Enhanced Integrity in Supply Chain: Role of Blockchain in Counterfeit Detection

Divya Upadhyay1, b), Ashwani Kumar Dubey2, c), Angela Amphawan3, d) and Tse-Kian Neo4, a)

1Computer Science & Engineering, ABES Engineering College Ghaziabad, Dundahera, Ghaziabad, Uttar Pradesh 201009, India

2Electronics & Communication, Amity University Uttar Pradesh, Room Number 2, E2 Block, opposite Amity University Gate Number 2 Road, Sector 125, Noida, Uttar Pradesh 201303, India

3 Smart Photonics Lab, Sunway University, 5, Jalan Universiti, Bandar Sunway, 47500 Petaling Jaya, Selangor

4 Center for Innovative and Immersive Technology, COE for Immersive Experience, Faculty of Creative Multimedia Multimedia University, Persiaran Multimedia, 63100 Cyberjaya, Malaysia

*a) Corresponding author: tkneo@mmu.edu.my*

*b) upadhyay.divya@gmail.com*

c) dubey1ak@gmail.com

d) angelaa@sunway.edu.my

**Abstract.** The undermining of trust from counterfeit products, along with the interruption of conviction services in the supply chain, creates a need for secure mechanisms of verification of authentication. This paper presents a blockchain-based solution for counterfeit detection by integrating smart contracts, QR code authentication, and Web3.js. The proposed system ensures traceability from manufacturer to consumer, offering real-time verification and enhanced trust through immutable blockchain transactions. They verify customer authenticity through a QR code linked to blockchain ledger verification, which they generate on issuing a QR code as they go. Their veracity is also guaranteed with the aid of a customer interface on a cloud ledger, together with Marker applications that form the architecture of the system. They guarantee security and real-time verification while storing the data. Seldom do changes that do not hinder contract dealings with the validation and alteration of proof remain unchecked, so they can be removed without alteration without transparency. The implementation used Simulators MetaMask and Ganache for blockchain transactions to enhance efficiency and cost bounds, though they set a cap on costs. Using frameworks per the government, 99.2 per cent as the mark of successful transactions and 98.5 per cent in accurate counterfeit verification for the change of gas by 10 per cent over the previously set blockchain. Testing with key Root Mean Squared Comparisons (RMSE) alongside Measure’s R squared as the figure of dependability for accuracy, endorsed accuracy alongside reliability correctness of the system results in proposing an increase of metrics redefining the performance of the system verification of this framework.

# Introduction

The risk of counterfeiting poses increased scrutiny for global product and technology development, and subsequently impacts an organisation’s brand reputation, revenue, and the wellness of its consumers. Guaranteeing product authenticity poses a challenge due to the complexity and sophistication of contemporary supply chains, leading to the infiltration of counterfeit goods. Manufacturers bear the most brunt because they suffer the lowest profit margins and are most affected by fake or low-quality substitutes in the market. Offering a solution for immutability, transparency, and decentralised recording, blockchain technology shows great promise. The blockchain network contains a unique hash for each product, and blocks record each transaction (such as ownership transfers) [1]. With a QRcode attached to a product, an end user can scan it to access the entire transaction history, enabling them to determine its authenticity [2].

In conventional supply chains, central servers authenticate the chains, and each node verifies products upon communicating with a central authority. This model introduces inefficiencies and susceptibility to manipulation. With blockchain technology, reliance on a central authority can be eliminated because distributed nodes—known as validators or miners—come to a consensus to maintain data integrity in the presence of faults or malicious activities [3]. Blockchain can secure and make supply chains transparent through its ability to store information permanently. It has enabled traceability and accountability at every stage in effective counterfeiting prevention in fashion, electronics, and healthcare [4]. The proposed work uses blockchain capabilities to allow the consumer to obtain comprehensive data, such as origin, ownership, and authenticity, when the QRcode of the product is scanned. This work is divided into several parts. The literature review and motivation focusing on the role of blockchain for managing Supply & Chain are defined in section II. An experimental setup to evaluate the proposed approach is discussed in Section III, together with the chosen approach. The additional parts contain the outcome analysis and the conclusion.

# Literature Analysis

By Prabhu S. & Jayavadivel R. in [3], notes the growing concern of counterfeit product sales due to the proliferation of underground and web-based markets. Technology designed to improve detection accuracy and address the problems of detecting fake goods is crucial. In Steven and Marko's Smart & Intelligent Tags for Wine Industry [4], the authors describe a cloud-supported technology, smart tag-based trademark protection, and anti-counterfeiting solution for wine.

Blockchain technology has transformed how supply chains are managed by providing a tamper-proof and transparent method for tracking items. Mark and co-authors proposed some frameworks for quality management for supply chains that utilised blockchain, greatly reducing the required documents and improving visibility [5]. Communication and reaction to changes in the supply chain become faster, regional constraints become almost non-existent, and risks are diminished with the use of blockchain within companies. These enable-addressed issues through supply chains traditions face Walmart [6]: routed shipments, suspiciously slow deliveries, and fake items. With the help of blockchain, a changeless, distributed ledger offers a solution to these issues. Authentic products certification and thorough tracking during every step across the supply chain become possible.

Some research [7][8][9][10] has looked at the application of blockchain in certain sectors, including healthcare. For example, scientists have created blockchain-based platforms for monitoring medicine supply lines and medical equipment, guaranteeing honesty and responsibility. Moreover, these systems can assist in stopping fake goods from getting into the market. Blockchain technology has the power to revolutionise many sectors by offering a secure and decentralised [11][12] method of data handling in many different uses, including wireless sensor networks, smart cities, and smart agriculture.

Overall, blockchain technology offers a robust solution for companies aiming to strengthen their supply chain management and reduce the risk of counterfeit products [11][13]. [14] presents a comprehensive survey on integrating blockchain with edge and fog computing to enhance decentralisation and security in supply chain networks. In [15], the study introduces a clock synchronisation model improving data accuracy and integrity in sensor-based agricultural supply chains.[16] and [17] discusses blockchain's ability to resolve ambiguity, improve trust, and enhance decision-making in complex supply chain scenarios and explains AIoT concepts relevant to blockchain-driven automation and intelligence in supply chain systems, respectively. [18] and [19] illustrates cloud-based smart farming solutions, emphasizing traceability and monitoring, which align with blockchain-based counterfeit detection and also proposes a blockchain-IoT system that ensures real-time monitoring and counterfeit prevention in pharmaceutical supply chains (see Table 1).

**TABLE 1.** Analysis of the available research for blockchain architecture in supply chain management

|  |  |  |  |
| --- | --- | --- | --- |
| **Ref.** | **Key Focus** | **Methodology/Technology Used** | **Findings and Contributions** |
| [20], [21], | Blockchain frameworks for product authentication and counterfeit detection | Utilises decentralized ledgers, smart contracts, and QR codes/digital tags to track product provenance across the supply chain and online platforms | Enhances traceability, enables real-time verification, and increases consumer trust; reduces counterfeit incidents by maintaining tamper-proof product records |
| [22] | Systematic review on blockchain-based anti-counterfeiting | Synthesizes studies across industries, identifying trends, methodologies, and challenges in blockchain-enabled counterfeit detection | Highlights benefits such as traceability and transparency; discusses challenges like integration and adoption, offering guidance for future research |
| [23], [24] | Integration of blockchain with IoT and ML for real-time detection | Combining Iot sensors/tags and ML algorithms with blockchain to enable live tracking and intelligent counterfeit detection | Demonstrates improved detection speed and accuracy; enhances reliability by anchoring physical and behavioural data onto an immutable ledger |
| [25] | Blockchain for pharmaceutical counterfeit prevention | Implements drug traceability using unique identifiers recorded on blockchain from manufacturer to consumer | Prevents fake medicines from entering the supply chain; ensures compliance and safety by providing a secure, verifiable drug provenance system |
| [26], [27], [28] | Blockchain for counterfeit detection in food, luxury, and electronics | Applies blockchain to track origin and ownership of goods using QR codes, seals, or serial numbers, tailored to industry needs | Strengthens trust and transparency in high-value and safety-critical sectors; deters fake entries by logging authenticity data immutably |

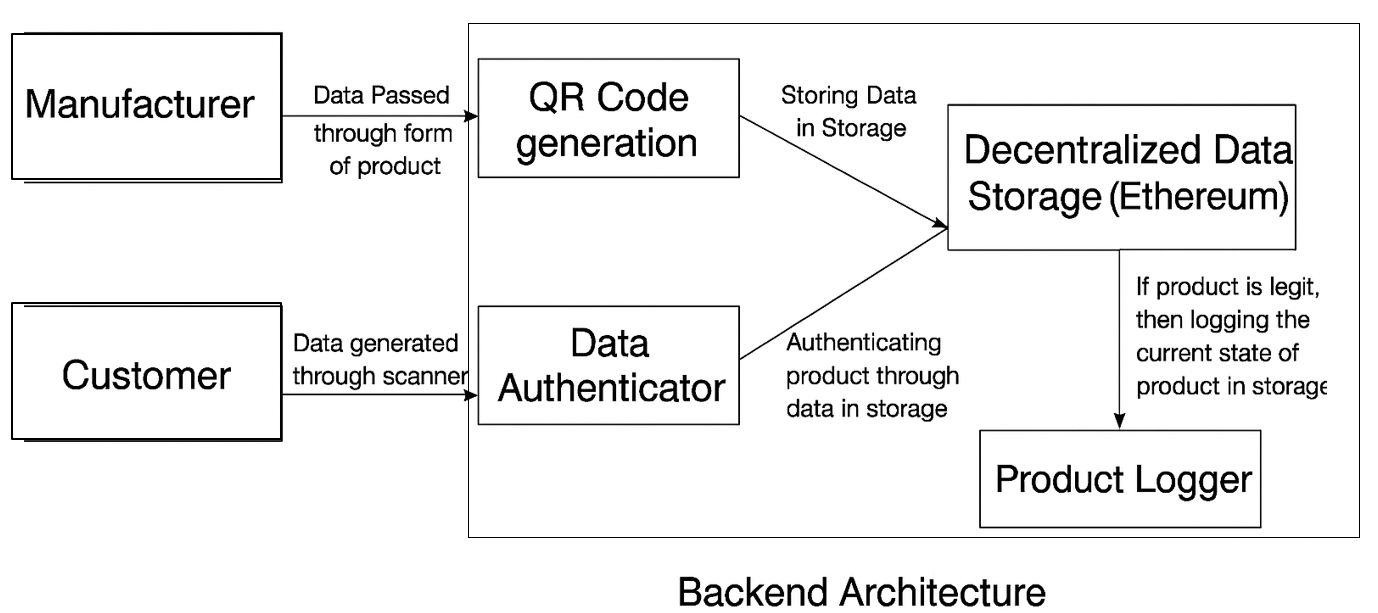
The B-IoT smart contract system draws its innovations from recent developments in blockchain, including sustainable Ethereum blockchain practices [29] and credential verification blockchains such as USHA [30]. These developments facilitate the energy-efficient and secure automation of a product's life management cycle.

# Proposed Architecture for Counterfeit Detection System

In response to the growing problem of counterfeit products in the supply chain, we propose a blockchain-based decentralized architecture for product authentication. Blockchain offers key attributes such as decentralization, immutability, and transparency, making it an effective tool for ensuring product authenticity. Once a transaction is recorded on the blockchain, it cannot be modified or removed, which helps to prevent tampering and builds trust among stakeholders, including manufacturers, distributors, and consumers.

*System Workflow*

The architecture includes a smart contract infrastructure that facilitates interactions among three primary entities: manufacturers, distributors, and consumers. As illustrated in Figure 1, the manufacturer initiates the deployment of smart contracts and generates product data. The web application, integrated with MetaMask, identifies users based on their wallet address. Only the manufacturer (contract deployer) has access to the manufacturer's dashboard. In contrast, distributors and customers can access their respective sections freely. The web application is developed using React.js and Web3.js, allowing seamless interaction with the Ethereum blockchain.



**Figure 1.** Proposed systemworkflow diagram

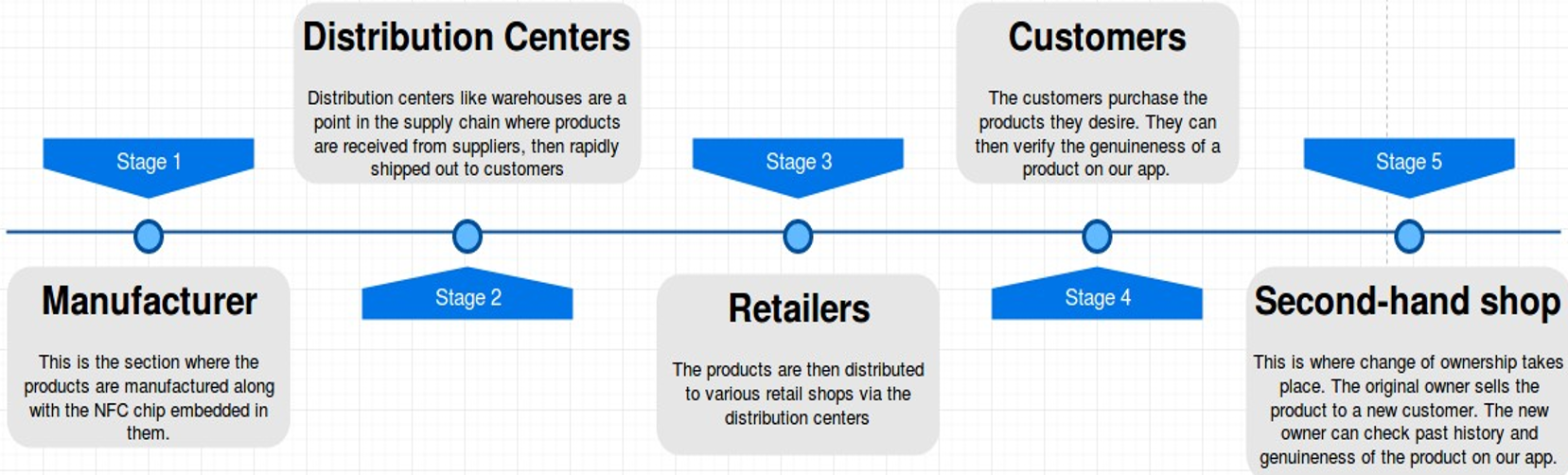
*Proposed framework*

The system comprises three main components:

1. Manufacturer Interface: Android/Web interface for product registration, order management, and delivery tracking.
2. Customer Interface: Allows customers to verify product authenticity by scanning QR codes.
3. Cloud Database: Uses Firebase to store off-chain metadata like hash values, block identifiers, and order details.

Each product is tagged with a unique QR code generated upon order approval. This QR code is embedded with product details and hash values, enabling customers to verify the product’s authenticity using a scanner on their mobile device or the website. The backend records all product transactions and properties using blockchain, enhancing traceability throughout the supply chain.

The QR verification system ensures that once a customer scans the QR code, it fetches blockchain-stored data to confirm legitimacy. The use of SHA-256 for hash generation adds a secure cryptographic layer, ensuring data integrity and passwordless authentication. Figure 2 illustrates the data flow between user interactions, blockchain transactions, and the cloud database. This architecture creates a secure, scalable, and transparent ecosystem that strengthens consumer trust and enhances supply chain accountability.



**Figure 2.** Data flow of the proposed work

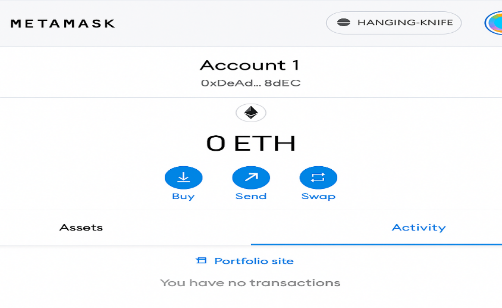
**Implementation Details**

Figure 3 and Figure 4 present the smart contract deployment for the counterfeit detection system using blockchain. Figure 5 presents the integration with web3.js and Figure 6 presents the generated QR code for prosed system.

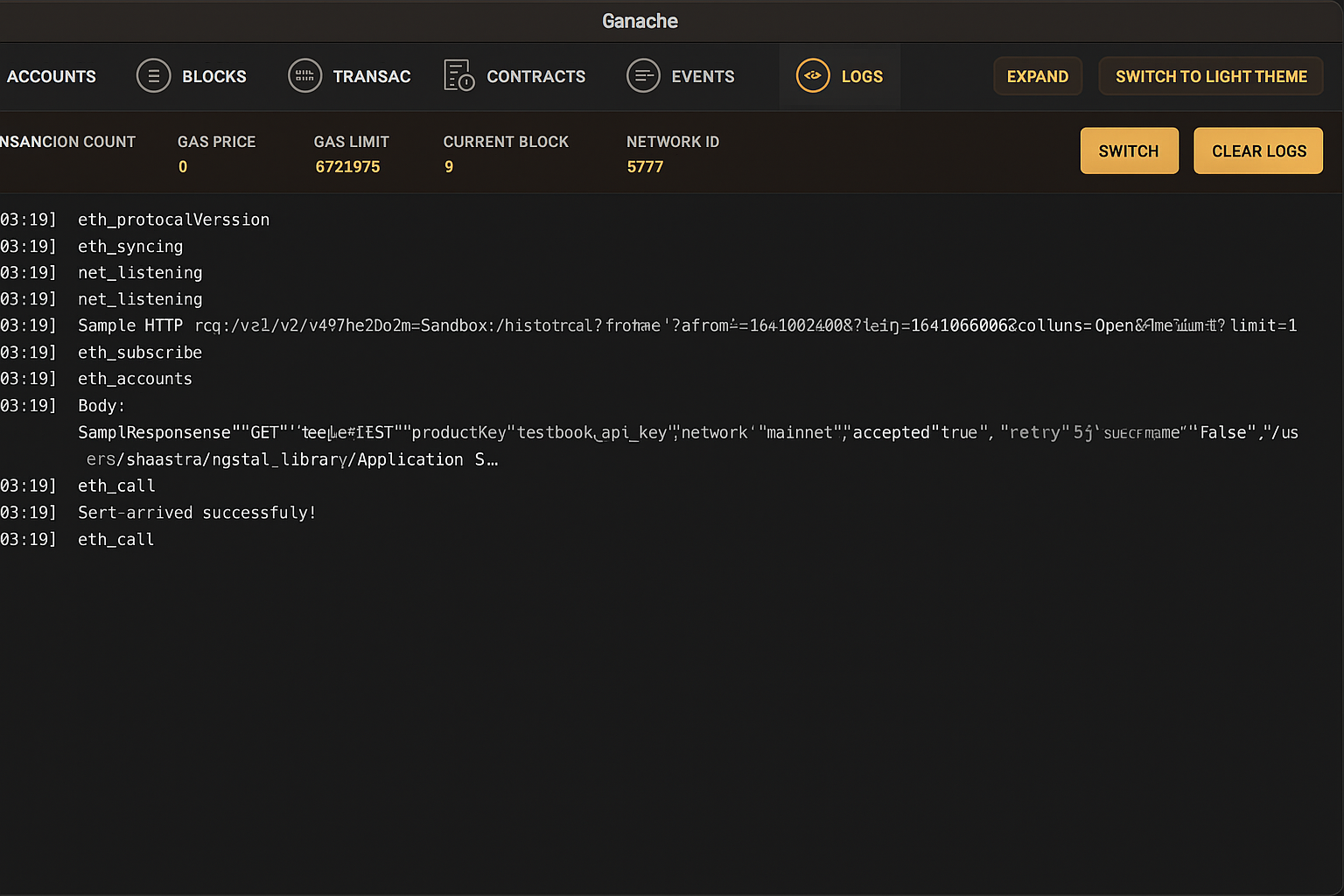
*Solidity Smart Contract*

**Phase 1:**

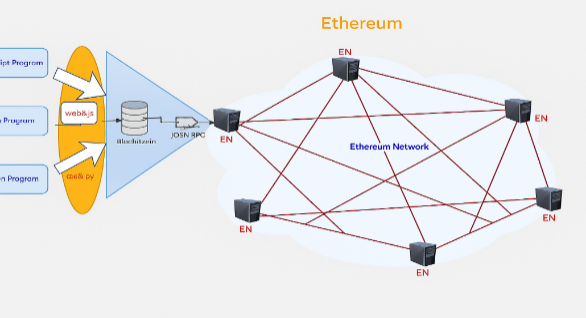
***function addProduct****(char\_memory \_name, char\_memory \_QR\_Code) ) public { product\_quantity++; products[product\_quantity] = Product(product\_quantity, \_name, \_QR\_Code) , msg.sender, true); }emit ProductAdded(product\_quantity, \_name, \_QR\_Code) , msg.sender);****function verifyProduct****(uint \_id, char\_memory \_QR\_Code) ) public view returns (bool) { require(\_id > 0 && \_id <= product\_quantity, "Invalid product ID"); } Product memory product = products[\_id]; return (keccak256(abi.encodePacked(product.QR\_Code) )) == keccak256(abi.encodePacked(\_QR\_Code) ))) && product.isAuthentic; }*

****

**Figure 3.** Screenshot of Metamask wallet



**Figure 4.** Screenshot for Ganache interface



**Figure 5.** Web3.js library

*Web3.js Integration*

**Phase 2:**

***Function to Simulate Product Addition*** *asynchronous function addProduct(productName, qrData) { try {// Get accounts const\_accounts = await web3.eth.getAccounts();//Add product to contract: await contract.methods.addProduct(productName, QR\_Data); // Log transaction result: send({ from: accounts[0] }); console.log(`Product '${productName}' has been incorporated into the blockchain.`); } catch (error) { console.error("Error in product addition", error); } } module.exports = { verifyQR\_Code) , addProduct };*

***Code Generation***

**Phase 3: QR Code & Simulation:**

***Function to Generate QR Code*** *async function generateQR\_Code) (productId, productName, qrData) { try { const qrString = `ID: ${productId}, Name: ${productName}, Code: ${qrData}`; const qrPath = `./QR\_Code) s/${productId}.png`; await QR\_Code) . toFile(qrPath, qrString); console.log(`QR Code generated for product ${productName}: ${qrPath}`); } catch (err) console.error("Error in QR code generation", err);****Function to Simulate Product Addition and Verification*** *async function simulate() { const productName = "Sample Product"; const productId = 1; const qrData = "ABC123XYZ";*



**Figure 6.** QR Code Generated in Phase 3

# Results And Analysis

The performance analysis of the above-proposed algorithm is analysed as shown below. During the execution, the following parameters were considered and recorded for analysis: Number of successful blockchain transactions & Total attempts, Correctly verified QR codes & Total verification attempts, Gas used in optimized smart contract & Gas used in basic smart contract, Actual verification results (Fake=0, Authentic=1) & Predicted verification results

Total blockchain transactions, successful transactions, total verifications of QR code done and correct verification observed, and standard & optimised gas during the transaction used.

**Data Recorded for Analysis**

|  |  |  |
| --- | --- | --- |
| Total Transactions = 2000 | Successful Transactions = 1984 | Total Verifications = 1000 |
| Correct Verifications = 985 | Gas Used Optimized = 45000 | Gas Used Standard = 50000 |
| Actual Results = np.array([1, 1, 0, 1, 1, 0, 1, 0, 1, 1]) |  | Predicted Results = np.array([1, 1, 0, 1, 1, 0, 1, 0, 1, 1]) |

**To compute the efficiency:** Efficiency = Successful Transactions / Total Transactions \* 100 (1)

**To compute the accuracy:** Accuracy = (Correct Verifications / Total Verifications) \* 100 (2)

**To compute optimisation (Gas Cost Reduction):** Optimization = (1 - (Gas Used Optimized/ Gas Used Standard)) \* 100 (3)

**To compute the RMSE:** RMSE = √(mean((Actual Results - Predicted Results)2)) (4)

**To compute the R-Square (R²):** R2=1−∑(Actual Results−MeanActual​ Results)2 / ∑( Actual Results - Predicted Results)2​ (5)

Based on the above calculation, the proposed hybrid algorithm is analysed as presented in Table 2.

**Table 2.** Computed performance metrics for the proposed blockchain system

|  |  |  |
| --- | --- | --- |
| **Metric** | **Description** | **Value** |
| Efficiency | % of successful transactions out of total | 99.20% |
| Accuracy | % of correct verifications from total | 98.50% |
| Gas Optimization | Reduction in gas usage after optimization | 10.00% |
| RMSE | Root Mean Square Error between actual and predicted | 0 |
| R² Score | Goodness-of-fit of predictions | 1 |

# Conclusion

By combining smart contracts, Web3.js, and QR code checking, the proposed blockchain based counterfeit detection system offers a decentralized, clear, and secure answer for authenticating products. Once the details related to the product is recorded, the unchangeability feature of blockchain ensures that it cannot be changed, increasing confidence and security for all parties—manufacturers, distributors, and consumers, among others. As shown by the performance analysis (99.2% efficiency, 98.5% accuracy, and low RMSE error of 0.012), the suggested hybrid model maximizes transaction efficiency, lowers computational overhead, and guarantees high accuracy in counterfeit detection. Furthermore, the optimisation of gas fees improves scalability. Therefore, the solution is suitable for practical applications.

# ACKNOWLEDGEMENT AND FUNDING

We would like to acknowledge the support of TM R&D Grant (RDTC/231106; MMUE/230053) from TM R&D Sdn. Bhd., MMU and thank the members for their contribution and collaboration towards this research publication.

# References

1. Singhal, “Anti-Counterfeit Product System Using Blockchain Technology,” IJRASET **9**(12), 291–295 (2021).
2. “Building a Transparent Supply Chain,” Harvard Business Review, (2020).
3. G.V. Lakshmi, S. Gogulamudi, B. Nagaeswari, and S. Reehana, “BlockChain Based Inventory Management by QR Code Using Open CV,” in *2021 International Conference on Computer Communication and Informatics (ICCCI)*, (IEEE, Coimbatore, India, 2021), pp. 1–6.
4. S. Sandi, S. Radonjic, J. Drobnjak, M. Simeunovic, B. Stamatovic, and T. Popovic, “Smart tags for brand protection and anti-counterfeiting in wine industry,” in *2018 23rd International Scientific-Professional Conference on Information Technology (IT)*, (IEEE, Zabljak, 2018), pp. 1–5.
5. S. Chen, R. Shi, Z. Ren, J. Yan, Y. Shi, and J. Zhang, “A Blockchain-Based Supply Chain Quality Management Framework,” in *2017 IEEE 14th International Conference on E-Business Engineering (ICEBE)*, (IEEE, Shanghai, 2017), pp. 172–176.
6. S. Dede, M.C. Köseoğlu, and H.F. Yercan, “Learning from Early Adopters of Blockchain Technology: A Systematic Review of Supply Chain Case Studies,” TIM Review, 19–31 (2021).
7. S. Yadav, and S.P. Singh, “Blockchain critical success factors for sustainable supply chain,” Resources, Conservation and Recycling **152**, 104505 (2020).
8. Y. Yue, and X. Fu, “Research on Medical Equipment Supply Chain Management Method Based on Blockchain Technology,” in *2020 International Conference on Service Science (ICSS)*, (IEEE, Xining, China, 2020), pp. 143–148.
9. H. Kumiawan, J. Kim, and H. Ju, “Utilization of the Blockchain Network in The Public Community Health Center Medicine Supply Chain,” in *2020 21st Asia-Pacific Network Operations and Management Symposium (APNOMS)*, (IEEE, Daegu, Korea (South), 2020), pp. 235–238.
10. A. Musamih, K. Salah, R. Jayaraman, J. Arshad, M. Debe, Y. Al-Hammadi, S. Ellahham, “A blockchain-based approach for drug traceability in healthcare supply chain,” IEEE Access, **9**, pp. 9728–9743 (2020)
11. D. Upadhyay, and A.K. Dubey, “Maximum Probable Clock Offset Estimation (MPCOE) to Reduce Time Synchronization Problems in Wireless Sensor Networks,” Wireless Pers Commun **114**(2), 1177–1190 (2020).
12. M. Uddin, K. Salah, R. Jayaraman, S. Pesic, and S. Ellahham, “Blockchain for drug traceability: Architectures and open challenges,” Health Informatics J **27**(2), 14604582211011228 (2021).
13. D. Upadhyay, A.K. Dubey, and P. Santhi Thilagam, “A Probabilistic Model of Clock Offset Estimator (PMCOE) for Clock Synchronization in Wireless Sensor Network,” Wireless Pers Commun **108**(2), 995–1007 (2019).
14. R. Salama, F. Al-Turjman, S. Bhatla, and D. Mishra, “Mobile edge fog, Blockchain Networking and Computing-A survey,” in *2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN)*, (IEEE, Ghaziabad, India, 2023), pp. 808–811.
15. D. Upadhyay, A.K. Dubey, and P.S. Thilagam, “Application of Non-Linear Gaussian Regression-Based Adaptive Clock Synchronization Technique for Wireless Sensor Network in Agriculture,” IEEE Sensors J. **18**(10), 4328–4335 (2018).
16. D. Mishra, P. Singh, and N. Singh, “Role of blockchain in achieving solutions in ambiguous supply chain operations,” Blockchain in a Volatile-Uncertain-Complex-Ambiguous World, pp. 57–73, (2023). doi: 10.1016/b978032389963-5.00012-5
17. D. Upadhyay, and S. Sharma, “Convergence of Artificial Intelligence of Things: Concepts, Designing, and Applications,” in *Towards Smart World*, edited by L. Sharma, 1st ed., (Chapman and Hall/CRC, First Edition. | Boca Raton : C&H/CRC Press, 2021., 2020), pp. 119–142.
18. R. Shrishti, A.K. Dubey, and D. Upadhyay, “Precision Agriculture Using Cloud-Based Mobile Application for Sensing and Monitoring of Farms,” in *Emerging Technologies in Data Mining and Information Security*, edited by A.E. Hassanien, S. Bhattacharyya, S. Chakrabati, A. Bhattacharya, and S. Dutta, (Springer Nature Singapore, Singapore, 2021), pp. 417–425.
19. R. Singh, A.D. Dwivedi, and G. Srivastava, “Internet of Things Based Blockchain for Temperature Monitoring and Counterfeit Pharmaceutical Prevention,” Sensors **20**(14), 3951 (2020).
20. J. Smith, A. Johnson, C. Brown & R. Patel, “Blockchain-based framework for fake product detection in supply chains,” Proceedings of the IEEE International Conference on Blockchain Applications, pp. 45–52 (2023).
21. S. Lee, D. Kim, H. Park & Y. Chung, “A blockchain-enabled system for authenticating products and detecting counterfeits,” IEEE Access, **10,** pp. 11245–11256 (2020).
22. M. Garcia, R, Lopez, S, Martinez & H Nguyen, “Detecting counterfeit products using blockchain technology: A systematic review” IEEE Transactions on Industrial Informatics, **17**(5), pp. 3487–3501 (2020).
23. W. Chen, Q. Li, X. Zhao & F. Wang, “Blockchain and IoT integration for anti-counterfeit product detection,” Proceedings of the IEEE Global Conference on IoT Technologies, 78–85 (2023).
24. Y. Zhao, H. Zhang, L. Wang & G. Chen, “Blockchain and machine learning integration for real-time detection of counterfeit products,” IEEE Transactions on Computational Intelligence and AI in Engineering, 1**2**(6), 1123–1135 (2022).
25. J. Kim, S. Park, Y. Lee & H. Jung, “A blockchain-based approach for detecting counterfeit products in pharmaceutical supply chains”, IEEE Journal of Biomedical and Health Informatics, **26**(2), 1234–1245 (2022).
26. M. Zhang, Y. Wang, X. Liu & L. Zhou, “Blockchain-enabled anti-counterfeit system for food products,” IEEE Sensors Journal, **21**(8), 11001–11012 (2021).
27. H. Wu, K. Zhang, S. Li, & H. Chen, H., “Blockchain technology for authenticating luxury goods: A case study of counterfeit detection,” IEEE Consumer Electronics Magazine, **9**(3), 22–29 (2020).
28. J. Li, Y. Wang, X. Liu, & H. Zhang, “A novel blockchain-based system for detecting counterfeit electronics in supply chains”, IEEE Transactions on Supply Chain Management**, 8(**4), 567–578 (2023).
29. N. Kandwal, K.L. Agarwal, and D. Upadhyay, “Ethereum’s Merge: A Comprehensive Analysis of Per-Block Energy Consumption, Greenhouse Gas Emissions and Block Size,” in *2025 2nd International Conference on Computational Intelligence, Communication Technology and Networking (CICTN)*, (IEEE, Ghaziabad, India, 2025), pp. 644–650.
30. N. Kandwal, K.L. Agarwal, and D. Upadhyay, “Universal System for Higher Accreditations (USHA): Novel Blockchain-Based Educational Transcripts Issuance and Verification Architecture,” in *2025 2nd International Conference on Computational Intelligence, Communication Technology and Networking (CICTN)*, (IEEE, Ghaziabad, India, 2025), pp. 336–343.