Access control of IoT devices based on smart contracts and double-layer channels

1st Hélio Salomao Pesanhane
Department of Informatics and Statistics
Federal University of Santa Catarina
Florianópolis, SC Brazil
pesanhane@gmail.com

2nd Fernando Luiz Koch
Department of Informatics and Statistics
Federal University of Santa Catarina
Florianópolis, SC Brazil
0000-0001-7136-3253

3rd Carlos Becker Westphall
Department of Informatics and Statistics
Federal University of Santa Catarina
Florianópolis, SC Brazil
0000-0002-5391-7942

***Abstract*—Blockchain technology has shown promise in addressing transparency, traceability, and accountability issues in the agrifood supply chain. However, the pursuit of transparency raises privacy concerns, and the integration of IoT devices brings about challenges in terms of performance, mobility, and data volume. We introduce a two-layer architecture for access control, specifically tailored to the attributes of IoT devices. The proposed architecture consists of individual blockchain channels for each Edge Cluster, along with a centralized superior channel responsible for storing contracts. Within each Edge Cluster, a master-slave relationship is established between the edge server and IoT devices.**

***Index Terms*—Internet of Things (IoT), blockchain, privacy, access control, smart contract.**

I. Introduction

The application of blockchain technology in managing the agrifood supply chain has gained attention for its inherent features of decentralization, transparency, and immutability [1]. This technology offers solutions to critical issues in traceability, data tampering, liability concerns, and visibility gaps within the supply chain [2], [3]. Despite its merits, the decentralized and transparent nature of blockchain introduces challenges related to data misuse and privacy, particularly when transactions are not validated by a single entity and are accessible to all participants.

In the agrifood supply chain, the integration of IoT devices and sensors has become integral, providing essential information during various stages such as production, harvesting, storage, and transport. This data, often commercially sensitive, is disseminated to consumers and data buyers [4]. However, two primary challenges emerge in this context:

1) **Ensuring Trust in Data**: Data buyers must verify the legitimacy of the data, ensuring it remains untampered, issued by legitimate devices, accurately reflects the state of the object in the specified timeframe, and was emitted from the designated location.
2) **Preserving Confidentiality**: Safeguarding the owner's information while provisioning data poses a significant hurdle.

Despite existing proposals for decentralized IoT systems, the majority remain centrally managed, allowing potential tampering and unauthorized disclosure. This undermines credibility in environments where multiple parties exchange information. Blockchain technology, with its decentralized, immutable, and transparent attributes, offers a solution. However, the computational and communication overhead for IoT devices [5] poses implementation challenges.

To address this, our study proposes a two-layer architecture for access control based on IoT device attributes. Each edge cluster will have a hyperledger channel, and a superior channel will store access control contracts. The edge server and IoT device will establish a master-slave relationship in each cluster. When a device requests access, the edge server retrieves a contract from the superior channel and executes it on the local channel.

Our contribution to the current state of the art includes:

- A distributed private data storage and access control framework ensuring the confidentiality, integrity, and availability of IoT data, with transactions recorded in the common ledger for transparency.
- A model for sharing IoT-generated data through an authorization contract, allowing access without compromising sensitive information or requiring trusted third-party intervention.
- A mechanism for defining granular access control policies, facilitating device- and use-case-specific rules.

II. Related Work

We conducted an exploration of the current landscape concerning the integration of Blockchain and IoT in agrifood supply chain management. Our emphasis was on scrutinizing existing work related to the preservation of data privacy and the implementation of access control mechanisms. Table I provides an overview of our analysis, organized into the following categories:

- **Privacy**: this critical aspect is closely linked to the sharing of IoT data and user personal information within a network. It is imperative to ensure that such information is disclosed only to authorized parties and at appropriate times. The access control mechanism assumes a pivotal role in establishing user trust while safeguarding their privacy. Data owners retain complete control over granular access to the data they share, empowering them to maintain full control over their information.

TABLE I
ANALYSIS OF THE STATE-OF-THE-ART

Projects	*Privacy*	*Confidentiality and Integrity*	*Access Control*	*Contract automation*	*Lightweight devices demand*	*Storage overhead relief*	*trusty data storage and sharing*
Lin et al (2019) [6]	✓	✓	✗	✓	✗	✓	✗
Shahid et al (2020) [7]	✗	✗	✗	✓	✗	✓	✗
Feng et al (2020) [8]	✓	✓	✗	✓	✗	✓	✗
Shakhbulatov et al (2019) [9]	✓	✗	✗	✗	✓	✓	✗
Tran et al (2021) [10]	✓	✗	✗	✓	✓	✓	✗
Yang et al (2021) [11]	✓	✓	✓	✓	✗	✓	✗
Our proposal	✓	✓	✓	✓	✓	✓	✓

- **Confidentiality and integrity**: ensuring that no resources are disclosed without proper authorization and taking all precautions to prevent improper modification of resources are essential considerations. The grammar used to formulate control and access rules must be precise and expressive, facilitating the revocation of access rights for users when necessary.
- **Access control**: serves as support to authentication and authorization mechanisms in an open environment where interconnected devices are prevalent. This prevents access to sensitive data, unauthorized changes, denial of service, etc. Here, we focus on the innovations introduced by the project in terms of access control, distinct from basic blockchain access control.
- Contract automation: involves the electronic representation of terms and conditions governing transactions between multiple parties.
- **Lightweight devices demand**: addressing the need for effective access control strategies to minimize overhead on IoT devices, which are typically characterized by limited memory, computing resources, and energy supply [12] [13].
- **storage overhead relief**: refers to the reduction in storage required by each node in the blockchain network, as well as blockchain traffic. Handling off-chain data using smart contracts when interacting with a blockchain is crucial, considering the potential negative impact of rapid data growth on query performance and the cost of data management [12], [5].
- **Trusty data storage and Sharing**: Encompasses the belief of a commercial participant in the agri-food supply chain that data is stored and shared honestly. Effective IoT data-writing access control mechanisms are necessary to ensure data integrity, especially when predicting food production or waste, providing valuable information for the food safety sector.

The works analyzed present various approaches to integrating blockchain and IoT in agrifood supply chain management. The following summaries provide insights into each entry in Table I.

Lin et al. (2019) [6] utilizes blockchain to store evidence information, with most data stored outside the blockchain. As a limitation, the proposal lacks emphasis on access control, lightweight device demand, and data-sharing considerations.

Shahid et al. (2020) [7] uses blockchain for recording transaction hashes, while true data are stored in IPFS. Limitations: IPFS content is publicly accessible, and the study does not explore encryption for sensitive data protection or direct integration of IoT devices.

Feng et al. (2020) [8] utilizes two cloud-based databases for private and public data, mapped using blockchain-stored hashes. Limitations: Ignores lightweight device demand, lacks evaluation of information credibility, and presents no innovation in access control mechanisms.

Shakhbulatov et al. (2019) [9] proposes a blockchain solution for tracking carbon footprints, using cluster-based record-keeping for privacy. Nonetheless, it lacks an access control mechanism for data read/write permissions, and does not address smart contracts or processes for sharing network data.

Tran et al. (2021) [10] proposes a privacy-preserving framework for smart agriculture using private channels for each farmer's IoT data. However, the proposal does not define an access control mechanism.

Yang et al. (2021) [11] implements a dual storage strategy with public information in a local database and private data encrypted on the blockchain. The proposal does not address challenges with lightweight devices and data sharing; private data access is non-transferable.

These analyses highlight the diversity of strategies in the literature but also reveal common limitations, such as insufficient consideration for access control mechanisms, lightweight device demands, and comprehensive data-sharing solutions. Our proposed two-layer architecture aims to address these gaps by providing a robust framework that enhances privacy, access control, and overall efficiency in managing IoT data within the agrifood supply chain.

A. Challenges and Opportunities

Upon conducting the analysis of the existing literature, it is evident that previous research has recognized the imperative need for a robust agrifood traceability system. Such a system must efficiently detect and prevent food safety issues, track responsibilities, and overcome the shortcomings associated with centralized approaches. Centralized models have been deemed unsuitable due to their lack of transparency, accountability, and audibility, as well as their dependence on third-party data storage and management.

In response to these challenges, researchers have advocated for the integration of blockchain technology in the agrifood supply chain, aiming to eliminate third-party intermediaries and ensure data immutability, transparency, traceability, and process automation. While these approaches have successfully addressed some challenges related to blockchain implementation, they also exhibit certain limitations.

- **Data-Write Access Control**: existing studies have overlooked the critical issue of data-write access control. Despite the immutability of blockchain data, uncertainty remains regarding the accuracy and honesty of recorded information. Dishonest users may generate false data for personal gain, and equipment malfunctions may transmit invalid data, risking the erosion of trust among chain members.
- **Privacy and Confidentiality**: current privacy and confidentiality approaches focus on concealing private data from unauthorized users but lack comprehensive access control mechanisms. The absence of mechanisms allowing subjects to grant or revoke access rights poses a limitation.
- **Storage and Dissemination of IoT Data**: limited research exists on the storage and dissemination of IoT data related to crop production and food status. These data are pivotal for advancing agriculture, ensuring food security, and predicting phenomena in the agrifood chain, such as crop diseases, yields, food conditions, and waste.
- **Demand for Lightweight Devices**: the issue of lightweight device demand has not been adequately addressed in existing proposals, hindering the seamless integration of these devices into the agri-food supply chain.
- **Utilization of Smart Contracts**: while the utilization of smart contracts shows promise, it is still in its early stages. Various activities within the agri-food supply chain demand automation, necessitating further exploration and development.

Given the identified challenges, there exist significant opportunities to contribute to the state-of-the-art by offering solutions that specifically address these issues. A comprehensive solution would focus on:

1) Developing robust data-write access control mechanisms to ensure the integrity of information within the blockchain.
2) Enhancing privacy and confidentiality measures by incorporating sophisticated access control mechanisms for granting, revoking, and managing access rights.
3) Conducting research on the storage and dissemination of IoT data, particularly in areas crucial for advancing agriculture and ensuring food security.
4) Addressing the demand for lightweight devices in the context of the agri-food supply chain.
5) Advancing the utilization of smart contracts for automated processes within the agri-food supply chain, fostering efficiency and information exchange.

By addressing these opportunities, future research can significantly contribute to the advancement and effectiveness of blockchain-integrated solutions in the agri-food supply chain.

III. Proposal

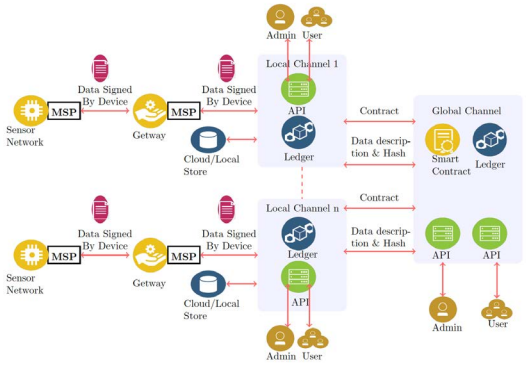

Fig. 1. Proposed Architecture

This study introduces a two-layer architecture illustrated in Figure 1 in response to the challenges identified in preceding sections, encompassing privacy invasion, data leakage, storage and network overhead, lightweight device demand, and data sharing issues. In this architecture, sensors and microcontrollers employing a lightweight messaging library for communication with small mobile devices. The Membership Service Provider (MSP) grants identity to sensors and gateways. When a sensor emits data, it signs and encrypts it using light encryption before forwarding it to the gateway. Subsequently, the gateway signs and encrypts the data using the device owner's identity and submits it to the blockchain. External users may access private data through a reading-access contract signed with the data owner.

In this design, critical information ensuring network traceability and transparency, along with data descriptions and hashes representing each edge channel, is housed in the upper channel. The device owner must be an enrolled user in the upper channel for an IoT device to record data in the cloud/local data store, managed through the edge channel, and to ensure data validity at the upper channel level. While participants of the common channel do not have direct access to the content of IoT data registered in the private channel, they place trust in this data due to adherence to contract terms defined and approved by upper channel participants. The data-writing process involves a two-tier authorization mechanism: a first-level check ensuring the device belongs to a valid participant in the local channel and a subsequent second-level verification based on attribute-based access control (ABAC) policies. Once device data registration is approved, a token with a defined validity period is generated, encrypted with the device's public key, and stored on the local channel. Verification of token validity and the transmitted value ensures compliance with allowed ranges.

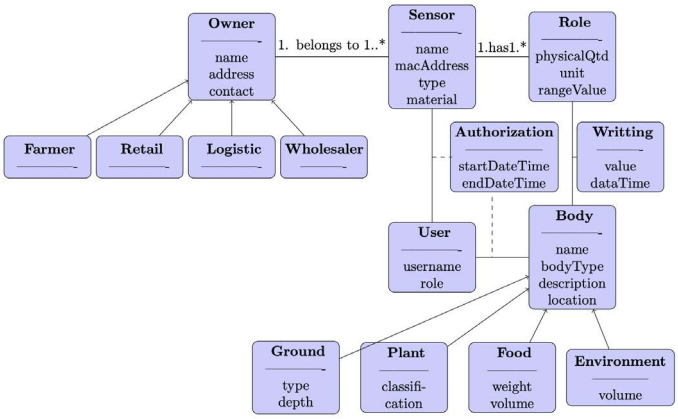

Fig. 2. Description of data writing and reading management.

A. Use Case: IoT Devices in the Agrifood Supply Chain

In the context of the agrifood supply chain, this study delves into the use case of IoT devices, focusing on the intricacies of data-writing access contracts and reading-access authorization contracts (depicted in Figure 2). The primary players in this scenario include the device owner, the devices responsible for recording collected data, and the authorized users granted access to retrieve this data.

This use case entails the following actors:

- **Device Owner**: representing entities such as farmers, government bodies, logistics companies, retailers, or wholesalers, possess a fleet of devices collecting data on various facets of the agrifood supply chain. This encompasses elements like soil conditions, plant health, food status, and environmental conditions within food storage facilities.
- **Devices**: each device within the ownership of the device owner is endowed with a unique identification and MAC address. These identifiers enable devices to seamlessly transmit data concerning the entities involved in the supply chain.

  Users: Users, granted explicit authorization by the device owner, are bestowed with the privilege to access and retrieve data based on the terms stipulated in the contract signed by the device owner.

For a sensor to successfully transmit data, it must fulfill specific criteria:

- Belonging to a participant registered as a local channel member.
- Possessing the requisite permissions to measure the physical quantity corresponding to the type of entity being measured.
- Emitting data within the predefined and allowed range, ensuring the accuracy and reliability of the transmitted information.

This use case outlines a structured framework wherein device owners orchestrate the flow of data from IoT devices, ensuring that authorized users can access pertinent information while maintaining the integrity and reliability of the data transmitted within the agrifood supply chain.

B. Advanced Attributes

Moreover, we proposed the utilization of the ABAC model, Natural Language Processing (NLP), and the object creation model for the administration of data transmitted by devices within the agri-food supply chain led to the formulation of the policy and attributes for the control of private data-writing access, which is outlined as follows:

P={ SA; OA; PA; EA } (1)

SA={deviceId, MacAdress, ownerId, participantType, roles{physicalQuantity, unit, range(min,max)} (2)

OA={ bodyId, bodyType, description } (3)

PA={ 1 grant, 0 deny } (4)

EA={ startTime, endTime, refCoordenates, distLimit } (5)

- **Policy (P)** is an attribute-based write access control policy that comprises the attributes SA, OA, PA, and EA.
- **Subject Attribute (SA)**: The device, when attempting to write private data, is characterized by various attributes, including its unique DeviceId, MAC address, and the unique identification of its owner, the participantType, roles, physicalQuantity, unit, range, and other relevant attributes.
- **Object attributes (OA)**: serve to identify the resource to be accessed, and consist of the following variables: ”bodyId”, which identifies the target object of measurement. ”bodyType”, which specifies the type of body, such as plant, food, or atmosphere, and ”description”, which provides detailed information about the object.
- **Environment Attributes (EA)** : handle the temporal and dynamic aspects of the access control scenario.
- **Permission Attribute (PA)** specifies whether the device is authorized to write the data, with a binary value of ”1” indicating allowance and ”0” denying access. The default value for PA is true.

To create the access control chain code, device ABAC attributes will be defined in the X509 certificates issued to identities on the blockchain network, and these identity attributes will be accessed within the chain code.

To record IoT data, an ABAC policy that complements an identity-based access control mechanism is configured at the network level in the hyperledger fabric. ABAC Contract Policy allows authentication of the device using a blockchain system, thereby proving its identity. Business-oriented verifications are performed to allow only the registration of data that really interest the owner and chain participants of the agri-food supply, thus giving more credibility to the registered data.

Figure 3 depicts the manner in which device attributes, edge, and top channels collaborate to perform ABAC policy contracts for device write access control.

A user can read the data emitted by a device or a certain body. Authorization for reading data is assigned to a user, and the contract for reading data is valid for only one user and is non-transferable.

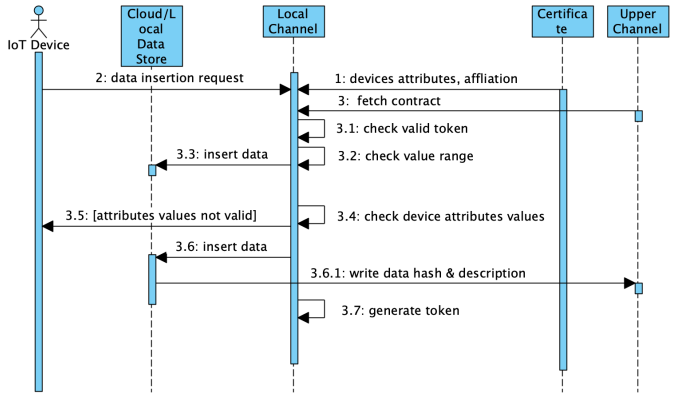

Fig. 3. sequence diagram illustrating the steps for writing data into cloud / local data store..

IV. Evaluation

This study proposes the use of a local channel to compute IoT device data within a private communication subnet, ensuring confidential transactions among specific members of the agrifood supply chain. Authentication and authorization within the local channel are facilitated by a Membership Service Provider (MSP), guaranteeing the legitimacy of each device, user, or identity joining the channel.

To register data on the channel or in a local database, devices must undergo authentication and authorization processes, mitigating the risk of invalid data registration through a smart contract invoked in the globally shared channel. Trusted entities at the upper channel level may participate in the local channel, enhancing transparency and data trustworthiness.

A. Lightweight Authentication Mechanism and Edge Computing

The implementation of a token-based authentication mechanism offers a lightweight approach, relying on the device's identity and Attribute-Based Access Control (ABAC) attributes during the initial access attempt. The token subsequently grants access to a specific resource for a defined time period, reducing computational expenses and conserving energy in IoT devices. Edge computing, executed within the local channel, ensures efficient handling of limited memory, computing resources, and energy, thereby minimizing system overhead.

B. Smart Contracts for Granular Access Control

The utilization of smart contracts, implementing ABAC access control policies, enables granular access control and permission management. This ensures that predefined access rights and permissions are automatically applied to IoT devices, restricting data access to authorized users only.

C. Data-Sharing Agreements and Identity Protection

For a user to access IoT data belonging to a chain member, a smart contract signed by both parties is required. This contract precisely defines the data accessible by the user, based on the identity of the owner, device, or the targeted entity for reading. The use of hash functions conceals the identities of the owner, user, and device within smart contracts, safeguarding sensitive information from potential leakage.

D. Performance Evaluation

The proposed methodology's performance was evaluated using metrics outlined in [14] and [15]. Specifically, latency and throughput of data writing to the ledger were assessed under the majority endorsement policy, utilizing both solo- and raft-ordering services. Solo exhibited a throughput of 342.58 transactions per second (TPS) with an average latency of 0.14 seconds, while raft achieved a throughput of 333.3 TPS, an average latency of 2.625 seconds, and a maximum latency of 3.671 seconds. These results demonstrate the efficiency of the proposed method in handling data transactions.

Additionally, a data recovery evaluation for varying sizes (8k to 512k) indicated times of 0.861 seconds for 8k and 1.076 seconds for 512k. Comparable results to those presented in [15] were achieved, with the added benefit of incorporating identity verification and contract reading for access control during data writing and reading operations.

Overall, the proposed methodology showcases robustness in authentication, access control, and transaction efficiency within the agrifood supply chain's IoT ecosystem.

V. Conclusions

Blockchain technology effectively addresses the issues of insufficient transparency, data manipulation, lack of accountability, and inadequate visibility that are prevalent in the agrifood supply chain through its attributes of decentralization, immutability, and traceability, However, the implementation of blockchain technology may also result in privacy concerns, particularly with the integration of Internet of Things (IoT) devices for monitoring agricultural production, harvesting, storage, and transport of food. These devices are limited in terms of computational resources, storage capacity, and energy consumption, making it challenging to manage and secure large-scale IoT environments using the current security, authentication, and access control solutions.

To address these challenges, this study introduces a two-layer access control architecture that utilizes IoT device attributes, including individual blockchain channels for Edge Clusters and a shared channel for contract storage. Within each cluster, the edge server and IoT device maintain a master-slave relationship. When access requests are triggered, contracts are retrieved from the upper channel for execution on the local channel, thereby addressing challenges associated with IoT data management and private data storage. The ABAC policy defined in this paper aims to explore the benefits of using ABAC, which allows devices to be authorized to write data about bodies without prior relatedness, and allows multiple devices to issue measurements of bodies without the knowledge of the rule creator. Users can acquire the right to

read IoT data by entering an ABAC policy agreement with the data owner.

Finally, the performance of the proposed method in data writing and retrieval using smart contracts was evaluated. Two distinct networks were established: one utilizing a solo network and the other using a raft as an ordering service. The registration of a transaction in the solo network had a maximum latency of 0.22 seconds and a throughput of 342.58 transactions per second, while the raft network had a maximum latency of 3.671 seconds and a throughput of 333.33 transactions per second. Furthermore, the proposed method was tested for recording different data sizes in the range 8K to 512K using Solo and CauchDB. The maximum latencies for these extremes were 0.861 s and 1.076 s for 8K and 512K, respectively. These results are comparable to those of previous studies despite the need to invoke contracts for reading and writing data.

REFERENCES

[1] A.Kamilaris, A.Fonts, F.X.Prenafeta-Bold, The rise of blockchain technology in agriculture and food supply chains, Journal. Trends in Food Science Technology, vol. 91, pp. 640–652 (2019), doi. 10.1016/j.tifs.2019.07.034

[2] C.Xie, Y.Sun, H.Luo, Secured data storage scheme based on blockchain for agricultural products tracking. pp. 45-50. IEEE, 2017 3rd International Conference on Big Data Computing and Communications (BIGCOM) (2017), doi.10.1109/BIGCOM.2017.43

[3] F.Tian, A supply chain traceability system for food safety based on haccp, blockchain amp; internet of things, pp. 1–6. IEEE, 2017 International Conference on Service Systems and Service Management. doi.10.1109/ICSSSM.2017.7996119

[4] M.S.Ali, K.Dolui, F.Antonelli, Iot data privacy via blockchains and ipfs, pp.1–7. ACM, Proceedings of the Seventh International Conference on the Internet of Things. New York, USA (2017) doi.10.1145/3131542.3131563

[5] A.Tripathi, K.Sharma, M.Bala, A.Kumar, V.Menon, A.Bashir, A Parallel Military-Dog-Based Algorithm for Clustering Big Data in Cognitive Industrial Internet of Things, journal. IEEE Transactions on Industrial Informatics,vol. 17, pp. 2134-2142 (2021), doi.10.1109/TII.2020.2995680

[6] Q.Lin, H.Wang, X.Pei, J.Wang, Food Safety Traceability System Based on Blockchain and EPCIS, IEEE Access, vol. 7, pp. 20698-20707, 2019, doi.10.1109/ACCESS.2019.2897792

[7] A.Shahid, A.Almogren, N.Javaid, F.A.Al-Zahrani, M.Zuair, M.Alam, Blockchain-Based Agri-Food Supply Chain: A Complete Solution, IEEE Access, vol. 8, pp. 69230–69243, 2020, doi.10.1109/ACCESS.2020.2986257.

[8] H.Feng, X.Wang, Y.Duan, J.Zhang, X.Zhang, Applying blockchain technology to improve agri-food traceability: A review of development methods, benefits and challenges, J Clean Prod, vol. 260, p. 121031, Jul. 2020, doi10.1016/j.jclepro.2020.121031

[9] D.Shakhbulatov, A.Arora, Z.Dong, R.Rojas-Cessa, Blockchain Implementation for Analysis of Carbon Footprint across Food Supply Chain, in 2019 IEEE International Conference on Blockchain (Blockchain), Jul. 2019, pp. 546–551. doi10.1109/Blockchain.2019.00079.

[10] Q.N.Tran, B.P.Turnbull, H.T.Wu, A. J. S. de Silva, K.Kormusheva, J.Hu, A Survey on Privacy-Preserving Blockchain Systems (PPBS) and a Novel PPBS-Based Framework for Smart Agriculture, IEEE Open Journal of the Computer Society, vol. 2, pp. 72–84, 2021, doi10.1109/OJCS.2021.3053032.

[11] X.Yang, M.Li, H.Yu, M.Wang, D.Xu, C.Sun, A Trusted Blockchain-Based Traceability System for Fruit and Vegetable Agricultural Products, IEEE Access, vol. 9, pp. 36282–36293, 2021, doi10.1109/ACCESS.2021.3062845.

[12] A.Tripathi, K.Sharma, M.Bala, Parallel Bat Algorithm-Based Clustering Using MapReduce, (eds) Networking Communication and Data Knowledge Engineering, In: Perez, G., Mishra, K., Tiwari, S., Trivedi, M. Lecture Notes on Data Engineering and Communications Technologies, vol 4. Springer, Singapore., pp. 73–82, (2018), doi.org/10.1007/978-981-10-4600-1-7

[13] A.Tripathi, K.Sharma, M.Bala,A Novel Clustering Method Using Enhanced Grey Wolf Optimizer and MapReduce,journal.Big Data Research,vol 14, pp. 93-100, issn. 2214-5796, (2018), doi.org/10.1016/j.bdr.2018.05.002

[14] Hyperledger Performance and Scale Working Group: Hyperledger Blockchain Performance Metrics, Creative Commons Attribution 4.0 International License, 2018.

[15] N.K.Lincoln: Hyperledger Fabric 1.4.0 Performance Information Report, IBM Blockchain Developer Tools, Version 1.0.