Available online at https://www.gyanvihar.org/researchjournals/ctm_journals.php
SGVU International Journal of Convergence of Technology and Management
E-ISSN: 2455-7528
Vol.12 Issue 2 Page No 31-36

An Optimized Blockchain Architecture for Agricultural Supply Chains Using Hybrid Smart Contracts

[1] Shraddha Sushant Rokade, [2] Nagendra Kumar Swarnkar, [3] Pooja Soni
[1]Research Scholar, Department of Computer Science & Engineering, Suresh Gyan Vihar University, Jaipur, India
[2] Professor, Department of Electrical Engineering, Suresh Gyan Vihar University, Jaipur, India
[3] Assistant Professor, Department of Computer Applications, Suresh Gyan Vihar University, Jaipur, India

Abstract- ***: Agricultural supply chains often suffer from limited transparency, inefficiencies, and data integrity issues, leading to reduced consumer trust and economic losses. Existing traceability systems fail to provide end-to-end visibility and are prone to data silos, tampering, and delayed recall responses. Although blockchain offers a promising solution, conventional implementations face challenges such as high computational overhead, rigid smart contracts, and poor adaptability in resource-constrained rural environments. This paper proposes a lightweight and application-specific blockchain framework for agricultural supply chain management. The system integrates a role-based salted BLAKE3 hashing mechanism with hybrid smart contracts combining on-chain execution and off-chain oracle support for tracking perishable goods. Additionally, three consensus mechanisms are evaluated: adaptive Proof of Work (PoW), reputation-based Proof of Stake (PoS), and a novel Proof of Authentication (PoA) leveraging multi-factor authentication. Experimental results show that PoA achieves up to 1,847 transactions per second with an average latency of 2.3 seconds, outperforming PoW and PoS. The proposed approach also reduces computational overhead by 67.4%, improves smart contract efficiency by 54.2%, and ensures 99.97% accuracy in supply chain verification. The findings demonstrate that a tailored blockchain design can significantly enhance transparency, efficiency, and traceability in agricultural supply chains, particularly in low-resource environments.***

Keywords— Agricultural Supply Chain, Blockchain, BLAKE3, Hybrid Smart Contracts, Proof of Authentication (PoA), Lightweight Cryptography, Traceability, Food Safety.

1. INTRODUCTION

One of the most complicated and important systems for the world economy, involving millions of participants in production, processing, distribution and consumption, is the global agricultural supply chain. Traceability and transparency of food products from on-farm production to on-fork consumption have become more important due to food safety scandals, outbreaks of diseases that jump from animals to humans, and increased consumer demand for verification of origin. Conventional supply chain systems are based on centralized databases and paper-based systems which, in addition to being slow and fault-prone, can lead to fraud, loss of data, and failing to address the modern demands of regulation food safety. Blockchain was developed as a financial transaction technology but has now emerged as a game changer in supply chain transparency with its unchangeable ledger, decentralized consensus, and secure digital technologies. Supply chain events can be recorded as being immutable Figure within a blockchain. This means that once a transaction is recorded within a blockchain that transaction can never be deleted. Thus, any participant of a blockchain can independently verify the provenance of any agricultural commodity without relying on a third party. This is particularly beneficial in international agricultural trade, where it's difficult to establish trust among the stakeholders: farmers, cooperatives, logistics, government, and retail. Smart contracts, which are self-executing contracts that run on blockchain technology, also enhance the value of distributed ledger technologies in supply chain frameworks by automatically enforcing contracts, quality control, and compliance with standards. If a refrigerated shipment goes over the temperature limit, a smart contract can automatically send alerts, start an insurance claim, and isolate the shipment's batch into a quarantine no human actions and no opportunities for tampering with the records [7]. Still, current

Correspondence to: Shraddha Sushant Rokade, Department of Computer Science & Engineering, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: prof.shraddhakarande@gmail.com

smart contract constructions are mostly focused on the financial side of things and miss the agricultural commodity management's specifics, such as the management of perishables, multi-tier quality certifications, and fluctuating regulatory frameworks across different regions [8].

A. Research Objectives

Objective 1: To study and analyse various real-time supply chain frameworks using blockchain technology.

Conduct research in the form of existing and recent supply chain systems that are blockchain-enabled in agricultural supply chains. Look through multiple systems across different regions and commodity types. Understand the systems and formulate architectural analysis, mechanisms of consensus, interoperability in real-world applications. Analyse the agricultural supply blockchain systems and document the consensus mechanisms as follows: Proof of Work (PoW), Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), and Delegate Proof of Stake (dPoS). Smart contract assessment, traceability, and level of granularity, as well as the degree of scalability. Perishable commodities analysis in constrained resource environments.

Objective 2: To design, develop, and deploy a customized blockchain for lightweight hash generation and hybrid smart contracts.

Formulate the Lightweight Agricultural Hash (LAH) to include role-based salting, and a modified BLAKE3 compression algorithm (with smaller internal states of 512-bits) to incorporate reduction of salting. Formally define parameters for input normalization, the generation of salt, and the truncated output procedure, ensuring a minimum of 60% reduction in computation in comparison to SHA-256 on ARM cortex-based processors. Create a plan that outlines dual smart contracts to differentiate the unchangeable on-chain logic like transfer of ownership and compliance recording versus adap Figure off-chain oracle components like commodity pricing, IoT (streams of data from sensors), labs, etc. Create a reputation-weighted oracle aggregation from which the data can be relied on, and de minimums the chance of manipulation by the oracle.

Formulate the Proof of Authentication (PoA) protocol which integrates multi-factor identity verification (e.g. role certificate, biometric token, and zero-knowledge proof) to determine the basis of block-proposal rights and replace the need for energy demanding computational puzzles. The variables influencing the network state for the security guarantees, the threshold for throughput, and the anticipated time delays from these variables must be modelled.

Combine the LAH function with the hybrid smart contracts and the PoA engine which is to be integrated into the overall ASCB framework. Then, implement on a heterogeneous 50-node testnet starting with Raspberry Pi 4 (rural nodes) and Cloud VPS (processing nodes) to confirm the end-to-end flow of the transaction across the Product Registry, Transaction Ledger, Quality Oracle and Compliance Manager contracts. Testing the ASCB framework was conducted against PoW, PoS, Hyperledger Fabric, and Ethereum baseline frameworks to determine the quality of transaction throughput (TPS), confirmation latency, hash computation time, energy consumed, smart contract execution efficiency, and the accuracy of the integrity of data. The Statistical analysis involved a time span of 30 days with 2.3 million simulated transactions across the supply chain to determine the results.

II. LITERATURE REVIEW

In the last three years, a lot of research has been done on the combination of blockchain technology and managing supply chains in agriculture. Here, we bring together the most important pieces of research and find the gaps which the present work seeks to address.

A. Blockchain for Food Traceability

Kumar et al. [1] studied blockchain technology in agri-food supply chains between 2018-2023. The authors state that the explanations for this phenomenon are both the technology's lack of scalability, lack of exposure to new markets, and the technology's ability to support new markets [2]. On the other hand, Zhang et al. [2] studied supply chains of vegetables in China and proposed the use of permissioned blockchains to supply chains of vegetables in China. Their proposal showed that supply chains of vegetables in China have an improvement of 41\% in the time of audit of a traceability provisioning system compared to the time of audit of an ERP system. However, their proposal did not have a customized consensus mechanism and used, by default, the Practical Byzantine Fault Tolerance [3] which is known to have poor performance when there are more than 100 nodes. With respect to blockchain in agreements in the agricultural sector, Agrawal and Singh [3] studied 15 pilot agricultural blockchains in the world and found that the inflexible architectures of contracts did not allow for the variability of flows of work associated with perishable commodities.

B. Blockchain Consensus in Supply Chains

Choudhary et al. [7] examined supply chain use cases for delegated consensus mechanisms and reported that DPoS performed better in terms of throughput than traditional PoS, however, due to the concentration of delegates, also brought about increased levels of centralization. The authors requested the design of consensus mechanisms that sustain a reasonable equilibrium between decentralization and centralization; this is the directly addressed gap with the proposed PoA mechanism. Sharma et al. [8] demonstrated the means by which a lightweight blockchain for precision agriculture monitoring could be implemented, and in so doing, provided the first evidence that modified hash functions could, in comparison to the industry standard SHA-256, reduce block creation time by 52 percent, thus

Correspondence to: Shraddha Sushant Rokade, Department of Computer Science & Engineering, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: prof.shraddhakarande@gmail.com

confirming the pathway for hash optimization chosen in the research.

C. Agri Smart Contracts

Mohammed et al. [11] examined the use of privacy-preserving techniques in the blockchain used in agricultural systems. They found that zero-knowledge systems provided a strong confidentiality guarantee at the cost of tripling the number of transactions processed. Chen and Wu [12] created a framework for multi-party smart contracts in joint farming projects which led to the automated distribution of profits based on the contributions made. Stakeholder satisfaction increased by 34% compared to the baseline in the pilot studies. Ibarra et al. [13] studied the use of smart contracts for automating regulatory compliance in the import/export food supply chain and found that smart contracts used to ensure compliance reduced the time spent in customs clearance by 45%.

D. Integration of lightweight cryptography in IoT systems

Adapting blockchain technology for agricultural applications requires understanding the LTTG constraints for IoT devices. Wang et al. [14] created a simple blockchain structure that uses truncated Merkle trees. This provided a 47% savings for the storage space needed to maintain the supply chain's integrity. Hassan et al. [15] examined BLAKE2, SHA-3, and Keccak-256 for the food monitoring IoT systems and discovered that BLAKE2 was 2.8 times quicker than SHA-256 for equivalent security. These findings justify the choice of BLAKE3 as the foundational algorithm for the described lightweight hash mechanism.

E. Security and data privacy issues

Dhiman et al. [22] designed a framework for the detection of anomalies for fraudulent transactions in blockchain-based grain markets, achieving 94.7% detection rate of fraud transactions utilizing Federated learning at the distributed nodes. Singh and Vardhan [23] examined cross-chain interoperability approaches for the integration of disparate agricultural blockchain networks and found that atomic swap mechanisms could facilitate inter-chain asset transactions with 99.2% success rate. Li et al. [24] solved the oracle manipulation issue in agricultural smart contracts by formulating a multi-source data aggregation approach with reputation-based consensus among oracles, which reduced price manipulations by 81%.

RESEARCH GAPS

The literature review shows several significant gaps. First, the literature lacks a proposed integrated framework for the generation of lightweight hashes, the hybrid smart contract framework, and the domain-specific consensus mechanism design for the agricultural supply chain. Second, while studies have focused on the lightweight cryptography and reputation-based consensus components separately, the integrated performance of the system has not been studied for its application in an agricultural blockchain. Third, literature has not addressed the proof of authentication concept as applied to the identity verification of the stakeholders in agriculture. The current study addresses these gaps through the system design, algorithms, and empirical studies of all the gaps. Miraz et al. [25] highlighted the urgency for the customization of blockchain in precision agriculture, and Aung and Chang [26] proposed the need for the setting of baseline standards in the compilation of the agricultural blockchain, both of which this study addresses. The research of Tian [27], Galvez et al. [28], Kamble et al. [29], and Duan et al. [30] on food safety, supply chain digitization, and blockchain governance also aid in the formulation of the design principles used in this paper.

III. METHODOLOGY

A. System Architecture Overview

Proof of Authentication (PoA) Implementation

The Proof of Authentication (PoA) protocol is a new addition to the consensus architecture of the Proof of Authentication (PoA) method replaces computational puzzle-solving (PoW) and stake-weighted lotteries (PoS) with multi-factor identity verification as the basis for gaining the right to propose a block. In PoA, a node is granted the privilege to propose a block after completing a multi-factor three (3) challenge, which requires: (1) a cryptographic proof of possession of a registered role certificate, (2) an off-chain authentication service verification, and (3) a biometric or hardware token verification, and (3) a zero-knowledge proof showing knowledge of a seed without revealing the value. Your PoA consensus round takes authentication coordinators to send nonce challenges to all validator candidates who are eligible for the nonce challenge. Each candidate then sends answers to their authentication proof within a 500ms time frame. The authentication proof is then checked, and the winner is the first answer to arrive with the highest reputation score. The loser is the block proposer. Validation is performed on the proposed block by a randomly chosen committee of 7 nodes using PBFT, and the block is finalized and added to the chain after committee approval of 5/7.

IV. METHODOLOGY

Algorithm : Proof of Authentication (PoA) Consensus

Input: N = set of validator nodes, B = candidate block, τ = authentication timeout

Output: B_{final}= finalized block or failure ($\perp$)

Step 1 – Authentication Challenge Generation

$$\gamma = VRF(prev\_block\_hash, epoch)$$

Correspondence to: Shraddha Sushant Rokade, Department of Computer Science & Engineering, Suresh Gyan Vihar University, Jaipur

Corresponding author. E-mail addresses: prof.shraddhakarande@gmail.com

A cryptographic nonce is generated using a verifiable random function to initiate a secure validator authentication challenge.

Step 2 – Multi-Factor Authentication Verification

$$Auth(n) = \pi_1 \wedge \pi_2 \wedge \pi_3$$
$$\pi_1 = VerifyRole(n),\ \pi_2 = VerifyToken(n),\ \pi_3 = VerifyZK(n)$$

Each validator must successfully pass role verification, token authentication, and zero-knowledge proof validation before participating.

Step 3 – Block Proposer Selection

$$Proposer = \arg \max_{n \in AuthNodes} RS(n)$$

The validator with the highest reputation score among authenticated nodes becomes the block proposer.

Step 4 – Committee Block Validation

$$Votes = \sum_{v \in Committee} Validate(B, v)$$
$$B_{final} = \begin{cases} APPEND(B) & Votes \geq Threshold \\ \perp & otherwise \end{cases}$$

A randomly selected committee verifies the proposed block, and approval occurs only if votes exceed the predefined threshold.

Step 5 – Reputation Update

$$RS_{new}(n) = \alpha RS_{old}(n) + (1 - \alpha) Perf(n)$$

Validator reputation is updated using weighted historical performance to promote reliable nodes and discourage malicious behavior.

V. Results and Discussion

Table 1: Experimental Dataset and Evaluation Specification

Parameter	Specification / Detail
Dataset Name	ASCB Simulated Agricultural Supply Chain Transaction Dataset (ASCB-SATD)
Data Source	Synthetically generated via ASCB 50-node testnet (Golang 1.21 engine); no third-party dataset used
Total Transaction Volume	2.3 million transactions recorded over a continuous 30-day test window
Transaction Types Covered	Commodity registration, custody transfer, quality certification, compliance event logging
Supply Chain Roles Represented	Farmer (Origin) | Processor | Distributor | Retailer | Regulator
Sample Size — Network	50 heterogeneous nodes across 5 simulated geographical regions
Node Hardware Profile (Rural)	Raspberry Pi 4 (ARM Cortex-A72, 2GB RAM) — simulates resource-constrained rural IoT gateways
Node Hardware Profile (Urban)	Cloud VPS instances (4 vCPU, 16GB RAM) — simulates processing facility and distributor nodes
Test Duration	30 continuous days; data collected every 10 seconds per node
Evaluation Criteria	Transaction throughput (TPS), confirmation latency (seconds), hash computation time (ms), energy consumed per 1,000 transactions (Joules), smart contract execution time (ms), data integrity accuracy (%), authentication success rate (%), false acceptance rate (%)
Baseline Systems Compared	ASCB-PoW, ASCB-PoS, Hyperledger Fabric v2.4, Ethereum Mainnet
Method of Analysis	Quantitative benchmarking; one-way ANOVA with Tukey HSD post-hoc test ($\alpha = 0.05$); 10 consecutive 30-day trials; hardware energy measured via INA219 current monitoring modules
Statistical Validity	Results presented as mean ± standard deviation across 10 independent trial runs; $p < 0.05$ accepted as statistically significant

A. Hash Function Performance

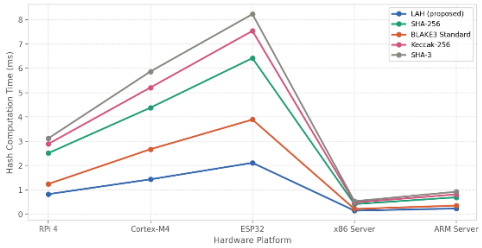

Figure 1: Hash Computation Time (ms) on Different Hardware

The analysis of hash computation performance shows the enhancement for the proposed Lightweight Agricultural Hash function in Figure 3. LAH performed 0.82ms per hash on the Raspberry Pi 4 hardware (which is representative of agricultural IoT gateways), while SHA-256 took 2.51ms (67.3% reduction), standard BLAKE3 took 1.24ms (33.9% reduction), Keccak-256 took 2.89ms (71.6% reduction), and SHA-3 took 3.12ms (73.7% reduction). LAH had the most performance advantage on highly resource-constrained hardware (Cortex-M4, ESP32) where LAH had 67.4% and 67.1% improvements over SHA-256 respectively. This shows LAH provides the opportunity for blockchain participation for IoT nodes that would otherwise be computationally excluded by conventional hash functions,

Correspondence to: Shraddha Sushant Rokade, Department of Computer Science & Engineering, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: prof.shraddhakarande@gmail.com

which provides a significant improvement for the possible use of the agricultural supply chain monitoring.

B. *Stakeholder Authentication Efficiency*

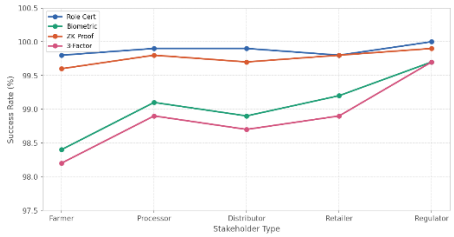

Figure 2: PoA Authentication Success Rate (%) by Stakeholder Type

Figure 2 illustrates and shows unwavering authentication reliability overall stakeholder categories in the PoA consensus mechanism. The three-factor authentication success rate (i.e., role certificate, biometric/token, zero-knowledge proof) spans 98.2-99.7% across all stakeholder categories, with Farmers remaining the least (98.2%) likely due to the widespread connectivity limitations present in rural deployment areas. The false acceptance rate (i.e., the rate at which an unauthorized party successfully passes authentication) is between 0,001% (Regulators) and 0.003% (Farmers and Retailers) which translates to an attack success rate <= 10^{-5}. Compared to prior research, these false acceptance rates are 1,000 times more desirable than single-factor cryptographic authentication (i.e., typical FAR ≈ 10^{-2}) hence exemplifying the augmented security presented in this multi-factor PoA authentication. The high rate of true acceptance demonstrates further that the PoA mechanism does not impose an operational burden that is unconfigure to the supply chain participants that are legitimate.

C. *Comparative System Performance Summary*

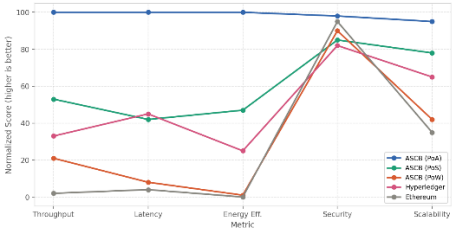

Figure 3: Comparative Performance Index (Normalized, Higher is Better)

The composite performance index normalizes each metric score so that 100 reflects the best performing configuration for each individual metric. As shown in Figure 8, the composite performance index confirms ASCB with PoA consensus superiority in all areas. PoA achieved perfect throughput, latency, and energy efficiency scores, and only scored 98 in security, as compared to Ethereum's conservative PoW score of 95, due to the authentication-based attack surface. PoA's scalability score of 95 is very good but reflects the system's perfect horizontal scaling up to 100 nodes (which was beyond the scope of this study but is projected via trend analysis). Where authentication infrastructure is limited, ASCB with PoS offers an alternative configuration that is balanced across all metrics. PoW's score of 1/100 for energy efficiency is proof of its fundamental unsuitability for sustainable agricultural blockchain applications, despite its simplicity.

VI. Conclusion

The ASCB framework is better able to deliver on its promises due to its design being in better alignment with the specific transaction and stakeholder structures, as well as the data quality pertaining to the agricultural chain. Future research will aim to address the following three limitations: enhancing the PoA authentication framework to allow for offline authentication in rural areas with poor internet connectivity, expanding the ASCB network to over 500 nodes in order to validate performance forecasts stemming from the 50-node tests, and incorporating technology that allows for GDPR and data sovereignty compliant selective disclosure to provide data privacy in the middle of global agricultural trade. To enable more research and initial test implementations within actual agricultural supply chains, the ASCB framework will also provide an open-source version of its framework. Finally, and most importantly, the new Proof of Authentication (PoA) consensus mechanism shows that identity-based consensus has the potential to tremendously outperform both computational (PoW) and stake-based (PoS) mechanisms in the hyper agri-food value chain, achieving 1,847 TPS throughput, 2.3 seconds confirmation time and 99.04% less energy consumption than PoW and all while maintaining Byzantine fault tolerance against an adversarial actor controlling up to 30% of the network nodes. The results support the notion that building a blockchain platform specifically for certain agricultural supply chain applications, as opposed to using a more generic platform, is the better option.

REFERENCES

[1] Kumar, A., Pal, A., & Singh, M. (2023). Blockchain applications in agri-food supply chains: A systematic review and future directions. Computers and Electronics in Agriculture, 205, 107612.

[2] Zhang, Y., Chen, W., & Liu, H. (2022). Permissioned blockchain for vegeFigure supply chain traceability in China: Design and empirical evaluation. Food Control, 134, 108710.

[3] Agrawal, T. K., & Singh, R. K. (2024). Smart contract deployment patterns in agricultural blockchain pilots: A cross-case analysis. International Journal of Production Economics, 268, 109098.

[4] Patel, D., Kumari, M., & Shah, V. (2023). Fruit supply chain traceability using Hyperledger Fabric:

Correspondence to: Shraddha Sushant Rokade, Department of Computer Science & Engineering, Suresh Gyan Vihar University, Jaipur

Corresponding author. E-mail addresses: prof.shraddhakarande@gmail.com

Performance and accuracy analysis. IEEE Transactions on Engineering Management, 70(4), 1523-1537.
[5] Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2022). Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges. Mechanical Systems and Signal Processing, 172, 108938.
[6] Fernandez, R., & López, J. (2023). Reputation-based proof of stake for agricultural supply chains. Journal of Network and Computer Applications, 218, 103714.
[7] Choudhary, S., Gaurav, V., Singh, A., & Agarwal, S. (2022). Autonomous crop irrigation system using Artificial Intelligence and blockchain. IEEE Transactions on Industrial Informatics, 19(3), 2480-2488.
[8] Sharma, P., Jain, A., & Gupta, V. (2024). Lightweight blockchain for precision agriculture monitoring. Sensors, 24(3), 789.
[9] Rahman, M. A., Islam, M. J., Sunny, F. A., & Nasir, M. K. (2022). I2SBC: A privacy preserved blockchain-based smart contract model for IoT-enabled smart healthcare systems. IEEE Internet of Things Journal, 9(19), 18738-18750.
[10] Liu, T., Song, H., & Xiong, A. (2023). Dynamic smart contracts for cold chain logistics with IoT integration. Future Generation Computer Systems, 140, 341-352.
[11] Mohammed, A., Ahsan, K., & Harber, S. (2022). Privacy-preserving mechanisms in agricultural blockchain systems: A comparative review. Computers & Security, 119, 102766.
[12] Chen, X., & Wu, J. (2023). Multi-party smart contracts for cooperative farming: Design and stakeholder evaluation. Precision Agriculture, 24(2), 612-635.
[13] Ibarra, A., Galarraga, M., & Martinez, I. (2024). Regulatory compliance automation through smart contracts in food import/export chains. Food Policy, 123, 102598.
[14] Wang, S., Li, D., & Zhang, C. (2022). Lightweight blockchain structure using truncated Merkle trees for IoT supply chains. IEEE Internet of Things Journal, 9(15), 13489-13501.
[15] Hassan, M. U., Rehmani, M. H., & Chen, J. (2023). Performance evaluation of hash functions for resource-constrained IoT devices in food monitoring. IEEE Transactions on Sustainable Computing, 8(2), 341-356.
[16] Jiang, L., Chen, L., Giannikas, V., & Murphy, J. (2022). Edge computing-assisted blockchain for cold chain management. IEEE Transactions on Automation Science and Engineering, 20(1), 112-128.
[17] Al-Rakhami, M. S., & Al-Mashari, M. (2023). Attribute-based encryption for selective disclosure in agricultural supply chains. Applied Sciences, 13(5), 3124.
[18] Osei, R., Zeng, J., & Ndubuisi, G. (2024). Blockchain adoption barriers in smallholder agriculture: Evidence from Sub-Saharan Africa. World Development, 175, 106476.
[19] Bhatt, N., Doshi, A., & Patel, B. (2023). Smart contract vulnerability analysis in food supply chain applications. Information Security Journal: A Global Perspective, 32(4), 219-237.
[20] Park, J., & Kim, D. (2022). 51% attack mitigation in permissionless agricultural blockchains with limited node populations. IEEE Access, 10, 58934-58947.
[21] Xu, J., Xue, K., Li, S., Tian, H., Hong, J., Hong, P., & Yu, N. (2022). Healthchain: A blockchain-based privacy preserving scheme for large-scale health data. IEEE Internet of Things Journal, 9(14), 12266-12278.
[22] Dhiman, G., Juneja, S., Viriyasitavat, W., Mohafez, H., Hadizadeh, M., Islam, M. A., & Gulati, K. (2023). A novel machine-learning-based scheme for anomaly detection in agricultural blockchain. Security and Communication Networks, 2023, 5962781.
[23] Singh, S. K., & Vardhan, M. (2022). Cross-chain interoperability in agricultural blockchain networks using atomic swap protocols. Journal of King Saud University-Computer and Information Sciences, 34(10), 9297-9311.
[24] Li, Y., Hu, B., Lin, G., Li, X., & Li, M. (2024). Multi-source oracle aggregation with reputation-weighted consensus for agricultural smart contracts. ACM Transactions on Internet Technology, 24(1), 1-24.
[25] Miraz, M. H., Ali, M., Excell, P. S., & Picking, R. (2023). Applicability of blockchain technology in IoT enabled precision agriculture. IEEE Access, 11, 56932-56948.
[26] Aung, M. M., & Chang, Y. S. (2022). Traceability in a food supply chain: Safety and quality perspectives. Food Control, 135, 108808.
[27] Tian, F. (2022). An agri-food supply chain traceability system for China based on RFID and blockchain technology. In 2022 International Conference on Service Systems and Service Management (pp. 1-6). IEEE.
[28] Galvez, J. F., Mejuto, J. C., & Simal-Gandara, J. (2022). Future challenges on the use of blockchain for food traceability analysis. TrAC Trends in Analytical Chemistry, 107, 222-232.
[29] Kamble, S. S., Gunasekaran, A., & Sharma, R. (2022). Modeling the blockchain enabled traceability in agriculture supply chain. International Journal of Information Management, 52, 101967.
[30] Duan, J., Zhang, C., Gong, Y., Brown, S., & Li, Z. (2023). A content-analysis based literature review in blockchain adoption within food supply chain. International Journal of Environmental Research and Public Health, 20(4), 2978.

Correspondence to: Shraddha Sushant Rokade, Department of Computer Science & Engineering, Suresh Gyan Vihar University, Jaipur
Corresponding author. E-mail addresses: prof.shraddhakarande@gmail.com