Blockchain-Powered Solution for Authenticating Genuine Products

Corresponding Author: **Mrs. V. Priyadharsini**, M.Tech.,(Ph.D),
Assistant Professor **Archana**, **Geethica Jayalakshmi**, **Devi**
Department of Information Technology, Panimalar Engineering College, Chennai-600123, India

Abstract

The spread of fake goods poses serious problems for industries like luxury goods, electronics, fashion, and pharmaceuticals, leading to monetary losses, harm to brand reputation, and a decline in consumer confidence. Conventional authentication techniques, like QR codes, RFID tags, and centralized databases, are insufficient for effective counterfeit deterrence because they are susceptible to duplication, tampering, and security flaws. To address these issues, this paper suggests a blockchain-based authentication system that uses a decentralized, transparent, and impenetrable ledger to confirm the legitimacy of products. The proposed framework makes it simple to verify product information by using MetaMask for secure user interactions and Ganache to simulate a local blockchain network. By automating procedures like product registration, ownership tracking, and authentication, smart contracts make sure that data is indestructible and verifiable throughout the supply chain. Blockchain technology greatly increases transparency and cuts the risk of fraud through doing away with the need for centralized systems. By scanning a QR code connected to blockchain records, customers can instantly access the product's history and confirm the authenticity of the product. This strategy strengthens consumer confidence and improves supply chain security. To improve counterfeit prevention and authentication techniques even more, future advancements could involve AI-driven fraud detection, predictive analytics, and IoT-enabled real-time tracking.

Index Terms: Blockchain, Product Authentication, Smart Contracts, Fraud Prevention, MetaMask, Ganache, QR Code

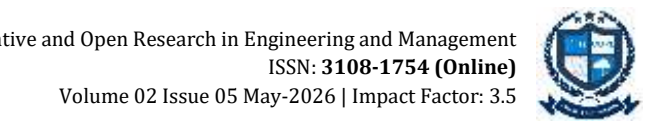
I INTRODUCTION

The proliferation of fake goods presents an important issue for sectors like luxury goods, electronics, fashion, and pharmaceuticals. It can result in large financial losses, harm to a brand's reputation, and even endanger consumer safety. Traditional authentication methods like QR codes, RFID tags, and centralized databases have proven limited as counterfeiters use more sophisticated techniques because of their susceptibility to tampering, duplication, and security flaws. These problems show how urgently a more transparent, reliable, and impenetrable authentication system is needed. A decentralized, unchangeable, and transparent framework for hindering counterfeiting is offered by blockchain technology. In contrast to conventional methods, blockchain ensures that product authentication data is safe and verifiable, strengthening supply chain tracking and trust.

The suggested system enables smooth and real-time product authenticity verification by using MetaMask for secure transactions and Ganache for blockchain simulation. By automating product registration, ownership tracking, and verification through smart contracts, this blockchain-based system for authentication greatly reduces the probability of a scam. By scanning a QR code linked to blockchain records, consumers can instantly access verified product information and verify the legitimacy of products. Future advances, such as IoT-enabled tracking and AI-driven fraud detection, will strengthen supply chain security, cease counterfeiting, and boost consumer confidence in a variety of industries.

II LITERATURE REVIEW

Blockchain technology[1], known for its decentralized and tamper-proof data management, has gained recognition as a secure and efficient solution for supply chain security and product authentication. Studies have demonstrated its ability to enhance transparency, traceability, and fraud prevention across various industries. Bohli and Gruschka (2013) investigated blockchain applications in secure computing, emphasizing the need for greater accuracy. Chen et al. (2017) introduced a blockchain-based supply chain model, but overlooked outsourced distribution, affecting its scalability. Toyoda et al. (2017) developed a product ownership management system utilizing



blockchain; however, accuracy limitations impacted its reliability. Ma et al. (2020) proposed a blockchain-powered anti-counterfeiting framework[13], yet unclear implementation strategies posed challenges. Singhal (2021) explored blockchain's role in counterfeit prevention, identifying issues related to accountability and traceability[10]. While existing studies highlight blockchain's potential, they also expose gaps in accuracy, scalability, and real-time verification. The proposed system aims to address these shortcomings by incorporating smart contracts, [4]MetaMask for secure transactions, and QR code-based authentication, ensuring a more reliable, efficient, and tamper-resistant counterfeit detection mechanism.

III PROPOSED SYSTEM AND ARCHITECTURE

The proposed blockchain-based authentication system aims to provide a decentralized, clear, and safe system for verifying the authenticity of goods[2]. Unlike conventional authentication methods that rely on centrally maintained databases, QR codes, or RFID tags that are vulnerable to fraud and tampering, this solution uses blockchain technology to create an unchangeable and legitimate record of product history. In the course of manufacturing, each product is assigned a Unique Identification Token (UID), which is subsequently recorded on the blockchain along with pertinent details including the serial number, manufacturing date, and ownership information. As the product moves from manufacturers to warehouses, distributors, and retailers, smart contracts are used to safely document each transaction. Consumers may verify the legitimacy of the product by scanning a QR code or entering its information[3][4].

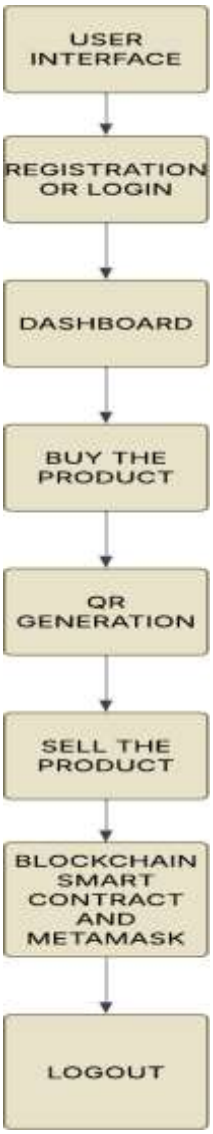


Figure 1. Architecture

IV SYSTEM MODULES

The proposed system comprises several essential modules, each aimed at improving usability, security, and efficiency in product authentication. These modules facilitate smooth interactions, secure authentication, and real-time verification utilizing blockchain technology[5].

1. Module for User Interface (UI)

Both desktop and mobile platforms can benefit from the user interface's responsive and intuitive design[1]. It includes functionalities such as search capabilities, tooltips, and support for multiple languages to enhance accessibility. Interactive

components like buttons and cards facilitate user navigation for product verification and account management.

2. Login Module

Users can authenticate securely through various methods, including username/password, blockchain wallet (private/public keys), or biometric login[2]. The module supports two-factor authentication (2FA) and password reset options to bolster security. Enterprise users have the option to implement Single Sign-On (SSO) for streamlined access, with session tokens ensuring ongoing authentication.

3. Dashboard Module

This module offers a comprehensive overview of transactions, verifications, and supply chain activities[4]. It presents real-time analytics regarding counterfeit detection and interaction history. The interface is customizable, featuring filters, notifications, and alerts for pending verifications.

4. Blockchain Integration Module

This module stores product information on a decentralized blockchain, guaranteeing immutability and security. Smart contracts oversee product registration, verification, and ownership transfers. Consensus mechanisms are employed to validate transactions, thereby preventing data tampering. It accommodates both public and private blockchain networks based on specific requirements[5].

5. Product Verification Module

This module allows users to scan QR codes or NFC tags for product authentication. It retrieves product information from the blockchain, including origin, batch number, and certification status[2]. Immediate feedback is provided, indicating whether the product is authentic or counterfeit. Ownership changes are updated in real-time, ensuring secure and transparent verification.

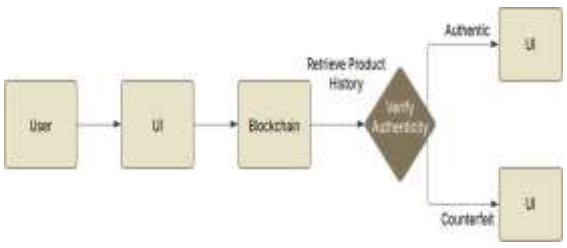


Figure 2. Product Verification

V IMPLEMENTATION

Development Tools

Ethereum serves as the foundational blockchain network for the development of the blockchain-powered authentication system, and Ganache offers a local testing and deployment environment. Smart contracts, which are essential for safely storing product authenticity data on the blockchain, are created and implemented using Solidity[6]. MetaMask is integrated as a digital wallet for handling transactions and gas fees in order to guarantee a seamless user experience. Because the frontend is constructed with Web3.js and React.js, users may interact with blockchain-based data with ease. Additionally, Node.js serves as the backend framework, dealing with API requests and facilitating efficient communication between the user interface and the blockchain network.

Smart Contract Functionality

Product registration, verification, and duplicate avoidance are the three main tasks that the smart contract is designed to carry out. A distinct hash is given to the producer upon product registration, and this hash is safely saved on the blockchain[7]. By accessing information from the blockchain, the verification function allows customers to scan a product's ID and verify its legitimacy. The contract enforces duplicate prevention to protect the system's integrity. This means that each product ID is only registered once, preventing fraudulent efforts to register the same product more than once.

VI TRADITIONAL VS. BLOCKCHAIN-BASED AUTHENTICATION

Product verification has long made use of typical authentication models like barcodes, RFID tags, QR codes, and centralized databases. These techniques do have a few inherent limitations though, such as being vulnerable to manipulation, relying upon the trust of third parties, and having centralized control, which can result in data breaches or counterfeiting. In contrast, blockchain technology offers a decentralized, unalterable ledger, guaranteeing increased security and openness. The primary differences between the blockchain-based approach and conventional methods of authentication are presented in this

section. The contrast of blockchain-based authentication systems and conventional authentication methods is shown in the table below:

Feature	Traditional Systems	Proposed Blockchain-Based System
Security	Prone to hacking and data manipulation	Tamper-proof due to blockchain immutability
Verification	Manual & slow process	Automated & real-time authentication
Data Storage	Centralized & vulnerable to cyberattacks	Decentralized & immutable
Transparency	Limited consumer access to product history	Complete traceability from manufacturing to ownership
Counterfeit Prevention	High risk of fake product duplication	Significantly reduces counterfeit risks
Ownership Tracking	Easily altered or falsified records	Blockchain ensures transparent, verified tracking

Table 1. Comparison between Tradition and Blockchain System

Figure 3. Latency in Product Production

The positive effects of blockchain technology in ensuring product security and authenticity are demonstrated by this comparison[11]. Contrary to conventional techniques, blockchain offers a decentralized, fraud-resistant solution that drops dependability on middlemen while boosting authentication processes' efficiency and trust.

VII EXPERIMENTAL SETUP & TESTING

Testing Environment

To guarantee cross-platform compatibility, the experimental configuration makes use of the Ubuntu 20.04 and Windows 11 operating systems. The Ethereum blockchain is utilized for testing, while the Goerli Testnet is used for decentralized testing in the actual world, while Ganache offers a local simulated blockchain environment for development. To facilitate transaction processing, the deployment of smart contracts, and smooth front-end interactions with the blockchain, essential tools including MetaMask, Truffle, Web3.js, and React.js are incorporated[12][13].

Test Situations

Several test scenarios are run in order to evaluate the system's functionality. Manufacturers' ability to correctly add products and enter their information on the blockchain is confirmed by the product registration test[1]. The product verification test makes sure that customers can scan a product's unique identifier to get and validate its information. Furthermore, blockchain immutability is assessed through security testing, which ensures that once data is saved, attempts to change or manipulate it will fail, protecting the integrity of the authentication system[2][8].

Metrics of Performance

Key performance measures are used to evaluate the system's effectiveness[15]. The speed at which product data is captured and retrieved from the blockchain is determined by evaluating transaction time. To reduce transaction costs, gas fee analysis is done to determine how cost-effective product registration and verification are. Lastly, a high volume of product entries is simulated to test scalability and determine how well the system can manage massive authentication requests. These tests guarantee the stability and dependability of the blockchain-based authentication solution.

Performance Metric	Product Registration	Product Verification	Ownership Transfer
Transaction Time	5.2 seconds	2.8 seconds	6.1 seconds
Gas Consumption	42,500 units	18,300 units	32,100 units
Accuracy	100%	100%	100%
Success Rate	100%	100%	100%

Table 2. Performance Metrics

VIII RESULT

The suggested blockchain-based system provides a decentralized, transparent, and safe method of product authentication. The system improves security and usability by using MetaMask for smooth user interaction and Ganache to simulate a local Ethereum blockchain. Product data is kept

unchangeable and readily traceable throughout the supply chain thanks to the incorporation of smart contracts[5]. The tamper-proof nature of blockchain records significantly reduces counterfeiting, increases consumer trust by enabling users to verify product authenticity in real-time, increases transparency by allowing stakeholders to track a product's entire journey, and improves security by removing vulnerabilities associated with centralized databases.

IX CHALLENGES AND FUTURE SCOPE

Although the system has many advantages, it also faces a number of difficulties, such as scalability issues because managing high volumes of blockchain transactions requires a lot of resources, adoption barriers because industries are hesitant to abandon traditional authentication methods, integration complexity because manufacturers, retailers, and consumers must coordinate seamlessly, and regulatory uncertainties because legal frameworks for blockchain-based authentication are still developing[7]. Future developments may concentrate on interoperability improvements to enable smooth cross-blockchain authentication, scalability improvements through Layer 2 solutions like Polygon to maximize transaction efficiency, AI integration for machine learning-based counterfeit detection, and IoT connectivity to connect blockchain with real-time tracking sensors in order to overcome these obstacles and promote wider industry adoption[3].

X CONCLUSION

The suggested blockchain-powered identification method provides a robust and safe way to fight counterfeit goods in a variety of sectors, including as luxury items, electronics, and pharmaceuticals. The technology guarantees a decentralized, transparent, and unchangeable verification process through the use of Ganache, MetaMask, and smart contracts. The potential for future developments, such as AI, IoT, and blockchain interoperability, underscores its capacity to transform supply chain security and consumer confidence, even as obstacles like scalability and regulatory concerns still exist. For organizations looking for increased security and dependability, this blockchain-based strategy offers a creative and practical substitute for conventional authentication techniques[6].

REFERENCES

[1] Prof.D.B. Khadse1, Sahil Tiwari2, “Blockchain-Powered Authenticity a Decentralized Solution for Fake Product Detection”, October 2024

[2] X. Zhang, Y. Wang, and J. Li, "Enhancing Product Traceability Using Blockchain and IoT: A Systematic Review," *Elsevier Computers & Industrial Engineering*, vol. 179, 2024.

[3] L. Fernandez, T. Suzuki, and K. Nakamura, "A Scalable Blockchain-Based Framework for Product Authentication in Global Trade," *MDPI Applied Sciences*, vol. 14, no. 2, pp. 198-210, 2024.

[4] M. Asim, H. F. Ahmad, S. Asim, and M. F. Khan, "Blockchain-Based Anti-Counterfeiting

System for Supply Chains," *IEEE Access*, vol. 11, pp. 45012-45025, 2023.

[5] S. Mukherjee, P. Roy, and S. Banerjee, "A Blockchain-Based Model for Secure Supply Chain Management," *Springer Journal of Blockchain Research*, 2023

[6] C. Oliveira, D. Ramos, and J. Silva, "Blockchain and AI for Fake Product Detection in E-commerce," *ResearchGate Preprint*, 2023.

[7] Article: “Product Authentication Technology Integrating Blockchain and Traceability Structure”, October 2022

[8] Dr.Vikas Reddy, Associate Professor, S J C Institute of Technology Chickaballapur,“Fake Product Identification Using Blockchain”, June 2022

[9] Zignuts Technolab, How blockchain architecture works? basic understanding of blockchain and its architecture, 2022.

[10] S. Idrees, M. Nowostawski, R. Jameel and A. Mourya, "Security Aspects of Blockchain Technology Intended for Industrial Applications", Electronics 10, 2021.

[11] A. Ghadge, A. Duck, M. Er and N. Cald, Deceptive counterfeit risk in global supply chains, 2021.

[12] I. Singhal, Anti-Counterfeit Product System Using Blockchain Technology, 2021.

[13] J. Ma, S.Y. Lin, X. Chen, H.M. Sun, Y.C.
Chen and H. Wang, A blockchain-based application system for product anti-counterfeiting, 2020.

[14] M.A. Benatia, D. Baudry and A. Louis, Detecting counterfeit products by means of frequent pattern mining, 2020.

[15] E. Daoud, D. Vu, H. Nguyen, and M. Gaedke, Improving fake product detection using ai-based technology, 2020.

[16] W. Viriyasitavat and D. Hoonsopon, "Blockchain characteristics and consensus in modern business processes", Journal of Industrial Information Integration, pp. 32-39, 2019