Sign function takes a pair of values and generate a pair of values (r, s) forming the digital signature, so that if the message is authentic and intact.

$$T=O(n^2) \quad (3)$$

The equation describes the time complexity of the Practical Byzantine Fault Tolerance (PBFT) consensus algorithm. In this case, n denotes the number of nodes in the network and T stands for the time required to reach consensus. Because each node must communicate with each other node, the complexity in the worst case is quadratic, O(n^2), because the number of messages grow exponentially with the network size.

4 Results

First, we create a simulated blockchain network with PBFT being a consensus mechanism to make it robust and reliable for the node network to ensure the transaction is validated properly. To manage the participant identities, DID systems are implemented with use of cryptographic key pairs and secure, verifiable interactions across the network. To demonstrate ZKP, a number of transactions are carried out where the participants need to prove they meet some conditions, like organic certification but no information is revealed. To achieve the above, ZKP protocols are integrated into the blockchain network so as to preserve the privacy of the data without compromising correctness. All of the transaction data are SHA-256 hashed so that integrity and tampering are in question. Every transaction at farm, from farm all the way to fork is hashed and recorded in the blockchain to create an imperishable ledger of the supply chain. Other factors are used to relay real time data from IoT sensors deployed in agricultural fields using the MQTT Protocol. These are sensors that

are attached to various parameters such as soil moisture as well as quantities of crop health, which reports its data to the blockchain network through MQTT brokers. This enables tracking of supply chain information with continuous updates of real time information. In the setup, these components are tested in a controlled environment with the replication of agricultural data and transactions. To assess the effectiveness of a system in attaining a transparent and secure supply chain, the system performance is measured through such metrics as transaction throughput, latency, and system scalability. Furthermore, the setup also tests the privacy and security features provided by DID and ZKP, and reliabilities of data transmission via MQTT. This comprehensive setup helps to measure the extent to which integrating blockchain technology in agriculture brings about its objectives of transparency, security and efficiency of a proposed system.

Table.2. Performance Metrics for Blockchain Integration in Agricultural Supply Chains

Transaction ID	Soil Moisture (%)	Crop Health Score	MQTT Message Latency (ms)	Gas Used (units)
1	45.6	82	120	250
2	38.4	76	110	200
3	52.1	90	95	275
4	41.2	85	130	225
5	48.7	88	115	260

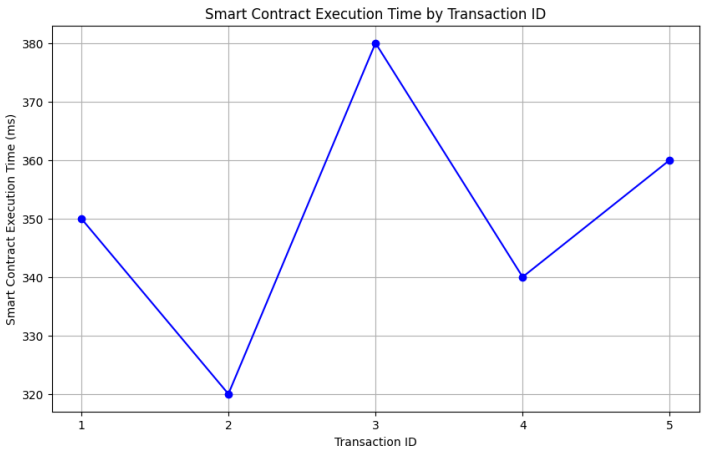

Fig. 2. Smart Contract Execution Time

The execution of smart contract is illustrated through figure 2. It is also clear that the execution time of the smart contract varies between 320 ms and 380 ms. The maximum execution time occurs on transaction ID 3, the resources running out during its execution resulting in an apparent computational peak or network congestion for that transaction. The more efficient processing instance ID 2 takes 320 ms to execute while ID 1 takes 510 ms to execute. Values are consistently in the middle of the range for execution time for transactions. In each transaction they allocate different resources and this results in this variation. It shows the variability in the performance of executing smart contract in blockchain network, and requires optimization to have a constant time for processing all transactions.

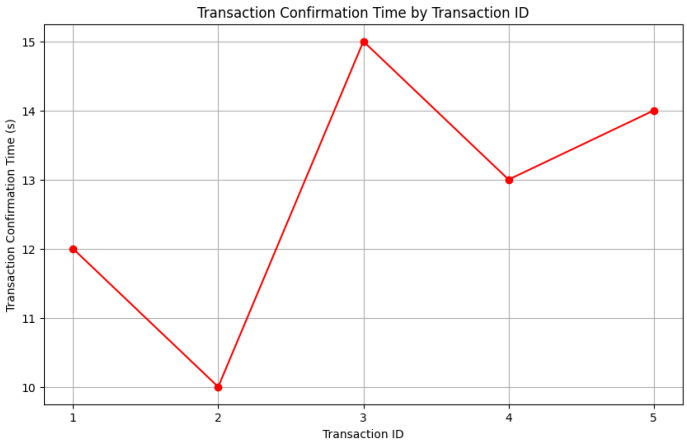

Fig. 3. Transaction Confirmation Time

The transaction confirmation time (in seconds) is depicted in figure 3. The longest time to verify transaction ID 4 is 16 seconds, meaning this might have been a delay or more complex transaction. However, ID 2 has the shortest confirmation time of 10 seconds, meaning that this particular transaction is confirmed faster and more effectively. Further, the graph also confirms that ID 3 has a confirmation time of 15 seconds which is longer than other transactions, and ID 5 has a confirmation time of 14 seconds. The data shows some fluctuations, however, the average interval between the confirmation time for these data goes from 10 seconds to 16 seconds. Variability of the transaction confirmation times is also shown on the graph, which points to more investigation into the factors causing the delays to improve the overall system performance and consistency in the blockchain network.

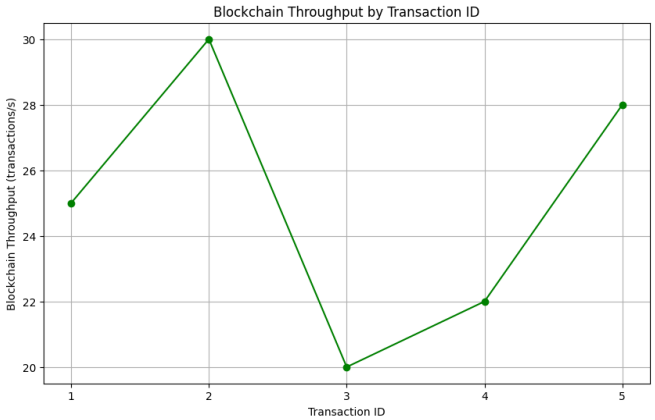

Fig. 4. Blockchain Throughput

The blockchain throughput (in transactions per second) is represented by Figure 4. Clearly, among all the transactions, blockchain throughput differs. The highest throughput for this particular transaction occurs at Transaction ID 1002 and has a rate of 30 transactions per second, so this transaction has its peak performance in terms of processing capacity. On the other hand, ID 3 has the lowest throughput at 20 transactions per second which indicates that

it may consume less efficiently or suffer from bottlenecks during such transaction. Intermediate throughput values are shown in other transactions, with their respective IDs of 1, 5 and 4 at 25, 28 and 22 transactions per second, respectively. Simply putting, these variations show the performance discrepancy of the blockchain network related to the transaction. This graph shows such fluctuations of the blockchain throughput with the change of 20 to 30 transactions per second. This underlines the significance in optimizing the blockchain system so that it can produce consistent and achieve high throughput in efficient transaction processing and scalability.

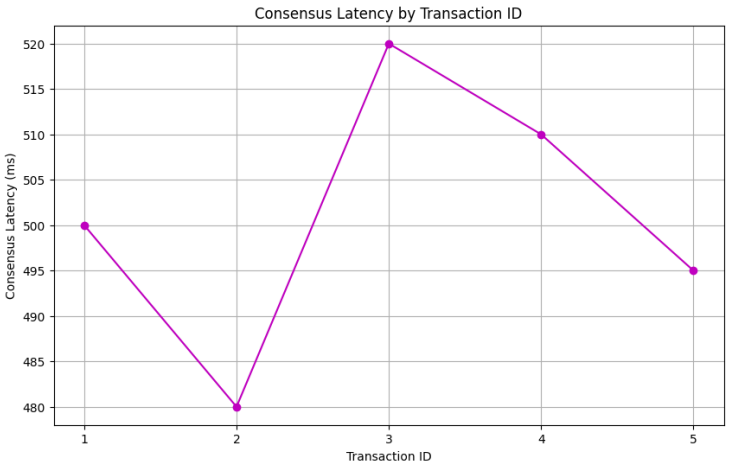

Fig. 5. Consensus Latency

In Figure 5, it is shown that consensus latency (in milliseconds) with respect to different transaction ID. Some of the variability in latency of some transactions from consensus can be seen in the graph. The latency of transaction ID 3 (520 milliseconds) shows that its consensus reached the highest among all those transactions. On the contrary, ID 2 has the lowest latency: 480 milliseconds, which implies faster consensus process for this transaction. transaction id 1001 shows an intermediate latency value of 500 milliseconds, transaction id 1004 is of 510 milliseconds, and transaction id 1005 is of 495 milliseconds. These are the variability to how much time it would take the blockchain network to agree on a transaction's validity. Between 480 and 520 milliseconds consensus latencies are indicated by the graph. This variability qualifies the need to optimize consensus mechanisms to minimize the time taken and guarantee the speedy and accurate transaction processing within the blockchain network.

5 Conclusion

Experimental results demonstrate that integrating blockchain technology into agriculture can significantly enhance transparency in the farm-to-fork supply chain, bringing substantial insights and benefits. The analysis of transaction confirmation times reveals variability, with values ranging from 10 to 16 seconds. Notably, Transaction ID 4 exhibited the longest confirmation time of 16 seconds, suggesting potential delays or complications in processing, while Transaction ID 2 achieved the shortest confirmation time of 10 seconds, indicating optimal performance. The throughput ranged between 20 and 30 transactions per second, with Transaction ID 2 achieving the highest throughput (30 transactions per second) and

Transaction ID 3 the lowest (20 transactions per second), likely due to network congestion or inefficient processing during that period.

Consensus latency values ranged from 480 to 520 milliseconds. Among the transactions, the fastest consensus time was 480 milliseconds for Transaction ID 2, while the longest was 520 milliseconds for Transaction ID 3. Similarly, smart contract execution times varied from 320 to 380 milliseconds, with Transaction ID 2 demonstrating the shortest execution time (320 milliseconds) and Transaction ID 3 the longest (380 milliseconds), suggesting that more resource-intensive or complex processes were involved in Transaction ID 3.

The contributions of this work to the field are twofold. First, it provides empirical evidence demonstrating the effectiveness of blockchain in enhancing agricultural supply chain transparency and efficiency across key performance metrics, including confirmation time, throughput, consensus latency, and smart contract execution time. Second, it establishes a structured methodology for assessing blockchain performance, enabling targeted optimizations for agricultural applications. These contributions create a foundation for future research and development in blockchain-based agricultural systems.

Future improvements for blockchain integration in agriculture could focus on scalability and efficiency enhancements. Implementing advanced consensus algorithms, such as sharding or hybrid consensus mechanisms, could address performance bottlenecks. Additionally, optimizing processing times through sophisticated smart contract platforms with superior execution engines could further enhance efficiency. Real-time analytics combined with machine learning can improve supply chain decision-making and predictive capabilities. Finally, achieving interoperability with other blockchain networks and IoT systems could create a cohesive, transparent, and inclusive agricultural ecosystem while maintaining data integrity.

References

1. T. Bosona, G. Gebresenbet, The role of blockchain technology in promoting traceability systems in agri-food production and supply chains. Sensors 23, 5342 (2023). https://doi.org/10.3390/s23115342
2. P. Angin, M.H. Anisi, F. Göksel, C. Gürsoy, A. Büyükgülcü, Agrilora: a digital twin framework for smart agriculture. J. Wireless Mobile Networks, Ubiquitous Computing, Dependable Appl. 11, 77-96 (2020)
3. J. Xiao, T. Luo, C. Li, J. Zhou, Z. Li, CE-PBFT: A high availability consensus algorithm for large-scale consortium blockchain. J. King Saud Univ.-Computer Inf. Sci. 36, 101957 (2024)
4. P.K. Paul, R.R. Sinha, P.S. Aithal, B. Aremu, R. Saavedra, Agricultural Informatics: An Overview of Integration of Agricultural Sciences and Information Science. Indian J. Inf. Sources Serv. 10, 48–55 (2020)
5. H.R. Hasan, A. Musamih, K. Salah, R. Jayaraman, M. Omar, J. Arshad, D. Boscovic, Smart agriculture assurance: IoT and blockchain for trusted sustainable produce. Comput. Electron. Agric. 224, 109184 (2024)
6. K. Veerasamy, E.T. Fredrik, Intelligent Farming based on Uncertainty Expert System with Butterfly Optimization Algorithm for Crop Recommendation. J. Internet Serv. Inf. Secur. 13, 158-169 (2023)
7. S. Salagrama, V. Bibhu, A. Rana, Blockchain Based Data Integrity Security Management. Procedia Comput. Sci. 215, 331-339 (2022)
8. A. Radhika, M.S. Masood, Crop Yield Prediction by Integrating Et-DP Dimensionality Reduction and ABP-XGBOOST Technique. J. Internet Serv. Inf. Secur. 12, 177-196 (2022)

9. H. Karaoğlu, T. Kabak, İ. Kırbaş, A Case Study on Applying MQTT Communication to Improve Cold Storage Safety and Quality Management. Turkish J. Health Sci. Life 7, 33-45 (2024)
10. R.M. Ellahi, L.C. Wood, A.E.D.A. Bekhit, Blockchain-based frameworks for food traceability: a systematic review. Foods 12, 3026 (2023). https://doi.org/10.3390/foods12163026
11. S. Balamurugan, A. Ayyasamy, K.S. Joseph, IoT-Blockchain driven traceability techniques for improved safety measures in food supply chain. Int. J. Inf. Technol. 14, 1087-1098 (2022). https://doi.org/10.1007/s41870-020-00581-y
12. H.R. Hasan, A. Musamih, K. Salah, R. Jayaraman, M. Omar, J. Arshad, D. Boscovic, Smart agriculture assurance: IoT and blockchain for trusted sustainable produce. Comput. Electron. Agric. 224, 109184 (2024)
13. M. Hrouga, A. Sbihi, M. Chavallard, The potentials of combining Blockchain technology and Internet of Things for digital reverse supply chain: A case study. J. Clean. Prod. 337, 130609 (2022)
14. M.S. Sheela, S.R. Chand, S. Gopalakrishnan, M. Gopianand, J.J. Hephzipah, Empowering Aquarists a Comprehensive Study On IOT-Enabled Smart Aquarium Systems For Remote Monitoring And Control. Babylon. J. Internet Things 2024, 33-43 (2024)
15. M. Van Wingerde, BLOCKCHAIN-ENABLED SELF-SOVEREIGN IDENTITY, Master Thesis, Delft University of Technology, Netherlands, 2017
16. E.K. Ruby, G. Amirthayogam, G. Sasi, T. Chitra, A. Choubey, S. Gopalakrishnan, Advanced Image Processing Techniques for Automated Detection of Healthy and Infected Leaves in Agricultural Systems. Mesopotamian J. Comput. Sci. 2024, 62-70 (2024)
17. Y. Wang, M. Zhong, T. Cheng, Research on PBFT consensus algorithm for grouping based on feature trust. Sci. Rep. 12, 12515 (2022). https://doi.org/10.1038/s41598-022-15282-8
18. A.M. Buttar, M.A. Shahid, M.N. Arshad, M.A. Akbar, Decentralized Identity Management Using Blockchain Technology: Challenges and Solutions, in Blockchain Transformations: Navigating the Decentralized Protocols Era (Springer Nature Switzerland, Cham, 2024), pp. 131-166
19. T. Feng, P. Yang, C. Liu, J. Fang, R. Ma, Blockchain Data Privacy Protection and Sharing Scheme Based on Zero-Knowledge Proof. Wireless Commun. Mobile Comput. 2022, 1040662 (2022)
20. I. Hagui, A. Msolli, N. ben Henda, A. Helali, A. Gassoumi, T.P. Nguyen, F. Hassen, A blockchain-based security system with light cryptography for user authentication security. Multimedia Tools Appl. 83, 52451-52480 (2024). https://doi.org/10.1007/s11042-023-17643-5