Archives available at journals.mriindia.com

International Journal on Advanced Electrical and Computer Engineering

ISSN: 2349-9338
Volume 14 Issue 01, 2025

Fake Product Identification by QR code

[1]Prof. V. G. Bharane, [2]Rathod Nitin, [3]Patole Hrishikesh, [4]Rananavare Siddhi, [5]Ranaware Vaishnavi
[1 2 3 4 5] S.B.Patil college of engineering, Indapur
Email: bharanevaishali11@gmail.com , nitinrathod0553@gmail.com, hrishikeshpatole1@gmail.com, siddhirananavare29@gmail.com, ranawarevaishnavi5@gmail.com

Peer Review Information

Submission: 11 Sept 2025

Revision: 10 Oct 2025

Acceptance: 22 Oct 2025

Keywords

Blockchain Technology, QR Code, Fake Product Identification, Supply Chain Management, Cybersecurity, Product Authentication

Abstract

Counterfeit products present a serious threat to industries, consumers, and economies, resulting in financial losses, brand damage, and safety risks. Traditional methods of product authentication are vulnerable to manipulation and lack transparency. To address this, the proposed system integrates Blockchain technology with QR codes to ensure authenticity and transparency across the supply chain. Each product receives a unique QR code at manufacturing, with its details stored securely on blockchain. Consumers can verify product genuineness in real-time by scanning the QR code via a mobile or web application. This tamper-proof, decentralized mechanism reduces counterfeiting, enhances trust, improves supply chain management, and safeguards consumers. The approach has wide applications in pharmaceuticals, electronics, luxury goods, and food industries, offering scalability and reliability for future anti-counterfeit measures.

Introduction

Counterfeiting is a growing global challenge that significantly impacts businesses, governments, and consumers. The rise in counterfeit goods has led to economic losses, diminished brand reputation, and public health risks. Conventional verification methods, such as holograms, barcodes, and RFID tags, often fail to provide robust protection against forgery due to their susceptibility to duplication. Blockchain technology has emerged as a powerful tool for tackling this issue. Its decentralized, immutable, and transparent nature ensures that product data cannot be tampered with once recorded. By coupling blockchain with QR codes, manufacturers can assign unique digital identities to products at the production stage. This not only strengthens supply chain integrity but also enables real-time verification by consumers. A blockchain- based fake product identification system eliminates reliance on intermediaries by allowing end-users to directly confirm product authenticity. Moreover, it offers additional advantages such as traceability, fraud detection, and secure transaction logging. The immutability of blockchain ensures trust among stakeholders, while QR codes provide ease of access through widely available smartphones.The integration of such a system into supply chains enhances transparency, ensures accountability, and safeguards consumer interests. Furthermore, it minimizes revenue losses for businesses and prevents unsafe counterfeit goods from reaching the market.This research explores existing systems, identifies their limitations, and proposes a scalable blockchain-QR code solution. It aims to strengthen product authentication, detect tampering attempts, and pave the way for secure, efficient, and trustworthy supply chain ecosystems.

Literature Survey

1. Fake Product Identification using Blockchain and QR Code (Gandhimathi K, Agathiyan J, Arvind R, Harisujith V, Lalith S, and Naveen Kumar D, 2025): This work addressed the issue of counterfeiting by enabling product authenticity checks using blockchain and QR codes. The study ensured transparency and traceability across the supply chain. Future scope involves implementing real-time fraud alerts and large-scale deployment across industries.

2. Fake Product Detection Using Blockchain Technology (Goli Sai Sampath Reddy, Jeedipalli Thrishul Reddy, and Jeripothula Ravi Kiran Goud, 2023):The authors focused on authenticity verification of products using blockchain ledgers and QR scanning. Their solution improved reliability in detecting counterfeit goods. The future scope highlights broader industry adoption and scalability enhancements.

3. Fake Product Identification System Using Blockchain (Jayshree R. Pansare, Nidhi Navandar, Samruddhi Gaikwad, Asmita Katkar, and Utkarsha Gangarde, 2023) : This study proposed a decentralized blockchain system with QR codes to ensure product genuineness without relying on direct- operated stores. The suggested system is particularly relevant to consumer trust- building. Future work includes applications in pharmaceuticals and luxury goods.

4. Identification of Counterfeit Product Using Blockchain (Darshan N and Mir Aadil, 2023):
The research emphasized ownership history verification through blockchain and QR code integration. Their approach highlighted better traceability and accountability in the supply chain. Future scope lies in expanding adoption in global supply chain networks.

5. Fake Product Detection Using Blockchain Technology (Srikrishna Shastri C, Vishal K, Sushmitha S, Lahari, and Ashwal R. Shetty, 2022):
The paper proposed blockchain and QR validation mechanisms to prevent counterfeiting. This strengthened security in product authentication. Future work focuses on IoT integration for automated detection and smart device collaboration.

6. A Product Authentication Scheme for Supply Chain via Smart Contracts and Facial Recognition (Srivatsa D, Aakash, Nithin, Sahisnu S, and Priyanka Kumar, 2021): The study addressed inadequate authenticity verification in supply chains by introducing blockchain combined with smart contracts and facial recognition. This hybrid approach improved accuracy and fraud resistance. Future work involves stronger biometric integrations and enterprise-level adoption.

7. Product Authentication and Traceability Using Blockchain (R. Subapriya, S. Karthikeyan, A. Gokul Prasath, and M. Shankar, 2023):
This research tackled transparency and traceability issues in supply chains by integrating blockchain with QR code scanning. Their solution increased reliability and consumer confidence. Future work suggests large-scale adoption in retail and logistics.

Methodology

The methodology for developing divided into the following phases:

Requirement Analysis

- User Registration & Authentication

Users (manufacturers, distributors, and consumers) must be able to register and authenticate securely.

- QR Code Generation

A unique QR code should be generated for every product at the manufacturing stage.

- Blockchain Data Storage

Product details (batch number, manufacturing date, expiry date, owner info) should be stored on blockchain.

System Design

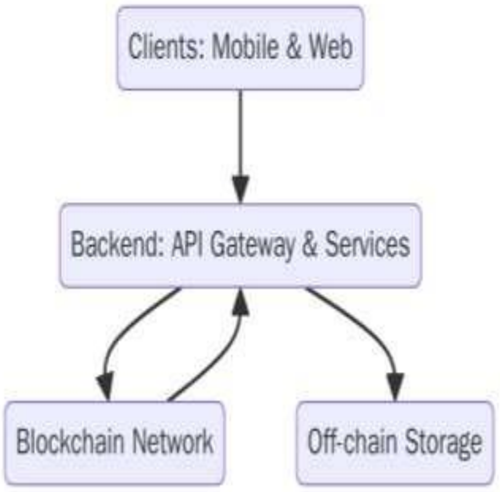
The system is a three-tier, microservice-oriented architecture that supports secure product identity issuance, tamper-evident storage on blockchain, and real-time consumer verification.

Modules

- Consumer Mobile App → Frontend for end- users to interact with products and services.
- Manufacturer / Admin Web Portal → Dashboard for admins/manufacturers to manage products and system data.
- API Gateway → Central entry point that routes all client requests to backend services.
- Auth Service → Handles user authentication, authorization, and security tokens.
- Product Service → Manages product lifecycle, metadata, and interactions with

blockchain/storage.

- QR Service → Generates and validates QR codes for product tracking.
- Notification Service → Sends real-time alerts and updates to users (mobile/web).
- Analytics & Audit → Logs activities, monitors performance, and provides audit trails.
- Off-chain Storage (IPFS/S3) → Stores large product data and media files off the blockchain.
- Blockchain Nodes → Network layer that validates transactions and interacts with smart contracts.



Implementation

- Clients: Mobile app for end-users and a web portal for manufacturers/admins.
- Backend: API Gateway routes requests to microservices such as Auth, Product, QR, Notifications, and Analytics.
- Blockchain Integration: Product Service writes transactions to blockchain nodes and executes Smart Contracts for authenticity and traceability.
- Storage: Large files or metadata stored off-chain (IPFS/S3) for efficiency.
- Communication: Notifications push updates back to clients in real-time.

Evaluation

- Scalability: Microservices architecture allows independent scaling of services (e.g., Notification Service during peak loads).
- Security: Blockchain ensures immutability; Auth Service protects user data with secure access tokens.
- Transparency: Audit and Analytics provide clear activity logs and trust for stakeholders.
- Performance: Off-chain storage improves response times by offloading heavy data away from blockchain.
- Reliability: Redundant blockchain nodes improve fault tolerance.

Future Enhancements

- Layer-2 Blockchain Integration: Improve transaction throughput and reduce costs.
- AI-powered Analytics: Use ML models to detect fraud or predict product lifecycle trends.
- Cross-chain Interoperability: Enable interaction with multiple blockchain networks for wider adoption.
- Decentralized Identity (DID): Strengthen authentication with blockchain-based identity verification.
- IoT Integration: Connect smart devices to automate product tracking and updates.

Limitations

- One of the major limitations is the reliance on blockchain for recording product transactions. While blockchain ensures transparency and immutability, it also introduces performance bottlenecks. Public networks in particular can be slow and expensive, as each transaction requires validation and confirmation from nodes. This makes real-time operations less efficient compared to traditional centralized databases.
- Although off-chain storage solutions like IPFS or S3 are used to handle large files and metadata efficiently, they create dependencies on external systems. This introduces a trade- off between decentralization and practicality. If the off-chain service experiences downtime or security breaches, data integrity and availability could be compromised, undermining trust in the system.
- The architecture's use of multiple microservices alongside blockchain integration increases system complexity. Each service requires dedicated management, monitoring, and updates, and issues often span across services. Debugging or upgrading the system demands specialized skills in both distributed systems and blockchain, which may not always be readily available, raising long-term operational costs.
- While microservices scale independently, blockchain itself presents scalability challenges. As transaction volumes increase, the network may struggle to handle the load, leading to slower response times. For end- users, this translates into delays in product verification or updates, which can negatively impact the overall user experience compared to conventional

centralized solutions.

- Even though blockchain enhances security, vulnerabilities in smart contracts or misconfigured backend services remain potential risks. Once deployed, flawed contracts are immutable and cannot be easily patched. Furthermore, the current design may not seamlessly integrate with other blockchains or legacy enterprise systems, creating interoperability challenges that limit adoption across industries.

Research Gap

Although blockchain-based product tracking architectures demonstrate transparency, immutability, and trust, there are still gaps that limit their large-scale adoption. Current systems suffer from scalability bottlenecks caused by blockchain's low throughput, which is not well-suited for high-frequency industrial transactions. Off-chain storage solutions, while solving size and cost issues, reintroduce centralization risks. Additionally, interoperability between multiple blockchain platforms remains largely unexplored, reducing the system's flexibility in diverse supply chains. Furthermore, research on integrating blockchain with emerging technologies like IoT and AI for predictive analytics is still in its infancy, leaving significant opportunities for improvement.

Problem Statement

Existing blockchain-integrated product tracking systems struggle to balance scalability, security, decentralization, and user experience. While they ensure authenticity and traceability, they face performance bottlenecks due to blockchain overhead, complexity in maintaining microservices, and dependency on off-chain storage. Moreover, the lack of robust interoperability frameworks and limited adoption of AI/IoT for automation prevent these systems from meeting the demands of modern, high- volume, and interconnected supply chains. This research addresses the need for a more scalable, secure, and interoperable architecture that overcomes these limitations.

Conclusion

The proposed architecture highlights the benefits of combining blockchain, off-chain storage, and microservices to enable transparent and auditable product management. However, the analysis reveals that limitations such as blockchain overhead, off-chain dependency, system complexity, scalability challenges, and security vulnerabilities remain. Addressing these issues requires integrating Layer-2 solutions, decentralized identity management, and cross- chain interoperability while leveraging IoT and AI for real-time insights. Future research should focus on optimizing hybrid on-chain/off-chain frameworks and developing standardized protocols to enable broader adoption across industries. By bridging these gaps, blockchain- enabled product tracking can evolve into a robust and scalable solution for next-generation supply chains.

References

Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

Buterin, "Ethereum: A next-generation smart contract and decentralized application platform," 2014.

Xu et al., "A taxonomy of blockchain-based systems for architecture design," Proc. IEEE Int. Conf. Softw. Archit., 2017.

Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," Applied Innovation Review, vol. 2, pp. 6–10, 2016.

Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," IEEE Access, vol. 4, pp. 2292–2303, 2016.

Zheng et al., "Blockchain challenges and opportunities: A survey," Int. J. Web Grid Serv., vol. 14, no. 4, pp. 352–375, 2018.

Swan, Blockchain: Blueprint for a New Economy. Sebastopol, CA: O'Reilly Media, 2015.

Lu and X. Xu, "Adaptable blockchain-based systems: A case study for product traceability," IEEE Software, vol. 34, no. 6, pp. 21–27, 2017.

H. Kim and M. Laskowski, "Toward an ontology-driven blockchain design for supply-chain provenance," Int. J. Intelligent Systems in Accounting, Finance and Management, vol. 25, no. 1, pp. 18–27, 2018.

K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, "Blockchain for AI: Review and open research challenges," IEEE Access, vol. 7, pp. 10127–10149, 2019.

J. Kwon and E. Buchman, "Cosmos: A network of distributed ledgers," 2019. [Online]. Available: https://cosmos.network

G. Wood, "Polkadot: Vision for a heterogeneous multi-chain framework," 2016. [Online]. Available: https://polkadot.network

M. Ali et al., “Blockstack: A global naming and storage system secured by blockchains,” in Proc. 2016 USENIX Annu. Tech. Conf.,
pp. 181–194.

Y. Zhang and J. Wen, “An IoT electric business model based on the protocol of bitcoin,” in Proc. IEEE Int. Conf. Information and Automation, 2015, pp. 1172–1175.

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, 2016, pp. 1–6.
16.

Kshetri, “Blockchain’s roles in strengthening cybersecurity and protecting privacy,”
Telecommunications Policy, vol. 41, no. 10,
pp. 1027–1038, 2017.

S. Rouhani and R. Deters, “Performance analysis of Ethereum transactions in private blockchain,” in Proc. IEEE Int. Conf. Cloud Computing Technology and Science, 2017,
pp. 1–7.

A. Gervais et al., “On the security and performance of proof of work blockchains,” in Proc. 23rd ACM SIGSAC Conf. Computer and Communications Security, 2016, pp. 3–