OPEN ACCESS

*International*
*Journal*
*Of Modern Engineering Research (IJMER)*

# Farm to Fork: A Comprehensive Guide to Implementing Blockchain in Agri-Food Supply Chain System

D. SHIVAMURTHY [1] M.Tech (C.S. & E), C. SHADAKSHARAIAH [2] M.Tech (C.S. & E)
[1] *Assistant Professor, Department of Information Science and Engineering, Bapuji Institute of Engineering and Technology, Davangere, Karnataka, India, Email: dscsebiet@gmail.com*
[2] *Assistant Professor, Department of Computer Science and Design, Bapuji Institute of Engineering and Technology, Davangere, Karnataka, India, Email:cshadaksharaiah@gmail.com*
[1] *Corresponding author: dscsebiet@gmail.com*

***ABSTRACT:*** *Supply chains are evolving into intricate networks, offering significant benefits in today's world. Concurrently, consumer interest in food product quality is increasing. However, ensuring data provenance and traceability throughout the supply chain poses challenges. Traditional centralized supply chains rely on third parties for trading, lacking transparency, accountability, and auditability. In our proposed solution, we introduce a comprehensive blockchain-based Agriculture and Food (Agri-Food) supply chain system, utilizing the features of blockchain and smart contracts on the ethereum network. While blockchain ensures data immutability, it doesn't fully address credibility, accountability, and product traceability issues. Thus, a reliable system is imperative to ensure traceability, trust, and delivery in Agri-Food supply chains. Our system records all transactions on the blockchain, subsequently uploading data to the Interplanetary File Storage System (IPFS). This system generates a hash of the data stored on the blockchain, ensuring an efficient, secure, and reliable solution. Additionally, we provide smart contracts and their algorithms to demonstrate entity interactions in the system. Moreover, we present simulations, evaluations of smart contracts, and security analyses, enhancing the robustness of our proposed solution.*

***KEY WORDS:*** *Supply chain, Block chain, Accountability, Traceability, Credibility, Reputation.*

---

Date of Submission: 06-06-2024 Date of acceptance: 19-06-2024

---

## I. INTRODUCTION

The Supply Chain Management (SCM) encompasses processes and sub-processes aimed at converting raw materials into final products, maximizing customer value, and gaining a sustainable competitive advantage [1]. It is essentially a network of entities involved from production to trading, segmented into several stages, with processes often spanning months [2]. Amidst this, tracking product quality issues to their origin becomes exceedingly challenging. Consumer demand for top-quality products and transparency in data provenance is rapidly rising, necessitating robust tracking from origin to end consumers [3]. To earn consumer trust, supply chain authorities must efficiently and accurately deliver information, while upholding quality, integrity, and credibility standards. Regulatory authorities worldwide enforce standards to enhance transparency, quality, and security in supply chain traceability systems, such as the Canadian and Chinese governments' mandates for product tagging and barcoding [4]. These regulations aim to enhance traceability system transparency and product quality assurance.

Beyond traceability, supply chain systems also serve as trade gateways, managing vast amounts of transactional data, adding complexity to network architecture. Centralized systems, common in supply chains, pose risks of inaccurate information representation and lack trust and credibility in financial transactions due to their centralized nature. Moreover, centralized storage schemes struggle with large data volumes, causing bottlenecks and performance issues. Distributed systems offer fault tolerance, scalability, concurrent processing, and improved storage schemes. Block chain emerging as the foundational technology of Bit coin, addresses the risks of centralized systems, offering decentralization, transparency, and immutability [6]. However, current blockchain networks face challenges in data-driven domains due to latency, storage, and throughput issues [7].

Various network architectures and consensus protocols aim to maintain blockchain integrity while enhancing throughput and storage capabilities [7], [8].

In Agri-Food supply chains, efficient product monitoring is critical for food safety, meeting consumer and governmental quality concerns, renewing traceability concepts. Blockchain's properties, like decentralization and transparency, play a significant role in supply chain evolution. Yet, challenges persist in establishing trust and ensuring product quality in blockchain-based Agri-Food supply chains. Additionally, traditional centralized storage schemes struggle with large data volumes in supply chain processes, leading to bottlenecks. Decentralized storage schemes, proposed in literature, aim to overcome latency, throughput, and bottleneck issues. For instance, a blockchain-based soybean traceability scheme utilizes ethereum smart contracts and the Inter Planetary File Storage System (IPFS) for complete traceability [9]. However, such systems face challenges of data accessibility and accountability.

Our paper addresses these challenges, contributing to blockchain-based Agri-Food supply chains with an end-to-end solution. We build upon a blockchain-based reputation system proposed earlier [12], leveraging ethereal smart contracts to ensure efficiency, security, and trust in supply chain activities. The main contributions of our proposed system include:

- Introducing an end-to-end distributed supply chain system, incorporating a traceability scheme, trading and delivery mechanisms, and a reputation system for entity credibility assurance, along with an autonomous transaction system.
- Achieving desired properties like accountability, credibility, auditability, autonomy, and authenticity.
- Offering a scalable and auditable alternative to existing Agri-Food supply chain systems, presenting smart contract algorithms and evaluating their vulnerability and cost efficiency over the ethereum network.
- Ensuring resilience against known attacks and providing essential security features. We conduct a detailed vulnerability assessment and discuss the system's robustness and security against malicious attacks.

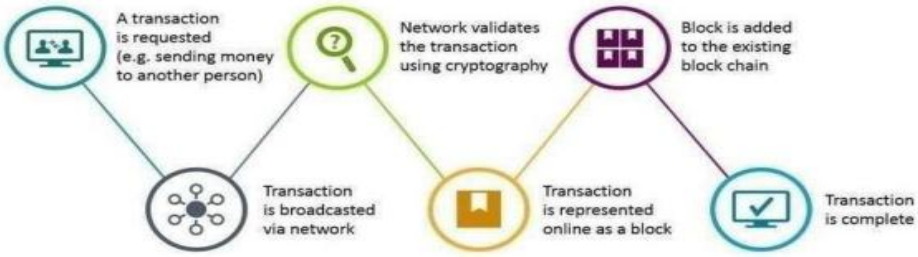



**Figure 1: Working of Blockchain**

## II. RELATED WORK

In this section, we analyze and compare various schemes aimed at enhancing Agri-Food supply chain systems, highlighting how they differ from our proposed solution. Ensuring food safety has become a critical concern in both commercial and academic circles. Many existing solutions rely on centralized systems, which are prone to issues such as fraud, tampering, and man-in-the-middle attacks [13]. As a result, the literature has introduced several blockchain-based traceability and information security schemes for Agri-Food supply chains. For example, one approach employs a traceability scheme that combines Hazard Analysis and Critical Control Points (HACCP), blockchain, and IoT [14]. To address blockchain's scalability issues, BigChainDB is integrated. Although this solution offers significant transparency and efficiency, it does not provide detailed product ownership information. Similarly, a case study on product traceability presents an origin-chain design that uses both private and public blockchains to ensure transparent and tamper-proof tracing [15]. While this solution effectively stores data on-chain and off-chain, there are ongoing concerns about security and privacy. Another proposal centers on blockchain-based food information security in supply chain management, providing more reliable solutions for accurate traceability, particularly in the Chinese market [16].

Decentralized solutions have also been investigated, such as a blockchain-based decentralized traceability process [17]. Despite its merits, the effectiveness of this solution is compromised by issues with auditability and integrity. Additionally, researchers have proposed blockchain and IoT-based solutions to address food safety concerns in Agri-Food supply chains [18], comparing platforms like Ethereum and Hyperledger for implementation. Storage mechanisms have also advanced, with decentralized systems like IPFS becoming more popular. One scheme suggests a robust storage solution for tracking Agri-Food products by combining IPFS with a secondary database for traceability [10], though the reliance on a secondary database introduces a single point of failure. Another proposal highlights efficient transaction handling for soybean

traceability, utilizing blockchain to remove the need for a trusted third party [9]. Payment mechanisms have been explored as well, with blockchain-based anonymity-preserving delivery methods being proposed [20], although these tend to compromise entity accountability. Auditability protocols designed for transparent and tamper-proof transactions are also discussed, but they often neglect merchant credibility [11].

Several proposals have tackled storage security concerns by integrating Ethereum blockchain with decentralized storage systems like IPFS [23]. However, these solutions face scalability challenges, particularly in IoT scenarios. Trustless privacy-preserving reputation systems have also been proposed, though they often lack performance analysis and are susceptible to malicious users [5]. In general, the adoption of blockchain in agriculture-based supply chain systems is rapidly increasing to improve transparency, traceability, and food safety. Building on the existing literature, we propose a blockchain-based solution designed to ensure accountability, auditability, and credibility in Agri-Food supply chain systems.

## III. SYSTEM MODEL

In this section, we introduce our innovative solution. We have designed a traceability framework that digitally monitors Agri-Food products from their origin to the end consumer. Our system incorporates a secure trading and delivery mechanism, enabling transactions among different entities within the Agri-Food supply chain. Furthermore, a reputation system is implemented to ensure the credibility of these entities. The proposed model is organized into three layers:

- **Data Layer:** This fundamental layer handles interactions among entities in the Agri-Food supply chain, including the trading of products accompanied by verifiable delivery proofs.
- **Blockchain Layer:** This layer is responsible for managing transactional data and tracking reputations, ensuring the integrity and security of trading and delivery activities. It enhances storage efficiency by storing only data hashes, while the actual data is maintained in the third layer.
- **Storage Layer:** This layer stores transaction and event data on IPFS (InterPlanetary File System), a decentralized storage solution renowned for its high throughput, low latency, and scalability. The blockchain layer enforces strict access controls to prevent unauthorized access.

The following sections explore how our system accomplishes traceability, detailing trade events and the auditable delivery process within the Agri-Food supply chain. Furthermore, we examine the mechanics of the reputation system and its benefits within our proposed framework.

### *3.1 TRACEABILITY*

Supply chain systems comprise numerous entities responsible for overseeing the entire journey of Agri-Food products from production to consumer delivery. Tracking and tracing this intricate process can be challenging. To achieve comprehensive traceability, we meticulously record each trading transaction from its inception, attaching the product's unique identity and lot number to subsequent transactions, thereby creating a hash chain. A "lot" refers to a grouping of products designated for trade within a warehouse, with each lot assigned a unique identifier. Transactional data is stored on IPFS to maintain the hash chain, while data hashes are recorded on the ethereum blockchain to address IPFS limitations. Access to and modification of blockchain data are regulated by access control strategies, ensuring network privacy and confidentiality. These strategies validate transactions exclusively for authorized users, allowing registered users to perform specific functions within smart contracts. Algorithm 1 outlines the entity registration process, where inputs such as entityAddress and entityType result in the registration of the respective entity as an authorized system user. These entities, integral to the data layer, are further detailed as follows.

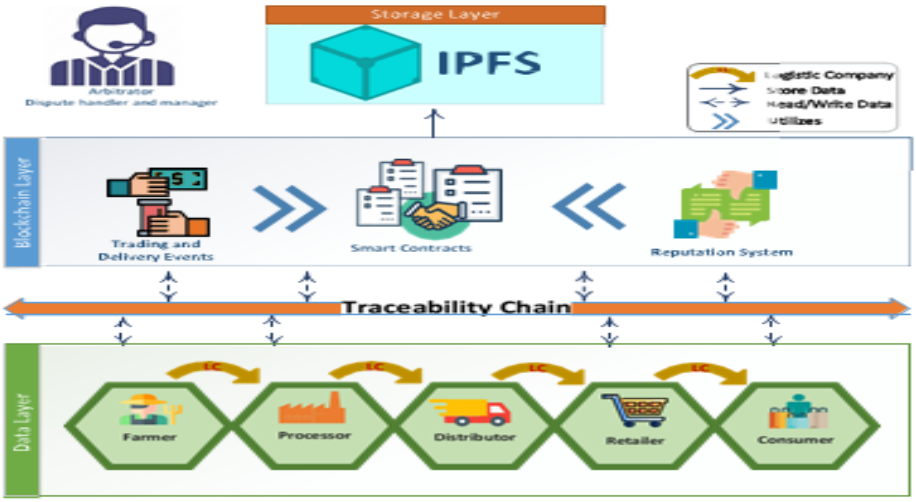



**Figure 2: Blockchain based end to end solution for agri-food supply chain.**

- **Farmer:** A farmer is the first entity in Agri-Food supply chain and is the first one to invoke smart contract for trading. Farmer produces large amount of crops and take the responsibility for assuring and monitoring the crops' growth details. He sells these crops to the processors.
- **Processor:** A processor buys the crops from farmers. He is responsible for eliminating extra material from the crops and converting them into a finalized product. Processor sells this finalized product to distributors.
- **Distributor:** A distributor maintains a warehouse by buying finalized products from processors and is responsible for selling it to the retailers.
- **Retailer:** A retailer buys the finished traceable products from distributors and sells them to customers in smaller quantities. Traceable product refers to specific identifiers of the goods that allow tracking the provenance data.
- **Consumer:** A Consumer is an end user who buys and consumes the products from retailers. A consumer verifies the credibility of a seller through reputation system before buying the products.
- **Logistic Company:** The Logistic Company (LC) is responsible for an auditable delivery of the products from product owners to the purchasers.
- **Arbitrator:** Arbitrator is an off-chain entity that is selected to monitor and manage the entire network. Additionally, it also acts as dispute handler.

The traceability process involves three smart contracts: the Registration Contract (RC), Add to Lot Contract (ALC), and Add Transaction Contract (ATC). To ensure a comprehensive traceability chain of transactions, these contracts require the addresses of their preceding contracts. Consequently, all three contracts are deployed to obtain their respective addresses, enabling complete traceability for end consumers and preserving data provenance. The RC is responsible for registering Agri-Food supply chain entities and their respective products.

Moreover, supply chain entities undergo registration on the network, with authorization strictly enforced during events. Only designated entities are permitted to execute specific transactions; for instance, solely arbitrators hold the authority to expel entities or malicious users from the system. Arbitrators, entities operating off-chain, oversee dispute resolution. All transactions, encompassing product registration, lot addition, and updates to transaction hashes, are permanently logged on the blockchain. The product owner assumes the responsibility of deploying the ALC alongside the RC, containing comprehensive product details, lot information, and transaction data. These transactions are inscribed onto the blockchain to ensure seamless product transfer within the Agri-Food supply chain. The traceability scheme ensures that all transactions are securely linked to the blockchain, guaranteeing thorough data provenance tracing.

### *3.2 TRADING AND DELIVERY*

Before exploring the trading and delivery mechanism, let's consider a scenario where the end consumer seeks information about traders' market reputation before initiating a transaction. This system aims to ascertain the trustworthiness of product owners, offering reassurance to consumers. Additionally, for product delivery among entities, the entire process is systematically tracked and documented on the blockchain, ensuring transparency and auditable delivery for end consumers. The trading and delivery process comprises three main

entities: the product owner, LC (courier service), and purchaser. The product owner initiates the sale within the supply chain, while the LC oversees the physical transfer of goods, and the purchaser aims to exchange ethers for a product. It's important to note that the LC is a registered entity within the system. In case of transaction disputes, arbitrators are responsible for off-chain dispute resolution. Please refer to Figure 3 for a visual depiction of the trading and delivery model.

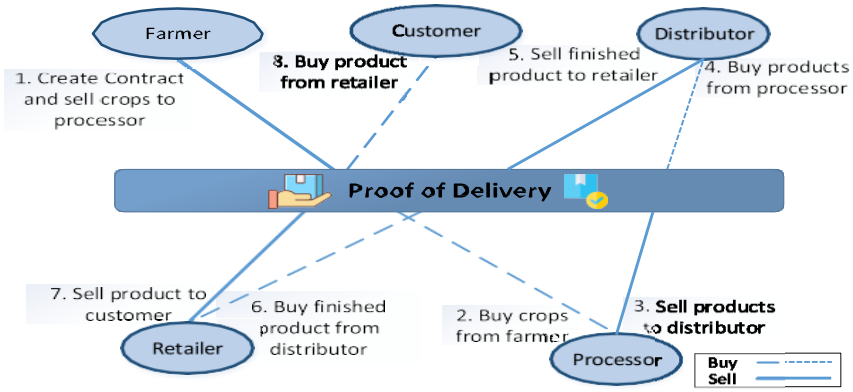



**Figure 3: Trading and Delivery mechanism.**

To commence the trading process, trading entities are initially registered with the smart contract, namely RC, and authenticated using their Ethereum addresses. Following this, the contract between the product owner and purchaser is initialized. During this phase, the purchaser selects the desired product and enters its unique code, P1, which serves as a distinct identifier for the product and is utilized by the LC. The product code, along with its details, is then transmitted to the product owner. Additionally, the product details, including the owner's information, image, and price, are uploaded to IPFS, and in exchange, an IPFS hash is generated to validate the product's authenticity during transfer. Upon receiving the product, the purchaser confirms successful delivery, and the logistics company receives payment. Furthermore, both parties contribute a security amount to the contract to confirm the trading transaction. The inclusion of a fine serves as a deterrent for potential disputes, with arbitrators authorized to resolve such issues off-chain. Once the transaction is confirmed, the purchaser submits the payment amount to the product owner.

In case of a dispute, all funds are transferred to the arbitrator's account and distributed according to the off-chain settlement procedure. Furthermore, once the transaction between the product owner and purchaser is completed, the smart contract between the product owner and LC is activated. This contract oversees the transportation of products from one location to another, ensuring the efficient management of the delivery process. As part of this process, both the product owner and purchaser contribute to transportation security, addressing concerns about potential manipulation.

Upon collection of the product for delivery, the LC conducts a pre-verification procedure. This involves using the IPFS hash to access the product details and comparing them with the actual product. Such verification helps prevent any alterations to the product during transit, thereby maintaining its authenticity throughout the delivery process.

### *3.3 REPUTATION SYSTM*

Embedded within the blockchain layer of the proposed model, a reputation system, illustrated in Figure 4, is integrated. This system holds significant importance in verifying the credibility of both product owners and the delivered assets. It ensures the immutability and integrity of registered reviews within the system. Unlike conventional reputation systems, reviews are stored in IPFS, while their corresponding hashes are retained in the blockchain, ensuring their integrity and permanence.

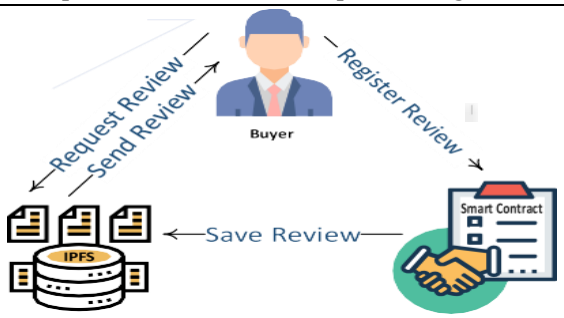



**Figure 4: Reputation system.**

Moreover, in the proposed solution, trading entities frequently take on dual roles as both sellers and buyers, with the exception of farmers and end customers. For instance, as depicted in Figure 4, retailers acquire end products from distributors and subsequently sell them to customers. Similarly, processors obtain crops from farmers, process them, and then vend the resulting products to distributors. Throughout this document, the terms "sellers" and "product owners," as well as "buyers" and "purchasers," are utilized interchangeably.

The reputation system allocates trust values to sellers, aiming to bolster confidence among trading entities. Whenever an entity purchases a product, it assigns ratings and provides reviews for the product owner, with these trust values reflecting the quality of services offered by the sellers. An entity's reputation varies depending on the trust values recorded in the blockchain-based supply chain, where a higher trust value signifies a greater level of trustworthiness for the seller. Purchasers rely on these trust values to assess the reliability of a product owner. As sellers can receive both positive and negative ratings, the trust value in the proposed solution is computed using the following equation (1). Where *Ratings* denotes sum of all ratings of a seller and $Total_{Rev}$ is the total number of reviews provided to the seller.

$$\text{TrustValue} = \Sigma\, Ratings/TotalRev \qquad (1)$$

The proposed system bolsters trust among trading entities by ensuring that buyers are informed about a seller's reputation prior to making a purchase. When entities engage in a smart contract for trading, a corresponding smart contract for reputation is also activated, furnishing reviews of available data sellers. Following a successful transaction, the buyer submits a review based on the received products, which is then stored in the seller's profile within the blockchain system. As depicted in Figure 4, the smart contract incorporates five functions: RegisterReview(), SearchReview(), SaveReview, SendReview(), and RequestReview(). These functions are responsible for registering a review, validating its content, saving it, transmitting it, and soliciting a new review, respectively. The RegisterReview() function accepts metadata, asset ratings, and review details as inputs, aiding end consumers in assessing both the product quality and the reputation of the product owner.

## IV. SIMULATIONS AND RESULTS

In this section, we discuss the assumptions, simulation tools, and performance results of the proposed system. The following are some key assumptions:

- The arbitrators within the system are honest and do not make biased decisions when resolving disputes.
- Arbitrators possess higher computational power compared to other entities in the network.
- No single entity in the network has enough computational power to compromise more than half of the network nodes.
- Only registered entities are allowed to buy or sell products in the market.

For simulation purposes, we employed Ethereum, an open-source platform for blockchain technology. The smart contracts were deployed on Ethereum's test network, Rinkeby. Ethereum offers support for developing decentralized applications utilizing blockchain technology. To assess the performance of the blockchain-based supply chain network, we utilized various tools: Remix Integrated Development Environment (IDE), Ganache, and MetaMask. Remix assists in writing, executing, and testing smart contracts, utilizing Solidity as the programming language. Ganache provides virtual accounts with a predefined amount of cryptocurrency, deducting the cryptocurrency from the account following each transaction. Each Ganache account possesses its own private key and unique address. MetaMask, a browser extension, serves as a bridge between Ganache and Remix IDE, facilitating their connection.

The system specifications are: Intel Core i5 processor at 2.4 GHz, 8 GB RAM, and 500 GB storage. The performance parameters used to evaluate the proposed solution are as follows:

- Transaction and execution cost (gas) of smart contracts
- Total gas consumed for input strings of varying lengths in the review system

- Mining time for input strings of same and different lengths in the reputation system
- Deployment cost of smart contracts
- Number of products registered in the Agri-Food supply chain

As depicted in Figure 5, the gas consumption of the reputation system's smart contract is illustrated, encompassing four functions: RegisterReview(), SearchRatings(), SearchReview(), and DoesReviewExist(). The graph indicates that the RegisterReview() function consumes the highest amount of gas for execution and transaction, primarily due to its responsibility for storing reviews to the user's profile on the blockchain and executing complex operations. Consequently, the transaction costs for the remaining functions are comparatively lower. The execution cost is influenced by the computational complexity of the transactions, while the transaction cost comprises both the execution cost and the expense of deploying the smart contract code to the Ethereum blockchain.

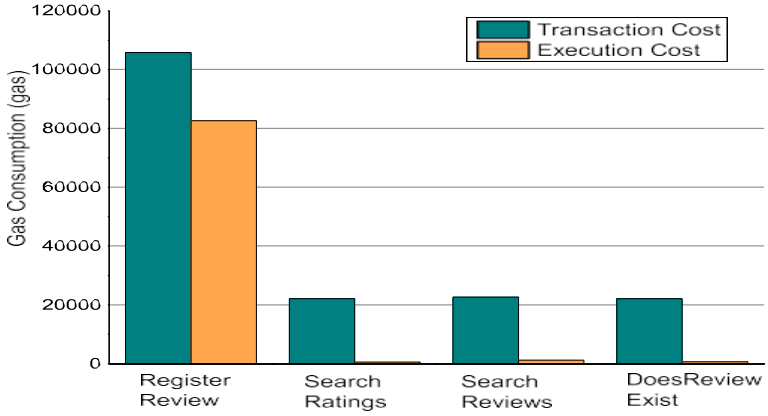



**Figure 5: Gas consumption of reputation system.**

## V. ANALYSES

As blockchain technology becomes increasingly prevalent across various industries, numerous types of attacks have emerged. This section provides an analysis of the vulnerabilities, robustness, and security of the proposed solution, detailing how it remains resilient against different types of attacks.

### *5.1 VULNERABILITY AND ROBUSTNESS*

Smart contracts are fundamental components of blockchain technology. The solution proposed in this paper utilizes multiple smart contracts for transactional activities. A smart contract is executable code that facilitates digital transactions while ensuring authenticity, credibility, and immutability. Once deployed on the blockchain, a smart contract cannot be modified and must be executed as written. If the code of a smart contract is vulnerable, it can significantly compromise the security of the blockchain.

As smart contracts are still evolving, they have some security gaps. During Ethereum's initial development, the Decentralized Autonomous Organization (DAO) hack was a major incident, resulting in the loss of 3.6 million ethers, equivalent to $70 million. The DAO was responsible for decentralized financial transactions via smart contracts. Other vulnerabilities in smart contracts, such as reentrancy bugs, time dependency, concurrency bugs, and call stack attacks, have also been identified. These vulnerabilities can cause significant losses to blockchain-based systems. The most well-known vulnerabilities are described as follows:

- **Call Stack Attack:** Also known as the call depth attack, this occurs when the call depth reaches 1024 frames, causing the calling function to fail. If a call or send function is used to call another contract, the call depth increases by one. If a call function recursively calls itself 1023 times, reaching the call stack limit of 1024, the next instruction fails.
- **Time Dependency Attack:** This miner-centric attack involves a miner manipulating the timestamp conditions to their advantage. When mining a transaction, the miner sets the transaction's timestamp, typically based on the miner’s physical machine time.
- **Concurrency Bug:** This miner-side issue falls under the category of transaction ordering dependency. It arises when two functions are executed simultaneously, often occurring when a data structure or database is being updated.

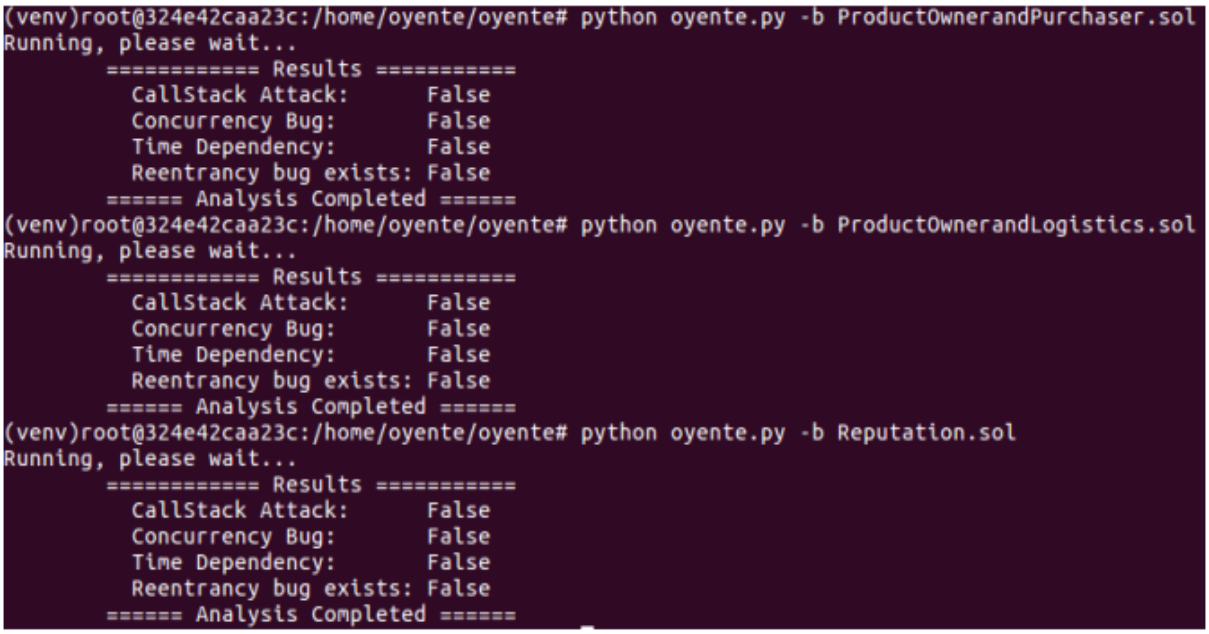
- **Reentrancy Vulnerability:** This well-known vulnerability, exemplified by the DAO attack, exploits path conditions to check for reentrancy conditions. In Ethereum, when a contract calls another contract, the current transaction waits for the call to finish. This can lead to situations where a transaction uses the intermediate state of the caller.

Therefore, it is crucial to analyze smart contract codes to ensure the system is robust against the aforementioned attacks. Oyente, an open-source security analyzer for Ethereum smart contracts. It analyzes smart contracts based on symbolic execution paths, where each path has a specific condition. The main responsibilities of Oyente are as follows:

- Exploring all possible execution paths using dummy values for variables
- Recording the contract's behavior in each path
- Summarizing the conditions for each path
- Checking for any property violations

According to an analysis, oyente flagged 8,833 out of 19,366 smart contracts as vulnerable, including the DAO smart contract. We tested our smart contracts with oyente for any security and vulnerability issues. Figure 6 clearly shows that all our contracts are robust against the mentioned vulnerability attacks, and all reported issues are false positives.


(a)




(b)

**Figure 6: Vulnerability analysis of smart contracts.**

### *5.2 MANAGERIAL IMPLICATIONS*

Our proposed blockchain-enabled Agri-Food supply chain system is designed to significantly improve the traceability of agricultural and food products. We have taken careful consideration of various factors essential for ensuring the security and efficiency of the supply chain. These aspects are thoroughly discussed in the subsequent sections.

**1. Accountability:** Our system achieves full decentralization by utilizing blockchain technology, which guarantees accountability through thorough log analysis. We enable arbitrators to participate in the system, giving them the authority to review logs in case of disputes. Regulators are provided access to blockchain data, allowing them to obtain necessary information for accountability. Additionally, implementing standard signature schemes protects nodes from malicious actions, reducing the possibility of denying responsibility.

**2. Credibility:** The credibility of our system hinges on the trust level established among its participants. To maintain this trust, our solution integrates a reputation system, ensuring reliability among entities like product owners, purchasers, and LCs (Letter of Credit). By harnessing the inherent features of blockchain technology, our solution is both credible and secure. It's important to note that the system remains resilient against hacking attempts, as compromising it would require control of over 51% of all nodes.

**3. Auditability:** The auditability of our entire system extends to all legitimate users, offering traceable smart contracts for monitoring transactions and events. blockchain technology provides transparency, immutability, and traceability advantages, guaranteeing the integrity of transactions. This ensures that all transactions are resistant to tampering.

**4. Autonomy:** The autonomy is a central feature of our solution, where all transactions and data exchanges take place through smart contracts. This setup safeguards against external interference, fostering autonomy and security within a trusted environment. Furthermore, the consensus-based verification of blocks is recognized as an autonomous aspect of blockchain-based solutions.

**5. Authenticity:** The authenticity is paramount within our solution, where all entities undergo thorough authentication before participating in transactions. This robust authentication process guarantees that only authorized entities can perform specific functions within the system, effectively thwarting potential man-in-the-middle attacks.

## VI. CONCLUSION

The integration of blockchain technology has brought substantial advantages to the supply chain industry, fostering decentralization and establishing a trustless environment for all operations. Nevertheless, even with blockchain's inherent trustless characteristics, instilling trust between sellers and buyers presents an ongoing challenge. Instances of malicious behavior by entities can lead to doubts regarding their credibility among buyers. Furthermore, the decentralized execution of supply chain processes is imperative to guarantee traceability, accountability, and security.

This paper introduces a comprehensive end-to-end solution tailored for blockchain-based Agri-Food supply chains. It delves into intricate details regarding traceability, trading, delivery, and reputation aspects. A meticulous evaluation of smart contract performance is conducted to ascertain both efficiency and robustness. The inclusion of a reputation system is proposed to safeguard the credibility of Agri-Food supply chain entities and uphold product quality ratings. Moreover, this system guarantees the immutability and integrity of transactions, meticulously recorded on the blockchain. The paper further presents algorithms and offers an in-depth discussion on smart contracts. Through simulations, our system's gas requirements for deploying and executing smart contracts are meticulously analyzed.

Despite the advancements made, blockchain-based systems continue to encounter obstacles in practical applications. Our future objectives include incorporating refund and return mechanisms into Agri-Food product trading. Additionally, the reputation system will store reviews from end consumers, but these reviews can sometimes be biased or fraudulent. To address this, we plan to implement a fake review detection system to help the reputation system identify and filter out false reviews. Moreover, we will conduct security analyses to focus on potential attacks against the reputation system.

## REFERENCES


[1]. M. Tripoli and J. Schmidhuber, ‘‘Emerging opportunities for the applica- tion of blockchain in the agri-food industry,’’ FAO and ICTSD, Rome, Italy, Tech. Rep. CC BY-NC-SA 3, 2018.

[2]. K. Malhotra, L. P. Ritzman, and S. K. Srivastava, Operations Management: Processes and Supply Chain. London, U.K.: Pearson, 2019.

[3]. J. F. Galvez, J. C. Mejuto, and J. Simal-Gandara, ‘‘Future challenges on the use of blockchain for food traceability analysis,’’ TrAC Trends Anal. Chem., vol. 107, pp. 222–232, Oct. 2018.

[4]. A. M. Turri, R. J. Smith, and S. W. Kopp, ‘‘Privacy and RFID technol- ogy: A review of regulatory efforts,’’ J. Consum. Affairs, vol. 51, no. 2,pp. 329–354, Jul. 2017.

[5]. A. Schaub, R. Bazin, O. Hasan, and L. Brunie, ‘‘A trustless privacy- preserving reputation system,’’ in Proc. IFIP Int. Conf. ICT Syst. Secur. Privacy Protection. Cham, Switzerland: Springer, 2016, pp. 398–411.

[6]. D. K. C. Lee, Ed., Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data. New York, NY, USA: Academic, 2015.

[7]. M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, P. McCallum, and A. Peacock, ‘‘Blockchain technology in the energy sec- tor: A systematic review of challenges and opportunities,’’ Renew. Sustain. Energy Rev., vol. 100, pp. 143–174, Feb. 2019.

[8]. A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, ‘‘On blockchain and its integration with IoT. Challenges and opportunities,’’ Future Gener. Comput. Syst., vol. 88, pp. 173–190, Nov. 2018.

[9]. K. Salah, N. Nizamuddin, R. Jayaraman, and M. Omar, ‘‘Blockchain-based soybean traceability in agricultural supply chain,’’ IEEE Access, vol. 7,pp. 73295–73305, 2019.

[10]. J. Hao, Y. Sun, and H. Luo, ‘‘A safe and efficient storage scheme based on blockchain and IPFS for agricultural products tracking,’’ J. Comput., vol. 29, no. 6, pp. 158–167, 2018.

[11]. S. Wang, X. Tang, Y. Zhang, and J. Chen, ‘‘Auditable protocols for fair payment and physical asset delivery based on smart contracts,’’ IEEE Access, vol. 7, pp. 109439–109453, 2019.

[12]. A. Shahid, U. Sarfraz, M. W. Malik, M. S. Iftikhar, A. Jamal, and N. Javaid, ‘‘Blockchain-based reputation system in agri-food supply chain,’’ in Proc. 34th Int. Conf. Adv. Inf. Netw. Appl. (AINA). Caserta, Italy: Univ. Campania Luigi Vanvitelli, Apr. 2020,

[13]. M. P. Caro, M. S. Ali, M. Vecchio, and R. Giaffreda, ‘‘Blockchain- based traceability in agri-food supply chain management: A practical implementation,’’ in Proc. IoT Vertical Topical Summit Agricult.-Tuscany (IOT Tuscany), May 2018, pp. 1–4.

[14]. F. Tian, ‘‘A supply chain traceability system for food safety based on HACCP, blockchain & Internet of Things,’’ in Proc. Int. Conf. Service Syst. Service Manage., 2017, pp. 1–6.

[15]. Z. Li, H. Wu, B. King, Z. B. Miled, J. Wassick, and J. Tazelaar, ‘‘A hybrid blockchain ledger for supply chain visibility,’’ in Proc. 17th Int. Symp. Parallel Distrib. Comput. (ISPDC), Jun. 2018, pp. 118–125.

[16]. M. Nakasumi, ‘‘Information sharing for supply chain management based on block chain technology,’’ in Proc. IEEE 19th Conf. Bus. Informat. (CBI), vol. 1, Jul. 2017, pp. 140–149.

[17]. Q. Lu and X. Xu, ‘‘Adaptable blockchain-based systems: A case study for product traceability,’’ IEEE Softw., vol. 34, no. 6, pp. 21–27, Nov. 2017.

[18]. D. Tse, B. Zhang, Y. Yang, C. Cheng, and H. Mu, ‘‘Blockchain application in food supply information security,’’ in Proc. IEEE Int. Conf. Ind. Eng. Eng. Manage. (IEEM), Dec. 2017, pp. 1357–1361.

[19]. Y.-P. Lin, J. Petway, J. Anthony, H. Mukhtar, S.-W. Liao, C.-F. Chou, and Y.-F. Ho, ‘‘Blockchain: The evolutionary next step for ICT E-agriculture,’’ Environments, vol. 4, no. 3, p. 50, 2017.

[20]. R. AlTawy, M. El Sheikh, A. M. Youssef, and G. Gong, ‘‘Lelantos: A blockchain-based anonymous physical delivery system,’’ in Proc. 15th Annu. Conf. Privacy, Secur. Trust (PST), Aug. 2017, pp. 15–1509.

[21]. K. Toyoda, P. T. Mathiopoulos, I. Sasase, and T. Ohtsuki, ‘‘A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain,’’ IEEE Access, vol. 5, pp. 17465–17477, 2017.

[22]. H. R. Hasan and K. Salah, ‘‘Blockchain-based proof of delivery of phys- ical assets with single and multiple transporters,’’ IEEE Access, vol. 6, pp. 46781–46793, 2018.