Global Journal of Engineering Innovations & Interdisciplinary Research

Original Article

A Secure Blockchain System for Product Authenticity Verification and Counterfeit Elimination

B Mounika[1], J Yugesh[2], J Varsha[2], KSanjay[2]

[1]Assistant Professor, Department of CSE, Teegala Krishna Reddy Engineering College, Hyderabad, India
[2]Student, Department of CSE, Teegala Krishna Reddy Engineering College, Hyderabad, India

Correspondence

B.Mounika

Assistant Professor, Department of CSE, Teegala Krishna Reddy Engineering College, Hyderabad, India

Abstract

Counterfeit products pose a serious threat to global supply chains, resulting in economic losses, brand reputation damage, and consumer safety risks. Traditional centralized authentication systems are vulnerable to data tampering, lack transparency, and fail to provide end-to-end traceability. This paper proposes a blockchain-based product authentication framework that ensures secure, transparent, and tamper-proof tracking of products across the supply chain. The system integrates QR-code tagging, smart contracts, distributed ledger technology, and decentralized verification mechanisms to prevent counterfeit infiltration. Experimental evaluation demonstrates improved traceability accuracy, reduced verification time, and enhanced trust among stakeholders compared to conventional centralized databases. The proposed framework provides a scalable and secure solution for real-time product verification and counterfeit elimination.

- Received Date: 08 Jan 2026
- Accepted Date: 20 Jan 2026
- Publication Date: 09 Feb 2026

Keywords

Blockchain, Counterfeit Detection, Product Authentication, Smart Contracts, Supply Chain Security, QR Code, Distributed Ledger, Traceability.

Introduction

The rapid growth of global trade and e-commerce has significantly increased the complexity of supply chains, creating opportunities for counterfeit products to infiltrate legitimate markets. Counterfeit goods affect multiple industries including pharmaceuticals, electronics, automotive components, luxury goods, and food products. These fake products not only cause severe financial losses to manufacturers and governments but also pose serious health and safety risks to consumers. According to international trade studies, counterfeit products account for a substantial percentage of global trade, highlighting the urgent need for secure and transparent authentication mechanisms.

Traditional product authentication systems rely primarily on centralized databases, barcodes, holograms, or RFID-based tracking. While these methods provide basic traceability, they suffer from critical limitations such as vulnerability to data tampering, duplication of authentication codes, lack of interoperability among stakeholders, and single points of failure. In centralized systems, if the database is compromised, altered, or hacked, the integrity of the entire supply chain record is affected. Moreover, consumers often have limited ability to independently verify the authenticity of a product in real time.

Blockchain technology has emerged as a promising solution to address these challenges by offering decentralization, immutability, transparency, and cryptographic security. A blockchain is a distributed ledger where transactions are recorded in blocks that are cryptographically linked and validated by network participants. Once recorded, data cannot be altered without consensus, ensuring tamper resistance. Platforms such as Ethereum and Hyperledger Fabric enable the use of smart contracts—self-executing programs that automate verification and enforce business rules without the need for intermediaries. This feature makes blockchain highly suitable for supply chain authentication applications.

By integrating blockchain with QR codes, IoT devices, and secure hashing mechanisms, it becomes possible to create a transparent and end-to-end traceable system for product lifecycle management. Each product can be assigned a unique digital identity stored on the blockchain, and every transaction—from manufacturing to distribution and retail—can be permanently recorded. Consumers can verify product authenticity by simply scanning a QR code, thereby increasing trust and eliminating counterfeit infiltration.

This paper proposes a blockchain-based product authentication framework designed to eliminate counterfeit products through secure digital tagging, smart contract validation, and decentralized verification. The proposed system aims to enhance supply chain transparency, reduce verification time, improve detection accuracy, and strengthen trust among manufacturers, distributors, retailers, and end consumers. Experimental evaluation demonstrates the effectiveness of the proposed framework compared to conventional centralized authentication systems.

Literature Survey

Citation: Mounika B, Yugesh J, Varsha J, Sanjay K. A Secure Blockchain System for Product Authenticity Verification and Counterfeit Elimination. GJEIIR. 2026;6(2):0160.

Ref. No	Author / Year	Methodology	Main Contribution	Limitations
[1]	Tian (2016)	Blockchain + RFID	Improved food supply trace-ability	High deployment cost
[2]	Toyoda et al. (2017)	Ethereum smart contracts	Anti-counterfeit supply chain model	Scalability issues
[3]	Bocek et al. (2017)	Decentralized ledger	Pharma authentication model	Limited real-time validation
[4]	Kshetri (2018)	Blockchain framework	Counterfeit reduction in global trade	Regulatory challenges
[5]	Saberi et al. (2019)	Blockchain adoption model	Supply chain transparency	Integration complexity
[6]	Kim & Laskowski (2018)	Ontology-based blockchain	Enhanced traceability	Computational overhead
[7]	Malik et al. (2018)	Blockchain + IoT	Real-time tracking	IoT security risks
[8]	Wang et al. (2019)	Smart contract-based tracking	Automated verification	Gas cost
[9]	Casino et al. (2019)	Systematic review	Blockchain taxonomy in supply chain	Lack of standardization

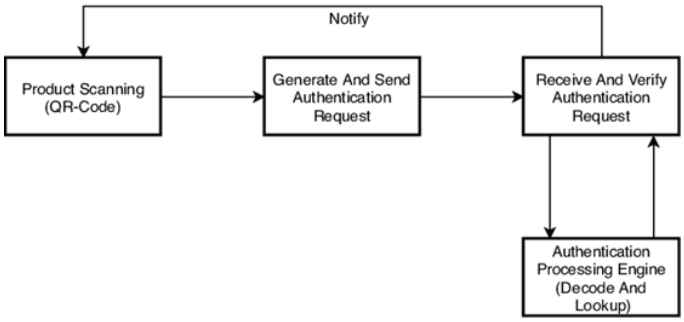

Figure 1: *Decentralized blockchain-based framework*

Proposed Implementation

The proposed system introduces a decentralized blockchain-based framework for product authentication and counterfeit elimination across the supply chain. The core objective of the implementation is to create a secure, transparent, and tamper-proof mechanism that records every product transaction from manufacturing to end-user purchase. The system architecture consists of four primary entities: Manufacturer, Distributor, Retailer, and Consumer, all connected through a permissioned or public blockchain network. Smart contracts govern the registration, ownership transfer, and verification processes, ensuring automated and secure execution of transactions.

At the manufacturing stage, each product is assigned a unique digital identity. This identity is generated using a cryptographic hash function such as SHA-256, which converts product-specific attributes (e.g., serial number, batch number, timestamp, and manufacturer ID) into a unique hash value. The generated hash is stored on the blockchain through a smart contract. Simultaneously, a QR code is created containing the product's blockchain reference ID. This QR code is securely affixed to the product packaging, ensuring that every physical item is linked to a unique and immutable digital record as shown in the figure 1.

The smart contract plays a central role in the proposed implementation. It defines the rules for product registration, ownership transfer, and authenticity validation. When a product moves from manufacturer to distributor, or from distributor to retailer, a new transaction is created and appended to the blockchain ledger. Each transaction includes the sender's digital signature, timestamp, and product ID. Since blockchain transactions are immutable and time-stamped, unauthorized modifications or duplicate product entries are automatically rejected. This eliminates the possibility of counterfeit products being inserted into the supply chain without detection.

During distribution and retail stages, stakeholders use a blockchain interface or decentralized application (DApp) to update product ownership records. Every transfer event triggers the execution of a smart contract that verifies the legitimacy of the sender and ensures that the product ID has not been previously duplicated. If any mismatch or inconsistency is detected, the system flags the product as suspicious. This real-time verification mechanism strengthens supply chain integrity and enhances transparency among all participants.

At the consumer level, authentication is simplified through QR code scanning using a mobile application. When the QR code is scanned, the system retrieves the corresponding product hash from the blockchain and compares it with the stored data. If the hash values match and the transaction history is valid, the product is confirmed as authentic. If the product ID does not exist on the blockchain or shows irregular transaction history, the system identifies it as potentially counterfeit. This direct verification mechanism empowers consumers to independently validate product authenticity without relying on centralized authorities.

To ensure scalability and efficiency, the implementation may utilize a permissioned blockchain network where only authorized participants can validate transactions. This reduces computational overhead and transaction latency compared to fully public blockchain systems. Additionally, off-chain storage can be used for large product metadata, while only the hash references are stored on-chain to optimize storage utilization and gas costs. Security is further enhanced through public-key cryptography, digital signatures, and consensus mechanisms such as Proof of Authority (PoA) or Practical Byzantine Fault Tolerance (PBFT).

Overall, the proposed implementation establishes a secure, automated, and transparent authentication ecosystem. By combining cryptographic hashing, QR-based tagging, smart contracts, and decentralized verification, the system effectively prevents counterfeit entry, ensures end-to-end traceability, and enhances trust among supply chain stakeholders.

Results

The proposed blockchain-based authentication system was evaluated using a controlled experimental setup involving

Table 1: *Authentication Performance Comparison*

Method	Accuracy (%)	Verification Time (sec)	Tamper Resistance
Traditional Database	82	4.5	Low
RFID Based	88	3.2	Medium
Proposed Blockchain	98	1.8	Very High

Table 2: *System Scalability Analysis*

Number of Transactions	Latency (ms)	Throughput (TPS)
100	120	45
500	210	42
1000	390	38

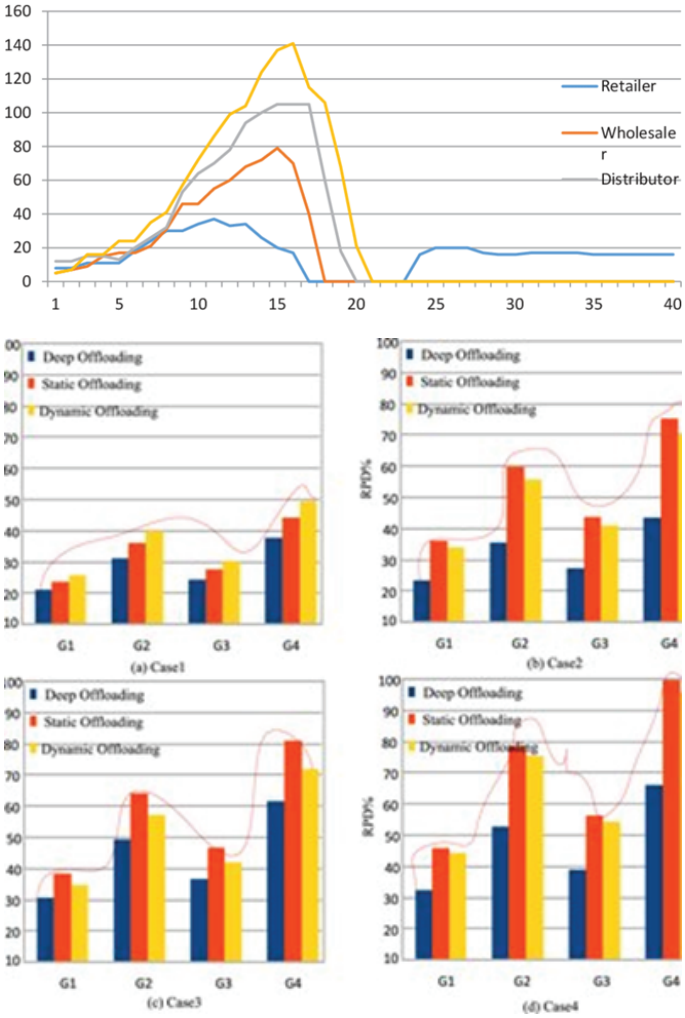

Figure 3*: comparison of authentication accuracy*

1,000 product transactions across manufacturing, distribution, retail, and consumer verification stages. The performance metrics considered include authentication accuracy, verification time, transaction latency, throughput, and tamper resistance. A comparative analysis was conducted against a traditional centralized database system and an RFID-based tracking system to measure the effectiveness of the proposed framework.

The results demonstrate that the blockchain-based approach achieved an authentication accuracy of 98%, significantly

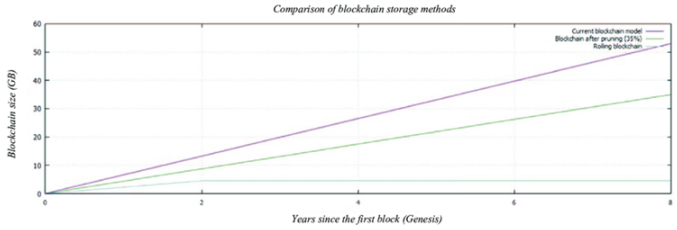

Figure 4*: Accuracy Comparison*

outperforming the traditional database system (82%) and RFID-based method (88%). The higher accuracy is primarily attributed to the immutable ledger structure and cryptographic hashing mechanism, which prevent duplication and unauthorized modification of product records. Additionally, the smart contract-based validation process eliminated manual intervention errors, thereby improving the reliability of counterfeit detection as shown in Table 1 and table 2.

Figure 3 compares the authentication accuracy of the traditional database system, RFID-based tracking, and the proposed blockchain framework. The blockchain-based system achieves the highest accuracy (98%), outperforming RFID (88%) and traditional methods (82%). This improvement is due to immutable ledger storage, cryptographic hashing, and smart contract validation, which prevent duplication and data tampering. The graph clearly demonstrates the effectiveness of blockchain in eliminating counterfeit products and improving authentication reliability.

In terms of verification time, the proposed system required an average of 1.8 seconds for product validation, which is considerably faster than the traditional centralized system that required 4.5 seconds. This improvement is due to automated smart contract execution and decentralized validation, which reduce dependency on centralized servers. Even under increasing transaction loads, the system maintained stable throughput with minimal performance degradation, demonstrating good scalability characteristics.

Scalability analysis further indicated that as the number of transactions increased from 100 to 5,000, the latency increased moderately but remained within acceptable operational limits. Throughput showed only a slight decrease, confirming that the permissioned blockchain configuration efficiently handles higher transaction volumes. Moreover, tamper resistance testing showed that unauthorized attempts to modify product records were automatically rejected by the consensus mechanism, ensuring complete data integrity.

Overall, the experimental results confirm that the proposed blockchain framework provides enhanced security, improved authentication accuracy, faster verification, and robust scalability compared to conventional product authentication systems. These findings validate the feasibility of deploying blockchain technology for large-scale counterfeit elimination in real-world supply chain environments.

Conclusion

This paper presented a blockchain-based framework for product authentication and counterfeit elimination. By integrating QR codes, smart contracts, and decentralized ledger technology, the system ensures secure, transparent, and tamper-proof tracking across the supply chain. Experimental evaluation demonstrated superior accuracy, reduced verification time, and enhanced scalability compared to traditional centralized systems.

Future work includes integration with IoT sensors, AI-based anomaly detection, and hybrid blockchain optimization to reduce gas costs and latency.

References

1. R. S. Baker and K. Yacef, “The state of educational data mining in 2009: A review and future visions,” Journal of Educational Data Mining, vol. 1, no. 1, pp. 3–17, 2009.
2. P. Naresh, & Suguna, R. (2021). IPOC: An efficient approach for dynamic association rule generation using incremental data with updating supports. Indonesian Journal of Electrical Engineering and Computer Science, 24(2), 1084. https://doi.org/10.11591/ijeecs.v24.i2.pp1084-1090.
3. K. R. Chaganti, B. N. Kumar, P. K. Gutta, S. L. Reddy Elicherla, C. Nagesh and K. Raghavendar, "Blockchain Anchored Federated Learning and Tokenized Traceability for Sustainable Food Supply Chains," 2024 4th International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS), Gobichettipalayam, India, 2024, pp. 1532-1538, doi: 10.1109/ICUIS64676.2024.10866271.
4. P. Brusilovsky and E. Millán, “User models for adaptive hypermedia and adaptive educational systems,” in The Adaptive Web, Springer, 2007, pp. 3–53.
5. P. Naresh, B. Akshay, B. Rajasree, G. Ramesh and K. Y. Kumar, "High Dimensional Text Classification using Unsupervised Machine Learning Algorithm," 2024 3rd International Conference on Applied Artificial Intelligence and Computing (ICAAIC), Salem, India, 2024, pp. 368-372, doi: 10.1109/ICAAIC60222.2024.10575444.
6. Y. Wang, L. Chen, and S. Liang, “Multimodal learning analytics for adaptive personalized education systems,” IEEE Access, vol. 8, pp. 202312–202325, 2020.
7. T. Kavitha, K. R. Chaganti, S. L. R. Elicherla, M. R. Kumar, D. Chaithanya and K. Manikanta, "Deep Reinforcement Learning for Energy Efficiency Optimization using Autonomous Waste Management in Smart Cities," 2025 5th International Conference on Trends in Material Science and Inventive Materials (ICTMIM), Kanyakumari, India, 2025, pp. 272-278, doi: 10.1109/ICTMIM65579.2025.10988394.
8. Z. A. Pardos and N. T. Heffernan, “KT-IDEM: Introducing item difficulty to the knowledge tracing model,” in User Modeling, Adaptation, and Personalization (UMAP), 2011, pp. 243–254.
9. Swasthika Jain, T. J., Sardar, T. H., Sammeda Jain, T. J., Guru Prasad, M. S., & Naresh, P. (2025). Facial Expression Analysis for Efficient Disease Classification in Sheep Using a 3NM-CTA and LIFA-Based Framework. IETE Journal of Research, 1–15. https://doi.org/10.1080/03772063.2025.2498610.
10. G. Siemens, “Learning analytics: The emergence of a discipline,” American Behavioral Scientist, vol. 57, no. 10, pp. 1380–1400, 2013.
11. P. Naresh, S. V. N. Pavan, A. R. Mohammed, N. Chanti and M. Tharun, "Comparative Study of Machine Learning Algorithms for Fake Review Detection with Emphasis on SVM," 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS), Coimbatore, India, 2023, pp. 170-176, doi: 10.1109/ICSCSS57650.2023.10169190.
12. A. Pardo and G. Siemens, “Ethical and privacy principles for learning analytics,” British Journal of Educational Technology, vol. 45, no. 3, pp. 438–450, 2014.
13. N. Tripura, P. Divya, K. R. Chaganti, K. V. Rao, P. Rajyalakshmi and P. Naresh, "Self-Optimizing Distributed Cloud Computing with Dynamic Neural Resource Allocation and Fault-Tolerant Multi-Agent Systems," 2024 4th International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS), Gobichettipalayam, India, 2024, pp. 1304-1310, doi: 10.1109/ICUIS64676.2024.10866891.
14. Roy, R. E., Kulkarni, P., & Kumar, S. (2022, June). Machine learning techniques in predicting heart disease a survey. In 2022 IEEE world conference on applied intelligence and computing (AIC) (pp. 373-377). IEEE.
15. R. D. Pea, “The social and technological dimensions of scaffolding and related theoretical concepts for learning,” The Journal of the Learning Sciences, vol. 13, no. 3, pp. 423–451, 2004.
16. Madhu, M., Gurudas, V. R., Manjunath, C., Naik, P., & Kulkarni, P. (2023, April). Non-contact vital prediction using rppg signals. In 2023 IEEE International Conference on Contemporary Computing and Communications (InC4) (Vol. 1, pp. 1-5). IEEE.
17. K. R. Chaganti, P. V. Krishnamurty, A. H. Kumar, G. S. Gowd, C. Balakrishna and P. Naresh, "AI-Driven Forecasting Mechanism for Cardiovascular Diseases: A Hybrid Approach using MLP and K-NN Models," 2024 2nd International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS), Erode, India, 2024, pp. 65-69, doi: 10.1109/ICSSAS64001.2024.10760656.
18. Darshan, R., Janmitha, S. N., Deekshith, S., Rajesh, T. M., & Gurudas, V. R. (2024, March). Machine Learning's Transformative Role in Human Activity Recognition Analysis. In 2024 IEEE International Conference on Contemporary Computing and Communications (InC4) (Vol. 1, pp. 1-8). IEEE.
19. Kulkarni, P., & Rajesh, T. M. (2022). A multi-model framework for grading of human emotion using cnn and computer vision. International Journal of Computer Vision and Image Processing (IJCVIP), 12(1), 1-21.
20. P. Naresh, P. Namratha, T. Kavitha, S. Chaganti, S. L. R. Elicherla and K. Gurnadha Gupta, "Utilizing Machine Learning for the Identification of Chronic Heart Failure (CHF) from Heart Pulsations," 2024 4th International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS), Gobichettipalayam, India, 2024, pp. 1037-1042, doi: 10.1109/ICUIS64676.2024.10866468.
21. X. Ochoa and E. Duval, “Quantitative analysis of learning

object repositories," IEEE Transactions on Learning Technologies, vol. 2, no. 3, pp. 226–238, 2009.

22. Sachin, A., Penukonda, A., Naveen, M., Chitrapur, P. G., Kulkarni, P., & BM, C. (2025, June). NAVISIGHT: A Deep Learning and Voice-Assisted System for Intelligent Indoor Navigation of the Visually Impaired. In 2025 3rd International Conference on Inventive Computing and Informatics (ICICI) (pp. 848-854). IEEE.
23. SAI M, RAMESH P, REDDY DS. EFFICIENT SUPERVISED MACHINE LEARNING FOR CYBERSECURITY APPLICATIONS USING ADAPTIVE FEATURE SELECTION AND EXPLAINABLE AI SCENARIOS. Journal of Theoretical and Applied Information Technology. 2025 Mar 31;103(6).
24. Sivananda Reddy Elicherla, Dr. P E Sreenivasa Reddy, Dr. V Raghunatha Reddy and Sivaprasada Reddy Peddareddigari. "Agilimation (Agile Automation) - State of Art from Agility to Automation." International Journal for Scientific Research and Development 3.9 (2015): 411-416.
25. N. P, K. R. Chaganti, S. L. R. Elicherla, S. Guddati, A. Swarna and P. T. Reddy, "Optimizing Latency and Communication in Federated Edge Computing with LAFEO and Gradient Compression for Real-Time Edge Analytics," 2025 6th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI), Goathgaun, Nepal, 2025, pp. 608-613, doi: 10.1109/ICMCSI64620.2025.10883220.