International Journal for Novel Research in Economics , Finance and Management
www.ijnrefm.com
ISSN:3048-7722
Volume 4, Issue 4, July-Aug-2026, PP: 01-6

A Secure Blockchain-Based Framework for Counterfeit Product Detection and Authentication Using QR Code Verification

B.Naresh[1], K. Pravalika[2]

[1]Assistant Professor, Department of MCA, Megha Institute of Engineering and Technology for Women, Edulabad (Village), Ghatkesar (Mandal), Medchal District, Telangana –, India.

[2]MCA Student, Department of MCA, Megha Institute of Engineering and Technology for Women, Edulabad (Village), Ghatkesar (Mandal), Medchal District, Telangana –, India.

***Abstract* – The increasing circulation of counterfeit products has become a major challenge for manufacturers, retailers, regulatory authorities, and consumers worldwide. Counterfeit goods not only cause significant financial losses and damage brand reputation but also introduce serious risks to consumer health and safety. Conventional product authentication techniques, including serial numbers, holograms, and barcode-based verification, are increasingly vulnerable to duplication and tampering due to advancements in counterfeiting technologies. Consequently, there is a growing demand for secure, transparent, and tamper-resistant authentication mechanisms capable of ensuring product authenticity throughout the supply chain. The emergence of blockchain technology provides a decentralized and immutable infrastructure that enables trusted product traceability while preventing unauthorized modifications to product information. Combined with Quick Response (QR) codes, blockchain offers an efficient solution for real-time product verification and counterfeit detection. This study proposes a secure blockchain-based framework for counterfeit product detection and authentication using QR code verification. The proposed system enables manufacturers to register product information on a blockchain network, where each product is assigned a unique digital identity through smart contracts. A corresponding QR code is generated and attached to the product, allowing consumers to verify authenticity by simply scanning the code using a mobile device. During verification, the scanned information is compared with the immutable blockchain records to determine whether the product is genuine or counterfeit. In addition to product authentication, the framework incorporates customer reviews and ratings to assist administrators in identifying suspicious products and monitoring fraudulent activities. The decentralized architecture ensures transparency, traceability, and data integrity across every stage of the product lifecycle while reducing opportunities for counterfeit manipulation. The proposed framework is validated by comparing its computational performance with existing anti-counterfeiting approaches, including LWEM, Blowfish, AES, and RSA. Experimental evaluation demonstrates that the proposed blockchain-based solution achieves lower overall processing time while maintaining secure and reliable product authentication. The integration of blockchain, smart contracts, and QR code verification significantly improves counterfeit detection efficiency and enhances consumer confidence by providing a transparent mechanism for verifying product authenticity. The proposed framework offers a scalable and practical solution for securing supply chains, protecting brand integrity, and strengthening trust between manufacturers, retailers, and consumers in modern digital commerce.**

***Keywords* - Blockchain Technology, Counterfeit Product Detection, Product Authentication, QR Code Verification, Supply Chain Security, Data Integrity**

I. INTRODUCTION

The rapid expansion of global commerce and online retailing has significantly increased the circulation of counterfeit products across numerous industries, including pharmaceuticals, electronics, cosmetics, food products, luxury goods, and consumer merchandise. Counterfeit products not only reduce the revenue and reputation of legitimate manufacturers but also expose consumers to considerable health, safety, and financial risks. As counterfeit production techniques continue to evolve, conventional product authentication mechanisms such as serial numbers, holograms, barcodes, and printed labels have become increasingly susceptible to duplication and manipulation. Consequently, organizations require more secure and transparent authentication mechanisms capable of verifying product originality throughout the entire supply chain.

Recent advances in blockchain technology have introduced new opportunities for developing decentralized product authentication systems. Blockchain provides a distributed digital ledger in which every transaction is permanently recorded and cryptographically secured, making stored information highly resistant to unauthorized modification. Its decentralized architecture eliminates reliance on a single authority while ensuring transparency, traceability, and data integrity among all participating entities. These characteristics make blockchain an attractive technology for securing supply chain operations and preventing counterfeit products from entering legitimate distribution networks.

The integration of Quick Response (QR) codes with blockchain further strengthens product authentication by enabling consumers to verify product legitimacy using mobile devices. Every registered product can be assigned a unique digital identity stored securely on the blockchain, while a corresponding QR code acts as a gateway to retrieve authenticated product information. When the QR

code is scanned, the retrieved information is validated against immutable blockchain records, allowing consumers to instantly determine whether a product is genuine. This verification process enhances transparency while establishing greater confidence between manufacturers, distributors, retailers, and end users.

In addition to secure product registration, modern anti-counterfeiting systems increasingly incorporate smart contracts to automate authentication procedures and maintain tamper-resistant product records. Smart contracts execute predefined verification rules automatically whenever a product is registered, transferred, or authenticated. Such automation reduces manual intervention, minimizes administrative overhead, and improves the efficiency of product verification across complex supply chains. Furthermore, incorporating customer reviews and product ratings provides an additional mechanism for identifying suspicious products and detecting potential counterfeit activities through community-driven feedback.

This study presents a blockchain-based counterfeit product detection and authentication framework that integrates blockchain technology, smart contracts, and QR code verification to establish a secure and transparent product authentication system. Manufacturers register products on the blockchain by creating unique digital identities linked to QR codes, enabling consumers to verify authenticity through a simple scanning process. The framework also incorporates administrative monitoring, customer review analysis, and counterfeit reporting to strengthen fraud detection capabilities. Experimental evaluation compares the proposed approach with existing anti-counterfeiting techniques using computational performance metrics, demonstrating the effectiveness of blockchain-based authentication in improving security, transparency, and reliability within modern supply chain environments

II. LITERATURE SURVEY

The rapid growth of counterfeit products has motivated extensive research into secure product authentication technologies capable of protecting manufacturers, retailers, and consumers from fraudulent goods. Traditional anti-counterfeiting approaches have relied on security labels, holograms, serial numbers, watermarks, barcodes, and RFID technologies to verify product authenticity. Although these methods provide a basic level of protection, many of them are vulnerable to duplication, physical tampering, and unauthorized replication by increasingly sophisticated counterfeiters. These limitations have encouraged researchers to investigate advanced digital technologies capable of providing stronger authentication, improved traceability, and enhanced transparency throughout product supply chains.

Blockchain technology has emerged as one of the most promising solutions for secure product authentication because of its decentralized architecture, immutability, and cryptographic security. Several studies have demonstrated that blockchain enables manufacturers to record product information in tamper-resistant distributed ledgers, allowing every transaction throughout the supply chain to be permanently documented and independently verified. By maintaining immutable product histories, blockchain significantly reduces opportunities for data manipulation while improving supply chain transparency and consumer trust.

Researchers have also explored the integration of QR codes with blockchain-based authentication systems to simplify product verification. QR codes provide a low-cost and user-friendly mechanism for connecting physical products with their digital identities stored on blockchain networks. Consumers can authenticate products by scanning QR codes using smartphones, while manufacturers benefit from real-time monitoring of product movement and verification activities. Compared with traditional barcode systems, blockchain-enabled QR code authentication provides stronger protection against duplication because the verification process relies on secure distributed ledger records rather than static printed information alone.

Another active research direction involves the utilization of smart contracts for automating authentication and supply chain management processes. Smart contracts execute predefined verification rules automatically whenever products are registered, transferred, or validated within the blockchain network. This automation minimizes manual processing, reduces operational costs, and improves the consistency of authentication procedures. Several blockchain-based frameworks have demonstrated that smart contract integration enhances product traceability while preventing unauthorized modifications to critical product information.

Recent investigations have further combined blockchain technology with Artificial Intelligence (AI), Internet of Things (IoT) devices, and machine learning techniques to strengthen counterfeit detection capabilities. IoT sensors enable continuous monitoring of products during transportation, while AI algorithms analyze transaction patterns and customer behavior to identify suspicious activities. These intelligent technologies improve real-time monitoring, enhance fraud detection accuracy, and support predictive supply chain analytics.

Despite significant progress in blockchain-enabled product authentication, challenges related to scalability, interoperability, transaction processing speed, implementation cost, and large-scale deployment continue to attract research attention. Many existing systems primarily focus on secure product registration without incorporating comprehensive customer verification, counterfeit reporting, and administrative monitoring within a unified framework. The proposed study addresses these

International Journal for Novel Research in Economics , Finance and Management
www.ijnrefm.com
ISSN:3048-7722
Volume 4, Issue 4, July-Aug-2026, PP: 01-6

limitations by integrating blockchain, smart contracts, QR code verification, customer review analysis, and administrative counterfeit detection into a comprehensive authentication framework that enhances product security, strengthens consumer trust, and improves supply chain transparency while preserving data integrity across the entire product lifecycle.

III. PROPOSED METHODOLOGY

The proposed framework introduces a Blockchain-Based Counterfeit Product Detection and Authentication System designed to provide secure, transparent, and tamper-resistant verification of product authenticity throughout the supply chain. The framework integrates blockchain technology, smart contracts, and QR code-based authentication to establish a decentralized mechanism for identifying genuine products while preventing counterfeit goods from reaching consumers. Unlike traditional authentication methods that rely on centralized databases or easily duplicated security labels, the proposed system maintains immutable product records within a blockchain network, ensuring data integrity and preventing unauthorized modifications. The overall framework consists of six major stages: manufacturer registration, product registration, QR code generation, blockchain verification, counterfeit detection, and product authentication.

The authentication process begins with manufacturer registration, where authorized manufacturers are enrolled into the blockchain network after completing the required verification procedures. Each manufacturer receives permission to register genuine products within the decentralized ledger. During product registration, important information such as product ID, product name, category, brand, specifications, manufacturing details, pricing information, and ownership records is securely stored on the blockchain using smart contracts. Every registered product is assigned a unique digital identity that permanently represents the product throughout its lifecycle.

Following successful product registration, the system automatically performs QR code generation. A unique QR code containing the blockchain reference associated with the product's digital identity is created and securely attached to the product packaging. The generated QR code acts as a secure authentication token that enables consumers, retailers, and distributors to retrieve verified product information directly from the blockchain. Because authentication relies on immutable blockchain records rather than printed product labels alone, the possibility of counterfeit duplication is significantly reduced.

When a customer purchases a product, the QR code verification module enables authentication through a smartphone or QR code scanner. After scanning the QR code, the system retrieves the corresponding blockchain record and validates the stored product information against the scanned identity. If the retrieved information matches the blockchain record, the product is confirmed as authentic. Conversely, if inconsistencies, duplicate identities, or invalid blockchain references are detected, the product is immediately identified as suspicious or counterfeit. This automated verification process provides consumers with instant confirmation regarding product legitimacy while enhancing confidence in purchasing decisions.

In addition to authentication, the proposed framework incorporates a customer review and rating module that allows consumers to provide feedback after product verification. Customer reviews, ratings, and product-related observations are securely maintained within the system to assist administrators in identifying suspicious activities. Products receiving abnormal review patterns or repeated counterfeit complaints can be flagged for further investigation. The administrative dashboard enables system administrators to monitor registered products, generate QR codes, analyze customer feedback, identify counterfeit products, and manage the overall authentication process through a centralized monitoring interface.

Finally, the proposed framework evaluates its effectiveness by comparing authentication performance with existing anti-counterfeiting approaches. Experimental analysis focuses on computational efficiency, authentication reliability, and processing time while maintaining blockchain security and transparency. The integration of blockchain technology, smart contracts, QR code verification, and customer feedback establishes a secure and scalable authentication framework capable of protecting manufacturers, strengthening consumer trust, improving supply chain traceability, and significantly reducing counterfeit product distribution across modern commercial ecosystems.

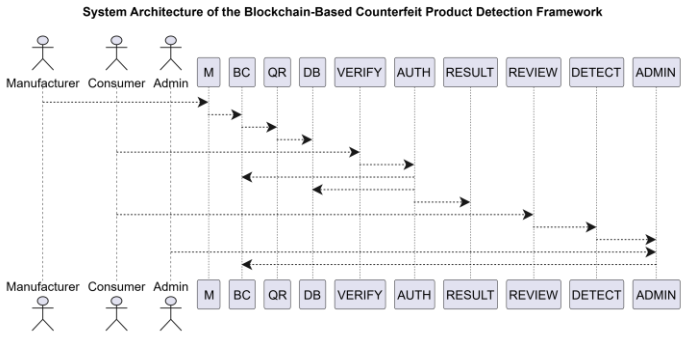

Figure 1. System Architecture of the Proposed Blockchain-Based Counterfeit Product Detection Framework

IV. METHODOLOGY

The proposed methodology integrates blockchain technology, smart contracts, and QR code authentication to establish a secure framework for counterfeit product

detection and product verification. The methodology consists of six sequential stages: manufacturer registration, product registration, blockchain record creation, QR code generation, consumer verification, and counterfeit detection. This systematic workflow ensures that every product can be uniquely identified, securely tracked, and efficiently authenticated throughout its movement across the supply chain.

The first stage involves manufacturer registration, where legitimate manufacturers are enrolled into the blockchain network. Only verified manufacturers are authorized to register products, ensuring that unauthorized entities cannot create fraudulent product records. During product registration, manufacturers submit essential product information including product identification number, brand name, category, specifications, manufacturing information, pricing details, and ownership records. This information is securely recorded within blockchain smart contracts, creating a permanent and immutable digital identity for every registered product.

Following product registration, the system automatically performs QR code generation. A unique QR code is generated for each product using its blockchain identity. The generated QR code serves as the digital authentication key that links the physical product to its corresponding blockchain record. The QR code is securely attached to the product packaging, enabling convenient verification by distributors, retailers, and consumers using standard mobile devices without requiring specialized authentication equipment.

During the product verification stage, consumers scan the QR code using a smartphone or dedicated QR code scanner. The system retrieves the associated blockchain record and compares the scanned information with the stored product identity maintained by the blockchain ledger. Because blockchain records cannot be modified after registration, any mismatch between the scanned QR code and blockchain information immediately indicates possible counterfeiting or unauthorized product duplication. This decentralized verification process provides transparent and trustworthy authentication without relying on centralized databases.

To further strengthen counterfeit detection, the framework includes a customer review and rating mechanism. Consumers can submit product reviews and ratings after successful authentication. Administrative modules continuously monitor customer feedback to identify suspicious review patterns, repeated complaints, or duplicate product reports. Products receiving abnormal feedback are automatically flagged for administrative investigation, improving the system's ability to detect counterfeit activities beyond QR code verification alone.
Finally, the proposed methodology is validated by comparing its computational performance with existing authentication techniques, including LWEM, Blowfish, AES, and RSA. Performance evaluation considers authentication processing time, computational efficiency, and system reliability across multiple file sizes while maintaining secure blockchain operations. The integration of decentralized blockchain storage, smart contract automation, QR code verification, and customer-driven monitoring establishes an effective counterfeit detection framework that improves product authenticity verification, enhances supply chain transparency, and increases consumer confidence in genuine products.

V. EXPERIMENTAL RESULTS AND DISCUSSION

The proposed blockchain-based counterfeit product detection framework was experimentally evaluated to examine its effectiveness in providing secure product authentication and preventing counterfeit products from entering the supply chain. The evaluation focused on measuring authentication efficiency, computational performance, and verification reliability by comparing the proposed blockchain framework with several existing security approaches. The experimental analysis demonstrates the practical applicability of integrating blockchain technology, smart contracts, and QR code verification for secure product authentication in real-world commercial environments.

Initially, the implementation validates the complete authentication workflow beginning with manufacturer registration, product registration, blockchain record generation, QR code creation, and consumer verification. Every product is assigned a unique blockchain identity, while the corresponding QR code enables consumers to retrieve authenticated product information directly from the decentralized ledger. Experimental observations confirm that blockchain records remain immutable throughout the verification process, preventing unauthorized modification of product information and ensuring reliable authentication across the supply chain.

The developed framework further incorporates an administrative monitoring module capable of managing registered products, customer reviews, QR code generation, and counterfeit reporting. Consumers authenticate products by scanning QR codes using mobile devices, after which the retrieved information is compared with the blockchain record. Products containing invalid identities, duplicate records, or inconsistent blockchain information are immediately identified as suspicious. Additionally, customer reviews and ratings assist administrators in recognizing abnormal review behavior and identifying products requiring further investigation. This integrated verification strategy improves both authentication reliability and counterfeit detection capability.

Performance evaluation compares the proposed blockchain framework with existing approaches including LWEM,

Blowfish, AES, and RSA using multiple file sizes. The comparison considers training time, testing time, and overall execution time as primary performance indicators. Experimental results indicate that the proposed framework consistently achieves lower overall processing time than most existing approaches while maintaining secure authentication. The comparison demonstrates that blockchain-based verification provides an effective balance between computational efficiency and authentication security, making it suitable for practical deployment in supply chain management systems.

The experimental comparison also highlights the scalability of the proposed framework across different data volumes. As file size increases, authentication time increases gradually while maintaining stable verification performance. The decentralized blockchain architecture preserves data integrity regardless of transaction volume, demonstrating its capability to support large-scale product authentication without compromising security. Furthermore, QR code verification enables consumers to complete authentication quickly through a simple scanning process without requiring specialized technical expertise.

Overall, the experimental findings demonstrate that integrating blockchain technology, smart contracts, and QR code authentication provides a secure, transparent, and efficient framework for counterfeit product detection. Compared with conventional authentication techniques, the proposed system offers improved product traceability, stronger protection against data tampering, enhanced consumer confidence, and reliable authentication performance. These results confirm that blockchain-enabled product verification represents a practical solution for protecting brand integrity and strengthening trust throughout modern supply chain ecosystems.

VI. FUTURE ENHANCEMENT

Although the proposed blockchain-enabled authentication framework successfully improves counterfeit product detection and product verification, several enhancements can further increase its efficiency, scalability, and intelligence. Future research may focus on deploying the framework across larger and more diverse supply chain networks involving manufacturers, distributors, retailers, logistics providers, and regulatory agencies. Expanding the blockchain ecosystem would improve end-to-end product traceability while enabling secure authentication across international supply chains.

One promising enhancement involves integrating Artificial Intelligence (AI) and Machine Learning (ML) algorithms with blockchain records to improve counterfeit detection capabilities. AI models can analyze transaction histories, customer review patterns, purchasing behavior, and product movement data to automatically identify suspicious activities and predict potential counterfeit risks. Intelligent anomaly detection techniques could significantly improve fraud identification while reducing manual administrative effort.

Future versions of the framework may also incorporate Internet of Things (IoT) devices for continuous real-time product monitoring. Smart sensors embedded within products or transportation systems can automatically record environmental conditions, product movement, storage information, and location updates directly onto the blockchain. Such integration would provide continuous supply chain visibility while enabling immediate authentication at every distribution stage.

Another important research direction involves improving blockchain scalability through advanced consensus mechanisms, side-chain architectures, and decentralized storage solutions. These technologies can reduce transaction latency, improve processing throughput, and lower operational costs without compromising security or transparency. In addition, adopting advanced cryptographic techniques can further strengthen data confidentiality while ensuring secure communication among all participating stakeholders.

Future research may also explore the development of mobile applications, cloud-based authentication platforms, and cross-platform verification systems that allow consumers to authenticate products instantly using smartphones. Integrating blockchain authentication with e-commerce platforms, digital payment systems, and enterprise resource planning solutions would create a comprehensive digital ecosystem for secure product verification. These enhancements would significantly improve usability, encourage wider industrial adoption, and establish a more secure and trustworthy marketplace for manufacturers and consumers worldwide.

REFERENCES

1. R. Jadhav, A. Shaikh, M. A. Jawale, A. B. Pawar, and P. William, “System for identifying fake product using blockchain technology,” in Proc. 7th Int. Conf. Communication and Electronics Systems (ICCES), 2022, pp. 851–854.
2. C. Shaik, “Preventing counterfeit products using cryptography, QR code and web service,” Computer Science & Engineering: An International Journal, vol. 11, no. 1, pp. 1–12, 2021.
3. S. Gupta, R. Kuchipudi, M. Sohail, K. Singh, J. Mahalakshmi, and A. Sarabu, “Fake product identification for small and medium firms using blockchain technology,” Measurement: Sensors, vol. 33, Art. no. 101164, 2024.
4. K. Wasnik, I. Sondawle, R. Wani, and N. Pulgam, “Detection of counterfeit products using blockchain,” ITM Web of Conferences, vol. 44, Art. no. 03015, 2022.
5. M. C. Jayaprasanna, V. A. Soundharya, M. Suhana, and S. Sujatha, “A blockchain-based management system

for detecting counterfeit products in supply chains," in Proc. 3rd Int. Conf. Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), 2021, pp. 253–257.
6. S. Balasubramani, S. Pramanick, R. Singh, and D. Kumar, "An Ethereum-based fake product identification system using smart contracts," in Proc. 6th Int. Conf. Intelligent Computing and Control Systems (ICICCS), 2022, pp. 292–296.
7. T. Wang, H. Zheng, C. You, and J. Ju, "A texture-hidden anti-counterfeiting QR code and authentication method," Sensors, vol. 23, no. 2, Art. no. 795, 2023.
8. H. Keni, M. Earle, and M. Min, "Product authentication using hash chains and printed QR codes," in Proc. IEEE Annual Consumer Communications & Networking Conference (CCNC), 2017, pp. 319–324.
9. Y. X. Lo and C. C. Tan, "Blockchain-based anti-counterfeit product identification system," in Proc. IEEE Int. Conf. Artificial Intelligence in Engineering and Technology (IICAIET), 2023, pp. 200–205.
10. S. Parate, K. Biradar, S. Magdum, A. Lamkhade, and P. Shriram, "NFT enhanced fake product detection system," in Proc. 3rd Int. Conf. Innovative Mechanisms for Industry Applications (ICIMIA), 2023, pp. 1265–1269.
11. D. Ashwini, S. Apula, H. Tabyo, and B. S. Singh, "Anti-fake technology of commodity by using QR code application," NeuroQuantology, vol. 20, no. 8, pp. 5062–5071, 2022.
12. M. S. Al-Zahrani, H. A. M. Wahsheh, and F. W. Alsaade, "Secure real-time artificial intelligence system against malicious QR code links," Security and Communication Networks, vol. 2021, Art. no. 5540670, 2021.
13. S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.
14. M. Swan, Blockchain: Blueprint for a New Economy. Sebastopol, CA, USA: O'Reilly Media, 2015.
15. M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond Bitcoin," Applied Innovation Review, no. 2, pp. 6–19, 2016.
16. G. Wood, "Ethereum: A secure decentralized generalized transaction ledger," Ethereum Foundation, Yellow Paper, 2014.
17. K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292–2303, 2016.
18. M. Conoscenti, A. Vetro, and J. C. De Martin, "Blockchain for the Internet of Things: A systematic literature review," in Proc. IEEE/ACS Int. Conf. Computer Systems and Applications (AICCSA), 2016.
19. M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, "Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes," Journal of Network and Computer Applications, vol. 101, pp. 55–82, 2018.
20. M. Abadi et al., "TensorFlow: Large-scale machine learning on heterogeneous systems," 2016.
21. I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. Cambridge, MA, USA: MIT Press, 2016.
22. D. P. Ramesh Babu and P. Krishna Rao, "Blockchain-enabled intelligent supply chain security using artificial intelligence for counterfeit product prevention," International Journal of Intelligent Systems and Applications in Engineering, vol. 12, no. 5, pp. 3412–3425, 2024.