

Blockchain-Powered Traceability and Security Platform for Agriculture

Kajal Jain¹, Sanjeev Rana²

¹Kajal Jain, Maharishi Markandeshwar (Deemed to be) University, India

²Sanjeev Rana, Maharishi Markandeshwar (Deemed to be) University, India

Abstract

Ensuring the safety and quality of essential agricultural commodities such as wheat, rice, and maize within government-operated supply chains has become increasingly critical due to persistent issues of contamination and safety breaches. Existing traceability processes covering the journey from government funding through raw material procurement to final consumer delivery remain insecure, costly, and complex, while lacking scalability for large-scale agri-food distribution. Additionally, consumers are often without adequate tools to assess product quality or detect contamination, limiting their ability to determine food safety. Blockchain technology presents a transformative approach to enhancing transparency, security, and traceability in both governmental and non-governmental agricultural supply chains. This study proposes a blockchain-based model employing smart contracts to track and record all transactions and interactions in the government corn supply chain. The system ensures real-time availability of trustworthy product information, promoting informed decision-making across stakeholders. Transaction records are stored on a public, tamper-proof ledger, guaranteeing operational transparency. The proposed BSIGSN framework enables secure, efficient, and immutable monitoring of corn products, supporting improved safety and quality assurance. Performance evaluations demonstrate that the framework achieves notable cost efficiency, scalability, and security, with reduced computational overhead compared to conventional supply chain systems.

Keywords: *Blockchain, agricultural supply chain, traceability, food safety, transparency, smart contracts, e-government, immutable ledger*

INTRODUCTION

Protecting public health in agriculture relies on closely monitoring production processes and making sure supply chain logistics stay efficient and secure. Growing concerns about food quality and contamination have led to renewed efforts to improve the security and traceability of agricultural supply chains [1]. For agricultural goods traded internationally, it is crucial to have reliable tracking systems and verified national certifications. Achieving traceability requires precise source identification and effective data exchange throughout the supply chain to collect, share, and manage essential information. However, dealing with the vast and complex data generated, processed, and transferred by many intermediaries poses a major challenge. Food contamination incidents and their public health consequences show how important traceability is for ensuring food safety [2]. To improve traceability in agriculture, experts recommend using technologies like barcodes and RFID systems. Still, most existing traceability systems depend on centralized data management, which makes them vulnerable to manipulation and administrative errors. In cases of contamination, quickly removing unsafe products from the market depends on strong coordination among multiple stakeholders. Although some parts of the supply chain may already be traceable, sharing information across all stages often remains slow and complicated. As a result, many researchers have looked into alternative ways to achieve efficient and secure traceability of resources [14]. One promising solution is blockchain technology, a decentralized ledger system that prevents unauthorized data changes. In blockchain, information is stored in blocks, each containing a unique cryptographic hash, transaction data, and the hash of the previous block, except for the first one, known as the genesis block [23]. The hash works like a digital fingerprint for each block, and changing a block alters its hash, protecting data integrity. The connection of blocks through these hashes creates a highly secure structure. This study examines the Ethereum blockchain, which can operate in both public and private modes, unlike many blockchains that are mainly public. Ethereum also allows the use of smart contracts, which rely on "gas," a token-based fee paid to miners for validating transactions. Every transaction or smart contract needs enough gas to execute successfully; otherwise, it may not go through. To maintain blockchain security, new blocks are added only after the network reaches consensus, preventing unauthorized tampering. Of the various consensus methods, this work uses Proof of Authority

(PoA)[16]. The growing significance of blockchain comes from its ability to build trust among stakeholders by allowing transparent, unchangeable transactions within the supply chain. As a secure, verifiable, and tamper-proof technology, it has great potential for managing complex government agricultural and food supply chains that involve various participants like farmers, processors, industries, consumers, and other intermediaries.

LITERATURE REVIEW

This research aims to create a technological framework that can be effectively used in the government sector and remain accessible throughout the food supply chain. This will promote operational continuity and consistency. Previous studies have introduced agricultural supply chain frameworks that use Information and Communication Technology (ICT). These tools help farmers make better decisions by providing them with crucial, timely information. Farmers who use such systems, especially those involved in various farming activities, are generally better informed than those who do not. These systems benefit from the growing use of personal computers and the decreasing costs of digital communication tools. Emerging technologies like RFID and blockchain, when combined with other solutions, improve traceability and build trust in the agri-food supply chain. They support the collection and real-time sharing of agricultural product data, ensuring food safety through secure storage, exchange, and monitoring of information. However, these frameworks can face challenges, including system fragmentation and dependence on centralized control, which make them vulnerable to potential data manipulation. Blockchain's decentralized structure fits well with distributed economic networks, providing a transparent infrastructure for supply chains. It is often seen as a transformative tool for improving traceability in farm products [27][17]. Various public and private blockchain models have been proposed to enhance transparency and security in agricultural supply chains [29]. While blockchain has clear benefits, implementing it in double-chain architectures can sometimes be inefficient, even though it may be cost-effective. Recent research has expanded blockchain applications to food industry supply chains and credit evaluation systems. This provides consumers with important information and serves as useful tools for government agencies and food safety regulators. Several studies have suggested big data and blockchain-based solutions to simplify and standardize supply chain operations. For instance, researchers have outlined strategies to normalize supply chain processes using these technologies. Blockchain is increasingly viewed as one of the most promising modern technologies, with the potential to drive the next major technological revolution. Many businesses are now actively looking into adopting blockchain to modernize traditional food systems by creating distributed, tamper-proof records. In 2017, IBM partnered with major global food companies like Nestlé and Walmart to integrate blockchain into the food supply chain [11]. In China, JD.com collaborated with Tsinghua University to trace food products using blockchain technology. Their goal is to enhance food safety and improve business operations through secure global networks. While these solutions have been effective for increasing traceability and transparency, they often do not address the monitoring and allocation of government funds within the food supply chain. Currently, there is heightened global interest in traceability across the entire food production process. In the case of corn products, research has shown that tracking and traceability are especially crucial, and consumer opinions on usability should also be taken into account [4]. A new solution based on the Ethereum blockchain and smart contracts has been proposed [9]. This would allow business operations in the corn supply chain to occur without relying on central authorities or external intermediaries, thus improving the accuracy, security, and reliability of stored data. Table 1 shows related work in the agricultural domain for products such as rice, wheat, and soybeans [19].

Table 1: Related work in the field of agricultural field

REFERENCE	OBJECTIVE	TECHNIQUE USED	LIMITATIONS
[7], [21]	To achieve transparency and traceability	Double-chain blockchain concept is used	Cost-effective, inefficient, double spending
[25], [28]	To achieve transparency and traceability.	Blockchain Technology is used	Cost-effective and inefficient

[5], [15]	To achieve transparency and traceability	ICT gadget is used	Central point of failure, involvement of central controller, and cost-effective
[10],[31]	To achieve traceability and reliable information	Technique of RFID and blockchain	It is susceptible to system fragmentation and central administration
[2],[8],[20]	To analyse farmers' decision-making in supply chain.	ICT gadget is used	Central point of failure, involvement of central controller, cost-effective and scalability issues
[3], [6]	To achieve transparency and traceability	Blockchain	Cost-effective and inefficient

2.1. Problem Statement

This study shows how Ethereum blockchain technology, along with smart contracts, can be used to monitor and manage government-run agricultural supply chains. The work presents an accountability framework specifically for corn supply chains, based on the Ethereum blockchain platform. Figure 1 illustrates the flow of commodities in the corn supply chain, highlighting the key stakeholders and their roles. The main contributions of this research include:

1. Developing a framework that uses Ethereum smart contracts to improve traceability and transparency in government-regulated corn supply chains.
2. Extending the framework to outline the key features of the proposed blockchain solution, focusing on improving communication among the various stakeholders in the supply chain.
3. Presenting and evaluating a smart contract algorithm that ensures proper interactions and the appropriate use of government-allocated funds by relevant entities in the corn supply chain.

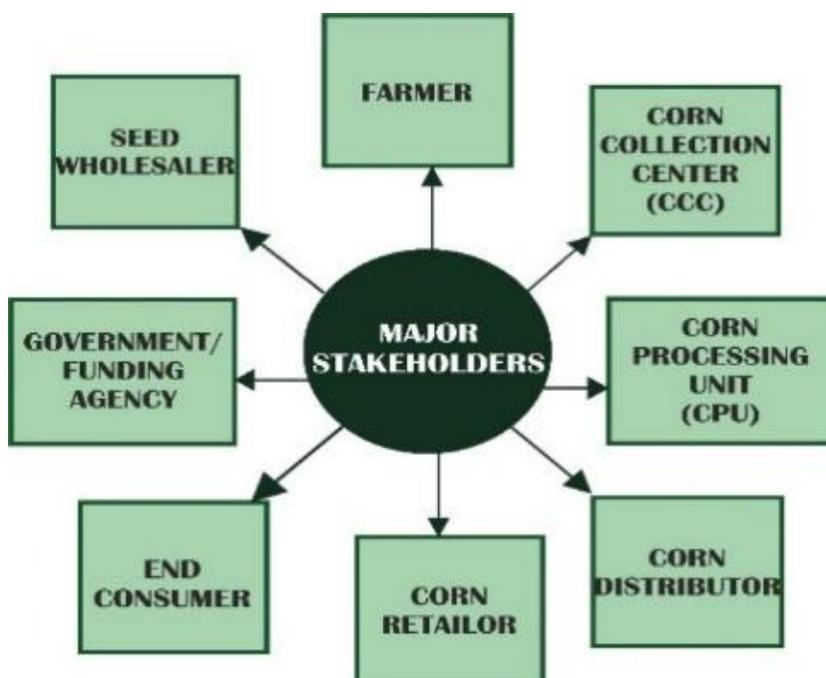


Figure 1: Major stakeholders involved in Corn Supply chain Management

RESEARCH METHODOLOGY

The Blockchain enabled Secure and Immutable Grain Chain (BSIGSN) model runs on a dedicated Ethereum blockchain network. Its nodes, spread across both private and public networks, validate transactions before they are added to the blockchain ledger. The model uses the Proof of Authority (PoA) consensus mechanism for executing smart contracts [26]. Like earlier supply chain management systems

that used PoA, any authorized organization that can collect, verify, and process transactions can operate as a mining node. These nodes work together to maintain a shared ledger with transaction data and results, which is accessible to all participating miners. Smart contracts in this framework handle transactions through specific function calls and event triggers. This setup enables stakeholders to monitor, trace, and receive timely updates when necessary. For example, information about corn products is recorded on the blockchain, with each entry linked to the product's expiry date. When a product expires, the relevant data is removed to make room for new transactions. This method improves transparency and traceability in the corn supply chain, ensuring consumer safety and allowing quick resolution of disruptions. Furthermore, the framework lets customers submit reviews of the products they buy. The public ledger is designed to store information selectively based on stakeholder roles, which helps reduce redundancy. [30] Figure 2 shows how the BSIGSN model works. The process involves eight main stakeholders; all connected through smart contracts.

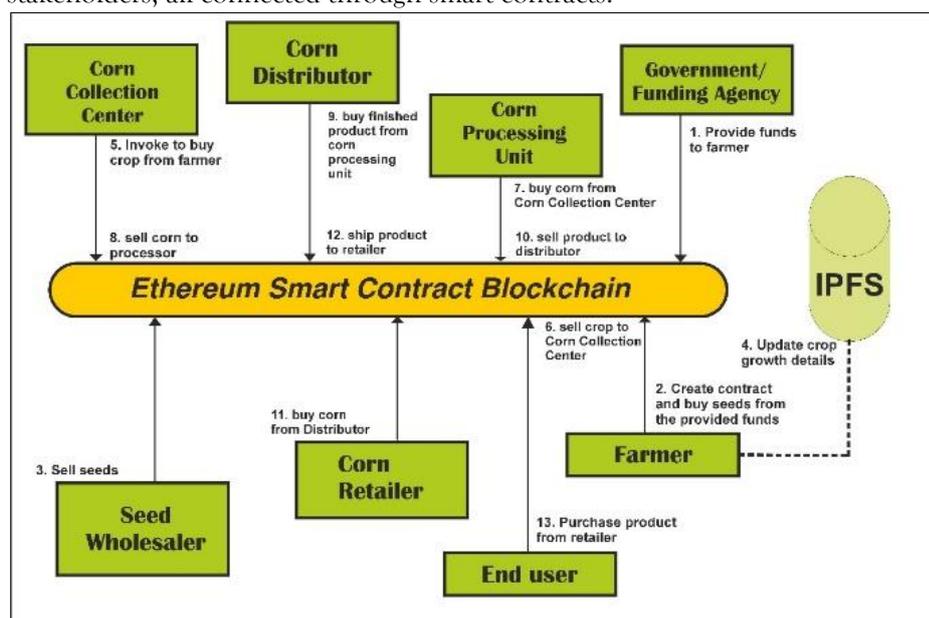


Figure 2: BSIGSN Model for Corn Supply chain Management

(1) The government is responsible for providing financial support to farmers. (2) Seed Wholesaler (SW): This entity supplies various corn seed varieties to a broad customer base while meeting international quality standards. Each seed product has a unique serialized Global Trade Item Number (GTIN) for identification. (3) Farmer: Purchases seeds from the SW and grows crops using resources from the government or funding agency and blockchain-based smart contracts[22]. These contracts track progress through unique seed identifiers. (4) Agricultural Producers: Update and maintain crop-related information in a distributed, tamper-resistant log on the InterPlanetary File System (IPFS)[12]. The cryptographic hash of this record is kept on the blockchain for verification. Producers also record corn yield output, along with details like quantity, quality, weight, and variety. They monitor environmental storage conditions, including temperature, humidity, and storage duration during the storage phase. (5) Corn Processing Unit (CPU): Buys corn from collection centers, processes it, and sells the products to distributors. (6) Corn Distributor (CD): Acquires processed corn products from the CPU and distributes them to retailers or directly to consumers. (7) Corn Retailer (CR): Obtains products from the CD, identified by Serialized Trade Identifiers (STI), and sells them in smaller amounts to end consumers. (8) End Consumer: Buys the final corn products from the CR for personal use. All products are labeled with both STI and GTIN codes for traceability. In this framework, every participant must be registered, authenticated, and have a distinct Ethereum account (EA) with a public-private key pair for signing and verifying transactions. This account uniquely identifies each stakeholder in the blockchain network. The traceability feature ensures that all transaction data remains unchanged and can be verified without depending on a centralized authority. This capability, applied across the entire supply chain, allows for precise tracking of the total corn volume produced and traded among verified entities[18]. Once recorded under agreed conditions, trade quantities remain unchanged. Grain varieties that meet different quality

classifications are not mixed for distribution, and the volume of each quality category is logged carefully. Moreover, farmers can upload electronic documents, such as crop images and land condition reports via IPFS, creating a trusted digital repository for validation. Shipment integrity can also be ensured using sensor-equipped containers, such as cameras, GPS, and 4G connectivity, which provide continuous updates on transport conditions. All stakeholders can access this data permanently through the blockchain. Standardized identifiers can also be used to validate product location data, while GPS-enabled shipping or storage containers allow for geotagging the locations of both products and key participants in the supply chain.

3.1. BSIGSN Framework for Agri-Security for Corn Supply Management Using Blockchain

This section explains how the BSIGSN framework operates to manage the government-regulated corn supply chain. The process starts with creating and deploying a smart contract. Each stakeholder registers their Ethereum Account (EA) within the contract framework. When a farmer requests financial help from the government or funding agencies, the system changes the farmer's status to "FundRequested." After the government transfers the allocated funds, the Government Agency (GA) status updates to "FundTransferred." The farmer then makes a seed procurement request from the designated Seed Wholesaler (SW). This prompts the system to update the farmer's status to "SupplyRequested," as outlined in Algorithm 1. The smart contract authenticates the farmer's identity and checks proof of payment. If both checks pass, the contract updates its internal state. It changes the farmer's status to "ServiceWait" and the SW's status to "SalesApproved." At this point, the smart contract sends progress notifications to all relevant parties in the network. If any eligibility requirements or transaction conditions are not met, the system automatically reverts all involved statuses to their original values and cancels the transaction.

Algorithm 1: Funds receiving by Farmer and Buying seeds from Seed Wholesaler (SW).

```

Rf is a set of all registered farmers
Ethereum Authorization (EA) of the government authority
transferring the funds to the farmer is known
Ethereum Authorization (EA) of farmer is known
Ethereum Authorization (EA) of Seed Wholesaler is known
CQuantity, CStype, CSBrand, CSPrice
1   ContractState Created
2   Farmer Status: FundsRequested through Government Program
3   GA Status: FundsTransferred
4   Farmer's Status: SupplyRequested
5   SW Status: Read
6   Consider only farmer is from Rf i.e. registered farmers
7   If farmer ¼ registered and CSPrice ¼ paid Then
8   Contract status! RequestOnProcess
9   Farmer status! ServiceWait
10  SW status! SalesApproved
11  Broadcast a notification message for the seeds sales
12  End
13  Else
14  Return to initial contract state and show an error
15  End
  
```

Algorithm 2: Selling of corn seeds from CCC to CPU

```

PCPU is the set of all registered CPU
EA of CPU is known
EA of CCC is known
CQuantity, CDatePurchased, CPPrice
1   ContractState: CornFromCPU
2   CCC Status: CornRequested
3   CPU Status: YieldFromFarmer
4   Consider only CPU is registered PCPU i.e.
registered CPUs
5   If Comsale ¼ Accepted and CPPrice ¼ paid Then
6   Contract status ! RequestApproved
7   CPU status ! WaitForCorn
8   CCC status ! CornReleaseSuccessful
9   Broadcast a notification message for the Corn sales
10  End
11  Else
12  Contract status ! RequestDenied
13  CPU status ! RequestNotSuccessful
14  CCC status ! CornReleaseFailed
15  Broadcast a notification message for the Corn sales
failure
16  end
17  else
18  Return to initial contract state and show an error
19  End
  
```

The third stage of the framework, outlined in Algorithm 3, focuses on managing transactions between Corn Distributors (CD) and Corn Retailers (CR) using the smart contract system. At this stage, the contract ensures that only verified and registered CRs can buy products. It checks if the sale agreement has been approved and if the payment has been completed successfully. If these checks pass, the smart contract allows the transaction, and the CD transfers the product to the CR. Once completed, the contract status updates to ProductBuyingSuccessful, while the statuses for the CD and CR change to ProductSoldToCR and ProductDeliverySuccessful, respectively. A notification of the successful transaction is sent to all active participants in the network, confirming the sale. On the other hand, if any conditions fail, the smart contract status changes to ProductBuyingDenied, and the CD and CR statuses update to ProductRequestFailed and ProductDeliveryFailed, respectively. In this case, a failure alert goes out to all participants, indicating that the product sale and delivery did not happen.

Algorithm 3: -Selling product to Corn Retailer (CR)

```

Input: RCR is the set of all registered CR
EA of CD is known
EA of CR is known
CQuantitySold, CDatePurchased, CDateProduced, CProductPayment
1 ContractState: CDSales
2 CD Status: CPProductReceived
3 CR Status: PreparedToBuy
4 Consider only CR is in RCR i.e. registered CRs
5 If Productsale ¼ Accepted and ProductPayment ¼ paid Then
6 Contract status ! ProductBuyingSuccessful
7 CD status ! ProductSoldToRCR
8 CR status ! ProductDeliverySuccessful
9 Broadcast a notification message for the corn product sales
10 End
11 Else
12 Contract status ! ProductBuyinDenied
13 CD status ! ProductRequestFailed
14 CR status ! ProductDeliveryFailed
15 Broadcast a notification message for the Corn product sales failure
16 end
17 else
18 Return to initial contract state and show an error
19 End
  
```

At this final stage of the framework, the end consumer—who represents the last entity in the supply chain—purchases the finished corn product from the Corn Retailer (CR). The detailed process flow governing this transaction is outlined in *Algorithm 4*.

Algorithm 4: -Selling Corn products to consumers.

```

Input: RCR is the set of all registered CR
EA of CR is known
EA of Consumer is known
CQuantitySold, CDatePurchased, CSalesID and
CProductID, CProductPayment
1 ContractState: SaleRequestApproved
2 CR Status: ProductDeliverySuccessful
3 Consumer Status: ReadyToPurchase
4 Consider only CR is registered RCR i.e. registered CRs
5 If CR to RCR and ProductPayment ¼ paid
Then
6 Contract status ! SoldToConsumer
7 CR status ! SalesSuccessful
8 Consumer status ! PurchaseSuccessful
9 Broadcast a notification message for the corn product
sales
10 end
Else
11 Contract status! SaleRequestDenied
12 CR status! SalesFailure
13 Consumer status! PurchaseFailed
14 Broadcast a notification message for the product
sales failure
15 Return to initial contract state and show an error
16 end
  
```

In this final purchase stage, three key variables are tracked: Date of Purchase, Sales Identification Number, and Product Identification Number. The process starts when the consumer's status is set to "Ready to Buy," the smart contract status is "Sale Request Accepted," and the Corn Retailer (CR) status is "Product Delivery Successful." Two main conditions must be met for the transaction to proceed: 1. The consumer can only purchase products officially listed by the CR. 2. The required payment must be successfully completed. If both conditions are met, the smart contract updates its state to "Sold to Consumer," the CR's status changes to "Sales Successful," and the consumer's status becomes "Purchase Successful." A success notification is sent to all relevant participants, confirming the sale to the consumer. If any condition fails, the smart contract state changes to "Sale Request Denied," the CR's status is updated to "Sales Failure," and the consumer's status is set to "Purchase Failed." In these cases, all participants receive a warning message indicating that the transaction was unsuccessful.

3.2. Implementation, Results, and Analysis

This section begins with the experimental setup and deployment followed by results and analysis subsections to measure the logic and performance of the BSIGSN framework

3.2.1. Experimental setup and deployment

The experiment to validate the proposed blockchain model used a divide-and-conquer strategy to test its effectiveness thoroughly. Implementation took place on Remix IDE with the Solidity programming language. MetaMask, a Chrome extension for Ethereum wallets, facilitated easier interaction with Ethereum networks. Remix IDE offered tools to test and debug smart contracts before deployment. For realistic blockchain simulation, the team used the Sepolia testnet, which runs on a Proof of Authority consensus algorithm. Access to all Ethereum nodes in this test environment was provided through Infura, a gateway service. To simplify testing and allow switching between different Ethereum test nets, the team integrated the Truffle Framework into the process. During validation, the team tested smart contract functions and modifiers to ensure that only authenticated Ethereum addresses could perform certain actions. This preserved security and role-based access. The team carefully reviewed transaction logs to confirm that information was transmitted correctly and that data accuracy was maintained throughout the testing phase. This thorough approach ensured a solid assessment of the model's functionality and secure operation within a simulated blockchain network.

3.2.2. RESULTS AND ANALYSIS

This section looks at whether the BSIGSN framework is practical by examining its security features and cost impacts to see if it's suitable for real-world use. It starts with a thorough discussion of the security aspects related to smart contracts, pointing out possible vulnerabilities and the measures in BSIGSN to lessen risks. This includes important factors like ensuring transaction authenticity, preventing unauthorized access, protecting data integrity, and keeping records on the blockchain unchanged. After the security review, the section discusses possible challenges and areas for future research that could improve the framework's strength and effectiveness. These areas include making the system more scalable, integrating new technologies, and optimizing consensus processes [24]. Next, the BSIGSN framework is compared to current agricultural supply chain solutions. The focus is on how it improves traceability, transparency, decentralization, and automation through the use of Ethereum smart contracts and blockchain technology. This comparison shows how BSIGSN provides real benefits over traditional centralized systems, especially in cutting down fraud and boosting trust among stakeholders. Finally, the section discusses the wider significance and applicability of this research, highlighting its potential impact not only on government-managed corn supply chains but also on other agricultural products and supply chain contexts. The discussion explains how the secure, cost-effective design and efficient operation of the BSIGSN framework make it a strong candidate for improving agricultural supply chain management worldwide.

3.2.3. Security analysis

1. Privacy

Privacy ensures that communication between two parties stays confidential and is not accessible to unauthorized third parties. To maintain this in our solution, we manage message encryption and decryption through an SSL session. This session is established only after a trusted handshake, which confirms the identities of the participating parties. Traditional centralized Public Key Infrastructure (PKI) models often lack transparency and rely heavily on Certificate Authorities (CAs) to distribute

cryptographic keys. This reliance can introduce vulnerabilities and dependencies. In contrast, using the Ethereum blockchain eliminates the need for a standard PKI system. Each participant gets a unique Ethereum Address, which contains asymmetric public key pairs used to encrypt messages exchanged over the SSL session. This decentralized method improves transparency and security since the blockchain naturally supports public key distribution without depending on central authorities. This setup offers stronger privacy guarantees for communication within the system.

2. Credibility

All communications on the Ethereum network between users are encrypted and resistant to tampering because of the blockchain's cryptographic foundations. Each transaction and message is signed securely with private keys linked to Ethereum Addresses (EAs). This process ensures authenticity and stops unauthorized changes. The blockchain also records exact timestamps and specific details tied to these EAs for every interaction. This unchangeable and time-stamped record of activities ensures the integrity of interactions among different entities in the network. Together, these features provide strong protection against common cyber threats like Man-in-the-Middle (MITM) attacks and replay attacks. Encryption and digital signatures prevent attackers from intercepting or altering communications without detection. Timestamps and unique EA details stop attackers from successfully reusing or duplicating real transactions. As a result, the system keeps a secure and trustworthy environment for communication and transactions on the Ethereum blockchain.

3. Authorization

Only authorized stakeholders get full access to all functions in the smart contract. If the system finds that a legitimate caller has been compromised or is involved in fraud, it triggers an error that restores all states to their previous condition and cancels the transaction. Additionally, any further interactions between stakeholders only start after they complete an authentication handshake. This handshake sets up a secure SSL channel for communication.

4. Non-repudiation

All transactions and events are carefully recorded in Ethereum's public ledger. This means that every call is securely logged and cannot be changed by the person who made it. This permanent record stops anyone from denying their actions because all activity is stored forever on the blockchain. Additionally, if someone tries to impersonate a stakeholder's Ethereum Address (EA), the system will catch the attempt. The attacker will not have the private key needed to create a valid digital signature for the message.

3.3.4. Cost Analysis

Every transaction on the Ethereum blockchain requires a fee called "gas," which is paid in Ether (ETH). This fee covers the computational resources needed to execute operations. The amount of gas used depends on the complexity of the smart contract code. Factors include loops, arrays, mappings, variable storage, and data types. When gas prices are higher, measured in Gwei (where 1 Gwei = 10^9 ETH), miners prioritize those transactions, which affects how quickly they are processed. Tools like ETH Gas Station help developers and users see transaction speeds relative to current gas prices. To avoid high costs, developers need to optimize their smart contracts by reducing inefficient code, especially costly loops and storage usage. One common strategy is to use the blockchain's immutable log and event system to record important data instead of storing large datasets on-chain. This approach helps save gas. Since gas prices can change due to network congestion, the time of day, and other factors, actual transaction costs can vary widely. Sometimes, they can become quite high during peak demand. Therefore, it is essential to monitor gas prices and design contracts with cost efficiency in mind for economical and effective smart contract deployment and operation on Ethereum.

3.2.5. Smart contract vulnerability analysis

The smart contracts in the BSIGSN framework were checked using the Slither Security Analysis Tool. This tool examines Ethereum Virtual Machine (EVM) bytecode and creates a detailed map of contract interactions. The analysis, summarized in Table 2, showed that the contracts are secure and free from vulnerabilities. Specifically, no unchecked exceptions were found that could lead to integer underflow or overflow errors. All execution tests were done with enough gas, which greatly lowered the chances of reentrancy attacks. The review also confirmed that there were no problems related to timestamp dependency or risks from interdependent transactions. Overall, the results indicate that the BSIGSN smart contracts work reliably and securely, with no major security issues.

Table 2: Vulnerability analysis report

PARAMETERS	VULNERABILITY IN EXISTING MODEL [2]	VULNERABILITY IN BSIGC MODEL
EVM Code Coverage	High	Low
Integer Underflow	Moderate	Low
Integer Overflow	Low	Moderate
Call stack Depth Attack Vulnerability	Moderate	Low
Transaction Ordering Dependence	Moderate	Low
Time Stamp Dependency	Low	Moderate

3.3. A Comparison of The BSIGSN Framework with Existing Agricultural Food Supply Chain Solutions

Table 3 compares the framework proposed in this paper with existing approaches from other researchers. In terms of ensuring data integrity, controlled information access, transparency, and traceability in the corn supply chain, conventional methods usually use smart contracts along with consensus mechanisms to tackle traceability problems. The authors also assess how practical their solutions are for real-world use, noting that they need few technical resources. For example, the study explores how to integrate Ethereum-based smart contracts with the Interplanetary File System (IPFS) for data storage. It uses several smart contracts to represent each entity in the supply chain. While this method is effective, it adds more computational demands compared to the framework proposed in this paper. Because of its public, permissionless nature, the Ethereum platform is one of the most commonly used blockchain solutions, letting any stakeholder join the network. Its main benefits are a large developer community, a well-developed ecosystem of decentralized applications (dApps), and its native cryptocurrency, Ether (ETH). However, Ethereum still faces significant issues, especially in scalability and high transaction costs, often called gas fees. Figure 3 provides a comparative analysis of different blockchain platforms.

Table 3: A Comparison of the BSIGSN framework with existing works

FEATURES	EXISTING MODEL [2]	BSIGC MODEL
Satisfaction feedback	No	Yes
Cost Analysis	No	Yes
Implementation and Testing	No	Yes
Security analysis	No	Yes
Vulnerability analysis	No	Yes
Low computational cost	No	Yes

DISCUSSION AND CONCLUSION

In response to the increasing need for secure and efficient solutions in agriculture and supply chain sectors, we developed and tested the BSIGSN framework on the Ethereum blockchain platform. By adding data encryption to blockchain transactions, the system encourages companies to handle their operations internally. It also allows for customization to meet different organizational needs. The smart contracts for this framework are very flexible and can be used on almost any blockchain. This ensures transactions happen immediately while keeping privacy, transparency, and security intact. The model provides strong traceability throughout the corn supply chain. It continuously monitors production and delivery, ensuring compliance with established regulations. Any party involved in wrongdoing within the supply chain can be quickly identified, lowering the risk of food contamination. Since the targeted corn crops share similar farming characteristics, the framework's ability to trace corn production also applies to other corn-related supply chains. Additionally, this method can be expanded for government monitoring of other crops such as wheat, beans, millet, and others. Potential users of this system include government agencies, corn processors, farmers, agronomists, agricultural organizations, merchants, food safety regulators, and crop scientists. The smart contracts were created using Solidity to work with the Ethereum blockchain. The overall approach can easily adapt to other blockchain platforms with minor changes.

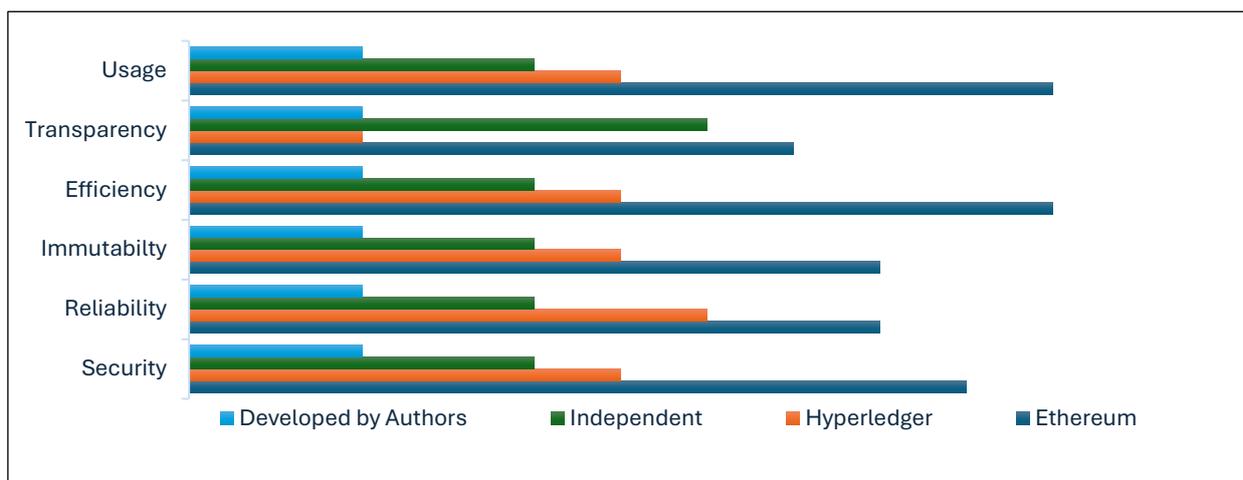


Figure 3: Comparison of used platform Ethereum with other blockchain platforms.

REFERENCES

- Cooper, Martha C., Douglas M. Lambert, and Janus D. Pagh. "Supply chain management: more than a new name for logistics." *The international journal of logistics management* 8, no. 1 (1997): 1-14.
- Salah, Khaled, Nishara Nizamuddin, Raja Jayaraman, and Mohammad Omar. "Blockchain-based soybean traceability in agricultural supply chain." *Ieee Access* 7 (2019): 73295-73305.
- Bhat, Showkat Ahmad, Nen-Fu Huang, Ishfaq Bashir Sofi, and Muhammad Sultan. "Agriculture-food supply chain management based on blockchain and IoT: a narrative on enterprise blockchain interoperability." *Agriculture* 12, no. 1 (2021): 40.
- Mendi, Arif Furkan. "Blockchain for food tracking." *Electronics* 11, no. 16 (2022): 2491.
- Thanapal, Pandi, J. Prabhu, and Mridula Jakhar. "A survey on barcode RFID and NFC." In *IOP Conference Series: Materials Science and Engineering*, vol. 263, no. 4, p. 042049. IOP Publishing, 2017.
- Westerkamp, Martin, Friedhelm Victor, and Axel Küpper. "Blockchain-based supply chain traceability: Token recipes model manufacturing processes." In *2018 IEEE international conference on internet of things (iThings) and IEEE CReen computing and communications (CReenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData)*, pp. 1595-1602. IEEE, 2018.
- Chen, Long, Lin William Cong, and Yizhou Xiao. "A brief introduction to blockchain economics." In *Information for efficient decision making: Big data, blockchain and relevance*, pp. 1-40. 2021.
- Zheng, Zibin, Shaoan Xie, Hong-Ning Dai, Weili Chen, Xiangping Chen, Jian Weng, and Muhammad Imran. "An overview on smart contracts: Challenges, advances and platforms." *Future Generation Computer Systems* 105 (2020): 475-491.
- Oliva, Gustavo A., Ahmed E. Hassan, and Zhen Ming Jiang. "An exploratory study of smart contracts in the Ethereum blockchain platform." *Empirical Software Engineering* 25 (2020): 1864-1904.
- Fahim, Shahriar, S. Katibur Rahman, and Sharfuddin Mahmood. "Blockchain: A comparative study of consensus algorithms PoW, PoS, PoA, PoV." *Int. J. Math. Sci. Comput* 3 (2023): 46-57.
- Latino, Maria Elena, Marta Menegoli, Mariangela Lazoi, and Angelo Corallo. "Voluntary traceability in food supply chain: a framework leading its implementation in Agriculture 4.0." *Technological Forecasting and Social Change* 178 (2022): 121564.
- Li, Lina, Dezheng Jin, Tingting Zhang, and Nianfeng Li. "A secure, reliable and low-cost distributed storage scheme based on blockchain and IPFS for firefighting IoT data." *IEEE Access* (2023).
- Aggarwal S, Chaudhary R, Aujla GS, Kumar N, Choo KKR, Zomaya AY. 2019. Blockchain for smart communities: applications, challenges and opportunities. *Journal of Network and Computer Applications* 144(5):13-48 DOI 10.1016/j.jnca.2019.06.018.
- Ali J, Kumar S. 2011. Information and communication technologies (ICTs) and farmers' decision-making across the agricultural supply chain. *International Journal of Information Management* 31(2):149-159 DOI 10.1016/j.ijinfomgt.2010.07.008.
- Atzei N, Bartoletti M, Cimoli T. 2017. A survey of attacks on Ethereum smart contracts (SoK). In: Maffei M, Ryan M, eds. *Principles of Security and Trust*. POST 2017. Lecture Notes in Computer Science. Vol. 10204. Berlin: Springer, 164-186.
- Jain, K., & Rana, S. (2024, September). Blockchain Consensus: Assessing Diverse Mechanisms for Distributed Agreement. In *2024 International Conference on Artificial Intelligence and Emerging Technology (Global AI Summit)* (pp. 660-665). IEEE
- Casino F, Kanakaris V, Dasaklis TK, Moschuris S, Rachaniotis NP. 2019. Modeling food supply chain traceability based on blockchain technology. *IFAC-PapersOnLine* 52(13):2728-2733 DOI 10.1016/j.ifacol.2019.11.620.
- Bosona T, Gebresenbet G. 2013. Food traceability as an inteCRal part of logistics management in food and agricultural supply chain. *Food Control* 33(1):32-48 DOI 10.1016/j.foodcont.2013.02.004.
- Yakubu, Bello Musa, Rabia Latif, Aisha Yakubu, Majid Iqbal Khan, and Auwal Ibrahim Magashi. "RiceChain: Secure and traceable rice supply chain framework using blockchain technology." *PeerJ Computer Science* 8 (2022): e801.

20. Opara LU. 2003. Traceability in agriculture and food supply chain: a review of basic concepts, technological implications, and future prospects. *Journal of Food, Agriculture & Environment* 1:101-106 DOI 10.1234/4.2003.323.
21. Nizamuddin N, Hasan HR, Salah K. 2018. IPFS-blockchain-based authenticity of online publications. In: Chen S, Wang H, Zhang LJ, eds. *Lecture Notes in Computer Science*. Vol. 10974. Cham: Springer.
22. Luu L, Chu DH, Olickel H, Saxena P, Hobor A. 2016. Making smart contracts smarter. In: *Proceedings of the ACM Conference on Computer and Communications Security*. New York: ACM, 254-269.
23. Foth M. 2017. The promise of blockchain technology for interaction design. In: *ACM International Conference Proceeding Series*, New York: Association for Computing Machinery.
24. Ge H, CRay R, Nolan J. 2015. Agricultural supply chain optimization and complexity: a comparison of analytic vs simulated solutions and policies. *International Journal of Production Economics* 159(2):208-220 DOI 10.1016/j.ijpe.2014.09.023.
25. Ali, Jabir, and Sushil Kumar. "Information and communication technologies (ICTs) and farmers' decision-making across the agricultural supply chain." *International Journal of Information Management* 31, no. 2 (2011): 149-159.
26. Toyoda, Kentaroh, Koji Machi, Yutaka Ohtake, and Allan N. Zhang. "Function-level bottleneck analysis of private proof-of-authority ethereum blockchain." *IEEE Access* 8 (2020): 141611-141621.
27. Lin W, Huang X, Fang H, Wang V, Hua Y, Wang J, Yin H, Yi D, Yau L. 2020. Blockchain technology in current agricultural systems: from techniques to applications. *IEEE Access* 8:143920-143937 DOI 10.1109/ACCESS.2020.3014522.
28. Perez, Daniel, and Benjamin Livshits. "Smart contract vulnerabilities: Does anyone care." *arXiv preprint arXiv:1902.06710* (2019): 1-15.
29. Jain, K., & Rana, S. (2024, August). A Review on Blockchain-Based Paradigm for the Management of Digital Assets in Healthcare. In *2024 IEEE 5th India Council International Subsections Conference (INDISCON)* (pp. 1-6). IEEE.
30. Mao D, Wang F, Hao Z, Li H. 2018. Credit evaluation system based on blockchain for multiple stakeholders in the food supply chain. *International Journal of Environmental Research and Public Health* 15(8):1627 DOI 10.3390/ijerph15081627.