Secure and Transparent Agri-Food Supply Chain Traceability with SSI and Blockchain-Enabled IoT

Jihene Khoualdi, Ilheme abedlmoula, Hella kaffel and Donia bensedrine

Abstract The agri-food supply chain encompasses multiple stages, including Production, Processing, and Distribution, and involves various stakeholders such as producers, processors, distributors, and consumers. Ensuring food quality, safety, and availability is critical to addressing growing consumer demands and meeting regulatory requirements for safe, authentic, and ethically sourced products. Effective traceability solutions are essential to prevent contamination, verify authenticity, reduce fraud, and enhance stakeholder accountability and trust. This paper introduces a blockchain-based solution integrating IoT and Self-Sovereign Identity (SSI) technologies to enhance transparency, security, and data integrity in agri-food supply chains. By leveraging blockchain's immutable ledger, the system provides tamper-proof and verifiable traceability data. The proposed solution combines Ethereum for traceability and IPFS for decentralized data storage, ensuring data privacy and security. A Proof of Concept demonstrates the system's feasibility, highlighting its potential to reinforce trust and accountability across the agri-food supply chain.

Key words: Blockchain, Decentralized Traceability, Honey Supply Chain, Transparency, IoT, privacy.

1 Introduction

The agri-food supply chain involves various stakeholders, including producers, processors, distributors, and retailers, all working together to deliver safe, high-quality

Jihene Khoualdi, LIPAH Laboratory, Faculty of Sciences of Tunis, University of Tunis El Manar, Tunis, 2092, Tunisia e-mail: jihene.khoualdi@etudiant-fst.utm.tn · Ilheme abedlmoula, LIPAH Laboratory, University of Sesame, Tunis, 2088, Tunisia e-mail: ilhem.abdelmoula@insat.ucar.tn · Hella kaffel, LIPAH Laboratory, Faculty of Sciences of Tunis, University of Tunis El Manar, Tunis, 2092, Tunisia e-mail: hella.kaffel@fst.utm.tn · Donia bensedrine, LIPAH Laboratory, University of Sesame, Tunis, 2088, Tunisia e-mail: donia.bensedrine@sesame.com.tn

products. As consumer awareness grows and regulations become stricter, reliable traceability is essential to ensure product safety, quality, and fraud prevention [1]. Honey, often adulterated, exemplifies these challenges. Its widespread consumption and vulnerability to fraud, such as mislabeling and adulteration with cheaper sweeteners, undermine consumer trust and authenticity. With global demand, especially in regions like the U.S., Saudi Arabia, and the UAE, expected to increase, the honey market is projected to grow from USD 10.2 billion to USD 13.5 billion by 2029 [2]. Traditional centralized systems in the honey supply chain face issues like data breaches and limited transparency, compromising traceability [4]. Emerging technologies like IoT, blockchain, and SSI offer promising solutions [6]. IoT enables real-time monitoring, blockchain ensures secure data storage, and SSI provides privacy-preserving identity management. However, existing solutions, such as IBM Food Trust and VeChain, still struggle with security vulnerabilities and scalability issues [7]. This paper proposes a multi-layered framework that integrates IoT, blockchain, and SSI to address these challenges, enhancing transparency, trust, and regulatory compliance in the agri-food ecosystem. Decentralized approaches using blockchain and IoT enable real-time monitoring and tamper-proof data storage, while SSI ensures decentralized stakeholder verification and reduces reliance on central authorities. The paper is organized as follows: Section 2 reviews related work and technologies, Section 3 presents the proposed architecture, Section 4 outlines the implementation methodology, Section 5 discusses experimental results, Section 6 evaluates the framework's strengths and limitations, and Section 7 concludes the paper.

2 Related Work and Motivation

Agri-food supply chains previously depended on paper-based systems, which were prone to errors, inaccuracies, and falsification, limiting the effectiveness of traceability and accountability [12]. As the demand for more reliable and transparent systems grew, centralized databases were introduced to improve traceability. However, these systems faced issues such as data silos, limited transparency, and heavy reliance on manual tracking methods like barcodes, all of which hindered real-time monitoring and decision-making [1]. Furthermore, centralized systems were susceptible to breaches and tampering, leading to a loss of trust in the supply chain integrity [11]. In response to these challenges, integrated solutions using blockchain and IoT technologies have emerged. Blockchain provides a secure, tamper-proof ledger, while IoT devices like RFID tags and sensors enable real-time data capture, tracking, and monitoring. These technologies enhance product quality, regulatory compliance, and transparency by allowing seamless and continuous monitoring throughout the supply chain [13, 14]. In the honey industry, blockchain and IoT have been explored to tackle traceability and fraud issues, with notable works such as Dobbins et al.'s "Blocks for Bees" [15], Runzel et al.'s smart honey supply chain proposal [17], and Madhwal et al.'s blockchain-based distribution system [19].

While these solutions show promise, challenges such as IoT-blockchain interoperability, scalability issues, and privacy concerns remain significant obstacles [5]. Integrating Self-Sovereign Identity (SSI) into these systems could address some issues by enabling decentralized control over digital identities and data sharing, enhancing security and privacy [22]. However, the adoption of SSI faces challenges, including technical complexity, regulatory compliance, and interoperability with existing systems [9]. Addressing these challenges is critical for creating a scalable, secure, transparent traceability framework in agri-food supply chains. Key research gaps include:

- Limitations of traditional traceability systems.
- Privacy and scalability issues with blockchain.
- Interoperability challenges between IoT devices and blockchain.
- Limited research on SSI integration with IoT and blockchain.

3 Multi-Layered Architecture for Agri-Food Traceability with SSI, IoT, and Blockchain

Our architecture, shown in Fig.1, combines blockchain, IoT, and self-sovereign identity (SSI) to enhance traceability and security in the agri-food supply chain. It assigns each actor a Decentralized Identifier (DID) and Verifiable Credentials (VCs) for controlled data access. The system is structured into six layers:

1. Actors Layer: Includes supply chain participants with defined roles, allowing consumers to access product data via RFID or QR codes for traceability.
2. Data Collection Layer: IoT sensors and RFID tags collect real-time data (temperature, humidity, location) and transmit it securely.
3. Preprocessing and Transmission Layer: Data is encrypted, stored on IPFS, and recorded on the blockchain for immutable traceability.
4. Security and Privacy Layer: Ensures data protection with encryption, hashing, and access controls.
5. Blockchain and Storage Layer: Records cryptographic hashes on the blockchain for immutability and transparency.
6. Access Control and User Interface Layer: Manages access with DIDs and VCs and provides a user interface with audit trails for accountability.

This architecture uses SSI for identity control and secure data sharing, while blockchain ensures data integrity, privacy, and transparency. It addresses interoperability, security, and privacy challenges, offering a reliable solution for traceability, product quality, and compliance in the agri-food supply chain.

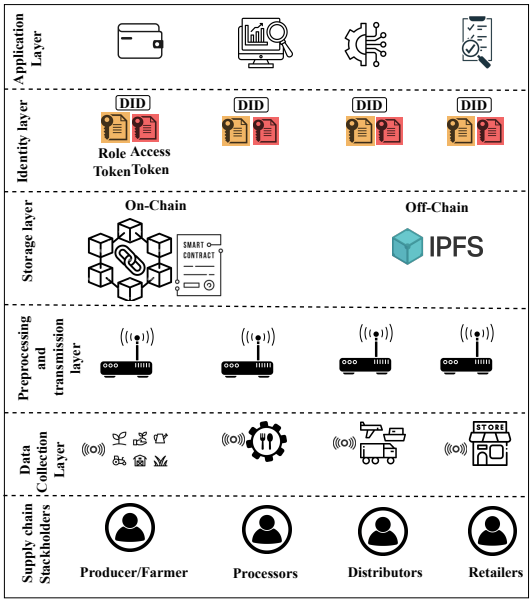

Fig. 1: Multilayered architecture.

4 Blockchain and IoT Integration for Enhanced Honey Supply Chain Traceability

The proposed architecture integrates blockchain with IoT to ensure traceability, authenticity, and quality control throughout the honey supply chain, addressing honey fraud. Data from smart beehives, which monitor temperature, humidity, and bee activity, is collected via a broker and processed through a secure gateway. The gateway uses mutual authentication with the mobile app, ensuring secure communication. The app then synchronizes with the blockchain through Metamask, storing data on IPFS and sending unique data hashes to the Ethereum blockchain for tamper-proof storage and integrity. This system improves security, transparency, and trust across the supply chain, as shown in Fig. 2. The architecture enhances traceability, guaranteeing honey quality and integrity from production to consumption, and promotes consumer trust. It verifies authenticity, ensures regulatory compliance, and provides transparency. Beekeepers capture essential data and use Decentralized Identifiers (DIDs) to issue Access-Based Verifiable Credentials (VCs) for secure data sharing. Processors issue Role-Based VCs for packaging and labeling compliance, while certification bodies assess quality using both Role-Based and Access-Based VCs. Distributors manage logistics and data access for traceability, and retailers offer consumers transparent data via Role-Based VCs. Regulatory authorities oversee compliance through audit permissions and privacy controls. Consumers can easily access traceability data through QR codes, confirming honey's origin and authen-

ticity. The solution integrates Smart Beehives, a Data Aggregation Broker, a Secure Transmission Gateway, IPFS, Ethereum Blockchain, and SSI to ensure secure data access. A use case was implemented to evaluate decentralized data-writing methods, focusing on privacy, security, and efficiency within the honey supply chain, thus fostering transparency and trust.

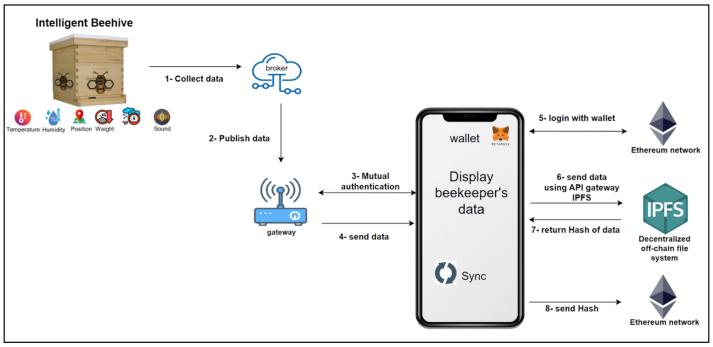

Fig. 2: Global architecture with Ethereum Blockchain.

4.0.1 Implementing IoT-Based Data Traceability and Verification in Supply Chains

The sequence diagram in Fig. 3 outlines secure data management in the honey supply chain. Data from smart beehives, including temperature and humidity, is sent via a broker to a Gateway, which authenticates with the mobile app using SHA-256 and a nonce. After successful authentication, the app syncs with the blockchain via Metamask, allowing data storage on IPFS and tamper-proof hash recording on Ethereum through smart contracts. For retrieval, the beekeeper requests data via Metamask, triggering hash verification on Ethereum and metadata validation on IPFS. If validated, the data is returned; otherwise, an alert is raised. Fig. 5 illustrates the issuance of a Role Verifiable Credential (Role VC) by the Ministry of Agriculture. The Holder generates the VC with their Decentralized Identifier (DID) and role, submits it for verification, and, upon approval, stores it on the blockchain. This system ensures secure data handling, transparency, and trust across the supply chain.

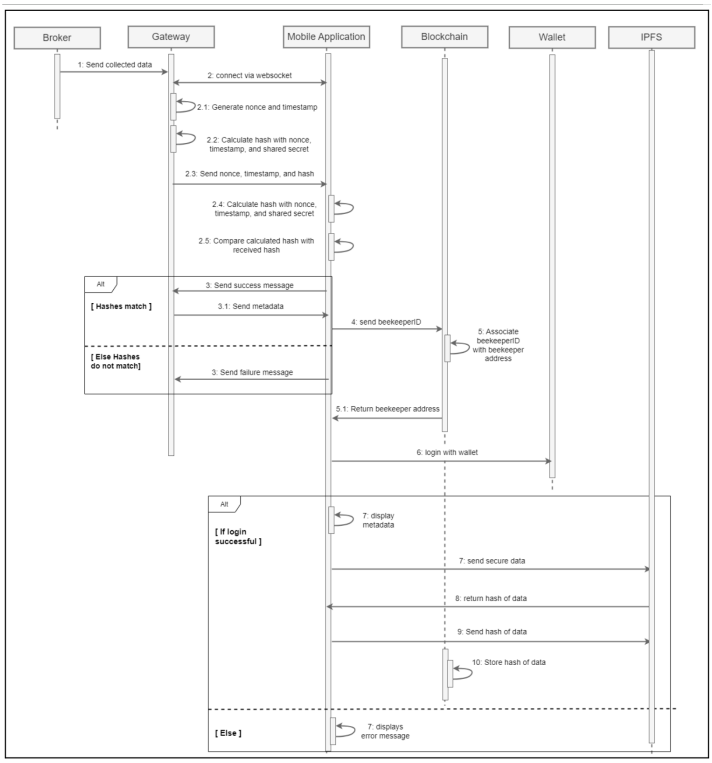

Fig. 3: The data flow based on a wallet.

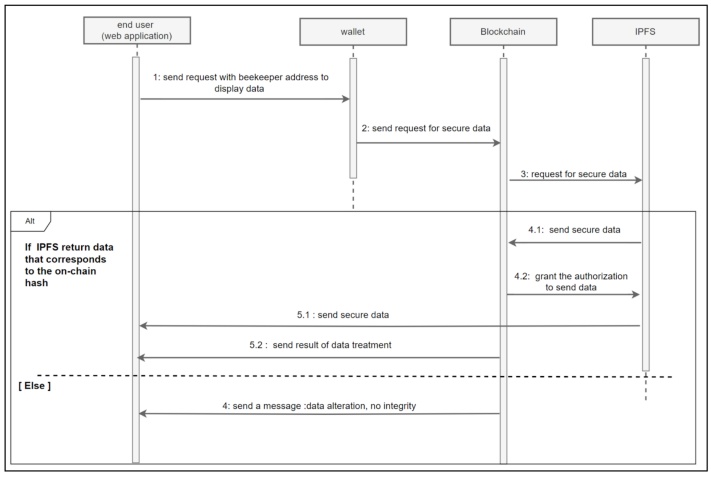

Fig. 4: Diagram of Data Reading.

4.0.2 Secure Issuance and Verification of Role Verifiable Credentials in Blockchain-Based Supply Chainsl

This section outlines the secure issuance and verification process for Role Verifiable Credentials (Role VCs) within a blockchain-based supply chain system, ensuring transparency, authenticity, and data integrity. As illustrated in Fig. 5, the Ministry of Agriculture issues a Role VC after the Holder generates it using their Decentralized Identifier (DID) and role. The Holder submits a verification request, and upon validation of the DID and role, the Ministry authorizes the credential. The Holder then signs the VC with their private key and submits it to the blockchain, which confirms the transaction and returns the block number and signed VC. If verification fails, the process halts, guaranteeing secure and tamper-proof transactions.Similarly, Fig. 6 highlights the steps for obtaining a Role VC. The Holder generates the VC, submits it for verification, and signs it upon authorization. The blockchain finalizes the process by storing the VC in a confirmed block and returning the details to the Holder. Failed verification prevents issuance, ensuring the integrity of the system. These mechanisms enhance traceability by allowing only verified roles to access and manage supply chain data, fostering transparency, trust, and robust data governance.

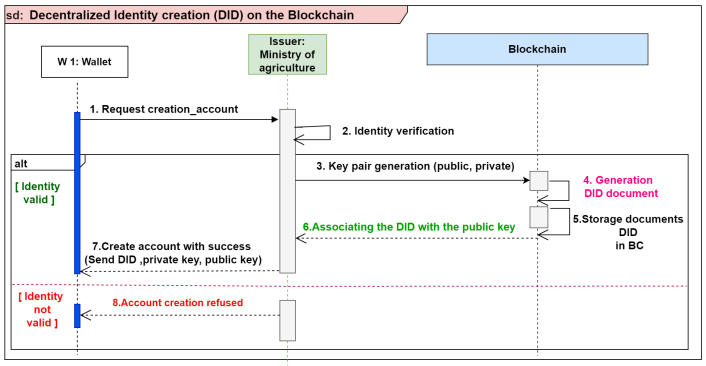

Fig. 5: Creation of a DID.

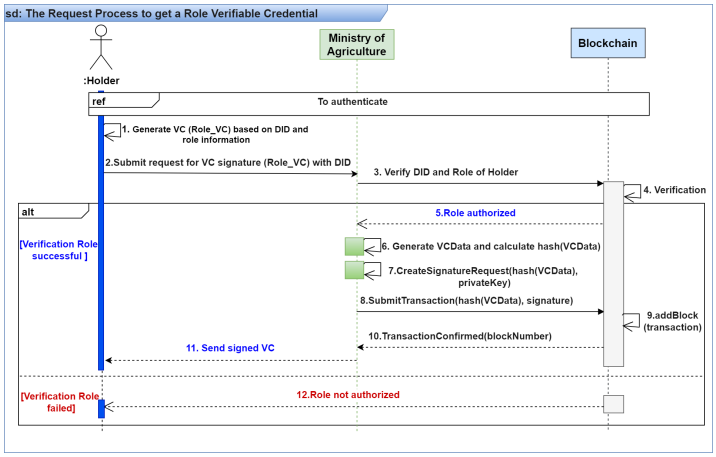

Fig. 6: The Request Process to get a Role Verifiable Credential.

5 Experimental Setup

Our solution integrates Ethereum and IPFS to enhance traceability and access management in the agri-food supply chain, ensuring secure, efficient, and privacy-preserving operations. IoT data is stored off-chain in IPFS, while Ethereum records only the corresponding hashes, creating tamper-proof records and reducing storage costs. A secondary blockchain leverages Self-Sovereign Identity (SSI) with verifiable credentials, enabling granular access control and protecting sensitive data.Two key smart contracts demonstrate the system's core functionality: HashStorage and BeekeeperContract. The HashStorage contract securely stores and retrieves IPFS hashes linked to beekeeper addresses, preserving data integrity and enabling efficient traceability with functions like storeIPFSHash and getIPFSHashByBeekeeperAddress. The BeekeeperContract manages beekeeper identities and hive data using structured mappings for secure associations. The Beekeeper structure includes beekeeper IDs, Ethereum addresses, and hive relationships, while the Hive structure records hive IDs, beekeeper IDs, and sensor data. Functions such as registerBeekeeper, registerHive, and processMetadata ensure proper identity mapping, metadata evaluation, and compliance with regulatory standards.Security and transparency are reinforced through the storeIpfsHash function, which guarantees secure metadata hash storage. Access control is enforced via MetaMask authentication and unique Ganache addresses, ensuring only authorized entities can interact with the system. The dual blockchain design also enables seamless integration of decentralized identity management, immutable data storage, and verified data transmission. The results of these implementations, along with the underlying processes, are illustrated in Fig. 7.

```
// SPDX-License-Identifier: SEE LICENSE IN LICENSE
pragma solidity ^0.5.0;

//import "./BeekeeperContract.sol";

contract HashStorage {
    address public owner;
    uint256 public numHashes;
    uint256[] public identifiers; // Array to keep track of keys
    //BeekeeperContract public beekeeperContract;// Reference to the BeekeeperContract's address
    struct HashInfo {
        bytes32 ipfsHash;
        address beekeeperAddress;
    }
    mapping(uint256 => HashInfo) public hashes;

    // Event to emit the stored IPFS hash
    event IPFSHashStored(uint256 identifier, bytes32 ipfsHash, address beekeeperAddress);
    // Event to signal the retrieval of the on-chain IPFS hash associated with a beekeeper address
    event IPFSHashRetrieved(address beekeeperAddress, bytes32 retrievedHash);

    modifier onlyOwner() {
        require(msg.sender == owner, "Only the owner can call this function");
        _;
    }
    //constructor(address _beekeeperContractAddress)
    constructor() public{
        owner = msg.sender;
        //beekeeperContract = BeekeeperContract(_beekeeperContractAddress); // Initialize the BeekeeperContract instance
    }
```

```
// SPDX-License-Identifier: SEE LICENSE IN LICENSE
pragma solidity ^0.5.0;

contract BeekeeperContract {
  // structure of the beekeepers
  struct Beekeeper {
   uint beekeeperId;
   uint[] hiveIds;
   address beekeeperAddress;
  }
  //structure of the hives
  struct Hive {
   uint hiveId;
   uint beekeeperId;
   uint sensorTemprature Value;
   uint sensorHumidityValue;
   uint sensorCO2Value;
   uint sensorWeightValue;
   bool hasPests;
   bool hasDiseases;
   bool isBeesStateOkay;
   bool isOrganicHoney;
   bool isTemperatureOkay;
   bool isHumidityOkay;
   bool isCo2Okay;
   bool isWeightOkay;
  }
   // mapping both beekeepers and hives
   mapping(uint => Beekeeper) beekeepers;
   mapping(uint => Hive) hives;
   mapping(uint256 => address) private beekeeperAddresses;
```

Fig. 7: hashStorage and beekeeper smart contract

6 Results and Discussion

This section describes the secure interaction flow between the broker, gateway, and web application for accessing and displaying beekeeping data. Beekeepers log in via MetaMask, which verifies their identity and retrieves their unique address from the Ganache blockchain. The address is used to access corresponding data securely through a smart contract, ensuring transparency and secure handling. The web interface Fig. 8 provides real-time hive data, including ”Beehive Data,” ”Bees’ State,” and ”Honey Quality,” retrieved via WebSocket and blockchain. It also displays essential metadata like GPS coordinates, beekeeper addresses, and hive IDs for comprehensive traceability. Fig.9 illustrate the mobile app’s secure login and metadata upload, where data is sent to IPFS Pinata, generating a metadata hash for integrity and safe storage. A comparative analysis highlights the benefits of blockchain-based supply chains over centralized systems, including enhanced transparency, security, and privacy. By leveraging IoT, IPFS, Ethereum, and SSI, the solution offers decentralized, immutable records with granular access control and privacy-preserving data management. Despite its advantages, challenges such as scalability and mobile wallet integration with blockchain networks require further optimization for resource efficiency.

7 Conclusion

This study presents a blockchain-based framework to enhance data integrity, transparency, and security in supply chain management. By utilizing blockchain’s immutable ledger and Self-Sovereign Identity (SSI), the framework ensures tamper-proof data, empowers participants with identity control, and balances confidentiality with compliance. The integration of IoT technology enables real-time monitoring

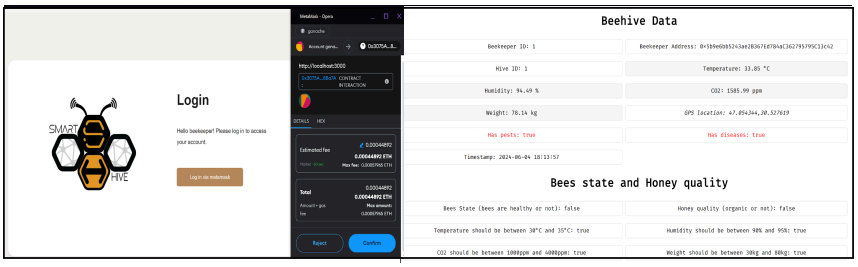

Fig. 8: Web Interface for Wallet Login and Data Display

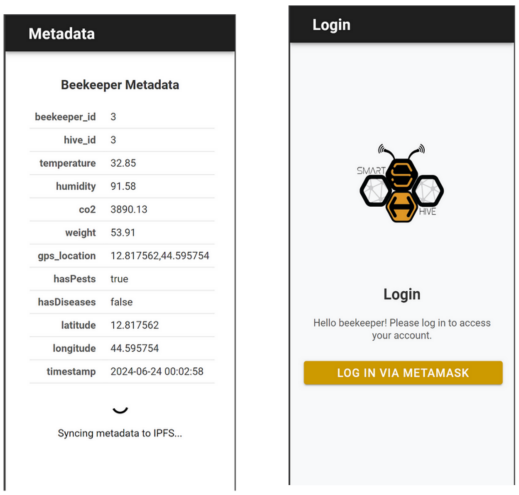

Fig. 9: Mobile application.

and data-driven decisions, while decentralized traceability ensures secure and transparent product tracking from origin to destination. A mobile wallet application securely stores data on IPFS, with Ethereum blockchain hashes guaranteeing privacy and authenticity. Future research could explore the application of this framework in sectors beyond agri-food, such as pharmaceuticals, manufacturing, and logistics, to improve transparency and security across various supply chains. Addressing scalability through Layer 2 solutions or alternative blockchain networks could optimize performance and reduce costs. Additionally, a comparative cost analysis would provide insights into the feasibility and sustainability of our solution. Developing adaptive privacy mechanisms would allow stakeholders to customize data visibility according to regulatory or business needs. This work establishes a flexible, scalable, and cost-effective solution for meeting the evolving traceability demands of modern supply chains.

Acknowledgements This work was produced in the TECHONEY project, that was supported by the the PRIMA programme (Project ID: 1711, Call: 2021, Topic ID: 2.3.1) with support from the European Union's Horizon 2020 research and innovation programme and the national research and innovation funding agencies of Spain (AEI, PCI2022-132917), France (ANR), Algeria (DGRSDT), Luxembourg (FNR, 16735444), Tunisia (MESRS), Morocco (MHESRI-M), Italy (MUR), and Turkiye (TÜBİTAK).

References

1. Aung, M.M., Chang, Y.S.: Traceability in a food supply chain: Safety and quality perspectives. In: Food Control, vol. 39, pp. 172–184 (2014). https://doi.org/10.1016/j.foodcont.2013.11.007
2. Zhao, G., Liu, S., Lopez, C., Lu, H., Elgueta, S., Chen, H., Boshkoska, B.M.: Blockchain technology in agri-food value chain management: A synthesis of applications, challenges and future research directions. In: Computers in Industry, vol. 109, pp. 83–99. Elsevier (2019)
3. Feng, H., Wang, X., Duan, Y., Zhang, J., Zhang, X.: Applying blockchain technology to improve agri-food traceability: A review of development methods, benefits and challenges. In: Journal of Cleaner Production, vol. 260, p. 121031 (2020). https://doi.org/10.1016/j.jclepro.2020.121031
4. Conoscenti, M., Vetro, A., De Martin, J.C.: Blockchain for the Internet of Things: A systematic literature review. In: 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), pp. 1–6. IEEE, Agadir, Morocco (2016). https://doi.org/10.1109/AICCSA.2016.7945805
5. Tian, F.: A supply chain traceability system for food safety based on HACCP, blockchain and Internet of Things. In: 2017 International Conference on Service Systems and Service Management, pp. 1–6. IEEE (2017)
6. Hmoud, A., Ali, G., Alanzi, R., Elkhediri, S.: IoT and Blockchain Integration Security. In: 2023 6th International Conference on Advanced Communication Technologies and Networking (CommNet), pp. 1–9. IEEE (2023). https://doi.org/10.1109/CommNet60167.2023.10365274
7. Wang, Y., Han, J.H., Beynon-Davies, P.: Understanding blockchain technology for future supply chains: a systematic literature review and research agenda. In: Supply Chain Management: An International Journal, vol. 24, no. 1, pp. 62–84 (2019). https://doi.org/10.1108/SCM-03-2018-0148
8. IBM Supply Chain Intelligence Suite - Food Trust. Available at: https://www.ibm.com/products/supply-chain-intelligence-suite/food-trust (Accessed: 2024-11-18)
9. Bălăceanu, E., Cojocaru, E., Simion.: Challenges in Integrating SSI with IoT and Blockchain for Traceability. In: Journal of Emerging Technologies in Computing Systems (2022).
10. Mohanta, B.K., Jena, D., Panda, S.S., Sobhanayak, S.: Blockchain technology: A survey on applications and security privacy challenges. In: Internet of Things, vol. 8, p. 100107 (2019). https://doi.org/10.1016/j.iot.2019.100107
11. Pearson, S., May, J., Gulliver, S.R.: Centralized vs Decentralized Supply Chain Models: Risks and Implications. In: European Conference on Information Systems (ECIS) (2021).
12. Regattieri, A., Gamberi, M., Manzini, R.: Traceability of food products: General framework and experimental evidence. In: Journal of Food Engineering, vol. 81, no. 2, pp. 347–356 (2007). https://doi.org/10.1016/j.jfoodeng.2006.10.032
13. Galvez, J.F., Mejuto, J.C., Simal-Gandara, J.: Future challenges on the use of blockchain for food traceability analysis. In: TrAC Trends in Analytical Chemistry, vol. 107, pp. 222–232 (2018). https://doi.org/10.1016/j.trac.2018.08.011

14. Kamble, S.S., Gunasekaran, A., Sharma, R.: Modeling the blockchain enabled traceability in agriculture supply chain. In: International Journal of Information Management, vol. 52, p. 101967 (2020). https://doi.org/10.1016/j.ijinfomgt.2019.05.023
15. Rochelle, C., Bhattacharjee, P.: March 22-23, 2018 East Tennessee State University, Johnson City, TN (2018).
16. Deng, Y., Xu, H., Wu, J.: Optimization of blockchain investment portfolio under artificial bee colony algorithm. In: Journal of Computational and Applied Mathematics, vol. 385, p. 113199 (2021). https://doi.org/10.1016/j.cam.2020.113199
17. Runzel, M.A.S., Hassler, E.E., Rogers, R.E.L., Formato, G., Cazier, J.A.: Designing a Smart Honey Supply Chain for Sustainable Development. In: IEEE Consumer Electronics Magazine, vol. 10, no. 4, pp. 69–78 (2021). https://doi.org/10.1109/MCE.2021.3059955
18. Paunovic, M., Alizadeh, Z.: Conceptual Blockchain Model for Honey Supply Chain System. In: Book of Proceedings of 5th International Scientific Conference Village and Agriculture (2022).
19. Madhwal, Y., Pieber, E., Yanovich, Y., Yakushkina, T.: Smart Contract Based Honey Production Supply Chain. In: Proceedings of the 2022 5th International Conference on Blockchain Technology and Applications, no. 4, pp. 70–76 (2022). https://doi.org/10.1145/3581971.3581981
20. Lukovac, P., Miletić, A., Radenković, B.: A System for Tracking Organic Honey Production Using Blockchain Technologies. In: Mihić, M., Jednak, S., Savić, G. (eds.) Sustainable Business Management and Digital Transformation: Challenges and Opportunities in the Post-COVID Era, pp. 239–254. Springer International Publishing, Cham (2023). ISBN 978-3-031-18645-5
21. Danieli, P.P., Lazzari, F.: Honey Traceability and Authenticity: Review of Current Methods Most Used to Face this Problem. In: Journal of Apicultural Science, vol. 66, no. 2, pp. 101–119 (2022). https://doi.org/10.2478/jas-2022-0012
22. Preukschat, A.: Self-Sovereign Identity: Decentralized Digital Identity and Verifiable Credentials. Manning Publications (2021)