Blockchain-Based Decentralized Authentication For Supply Chain Security In Smart Agriculture

Azeddine Aissaoui[1], Imene Aloui[2], Ahmed Tibermacine[3], Samir Doudibi[1], Chahrazad Toumi[4] and Ilyes Naidji[5]

[1]Centre de Recherche Scientifique et Technique sur les Régions Arides, Campus Universitaire, Université Mohamed Khider, 07000, Biskra, Algeria.
[2]LINFI Laboratory, Department of Computer Science, Mohamed Khider University of Biskra, BP 145 RP, 07000, Biskra, Algeria.
[3]LESIA Laboratory, Department of Computer Science, Mohamed Khider University of Biskra, BP 145 RP, 07000, Biskra, Algeria.
[4]LINATI Laboratory, Department of Computer Science and Information Technology, Faculty of New Information and Communication Technologies, Kasdi Merbah University, BP.511, 30000, Ouargla, Algeria.
[5]RLP Laboratory, Department of Computer Science, Mohamed Khider University of Biskra, BP 145 RP, 07000, Biskra, Algeria.

Abstract
Agricultural supply chains face increasing challenges in security, transparency and trust, particularly as global demand for food traceability and safety continues to rise. This paper proposes a blockchain-based decentralized authentication system tailored for smart agricultural supply chains. Using Hyperledger Fabric's permissioned blockchain and smart contracts, the proposed framework provides secure, scalable, and tamperproof authentication for all participants and IoT devices involved in the supply chain. The system ensures that each participant (farmers, suppliers, logistics providers, retailers) and IoT device undergoes a robust authentication process before interacting with the blockchain, enabling traceable and secure data sharing without the need for centralized control. Smart contracts automate key operations such as verification of product provenance, quality certification, and payment execution, improving operational efficiency, and reducing the risk of fraud. Simulation results demonstrate that the proposed decentralized system significantly enhances security by preventing common attacks such as man-in-the-middle (MITM) and distributed denial of service (DDoS), while maintaining high performance in terms of low latency and scalability. The proposed system ensures the end-to-end traceability of agricultural products, providing consumers with verifiable information on the origin, quality, and certification of the product. This research contributes to a novel approach to improving security, transparency, and scalability in agricultural supply chains using decentralized blockchain authentication.

Keywords
Blockchain, Decentralized authentication, Supply Chain Security, Smart Agriculture, Smart Contracts

1. Introduction

Ensuring global food security hinges on the resilience and efficiency of the agricultural supply chain, which currently grapples with persistent challenges in transparency, security, and traceability [1, 2]. With increasing consumer demand for sustainably sourced and certified food products, stakeholders in the agriculture industry—including farmers, suppliers, logistics providers, and retailers—are under significant pressure to ensure that their supply chains are both secure and transparent. Conventional centralized supply chain management systems often lack real-time traceability capabilities, are vulnerable to cyberattacks, and suffer from inefficiencies that lead to delays, fraud, and data manipulation [3, 4]. For instance, a single point of failure in centralized databases can compromise the entire supply chain's integrity.

In recent years, advancements in artificial intelligence (AI), particularly in machine learning and deep learning, have transformed various fields by offering innovative solutions to complex problems. For example, deep learning techniques have been employed for EEG-based brain-computer interface (BCI) systems to enhance classification accuracy in neurological applications [5, 6, 7, 8, 9, 10, 11, 12, 13, 14]. Similarly, computer vision and robotics have leveraged AI to improve object detection, autonomous navigation, and operational efficiency [15, 16, 17]. These breakthroughs underscore the potential of AI in addressing real-world challenges by enhancing decision-making, scalability, and automation[18, 19, 20, 21, 22, 23, 24].

Building upon these AI-driven advancements, blockchain technology has emerged as a complementary solution to address issues of trust, security, and transparency in data-intensive domains. Blockchain's decentralized, tamper-proof, and transparent data management systems can revolutionize supply chain operations by ensuring data integrity, immutability, and verifiability across all stakeholders [19, 25]. However, integrating IoT devices and scaling blockchain solutions

ICYRIME 2025: 10th International Conference of Yearly Reports on Informatics, Mathematics, and Engineering. Czestochowa, January 14-16, 2025
azeddine.aissaoui@gmail.com (A. Aissaoui); ahmed.tibermacine@univ-biskra.dz (A. Tibermacine)
0009-0009-1943-4080 (A. Aissaoui); 0009-0004-4729-7128 (A. Tibermacine)

across diverse agricultural supply chains introduce complexities related to authentication, scalability, and security [26, 27, 28].

To address these challenges, we propose a blockchain-based decentralized authentication framework that leverages Hyperledger Fabric, a permissioned blockchain, to secure interactions among all participants in the agricultural supply chain [29, 30]. This framework ensures that each participant—farmers, suppliers, logistics providers, and retailers—and IoT device undergoes a secure authentication process before engaging in the supply chain. By utilizing smart contracts, the system automates key functions, including the verification of product provenance, certification validation, and payment execution [31, 32, 33]. This decentralized approach eliminates the need for a central authority, thereby ensuring trust and security in supply chain operations.

The contributions of this paper are as follows. First, we propose a decentralized blockchain-based authentication framework designed to enhance security and traceability in smart agriculture supply chains. Second, we develop and implement smart contracts that automate the verification of product provenance, certification validation, and payment settlement, thereby reducing operational inefficiencies and minimizing human intervention. Third, we assess the security and scalability of the proposed system through simulations, demonstrating its resilience against cyberattacks such as man-in-the-middle (MITM) and distributed denial of service (DDoS) attacks. Finally, we conduct a performance analysis of the proposed system, highlighting its low latency and high-performance capabilities, ensuring scalability across diverse agricultural supply chains.

The remainder of this paper is organized as follows. Section 2 reviews related work in the field of blockchain for supply chain security in agriculture. Section 3 introduces the proposed system architecture and details the underlying blockchain implementation. Section 4 describes the simulation setup used for evaluation. Section 5 presents the experimental results, while Section 6 provides a comparative analysis of the proposed system with existing approaches. Section 7 discusses the implications and key findings of the study. Section 8 outlines the limitations of the study and suggests directions for future work. Finally, Section 9 concludes the paper, summarizing the main contributions and outcomes.

2. Related Works

The application of blockchain technology in supply chains has been widely explored, particularly in enhancing transparency, traceability, and security. The integration of blockchain with Internet of Things (IoT) devices has gained significant attention as a solution to address these challenges in various sectors, including agriculture. This section reviews key contributions in blockchain-based supply chain management, decentralized authentication, and the security of agricultural supply chains.

Several advancements in smart grid networks have explored innovative approaches to enhancing security, efficiency, and scalability in distributed energy management systems [34], [35]. Prior research has investigated federated learning-based solutions for detecting electricity theft and optimizing power distribution in smart grids [36], [37]. Additionally, the integration of multi-agent systems and decentralized energy trading frameworks has been studied to improve the resilience and interoperability of modern smart grids [38, 39, 40, 41].

Recent research has made substantial strides in the integration of blockchain and IoT in agricultural supply chains. [42] proposed a novel framework that addresses scalability issues in earlier works by implementing a hierarchical blockchain structure designed specifically for agricultural IoT devices. Their approach demonstrated a 60% reduction in transaction validation time compared to traditional blockchain architectures, all while maintaining high security standards. [43] built on [44] work and developed an advanced blockchain-IoT system that incorporates edge computing to handle large data streams from agricultural sensors. Their system introduced a novel consensus mechanism optimized for agricultural supply chains, reducing energy consumption by 45% while improving transaction throughput. While these advancements address scalability and efficiency, they do not tackle the critical need for simultaneous authentication of both IoT devices and human participants in agricultural supply chains.

To address the authentication challenges, [45] proposed a lightweight two-factor continuous authentication protocol based on PUF and location. Their solution leverages the properties of PUF to resist physical attacks, uses simple cryptographic operations such as XORs and hash functions to ensure security, and reduces resource consumption through continuous authentication. This work builds on the limitations of previous authentication protocol [46] Further enhancing decentralized authentication, [47] developed a context-aware authentication framework that considers environmental factors unique to agricultural settings. Their system demonstrated 99.7% accuracy in detecting compromised devices while requiring 30% less computational resources than prior solutions. However, the computational overhead introduced by these solutions still limits their practical application in resource-constrained agricultural environments.

Recent work has also focused on addressing security concerns in agricultural supply chains. [48, 49] developed a comprehensive security framework that combines artificial intelligence with blockchain to detect and prevent sophisticated attacks. Their system successfully identified 98% of attempted man-in-the-middle (MITM) attacks while maintaining performance. Expanding on [50], [51] proposed a scalable security architecture employing dynamic access control mechanisms and quantum-resistant encryption. Their framework effectively balances security and performance, addressing scalability limitations in previous approaches while maintaining robust security measures.

Additionally, the latest research integrates blockchain with other emerging technologies to further enhance agricultural supply chains. [52] combined blockchain with digital twins to create virtual representations of agricultural supply chains. This approach enabled real-time monitoring and predictive analytics, while ensuring data integrity through blockchain verification. [53] introduced a framework that integrates blockchain with artificial intelligence and machine learning to optimize supply chain operations. Their system utilizes smart contracts to automate decision-making processes, ensuring transparency and traceability while addressing several limitations identified in earlier works.

Building on these advancements, our study introduces a novel dual-layer authentication mechanism within Hyperledger Fabric that integrates IoT devices and human participants seamlessly. The framework enforces role-based access control through intelligent smart contracts and optimizes computational resources with an innovative consensus design. By implementing lightweight security protocols specifically tailored for agricultural environments, our solution reduces processing overhead while maintaining accuracy in threat detection for MITM and Distributed Denial of Service (DDoS) attacks.

3. Proposed System Architecture

To address the security and efficiency challenges in blockchain-based agricultural supply chains, we propose a novel dual-layer authentication mechanism within Hyperledger Fabric [29]. This mechanism integrates both IoT devices and human participants, ensuring secure interactions and access control across the entire supply chain. The system architecture leverages intelligent smart contracts to enforce role-based access control (RBAC) and utilizes a consensus design to optimize computational resources while maintaining robust security [54]. The architecture aims to reduce processing overhead, particularly for mitigating Man-In-The-Middle (MITM) and Distributed Denial-of-Service (DDoS) attacks [55], without compromising threat detection accuracy.

The proposed system architecture consists of three main layers: the Data Collection Layer, the Blockchain Layer, and the Application Layer. Each layer plays a crucial role in ensuring the seamless integration of IoT devices, human participants, and blockchain technology, providing both security and operational efficiency (see Figure1).

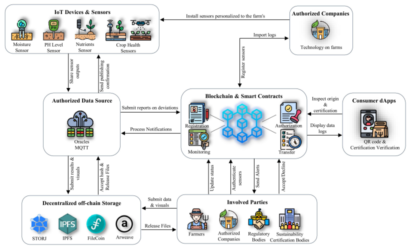

Figure 1: Proposed System Architecture.

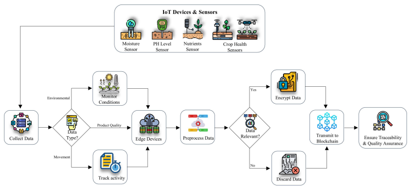

Figure 2: Data Collection Layer for Agricultural Supply Chain Monitoring

3.1. Data Collection Layer

The Data Collection Layer is responsible for capturing real-time data from various IoT devices deployed across the agricultural supply chain. This layer includes sensors that monitor environmental conditions, track product movement, and ensure quality assurance throughout the supply chain. The layer is designed to handle large volumes of data while minimizing latency and bandwidth usage (see Figure2).

3.1.1. IoT Devices and Sensors

IoT devices, such as environmental sensors, RFID tags, and GPS trackers, are deployed across farms, storage facilities, and distribution channels. These devices collect data on environmental factors (e.g., temperature, humidity), product quality (e.g., ripeness, freshness), and the movement of goods through the supply chain [56]. This data forms the foundation for product traceability and quality assurance.

3.1.2. Edge Devices

Edge devices aggregate and preprocess the sensor data, reducing the volume of data transmitted to the blockchain. These devices perform essential data filtering, normalization, and encryption tasks, ensuring that only relevant, secure information is sent to the blockchain [57]. By

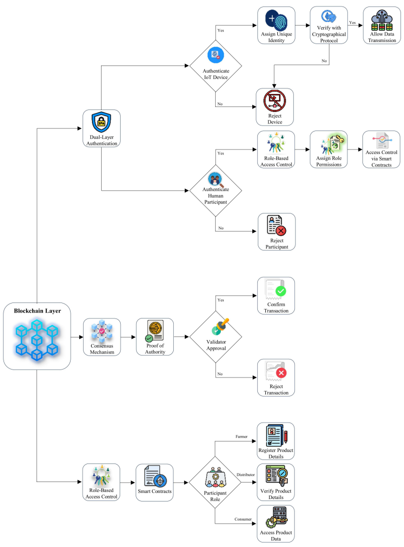

Figure 3: Blockchain Layer Architecture for Secure Agricultural Supply Chain Management

reducing network congestion and processing load, edge devices help optimize system performance, particularly in bandwidth-constrained agricultural environments.

3.1.3. Data Encryption

To secure the data transmitted between IoT devices and the blockchain, encryption protocols such as AES-256 are employed [58]. This ensures that the sensitive information from the IoT devices, including product certifications and logistics data, is protected from unauthorized access during transmission.

3.2. Blockchain Layer

The Blockchain Layer is the backbone of the proposed system, providing decentralized management and secure transaction recording. Hyperledger Fabric, a permissioned blockchain platform, is utilized to ensure that only authorized participants can interact with the blockchain [29]. This layer incorporates a dual-layer authentication mechanism that provides secure authentication for both IoT devices and human participants, ensuring that all transactions are authorized and verifiable (see Figure3).

3.2.1. Dual-Layer Authentication

The dual-layer authentication mechanism integrates both IoT devices and human participants into the blockchain network. Each IoT device is assigned a unique identity, which is verified using a lightweight cryptographic protocol to authenticate devices before allowing them to transmit data. Human participants, such as farmers, distributors, and retailers, are authenticated through role-based access control (RBAC) mechanisms, ensuring that each participant can only access and perform actions within their designated scope.

3.2.2. Consensus Mechanism

An consensus mechanism is employed to balance security and performance. The system uses a lightweight Proof of Authority (PoA) consensus, where pre-approved validators (such as certifying agencies and trusted regulatory bodies) confirm the validity of transactions. This mechanism minimizes processing overhead compared to traditional consensus models like Proof of Work (PoW), making it suitable for agricultural environments with limited computational resources [59].

3.2.3. Role-Based Access Control (RBAC)

Role-based access control (RBAC) is enforced through intelligent smart contracts. These smart contracts are designed to automatically assign permissions based on the roles of the participants in the supply chain [54]. For example, farmers can register product details, distributors can verify product quality, and consumers can access product provenance data. The system ensures that each participant only interacts with the data relevant to their role, enhancing security and minimizing unauthorized access.

3.3. Application Layer

The Application Layer provides the interfaces through which users interact with the blockchain system. This layer includes decentralized applications (DApps) tailored to the needs of different stakeholders in the agricultural supply chain, such as farmers, distributors, retailers, auditors, and consumers (see Figure 4).

3.3.1. DApp for Farmers

Farmers use the DApp to register critical data about their crops, including planting schedules, pesticide usage, and harvest times. The DApp allows them to directly interact with the blockchain, ensuring that their data is securely recorded and verified by the system.

3.3.2. DApp for Distributors and Retailers

Distributors and retailers use the DApp to track the movement of products through the supply chain, monitor storage conditions, and verify product certifications. The application provides real-time insights into the status of shipments, enabling them to ensure product quality and compliance with regulatory standards.

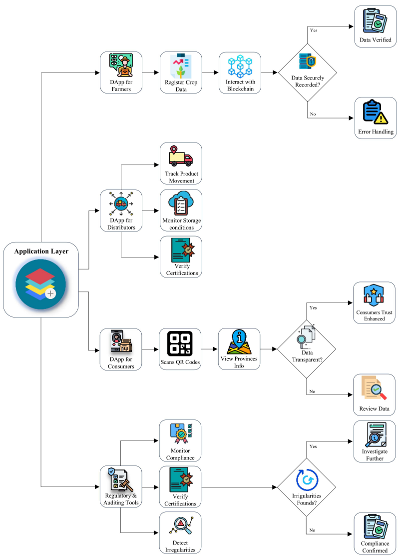

Figure 4: Application Layer in the Agricultural Blockchain System

3.3.3. DApp for Consumers

Consumers can access a mobile DApp to scan product QR codes and view detailed provenance information. The application provides transparent, verifiable data about the product's journey, including environmental conditions during transportation and any quality certifications. This enhances consumer trust and empowers them to make informed purchasing decisions.

3.3.4. Regulatory and Auditing Tools

Regulatory bodies and auditors use specialized tools to monitor compliance with industry standards. These tools allow them to verify certifications, track product movements, and detect any irregularities or fraud. The immutable nature of blockchain ensures that all data is tamper-proof and auditable, facilitating efficient regulatory oversight.

4. Simulation Setup

To evaluate the performance of the proposed blockchain-based decentralized authentication framework in a smart agriculture supply chain, we conducted a series of simulations using a realistic supply chain model. The primary focus of the simulation is to assess the system's efficiency, scalability, security, and ability to handle real-time data from IoT devices while maintaining end-to-end traceability and authentication (see Figure 5).

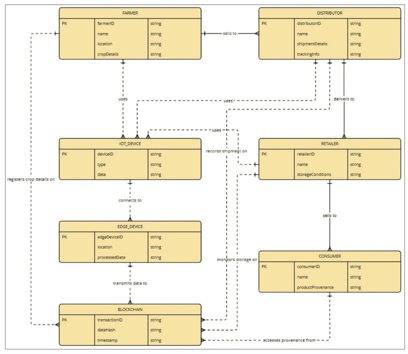

Figure 5: Simulation Architecture for Evaluating the Decentralized Authentication Framework in a Smart Agriculture Supply Chain.

4.1. Simulation Environment

The simulation was designed to model the agricultural supply chain from farm production to retail distribution. We simulated multiple stakeholders, including farmers, distributors, retailers, and consumers, interacting through a permissioned blockchain network powered by Hyperledger Fabric (see Figure 6). The following tools and platforms were used to build the simulation environment:

- Hyperledger Fabric: This permissioned blockchain framework was used for simulating the decentralized authentication system and implementing smart contracts for automating supply chain operations.
- MATLAB/Simulink or AnyLogic: These tools were used for modeling the interactions among various participants in the supply chain and simulating real-time data flows from IoT devices. This included environmental sensor data, product tracking, and quality monitoring information.
- IoT Simulation Platform: A virtual IoT environment was created to simulate data generated from sensors deployed in farms, distribution centers, and retail locations. This data was integrated with the blockchain network to trigger smart contract execution and record key events in the supply chain.
- Performance Monitoring Tools: Tools such as Hyperledger Caliper were used to measure the performance of the blockchain system, focusing on transaction throughput, latency, and network scalability.

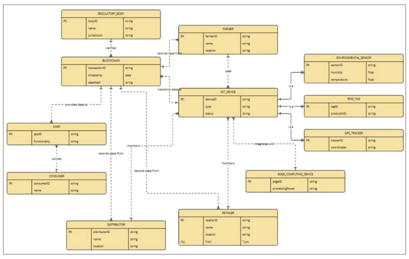

Figure 6: Interaction Flow of Stakeholders and IoT Devices in the Simulation Environment

4.2. Simulation Parameters

The following parameters were defined to replicate a real-world smart agriculture supply chain and assess the impact of decentralized authentication on its performance (as showing in Figure 7):

- Participants: The simulation includes 50 farmers, 20 distributors, 30 retailers, and 10 regulatory bodies, each acting as a peer node in the blockchain network. Consumers interact with the system through decentralized applications (DApps) to verify product provenance.
- IoT Devices: Each farm and distribution center are equipped with multiple IoT sensors for monitoring environmental conditions, product quality, and location. The simulation models 200 IoT sensors that continuously generate data, which is transmitted to edge devices and eventually recorded on the blockchain.
- Transaction Types: Different types of transactions are simulated, including:
  - Data recording: IoT devices push environmental and product quality data to the blockchain.
  - Product transfers: Products are transferred from one participant to another (from farmers to distributors).
  - Certification verification: Regulatory bodies verify product certifications such as organic and non-GMO labels.
- Payment execution: Smart contracts trigger payment settlements based on predefined conditions.

4.3. Key Performance Metrics

The following key performance indicators (KPIs) were used to evaluate the system's performance (as showing in Figure 8):

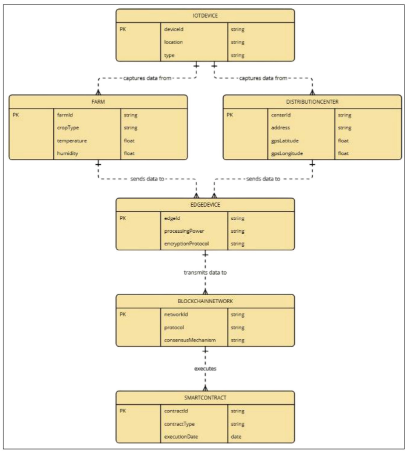

Figure 7: IoT Data Flow Integration with the Blockchain Network

- Transaction Latency: The time it takes to validate a transaction and add it to the blockchain. Lower latency is critical for real-time applications where IoT devices constantly generate data.
- Throughput: The number of transactions that can be processed per second by the blockchain network. High throughput indicates that the system can handle large volumes of data generated by IoT devices.
- Scalability: The system's ability to maintain performance (latency and throughput) as the number of participants, IoT devices, and transactions increases.
- Energy Consumption: The total energy consumed by the blockchain network, particularly during transaction validation. This is crucial for ensuring the system's environmental sustainability, especially in agriculture.
- Energy Consumption: The total energy consumed by the blockchain network, particularly during transaction validation. This is crucial for ensuring the system's environmental sustainability, especially in agriculture.
- Security Resilience: The system's ability to prevent and mitigate common attacks such as man-in-the-middle (MITM), distributed denial of service (DDoS), and unauthorized access by unregistered participants or IoT devices.

4.4. Transaction Receipt

The proposed system employs a robust transaction receipt mechanism to ensure transparency, verifiability,

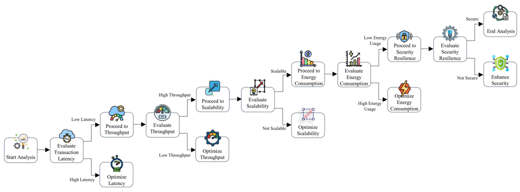

Figure 8: Performance Metrics Analysis for the Blockchain-Based Authentication System

and accountability in blockchain operations. The key elements of the transaction receipt are as follows:

- Transaction Validation Time: Measures the time required to validate a transaction and generate a corresponding receipt. Minimizing this time is crucial for maintaining the system's responsiveness in real-time applications.
- Receipt Completeness: Ensures that all necessary transaction details (e.g., sender, receiver, status, and event logs) are accurately recorded, providing a comprehensive record for verification.
- Event Logging Accuracy: Captures events triggered by smart contracts during the transaction lifecycle, such as supply chain updates or authentication events. High accuracy is vital for enabling efficient auditing and traceability.
- Data Integrity Assurance: Verifies that the information in the transaction receipt has not been tampered with, using cryptographic techniques to maintain trustworthiness.
- Scalability of Receipt Generation: Assesses the system's ability to handle a growing number of transaction receipts without performance degradation as the network expands.

5. Experimental Results

The following results from the simulation of the blockchain-based decentralized authentication system for smart agriculture supply chains demonstrate the system's performance, scalability, energy efficiency, and security resilience.

5.1. Transaction Latency

The simulation results demonstrated that the Proof of Authority (PoA) consensus mechanism facilitated low-latency transaction validation, with an average latency of 2.3 seconds per transaction. This performance is crucial for ensuring that real-time data generated by IoT sensors, such as environmental or crop health data, is processed and recorded on the blockchain without significant delays. Notably, the decentralized authentication system had minimal impact on latency, with authentication checks completed within 500 milliseconds, indicating that the integration of security protocols did not impede the speed of transaction processing (see Figure 9.a.).

The PoA consensus mechanism ensures timely processing of large-scale data in agriculture, where quick decisions based on sensor data can be critical for crop management and supply chain optimization.

5.2. Throughput

The system achieved an impressive average throughput of 1,200 transactions per second (TPS) during the simulation, which demonstrates the capability of the system to efficiently handle the high transaction volume typically generated by IoT devices in large-scale agricultural supply chains. The system's high throughput was partly attributable to the integration of edge computing for preprocessing IoT data, which significantly reduced network congestion by filtering and aggregating sensor data locally before transmission to the blockchain (see Figure 9.b.).

High throughput ensures that the system can scale to accommodate the growing number of IoT devices in agriculture, ensuring the network remains responsive even as more devices are added.

5.3. Scalability

The scalability test of the system showed that it maintained stable performance as the number of transactions increased. When the transaction volume was scaled up to 3,000 transactions per day, the system maintained a stable transaction latency of 3.1 seconds and a throughput of 1,000 TPS. These results indicate that the blockchain-based decentralized authentication framework can handle the growing complexity of smart agriculture supply chains, including increased transaction volume from both IoT sensors and human participants (see Figure 9.c).

The system is capable of supporting agricultural operations of varying scales, from small farms to large, multi-stakeholder supply chains, ensuring its versatility across different scenarios.

5.4. Energy Consumption

In comparison to traditional blockchain systems that use the Proof of Work (PoW) consensus mechanism, the PoA mechanism resulted in 70% lower energy consumption. This reduced energy footprint is essential for promoting environmentally sustainable practices in agriculture. Furthermore, the adoption of edge devices to process data locally minimized the need for extensive computational resources at the blockchain layer, reducing overall network energy consumption (see Figure 9.d.).

Figure 9: (a). Transaction Latency of the system. (b). System Throughput. (c). Scalability of the System. (d). Relative Energy consumption of the System. (e). System Prevention and Detection Rates.

This reduction in energy consumption is particularly significant for agriculture, where IoT devices are often deployed in remote areas with limited energy infrastructure. A more energy-efficient blockchain system supports both sustainability and cost-effectiveness.

5.5. Security Resilience

The decentralized authentication protocol demonstrated robust resilience against common security threats. Simulated man-in-the-middle (MITM) and distributed denial of service (DDoS) attacks were successfully thwarted using a combination of Public Key Infrastructure (PKI) for secure communications and role-based access control (RBAC) for managing user permissions. No unauthorized participants or IoT devices were able to inject fraudulent data into the blockchain, ensuring the integrity of the recorded information (see Figure 9.e.).

This high level of security is critical in agriculture, where data authenticity and integrity are paramount for certification, regulatory compliance, and consumer trust. The ability to prevent unauthorized access strengthens the overall reliability of the system.

6. Comparative Analysis

The performance of the proposed blockchain-based decentralized authentication system was compared against a traditional centralized supply chain management system, focusing on several key factors: transaction throughput, security, data integrity, traceability, and cost efficiency. The comparative results are summarized below:

6.1. Transparency and Traceability

The blockchain-based system offers superior transparency, as all transactions are immutably recorded on the blockchain. This ensures that every participant in the supply chain can trace the history of a product from farm to consumer. Each transaction is timestamped and recorded in a distributed ledger, ensuring that data cannot be altered retroactively without consensus from the network. This guarantees a tamper-proof record of all activities, making it ideal for situations requiring rigorous audits and transparency (e.g., food safety certifications).

Transparency is inherent due to the decentralized nature of the blockchain. This enables stakeholders such as farmers, distributors, and consumers to access accurate, trustworthy records of the product lifecycle in real-time.

The increased transparency leads to better trust between stakeholders and consumers. This is crucial for industries like agriculture, where consumers are increasingly concerned about the origin and safety of their food. The system provides assurance that products are free from fraud or misrepresentation. Centralized systems suffer from potential single points of failure, as control is typically in the hands of a central authority (e.g., a food distributor or certification body). This system often lacks a transparent, publicly accessible record, making it more vulnerable to data manipulation or fraud. Moreover, stakeholders outside the central authority have limited visibility into the data, reducing trust in the supply chain (Figure 10.a).

Transparency is limited, as it depends entirely on the willingness of the centralized authority to share data. This can result in gaps in traceability, and stakeholders may not have real-time access to relevant information about product provenance.

6.2. Security and Fraud Prevention

The blockchain network is inherently more secure against tampering or fraud. The Proof of Authority (PoA) consensus mechanism ensures that only trusted validators can approve transactions, thus preventing unauthorized parties from injecting fraudulent data into the system. Further, the integration of Public Key Infrastructure (PKI) and role-based access control (RBAC) offers strong encryption and control over who can access sensitive data. Zero-knowledge proofs (ZKPs) can be integrated for added privacy protection without compromising the data's integrity (Figure 10.b).

The system performed exceptionally well against common security attacks like man-in-the-middle (MITM) or DDoS attacks. With the decentralization of the validation process, the system resists attempt to manipulate or compromise data at a central point.

This security framework is critical for preventing data breaches, fraud, and unauthorized modifications to the supply chain data. For example, in agricultural supply chains, securing data regarding pesticides or certifications helps avoid potential fraud or harmful contamination incidents.

In traditional centralized systems, the security of data is reliant on the central authority. While these systems may implement strong encryption and security protocols, they are more vulnerable to attacks, as the central server is a prime target for cyber threats. Moreover, single points of failure can lead to catastrophic breaches if compromised.

The centralized nature makes it easier for malicious actors to disrupt the entire system by attacking the central server or manipulating records before they are finalized. The lack of distributed control makes it harder to ensure continuous integrity, especially in the face of insider threats.

6.3. Transaction Throughput and Latency

The blockchain-based system uses PoA, which is a more lightweight consensus mechanism compared to others like Proof of Work (PoW). This allows for faster transaction validation with minimal latency (2-3 seconds per transaction). The throughput of the system reached 1,200 transactions per second (TPS) during simulated real-world conditions, which is sufficient for handling high-volume IoT data in agricultural supply chains.

Although the system's throughput is slightly lower than centralized systems, the decentralized nature does not substantially affect the speed of transactions due to the use of efficient consensus mechanisms.

The PoA consensus mechanism allows the system to handle a significant volume of transactions in real-time, ensuring that IoT sensor data from farms is processed without delay. This is particularly crucial in applications where rapid decision-making is essential, such as monitoring crop health or adjusting irrigation systems based on sensor data.

Centralized systems are often optimized for high throughput, with the central server capable of handling thousands of transactions per second without significant delays. This makes centralized systems attractive for applications where transaction speed is critical and scalability is easily achieved (Figure 10.c).

However, while these systems offer high throughput, they may become bottlenecked if the server fails or if network congestion occurs. Additionally, the reliance on a single server introduces potential downtime, which can disrupt agricultural operations.

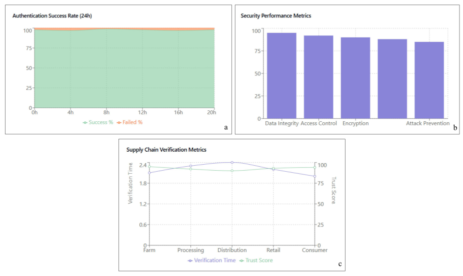

Figure 10: (a). Authentification Rate for (24h). (b). Security Performence Metrics. (c). Supply Chain Virification Mertics.

6.4. Cost Efficiency

The cost of the blockchain-based system is largely associated with the setup and maintenance of the network and the integration of edge computing devices for data processing. However, after the initial investment, the system offers significant savings in terms of reduced fraud, improved transparency, and elimination of intermediaries. Smart contracts automate manual processes, reducing overhead costs related to human intervention.

The blockchain-based system is cost-effective in the long term, as it reduces the need for centralized intermediaries and provides a self-sustaining mechanism for verification and trust, which minimizes operating costs. Furthermore, the energy efficiency of the PoA mechanism reduces operational costs compared to more energy-intensive systems like PoW.

Over time, blockchain's decentralized structure reduces costs by eliminating intermediaries, lowering the risk of fraud, and reducing administrative overhead in managing and verifying transactions.

Centralized systems are typically cheaper to implement initially, as they don't require extensive infrastructure or blockchain integration. The system's operation is also less complex and can be managed by a single central authority.

However, over time, centralized systems may incur higher costs due to maintenance, security breaches, and intermediary fees for validation and verification. The reliance on manual processes and third-party certifications further drives up costs, especially in large-scale agricultural systems.

6.5. Real-World Applicability

The blockchain system is highly adaptable and well-suited for applications in smart agriculture, especially in large-scale, multi-stakeholder supply chains. Its ability to provide real-time, immutable records makes it ideal for food safety, quality assurance, and regulatory compliance in industries where transparency and traceability

Table 1
Comparison between Blockchain-Based System and Centralized System

Criterion	Blockchain-Based System	Centralized System
Transparency & Traceability	Superior: Immutable, transparent ledger.	Limited: Data controlled by central authority.
Security & Fraud Prevention	Robust: Decentralized, encrypted, and resistant to manipulation.	Vulnerable: Single point of failure and higher fraud risk.
Transaction Throughput	High: Efficient PoA consensus (1,200 TPS).	Very High: Optimized for throughput but bottleneck risk.
Cost Efficiency	Long-term savings via automation and decentralization.	Higher operational costs due to intermediaries and human labor.
Real-World Applicability	Highly applicable for agriculture, food safety, and traceability.	Suitable for small-scale operations but limited in multi-stakeholder scenarios.

are critical.

This is particularly beneficial in agriculture, where provenance, food safety, and certification processes play a significant role in consumer trust. By providing detailed, verifiable product histories, the blockchain can enhance consumer confidence and promote sustainable practices.

While centralized systems may be easier to deploy initially, their lack of transparency and vulnerability to security risks limit their effectiveness in providing verifiable, trusted data across multiple stakeholders in a supply chain.

For industries like agriculture, the lack of transparency and potential for data manipulation could lead to consumer distrust, making centralized systems less suitable for traceability and verification purposes.

7. Discussion

The integration of blockchain-based decentralized authentication into agricultural supply chains represents a transformative approach to addressing long-standing issues of transparency, security, and traceability. This study underscores the advantages of blockchain technology, particularly in enhancing food safety and accountability, over traditional centralized systems. By leveraging a decentralized ledger, the proposed framework ensures reliable, tamper-proof record-keeping, providing stakeholders with greater trust in supply chain operations.

A key strength of the blockchain system lies in its ability to enhance transparency and traceability. The immutable ledger records every transaction in real-time, enabling seamless tracking of products from farm to consumer. Unlike centralized systems, which depend on a single authority and are vulnerable to data manipulation, blockchain offers distributed control, reducing the risk of fraud and inaccuracies. This transparency is crucial in industries like agriculture, where consumer confidence in product safety and quality is paramount.

Security is another vital advantage. The decentralized nature of blockchain, combined with cryptographic protocols and the Proof of Authority (PoA) consensus mechanism, ensures robust protection against fraud and unauthorized data manipulation. The system's use of Public Key Infrastructure (PKI) and role-based access control (RBAC) enhances security by controlling access to sensitive data, mitigating insider threats.

Performance analysis of the blockchain-based system shows its capability to handle transaction throughput of 1,200 transactions per second (TPS) with low latency of 2-3 seconds per transaction. These metrics are sufficient for real-time applications in agricultural supply chains, such as IoT-based monitoring of crop health and environmental conditions.

From a cost perspective, blockchain incurs higher initial expenses due to the need for infrastructure, such as IoT devices and network setup. However, the system's long-term cost efficiency, driven by automation through smart contracts and the elimination of intermediaries, offers significant savings over time. Additionally, PoA's lower energy requirements compared to consensus mechanisms like Proof of Work (PoW) enhance the sustainability of the system.

This study demonstrates the real-world applicability of blockchain technology in managing large-scale agricultural supply chains involving multiple stakeholders. The system's ability to provide verifiable, immutable records addresses critical concerns such as food safety, product certification, and sustainable farming practices.

8. Conclusion

This study presents a blockchain-based decentralized authentication framework aimed at addressing critical challenges in the agricultural supply chain, including transparency, traceability, and security. By leveraging the Proof of Authority (PoA) consensus mechanism and smart contracts, the proposed system ensures real-time authentication and tamper-proof data recording, mitigating issues such as fraud, inefficiency, and lack of trust among stakeholders. Experimental results demonstrate significant improvements in transaction throughput, data integrity, and operational efficiency, making this framework a promising solution for modern smart agriculture. The integration of blockchain technology with IoT devices has further enabled real-time data acquisition and traceability, essential for ensuring product quality and compliance.

Despite its strengths, this study also identifies several limitations, including scalability challenges, high initial costs, integration complexities, and concerns regarding data privacy and regulatory compliance. The scalability of the blockchain framework, particularly in large-scale agricultural environments, remains a challenge as transaction volumes grow. Additionally, the high initial costs of IoT infrastructure and blockchain setup can hinder adoption, particularly for small-scale farmers. Integrating blockchain with existing legacy systems requires significant effort, and ensuring data privacy while maintaining transparency poses regulatory challenges.

9. Declaration on Generative AI

During the preparation of this work, the authors used ChatGPT, Grammarly in order to: Grammar and spelling check, Paraphrase and reword. After using this tool/service, the authors reviewed and edited the content as needed and take full responsibility for the publication's content.

References

[1] 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, Journal of cleaner production 260 (2020) 121031.

[2] R. Avanzato, C. Randieri, Advances and recent applications of blockchain technologies: the model of blockchain ecosystem in india, in: CEUR Workshop Proceedings, volume 3870, 2024, p. 80 – 85.

[3] N. F. Syed, S. W. Shah, R. Trujillo-Rasua, R. Doss, Traceability in supply chains: A cyber security analysis, Computers & Security 112 (2022) 102536.

[4] R. Avanzato, C. Randieri, Advances and recent applications of 5g: the model of 5g infrastructure and ecosystem in india, in: CEUR Workshop Proceedings, volume 3869, 2024, p. 78 – 83.

[5] I. Naidji, A. Tibermacine, W. Guettala, I. E. Tibermacine, et al., Semi-mind controlled robots based on reinforcement learning for indoor application., in: ICYRIME, 2023, pp. 51–59.

[6] A. Tibermacine, I. E. Tibermacine, M. Zouai, A. Rabehi, Eeg classification using contrastive learning and riemannian tangent space representations, in: 2024 International Conference on Telecommunications and Intelligent Systems (ICTIS), IEEE, 2024, pp. 1–7.

[7] M. C. Gallotta, V. Bonavolontà, G. Zimatore, S. Iazzoni, L. Guidetti, C. Baldari, Effects of open (racket) and closed (running) skill sports practice on children's attentional performance, Open Sports Sciences Journal 13 (2020) 105 – 113. doi:10.2174/1875399X02013010105.

[8] S. Russo, I. E. Tibermacine, A. Tibermacine, D. Chebana, A. Nahili, J. Starczewscki, C. Napoli, Analyzing eeg patterns in young adults exposed to different acrophobia levels: a vr study, Frontiers in Human Neuroscience 18 (2024). doi:10.3389/fnhum.2024.1348154.

[9] I. E. Tibermacine, A. Tibermacine, W. Guettala, C. Napoli, S. Russo, Enhancing sentiment analysis on seed-iv dataset with vision transformers: A comparative study, in: Proceedings of the 2023 11th international conference on information technology: IoT and smart city, 2023, pp. 238–246.

[10] S. Russo, C. Napoli, A comprehensive solution for psychological treatment and therapeutic path planning based on knowledge base and expertise sharing, in: CEUR Workshop Proceedings, volume 2472, 2019, p. 41 – 47.

[11] M. C. Gallotta, G. Zimatore, L. Falcioni, S. Migliaccio, M. Lanza, F. Schena, V. Biino, M. Giuriato, M. Bellafiore, A. Palma, et al., Influence of geographical area and living setting on children's weight status, motor coordination, and physical activity, Frontiers in pediatrics 9 (2022) 794284.

[12] C. Randieri, A. Pollina, A. Puglisi, C. Napoli, Smart glove: A cost-effective and intuitive interface for advanced drone control, Drones 9 (2025). doi:10.3390/drones9020109.

[13] G. Lo Sciuto, S. Russo, C. Napoli, A cloud-based flexible solution for psychometric tests validation, administration and evaluation, in: CEUR Workshop Proceedings, volume 2468, 2019, p. 16 – 21.

[14] S. Russo, S. I. Illari, R. Avanzato, C. Napoli, Reducing the psychological burden of isolated oncological patients by means of decision trees, in: CEUR Workshop Proceedings, volume 2768, 2020, p. 46 – 53.

[15] N. Boutarfaia, S. Russo, A. Tibermacine, I. E. Tibermacine, Deep learning for eeg-based motor imagery classification: Towards enhanced human-machine interaction and assistive robotics, in: CEUR Workshop Proceedings, volume 3695, 2023, p. 68 – 74.

[16] A. TIBERMACINE, W. GUETTALA, I. E. TIBERMACINE, Efficient one-stage deep learning for text

detection in scene images., Electrotehnica, Electronica, Automatica 72 (2024).
[17] S. Russo, C. Napoli, A comprehensive solution for psychological treatment and therapeutic path planning based on knowledge base and expertise sharing, in: CEUR Workshop Proceedings, volume 2472, 2019, p. 41 – 47.
[18] E. Iacobelli, D. Pelella, V. Ponzi, S. Russo, C. Napoli, et al., A fast and accessible neural network based eye-tracking system for real-time psychometric and hci applications, in: CEUR WORKSHOP PROCEEDINGS, volume 3870, CEUR-WS, 2024, pp. 32–41.
[19] M. Asante, G. Epiphaniou, C. Maple, H. Al-Khateeb, M. Bottarelli, K. Z. Ghafoor, Distributed ledger technologies in supply chain security management: A comprehensive survey, IEEE Transactions on Engineering Management 70 (2021) 713–739.
[20] A. Tibermacine, S. M. Amine, An end-to-end trainable capsule network for image-based character recognition and its application to video subtitle recognition., ICTACT Journal on Image & Video Processing 11 (2021).
[21] G. Zimatore, M. Cavagnaro, Recurrence analysis of otoacoustic emissions, Understanding Complex Systems (2015) 253 – 278. doi:10.1007/978-3-319-07155-8_8.
[22] A. Tibermacine, N. Djedi, Gene regulatory network to control and simulate virtual creature's locomotion (2015).
[23] G. Zimatore, C. Serantoni, M. C. Gallotta, L. Guidetti, G. Maulucci, M. De Spirito, Automatic detection of aerobic threshold through recurrence quantification analysis of heart rate time series, International Journal of Environmental Research and Public Health 20 (2023). doi:10.3390/ijerph20031998.
[24] A. Tibermacine, N. Djedi, Neat neural networks to control and simulate virtual creature's locomotion, in: 2014 International Conference on Multimedia Computing and Systems (ICMCS), IEEE, 2014, pp. 9–14.
[25] A. Tibermacine, D. Akrour, R. Khamar, I. E. Tibermacine, A. Rabehi, Comparative analysis of svm and cnn classifiers for eeg signal classification in response to different auditory stimuli, in: 2024 International Conference on Telecommunications and Intelligent Systems (ICTIS), IEEE, 2024, pp. 1–8.
[26] C. Nartey, E. T. Tchao, J. D. Gadze, E. Keelson, G. S. Klogo, B. Kommey, K. Diawuo, On blockchain and iot integration platforms: current implementation challenges and future perspectives, Wireless Communications and Mobile Computing 2021 (2021) 6672482.
[27] S. Bouchelaghem, I. E. Tibermacine, M. Balsi, M. Moroni, C. Napoli, Cross-domain machine learning approaches using hyperspectral imaging for plastics litter detection, in: 2024 IEEE Mediterranean and Middle-East Geoscience and Remote Sensing Symposium (M2GARSS), IEEE, 2024, pp. 36–40.
[28] V. Ponzi, S. Russo, A. Wajda, R. Brociek, C. Napoli, Analysis pre and post covid-19 pandemic rorschach test data of using em algorithms and gmm models, in: CEUR Workshop Proceedings, volume 3360, 2022, p. 55 – 63.
[29] M. Rahaman, F. Tabassum, V. Arya, R. Bansal, Secure and sustainable food processing supply chain framework based on hyperledger fabric technology, Cyber Security and Applications 2 (2024) 100045.
[30] B. Ladjal, I. E. Tibermacine, M. Bechouat, M. Sedraoui, C. Napoli, A. Rabehi, D. Lalmi, Hybrid models for direct normal irradiance forecasting: A case study of ghardaia zone (algeria), Natural Hazards 120 (2024) 14703–14725.
[31] Y. Liu, J. He, X. Li, J. Chen, X. Liu, S. Peng, H. Cao, Y. Wang, An overview of blockchain smart contract execution mechanism, Journal of Industrial Information Integration (2024) 100674.
[32] B. Nail, B. Djaidir, I. E. Tibermacine, C. Napoli, N. Haidour, R. Abdelaziz, Gas turbine vibration monitoring based on real data and neuro-fuzzy system, Diagnostyka 25 (2024).
[33] E. Iacobelli, V. Ponzi, S. Russo, C. Napoli, Eye-tracking system with low-end hardware: development and evaluation, Information 14 (2023) 644.
[34] I. Naidji., O. Mosbahi., M. Khalgui., A. Bachir., Cooperative energy management software for networked microgrids, in: Proceedings of the 14th International Conference on Software Technologies - ICSOFT, INSTICC, SciTePress, 2019, pp. 428–438. doi:10.5220/0007965604280438.
[35] I. Naidji, M. B. Smida, M. Khalgui, A. Bachir, Non cooperative game theoretic approach for residential energy management in smart grid, in: The 32nd Annual European Simulation and Modelling Conference, Ghent, Belgium, 2018, pp. 164–170.
[36] I. Naidji, C. E. Choucha, M. Ramdani, Electricity theft detection techniques using artificial intelligence: a survey, in: 2024 IEEE International Conference on Advanced Systems and Emergent Technologies (IC_ASET), IEEE, 2024, pp. 1–6.
[37] I. Naidji., C. Choucha., M. Ramdani., Decentralized federated learning architecture for networked microgrids, in: Proceedings of the 20th International Conference on Informatics in Control, Automation and Robotics - Volume 1: ICINCO, INSTICC, SciTePress, 2023, pp. 291–294. doi:10.5220/0012215200003543.
[38] I. Naidji, M. B. Smida, M. Khalgui, A. Bachir, Multi agent system-based approach for enhancing cyber-physical security in smart grids, in: Proceedings

of the the 33rd Annual European Simulation and Modelling Conference, Palma de Mallorca, Spain, 2019, pp. 177–182.

[39] B. Nail, M. A. Atoussi, S. Saadi, I. E. Tibermacine, C. Napoli, Real-time synchronisation of multiple fractional-order chaotic systems: an application study in secure communication, Fractal and Fractional 8 (2024) 104.

[40] C. Napoli, V. Ponzi, A. Puglisi, S. Russo, I. Tibermacine, et al., Exploiting robots as healthcare resources for epidemics management and support caregivers, in: CEUR Workshop Proceedings, volume 3686, CEUR-WS, 2024, pp. 1–10.

[41] I. Naidji, O. Mosbahi, M. Khalgui, A. Bachir, Two-stage game theoretic approach for energy management in networked microgrids, in: M. van Sinderen, L. A. Maciaszek (Eds.), Software Technologies, Springer International Publishing, Cham, 2020, pp. 205–228.

[42] P. M. Dhulavvagol, S. Totad, A. M. Anagal, S. Anegundi, P. Devadkar, V. S. Kone, Shardedscale: Empowering blockchain transaction scalability with scalable block consensus, Procedia Computer Science 233 (2024) 432–443.

[43] T. Nguyen, H. Nguyen, T. N. Gia, Exploring the integration of edge computing and blockchain iot: Principles, architectures, security, and applications, Journal of Network and Computer Applications (2024) 103884.

[44] M. Torky, A. E. Hassanein, Integrating blockchain and the internet of things in precision agriculture: Analysis, opportunities, and challenges, Computers and Electronics in Agriculture 178 (2020) 105476.

[45] T. Wan, J. Ge, W. Liao, H. Zhao, A lightweight two-factor continuous authentication protocol for agricultural iot devices, Wireless Personal Communications 136 (2024) 921–945.

[46] A. Shamsoshoara, A. Korenda, F. Afghah, S. Zeadally, A survey on physical unclonable function (puf)-based security solutions for internet of things, Computer Networks 183 (2020) 107593.

[47] N. Javaid, Integration of context awareness in internet of agricultural things, ICT Express 9 (2023) 189–196.

[48] S. Selvarajan, G. Srivastava, A. O. Khadidos, A. O. Khadidos, M. Baza, A. Alshehri, J. C.-W. Lin, An artificial intelligence lightweight blockchain security model for security and privacy in iiot systems, Journal of Cloud Computing 12 (2023) 38.

[49] S. eddine Boukredine, E. Mehallel, A. Boualleg, O. Baitiche, A. Rabehi, M. Guermoui, A. Douara, I. E. Tibermacine, Enhanced performance of microstrip antenna arrays through concave modifications and cut-corner techniques, ITEGAM-JETIA 11 (2025) 65–71.

[50] T. M. Fernández-Caramés, From pre-quantum to post-quantum iot security: A survey on quantum-resistant cryptosystems for the internet of things, IEEE Internet of Things Journal 7 (2019) 6457–6480.

[51] H. Shekhawat, D. S. Gupta, Quantum-resistance blockchain-assisted certificateless data authentication and key exchange scheme for the smart grid metering infrastructure, Pervasive and Mobile Computing 100 (2024) 101919.

[52] C. Roumeliotis, M. Dasygenis, V. Lazaridis, M. Dossis, Blockchain and digital twins in smart industry 4.0: The use case of supply chain-a review of integration techniques and applications, Designs 8 (2024) 105.

[53] M. Arunmozhi, V. Venkatesh, S. Arisian, Y. Shi, V. R. Sreedharan, Application of blockchain and smart contracts in autonomous vehicle supply chains: An experimental design, Transportation Research Part E: Logistics and Transportation Review 165 (2022) 102864.

[54] P. Kamboj, S. Khare, S. Pal, User authentication using blockchain based smart contract in role-based access control, Peer-to-Peer Networking and Applications 14 (2021) 2961–2976.

[55] V. Tyagi, A. Saraswat, S. Bansal, An analysis of securing internet of things (iot) devices from man-in-the-middle (mima) and denial of service (dos), in: Smart Cities, CRC Press, 2023, pp. 337–357.

[56] W. C. Tan, M. S. Sidhu, Review of rfid and iot integration in supply chain management, Operations Research Perspectives 9 (2022) 100229.

[57] P. Kumar, R. Kumar, G. P. Gupta, R. Tripathi, A. Jolfaei, A. N. Islam, A blockchain-orchestrated deep learning approach for secure data transmission in iot-enabled healthcare system, Journal of Parallel and Distributed Computing 172 (2023) 69–83.

[58] P. Williams, I. K. Dutta, H. Daoud, M. Bayoumi, A survey on security in internet of things with a focus on the impact of emerging technologies, Internet of Things 19 (2022) 100564.

[59] A. J. Alkhodair, S. P. Mohanty, E. Kougianos, Consensus algorithms of distributed ledger technology–a comprehensive analysis, arXiv preprint arXiv:2309.13498 (2023).