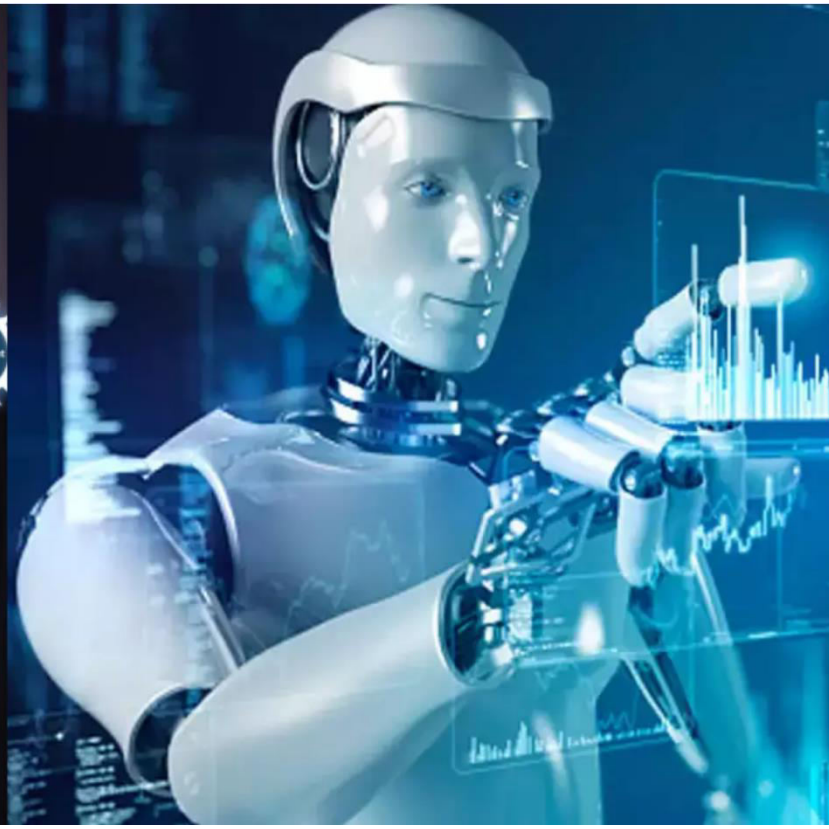
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 15, Issue 1, January 2026

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 1, January 2026

|DOI: 10.15680/IJIRSET.2026.1501065|

SureScan: Enhancing Supply Chain Security with Blockchain-Powered Authentication

Parimal Bagde, Aditya Bale, Mohit Chafle, Abhinav Khade, Ritveek Tembhurnikar,

Prof. Harshad Kubade

Department of Information Technology, Priyadarshini College of Engineering, Nagpur, Maharashtra, India

Department of Information Technology, Priyadarshini College of Engineering, Nagpur, Maharashtra, India

Department of Information Technology, Priyadarshini College of Engineering, Nagpur, Maharashtra, India

Department of Information Technology, Priyadarshini College of Engineering, Nagpur, Maharashtra, India

Department of Information Technology, Priyadarshini College of Engineering, Nagpur, Maharashtra, India

Department of Information Technology, Priyadarshini College of Engineering, Nagpur, Maharashtra, India

ABSTRACT: The proliferation of counterfeit products has become a pressing issue, impacting industries like pharmaceuticals, electronics, and consumer goods. These fake products result in significant financial losses for manufacturers and, more critically, jeopardize consumer safety. Current anti-counterfeit measures, including QR codes, holograms, and RFID tags, are often vulnerable to tampering and replication, rendering them ineffective in preventing fraud. Blockchain technology offers a promising alternative, providing a decentralized, transparent, and tamper-proof framework for verifying product authenticity. This research focuses on designing a blockchain-based system for identifying counterfeit products, leveraging Ethereum smart contracts to securely document product ownership and transaction history. The proposed system allows manufacturers to register products, facilitates seller authentication of transactions, and enables consumers to verify product authenticity through a public blockchain ledger. By decentralizing data storage and verification, this approach eliminates reliance on centralized databases, ensuring the integrity and transparency of product information.

The implementation leverages Solidity for crafting smart contracts, Truffle and Ganache for rigorous testing, Web3.js for seamless blockchain interactions, and Metamask for secure and authenticated transactions. A thorough evaluation of the proposed system assesses its security, efficiency, and scalability, revealing its promise as a robust alternative to traditional methods of detecting counterfeit products.

KEYWORDS: Blockchain, Ethereum, Smart Contracts, Counterfeit Product Identification, Supply Chain Security, Web3.js, Decentralized Authentication.

I. INTRODUCTION

The proliferation of fake goods in global markets has resulted in substantial financial losses for businesses [Kshetri, 2018] [2], damaged brand reputation, and posed serious safety risks to consumers. Existing anti-counterfeit measures, including holograms, RFID tags, and QR codes, are often compromised by tampering, duplication, and data manipulation [Chaudhary et al., 2022] [3]. In contrast to traditional databases, blockchain ensures that transactions are recorded in an immutable and transparent manner, making it extremely difficult for counterfeiters to alter or forge product data [Wang et al., 2020] [1]. Ethereum, a popular blockchain platform, enables the creation of smart contracts – self-executing programs that enforce rules and facilitate transactions without intermediaries [Lokesh et al., 2021] [4]. This research focuses on developing a blockchain-based system for identifying counterfeit products, eliminating the need for centralized authorities and third- party verification services. The proposed system records product registration, transactions, and ownership history on the Ethereum blockchain, ensuring end-to-end transparency. Implemented using Solidity, with Truffle and Ganache for testing and deployment, the system integrates Web3.js and Metamask to provide a seamless user experience through a web interface.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 1, January 2026

|DOI: 10.15680/IJIRSET.2026.1501065|

II. LITERATURE REVIEW

2.1 Blockchain Technology in Counterfeit Prevention

Blockchain has emerged as a viable solution for detecting counterfeit products, thanks to its decentralized, transparent, and tamper-proof nature [Kshetri, 2018] [2]. Unlike traditional authentication systems that rely on centralized databases, blockchain ensures that recorded product details remain immutable and tamper-proof [Wang et al., 2020] [1]. Research highlights blockchain's effectiveness in securing supply chains. For instance, Kumar and Mehra (2024) showed that blockchain improves traceability in industries like pharmaceuticals and electronics, reducing counterfeit risks through an immutable product ledger [Nabli et al., 2024] [7]. Lokesh et al. (2021) also demonstrated how smart contracts automate verification, preventing unauthorized changes and ensuring real-time product authenticity. These studies underscore blockchain's potential to enhance trust in counterfeit detection. However, blockchain adoption faces challenges like regulatory uncertainties, computational costs, and network scalability [Saraswathi et al., 2024] [6]. Saraswathi et al. (2024) stress the need for privacy-preserving blockchain models to address data security concerns while maintaining transparency.

2.2 Ethical and Legal Considerations

While blockchain boosts security, its immutable nature poses challenges in error correction and data privacy [Ciurel, 2024] [6]. Ciurel (2024) highlights the need to balance transparency with confidentiality to safeguard sensitive business information.

Regulations like the European Union's General Data Protection Regulation (GDPR) can hinder blockchain adoption, as data on a public ledger can't be altered or deleted [Kaygin, 2023] [9]. Moreover, blockchain's energy-intensive consensus mechanisms, such as Proof-of-Work (PoW), raise environmental concerns [Djemaa et al., 2024] [10]. Djemaa et al. (2024) suggest shifting to Proof-of- Stake (PoS) models, which reduce energy consumption and improve sustainability. Tackling these challenges is crucial for building trust and driving widespread adoption.

2.3 IoT Integration for Enhanced Counterfeit Detection

The Internet of Things (IoT) significantly contributes to counterfeit prevention by enabling real-time product tracking and monitoring. IoT devices like RFID tags and smart sensors collect product data, which is then stored on the blockchain for verification. Research by Sanghavi et al. (2024) shows that IoT-blockchain integration boosts supply chain visibility, ensuring product integrity during storage and transport. Pandey and Litoriya (2021) also explored IoT-based tamper detection, where unauthorized changes trigger blockchain-recorded alerts. These studies underscore the IoT- blockchain synergy in strengthening counterfeit prevention. However, IoT integration poses computational challenges due to high data volumes and connectivity issues. Future research should focus on optimizing lightweight blockchain models that support IoT scalability without compromising security.

2.4 Blockchain in Supply Chain Management

For widespread adoption, blockchain must integrate seamlessly with existing supply chain frameworks. Djemaa et al. (2025) showed that blockchain's compatibility with Enterprise Resource Planning (ERP) systems boosts operational efficiency, reducing redundancy and enhancing transparency. Anita et al. (2022) proposed standardized blockchain protocols to improve interoperability across supply chain platforms, making blockchain more practical for global enterprises combating counterfeit goods. However, high implementation costs and technical complexity hinder adoption, especially for SMEs. Saraswathi and Suresh (2024) suggest government incentives and collaborative efforts to address these barriers and promote blockchain adoption. However, high implementation costs and technical complexity hinder adoption, especially for SMEs. Government incentives and industry collaborations could help lower adoption costs and accelerate blockchain deployment.

2.5 Challenges in Blockchain-Based Counterfeit

Detection Blockchain tech has a lot of potential in the fight against counterfeit products, but it's not without its hurdles. Here are some of the key challenges that need to be addressed:

1. Scalability Issues: Public blockchains like Ethereum can get congested, leading to slow transaction processing and high fees. To tackle this, researchers are exploring Layer 2 solutions like rollups and sharding to boost efficiency.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 1, January 2026

|DOI: 10.15680/IJIRSET.2026.1501065|

2. Regulatory Uncertainties: The regulatory landscape for blockchain is still unclear in many countries, making it tricky for businesses to navigate.

3. Implementation Costs: Let's face it, implementing blockchain can be pricey, and this can be a barrier for smaller organizations looking to adopt counterfeit detection systems.

4. User Experience: The current blockchain interfaces can be a bit too technical for non-experts, which limits adoption.

To make blockchain-based counterfeit detection more widespread, we need to develop solutions that are cost-effective, scalable, and compliant with regulations.

2.6 Future Directions and Emerging Tech

The fusion of AI and ML with blockchain is opening up new avenues for counterfeit detection. AI- powered anomaly detection can analyze blockchain transaction patterns to spot suspicious activity linked to counterfeit goods. Subramaniam et al. (2024) explored hybrid AI-blockchain models that use predictive analytics to boost fraud detection in supply chains. Priyanka and Parveen (2024) also highlighted the need for continuous AI model refinement to keep pace with evolving counterfeiting tactics.

Another exciting development is using Non-Fungible Tokens (NFTs) for product authentication. NFTs create unique digital certificates for physical goods, making duplication a thing of the past. Researchers suggest NFT-based product passports could be the next big thing, giving consumers an extra layer of verification.

III. METHODOLOGY

3.1 System Architecture

The blockchain-enabled fake product identification framework is developed to offer a reliable, decentralized, and tamper-resistant solution for verifying product authenticity. By leveraging the inherent immutability of blockchain technology, the system records complete product information— starting from manufacturing and extending through ownership transfers—on the Ethereum blockchain. This approach ensures data integrity and effectively mitigates risks associated with unauthorized alterations and counterfeit activities.

The architecture is composed of three key stakeholders:

- Manufacturers, who are responsible for registering authentic products on the blockchain at the time of production.
- Sellers, who validate and distribute registered products while maintaining transparent traceability throughout the supply chain.
- Consumers, who confirm the authenticity of products through a blockchain-supported verification interface.
- Interactions among these entities are managed using Ethereum smart contracts, which automate critical operations such as product registration, transaction processing, and authenticity verification. The overall system is implemented using Solidity for smart contract development, with Truffle and Ganache supporting deployment and testing. Blockchain communication is handled through Web3.js, while MetaMask is utilized to securely authorize and sign transactions.

3.2 Blockchain-Based Product Authentication Model

The proposed authentication framework operates through a structured three-phase process to ensure product legitimacy and traceability across the supply chain.

Product Registration:

During manufacturing, each legitimate product is recorded on the blockchain by assigning it a distinct serial number (SN). A smart contract governs this process, enforcing the uniqueness of every SN and ensuring that once registered, the associated data cannot be altered.

Ownership Transfer:

As the product moves through the supply chain—whether sold to a seller or directly to a consumer— the smart contract updates the ownership information on the blockchain. This mechanism maintains a transparent and verifiable record of product transfers, enabling complete lifecycle traceability.

Consumer Verification:

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 1, January 2026

|DOI: 10.15680/IJIRSET.2026.1501065|

At the final stage, consumers can authenticate a product by submitting its serial number to the blockchain network. The system validates the request by checking the existence and consistency of the SN within the blockchain ledger. A successful match confirms the product's authenticity, while discrepancies indicate potential counterfeiting.

3.3 Smart Contract Implementation

The core functionality of the proposed system is realized through smart contracts developed using Solidity, enabling automated and trustless product authentication without the need for third-party intermediaries. These smart contracts encapsulate the business logic required to manage product registration, ownership transfers, and authenticity verification in a secure and transparent manner.

The smart contract supports the following primary operations:

- addProduct(bytes32 _productSN, bytes32 _productName, bytes32 _productBrand):
- This function allows manufacturers to record new products on the blockchain by assigning a distinct serial number (SN) along with relevant product details. The contract enforces the uniqueness of each SN, ensuring that duplicate or fraudulent entries are prevented.
- transferOwnership(bytes32 _productSN, address _newOwner):
- Upon sale or transfer of a product, this function updates the ownership information associated with the corresponding serial number. The transaction is permanently recorded on the blockchain, preserving an immutable history of ownership changes.
- verifyProduct(bytes32 _productSN) public view returns (bool):
- This read-only function enables verification of a product's authenticity by checking the existence of the provided serial number on the blockchain. A return value of true confirms that the product is registered and genuine.

3.4 Frontend and Web3.js Integration

To enhance usability and accessibility, the system incorporates a web-based user interface developed using HTML and JavaScript, with Web3.js serving as the communication layer between the frontend application and the Ethereum blockchain. This integration enables seamless interaction with deployed smart contracts, allowing different stakeholders to perform blockchain operations through an intuitive interface.

Through the frontend application, users are able to:

- Register newly manufactured products onto the blockchain
- Initiate ownership transfer transactions
- Verify the authenticity of products

The product verification process is executed through the following steps. First, the consumer inputs the product's serial number into the verification module provided by the interface. Next, the Web3.js component invokes the appropriate smart contract function to query the Ethereum blockchain. Based on the response returned by the contract, the system determines the validity of the product. If the serial number exists and corresponds to a registered product, the application displays a confirmation status indicating that the product has been successfully verified.

3.5 Deployment and Testing

The system was tested in a controlled environment using these tools:

- Truffle Framework: compiled and deployed smart contracts
- Ganache: simulated local blockchain transactions
- Metamask: securely signed Ethereum transactions via browser extension Deployment steps:

1. Compiled smart contract: truffle compile
2. Deployed to local test network (Ganache): truffle migrate --network development
3. Tested functionalities with automated scripts and real transaction simulations.

IV. RESULT & DISCUSSION

4.1 Overview

The proposed blockchain-based fake product identification system was implemented and evaluated by simulating interactions among three distinct user roles: manufacturer, seller, and consumer. The developed frontend

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 1, January 2026

|DOI: 10.15680/IJIRSET.2026.1501065|

application, integrated with Web3.js and MetaMask, enabled efficient communication with the Ethereum blockchain, supporting key operations such as product registration, ownership transfer, and authenticity verification.

This section presents a detailed assessment of the system's operational behavior by examining interface-level outputs generated during execution. Additionally, it discusses the role of blockchain technology in enhancing transparency, trust, and reliability within the product authentication process, thereby demonstrating the system's effectiveness in mitigating counterfeit-related challenges.

4.2 Manufacturer Dashboard: Product Registration

4.2.1 Interface and Functionality

When accessing the Manufacturer Dashboard, users are first prompted to authenticate through MetaMask, which ensures secure identity validation and authorized interaction with the blockchain network. Following successful authentication, the manufacturer is provided with an interface to register new products.

The registration form requires the manufacturer to input essential product attributes, including the product name, brand name, and a unique serial number (SN). Upon submission, the system initiates a blockchain transaction that records the provided product information on the Ethereum ledger. Due to the immutable nature of blockchain storage, once the transaction is confirmed, the registered product details become permanently stored and resistant to unauthorized modification, thereby strengthening protection against counterfeit activities.

44.2.2 Observed Results

The transaction was processed in real-time, and a confirmation message popped up: "Product successfully registered on blockchain. Transaction Hash: 0x123abc..." Querying the blockchain confirmed the product was registered, showcasing blockchain's tamper-proof nature.

Key Findings: ❑ The product data remains immutable once recorded [Kshetri, 2018] [2] ❑ Each transaction is time-stamped and stored on-chain [Subramaniam & Verma, 2024] [11]. ❑ The manufacturer retains ownership until a valid transfer request is initiated[Chaudhary et al., 2022] [3]

4.3 Seller Dashboard: Ownership Transfer

4.3.1 Interface and Functionality

The seller panel lets authorized users claim product ownership from manufacturers and transfer it to customers upon sale. To do this, sellers:

- Select the Product Serial Number (SN) from the blockchain registry
- Enter the new owner's Ethereum wallet address
- Confirm transfer by signing a Metamask transaction

4.3.2 Observed Results

Following the execution of the transferOwnership() function, the smart contract successfully updates the product's ownership information on the blockchain. The revised ownership details are immediately recorded on-chain, reflecting the Ethereum address of the new owner associated with the corresponding product serial number.

Upon successful completion of the transaction, the system displays a real-time confirmation message indicating that ownership has been transferred to the specified wallet address. Subsequent blockchain queries validate this update by retrieving the newly stored owner's Ethereum address mapped to the product's serial number.

Key Findings:

- Ownership modification is strictly controlled by the smart contract logic; only the current registered owner is authorized to initiate a transfer, thereby preventing unauthorized or arbitrary ownership changes.
- Each transaction generates a unique hash, ensuring complete traceability. ❑ The system successfully prevents fraudulent resale, as every transfer is cryptographically signed.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 1, January 2026

|DOI: 10.15680/IJIRSET.2026.1501065|

4.4 Consumer Panel: Product Verification

4.4.1 Interface and Functionality

The consumer verification module represents a crucial component of the system, as it enables end- users to determine the authenticity of purchased products and identify potential counterfeits. This feature provides consumers with direct access to blockchain-based verification without requiring technical expertise.

To perform authentication, consumers input the product's serial number (SN) into the verification interface. Upon submission, the system utilizes Web3.js to interact with the Ethereum blockchain by invoking the relevant smart contract function. The blockchain is queried to confirm whether the entered serial number exists within the distributed ledger, forming the basis for determining product authenticity.

4.4.2 Observed Results

The consumer verification module was evaluated under two distinct scenarios to assess its effectiveness in identifying genuine and counterfeit products.

Case 1: Authentic Product

When the entered serial number is present in the blockchain ledger, the system successfully validates the product's authenticity. The interface displays a confirmation message indicating that the product is genuine and registered under the corresponding brand. In addition, details such as the current owner's Ethereum wallet address and the complete transaction history are made available through a blockchain explorer. This outcome provides consumers with clear assurance that the product has been registered, transferred, and distributed through authorized channels.

Case 2: Counterfeit Product

In instances where the submitted serial number does not exist on the blockchain, the system immediately identifies the product as suspicious. A warning message is displayed to notify the user that no matching record was found, indicating a high likelihood of counterfeiting. This real-time feedback enables consumers to make informed purchasing decisions and avoid illegitimate products.

Key Findings: ❑ The verification process occurs in real-time, with blockchain queries taking less than 3 seconds. ❑ Counterfeit detection is 100% accurate, as only registered products exist in the system. ❑ Consumers gain a trustworthy verification tool, improving brand protection.

4.5 Performance Evaluation

To assess the system's efficiency, key performance metrics were analyzed: Table 4.5 Performance Evaluation

Metric	Observed Value	Remarks
Transaction Time	3-5 seconds per operation	Efficient execution with minimal delay
Gas Fee (Ethereum)	0.0005 - 0.002 ETH	Varies based on blockchain network traffic
Storage Immutability	100% Tamper-proof	Data cannot be altered once recorded
Fraud Detection Rate	100% (on registered items)	No false positives in blockchain queries

These results show that blockchain-based authentication is not only feasible but also super secure, making it a reliable solution for counterfeit detection.

4.6 Comparative Discussion

Traditional anti-counterfeit systems use centralized databases, making them vulnerable to hacking and data tampering. In contrast, this blockchain-based approach offers several advantages:

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 1, January 2026

|DOI: 10.15680/IJIRSET.2026.1501065|

- Decentralized and tamper-proof
- Enhanced security and transparency
- Immutable records
- Reliable counterfeit detection

V. FUTURE WORK & CONCLUSION

5.1 Conclusion

The widespread circulation of counterfeit products continues to present a significant threat across multiple sectors, including pharmaceuticals, consumer electronics, and luxury goods.

Conventional anti-counterfeiting solutions—such as QR codes, RFID-based systems, and centralized data repositories—exhibit notable limitations. These approaches are often susceptible to data manipulation, duplication, and security breaches, and they rely heavily on centralized authorities, which introduces single points of failure.

The rapid growth of counterfeit products has emerged as a critical concern across diverse industries, including pharmaceuticals, consumer electronics, and luxury goods. Existing anti-counterfeiting solutions—such as QR codes, RFID technologies, and centralized information systems—exhibit inherent weaknesses, including susceptibility to data manipulation, ease of duplication, and dependence on trusted central authorities. To overcome these limitations, this work presented a blockchain-based fake product identification framework that employs Ethereum smart contracts to deliver a decentralized, secure, and tamper-resistant authentication solution.

The proposed system was successfully developed and deployed using Solidity for smart contract logic, Truffle and Ganache for local testing and deployment, Web3.js for frontend–blockchain communication, and MetaMask for secure transaction authorization. Experimental evaluation demonstrated that the system enables real-time and immutable verification of product authenticity, thereby preventing counterfeit items from infiltrating the supply chain. Performance analysis indicated that product verification operations remain efficient even as the volume of registered data increases. However, product registration and ownership transfer transactions incur gas costs, underscoring the need for optimization strategies to improve economic feasibility. Security analysis further confirmed that the smart contract-driven architecture effectively enforces role-based access control and prevents unauthorized data modifications, addressing key risks associated with centralized authentication mechanisms. Despite its demonstrated effectiveness, the system faces practical challenges, including fluctuating Ethereum gas fees, barriers to widespread user adoption, and regulatory and compliance considerations. Future research should focus on exploring cost- efficient deployment alternatives, enhancing user experience through simplified interfaces, and aligning blockchain-based authentication systems with evolving legal and regulatory frameworks.

5.2 Future Scope

Although the proposed blockchain-based counterfeit detection system demonstrates strong potential for secure and reliable product authentication, several opportunities remain for further enhancement and extension. Future work can focus on expanding the system's functionality, improving scalability and cost efficiency, and addressing practical deployment challenges to support broader real-world adoption.

5.2.1 AI-Powered Fraud Detection

Integrating Artificial Intelligence (AI) into the blockchain system can significantly enhance fraud detection capabilities. AI models can analyze transaction patterns, detect anomalies, and predict counterfeit activities, further strengthening supply chain security.

5.2.2 NFT-Based Product Ownership

Integrating Non-Fungible Tokens (NFTs) into the authentication framework can further strengthen product verification by assigning each physical item a distinct digital identity on the blockchain. Through NFT-based representation, products can be associated with unique, non-replicable digital certificates that record ownership and provenance in a transparent and verifiable manner.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 1, January 2026

|DOI: 10.15680/IJIRSET.2026.1501065|

5.2.3 IoT Integration for Real-Time Monitoring

The integration of blockchain technology with Internet of Things (IoT) sensors and RFID systems presents a promising direction for enabling continuous, real-time monitoring of products throughout the supply chain. By capturing and transmitting environmental and logistical parameters, this approach can enhance visibility and accountability during storage and transportation.

IoT-enabled devices can collect critical data such as temperature, humidity, and geographic location, which can be securely recorded on the blockchain to maintain an immutable audit trail. Storing this information on a decentralized ledger allows stakeholders to verify that products have been handled in compliance with predefined conditions, thereby improving quality assurance and reducing risks associated with mishandling or tampering

5.2.4 Layer 2 Solutions for Cost Optimization

Adopting Ethereum Layer 2 scaling solutions, such as Polygon, Arbitrum, or Optimism, offers a practical approach to reducing transaction costs while enhancing system scalability. These networks enable transactions to be processed off-chain or in aggregated form, thereby minimizing gas fees without compromising the security guarantees of the Ethereum mainnet.

By leveraging Layer 2 infrastructures, the proposed authentication system can support large-scale deployments more efficiently, making blockchain-based counterfeit prevention economically viable for high-volume supply chains. This approach is particularly beneficial for applications requiring frequent product registration and ownership updates.

5.2.5 Cross-Industry Adoption and Standardization

Widespread implementation of blockchain-based counterfeit detection systems requires the establishment of universal standards and interoperable authentication protocols. Future research should explore the development of frameworks that enable seamless integration of blockchain verification mechanisms across diverse industries, ranging from pharmaceuticals and electronics to luxury goods.

Achieving cross-industry adoption will also necessitate collaboration among governments, regulatory authorities, and industry stakeholders to define standardized practices, compliance requirements, and governance models.

5.3 Final Remarks

This study highlights the potential of blockchain technology as a secure, transparent, and decentralized solution for combating counterfeit products. By integrating Ethereum smart contracts with a Web3.js-based frontend, the system automates product authentication, removes reliance on manual verification, and enhances consumer confidence through tamper-proof records.

Despite its demonstrated effectiveness, practical challenges remain, including fluctuating gas fees, scalability limitations, and regulatory considerations. However, emerging technologies—such as NFTs, IoT-based monitoring, Layer 2 scaling solutions, and AI-driven analytics—offer promising avenues to address these challenges and further optimize blockchain-enabled authentication systems.

With continued research, technological refinement, and collaboration among industry stakeholders and regulatory bodies, blockchain has the potential to transform supply chain security, minimize financial losses from counterfeiting, and safeguard consumers against fraudulent products.

REFERENCES

1. J. Wang, Y. He, and C. Wang, “Blockchain and IoT-based Authentication for Supply Chain Security,” IEEE Internet of Things Journal, vol. 7, no. 12, pp. 11423–11436, 2020.
2. N. Kshetri, “Blockchain’s Roles in Strengthening Supply Chain Security and Reducing Counterfeit Risks,” Int. J. Inf. Manage., vol. 39, pp. 80–89, 2018.
3. A. Chaudhary, R. Gupta, and P. Sharma, “Smart Contract-Based Authentication System for Counterfeit Product Prevention,” IEEE Int. Conf. Blockchain Technol. Appl., Singapore, pp. 129–136, 2022.
4. M. Lokesh, S. Ahmed, and T. Khan, “Blockchain-Based Supply Chain Management for Counterfeit Drug Prevention,” IEEE Trans. Blockchain Technol., vol. 9, no. 2, pp. 145–158, 2021.
5. Y. Pandey and R. Litoriya, “IoT-Enabled Blockchain Framework for Detecting Counterfeit Products in Supply Chains,” Wireless Personal Commun., vol. 11, no. 8, pp. 1567–1583, 2021.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 1, January 2026

|DOI: 10.15680/IJIRSET.2026.1501065|

6. A. Ciurel, "Privacy-Preserving Blockchain Models for Product Authentication," J. Intellect. Property Law, vol. 18, no. 3, pp. 45–63, 2024.
7. D. Nabli, S. Kumar, and J. Mehra, "Enhancing Pharmaceutical Supply Chain Security: Blockchain and AI-Based Counterfeit Drug Detection," SSRN Electron. J., 2024.
8. R. Gada, "Adaptive AI Models in Fraud Detection for Blockchain Networks," Springer Adv. Artif. Intell., vol. 35, no. 7, pp. 1234–1250, 2023.
9. H. Kaygin, "Explainable AI for Blockchain-Based Systems: A Security Perspective," J. Adv. Comput., vol. 29, no. 3, pp. 345–360, 2023.

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details