International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Fake Product Detection Through QR Based Blockchain System

Prof. Ramya H[1], Shravan Balaji[2], Aneesa Atther[3], Sunil Balachandra Naik[4], Rakshitha SJ[5]

[1,2,3,4,5]Department of AIML, Sri Krishna Institute of Technology Bengaluru, India

Abstract

The proliferation of counterfeit merchandise in global markets creates substantial economic losses for legitimate manufacturers while exposing consumers to both financial risks and safety hazards. Conventional authentication mechanisms predominantly rely on centralized architectures that remain vulnerable to malicious manipulation, undermining consumer confidence in product authenticity verification. This research introduces a *distributed ledger-based authentication framework* that leverages QR code technology to create an immutable record of product information. The proposed architecture enables manufacturers to register individual products along with their constituent component specifications, which undergo crypto- graphic transformation into hash values that are subsequently aggregated to generate a comprehensive product fingerprint. This cryptographic fingerprint and associated product metadata are recorded within an Ethereum smart contract infrastructure, while a corresponding QR code serves as the physical-digital interface for authentication. During the verification phase, con- sumers scan the embedded QR code, triggering a system query to the blockchain that reconstructs the hash value from retrieved component data and compares it against the stored cryptographic signature. Matching hash values confirm product authenticity, whereas discrepancies indicate potential counterfeiting or tam- pering. The framework enhances supply chain transparency, establishes tamper-evident data integrity, and fosters trust re- lationships between stakeholders in the product ecosystem.

Keywords: Distributed ledger technology, cryptographic authentication, counterfeit prevention, product traceability, de- centralized verification, Ethereum blockchain

INTRODUCTION

The counterfeit goods market has emerged as a critical chal- lenge spanning multiple industrial sectors including pharma- ceuticals, electronics, luxury goods, and consumer products. Sophisticated replication techniques enable counterfeit items to achieve visual parity with authentic merchandise, rendering traditional visual inspection methods ineffective for consumers attempting to distinguish genuine products from fraudulent replicas. This phenomenon generates cascading negative con- sequences including compromised consumer safety, brand reputation degradation, intellectual property violations, and substantial revenue erosion for legitimate manufacturers.

Contemporary product authentication solutions predom- inantly operate through centralized database architectures maintained by manufacturers or third-party certification enti- ties. These centralized

systems present inherent vulnerabilities: compromised servers enable unauthorized data manipulation, single points of failure create system-wide risks, and con- sumers lack independent mechanisms to verify data authen- ticity and integrity. The absence of transparent, independently verifiable authentication mechanisms perpetuates consumer mistrust and enables counterfeit proliferation.

Distributed ledger technology addresses these limitations through its foundational architecture of cryptographically linked data structures distributed across decentralized node networks. Once transaction data receives network consensus and undergoes immutably recorded within the blockchain infrastructure, subsequent modification attempts become com- putationally impractical and immediately detectable through hash verification mechanisms. The integration of blockchain architecture with machine-readable QR code interfaces creates an accessible verification framework that enables end-users to authenticate products through simple scanning operations.

This paper presents a comprehensive blockchain-enabled authentication framework for counterfeit detection utilizing QR code technology. Manufacturers register products within an Ethereum-based distributed ledger environment, generating unique QR code identifiers that encode blockchain reference data for each registered item. Consumers authenticate products by scanning QR codes through mobile applications or web interfaces, initiating real-time verification against immutable blockchain records. The system architecture ensures trans- parency, security, and tamper-resistance throughout the prod- uct authentication lifecycle.

LITERATURE SURVEY

Numerous research initiatives have explored blockchain applications for product authentication and supply chain trans- parency enhancement.

Multiple systems establish product-blockchain associations through unique identifier schemes stored within distributed ledger infrastructure. User authentication workflows typi- cally involve scanning product codes through mobile applica- tions or web platforms, triggering system verification against blockchain records to confirm product validity. These architec- tural approaches commonly employ asymmetric cryptography or QR code technology for product identity representation, while leveraging smart contract logic for data management and verification operations.

Alternative research directions emphasize comprehensive supply chain traceability, where each supply chain stage (manufacturing, distribution, retail, consumer delivery) gener- ates blockchain-recorded transactions. This creates end-to-end product journey documentation from origin through final sale, significantly complicating counterfeit insertion into legitimate supply chains. Certain implementations integrate Internet of Things (IoT) sensor networks for automated logistics event recording and real-time supply chain monitoring.

Existing methodologies, however, frequently prioritize batch-level or shipment-level tracking over individual unit verification. Additionally, numerous systems record singular product identifiers without incorporating granular component- level specifications. This architectural limitation enables iden- tifier cloning attacks where adversaries replicate QR codes or barcodes onto counterfeit products, exploiting the lack of component-level verification.

The proposed framework addresses these research gaps through:

- Component-level cryptographic hashing that transforms individual product component specifications (such as pro- cessor, battery, memory, display components in electronic devices) into unique hash values.

- Hierarchical hash aggregation through Merkle tree struc- tures that combine component hashes into a singular root hash representing the complete product configuration.
- Blockchain storage of the root hash with QR code link- age, creating an authentication mechanism resistant to identifier cloning.

This architectural approach significantly elevates cloning diffi- culty, as component specification modifications produce hash mismatches during verification operations.

Gap Analysis and Problem Statement

A. *Gap Analysis*

Analysis of existing authentication systems and practical deployment observations reveals several critical limitations:

Transparency deficiency: Consumers frequently lack visibility into product information provenance and au- thenticity. Traditional retail channels and intermediary systems may not provide trustworthy verification, leaving consumers vulnerable to misinformation.

Centralization vulnerabilities: Numerous authentication solutions store critical data in centralized database infras- tructures susceptible to tampering, insider threats, single- point failures, and unauthorized access.

Identifier replication attacks: Adversaries can dupli- cate QR codes or barcodes from authentic products and reproduce them on counterfeit items, undermining identifier-based authentication when verification systems lack component-level validation.

Consumer trust erosion: These systemic limitations prevent consumers from accessing reliable, straightfor- ward mechanisms to verify product authenticity prior to purchase decisions.

B. *Problem Statement*

Contemporary markets experience significant counterfeit product infiltration, with fraudulent items achieving visual similarity to authentic merchandise. Conventional verification infrastructures rely predominantly on centralized architectures vulnerable to manipulation, creating authentication challenges for consumers. An urgent need exists for secure, transparent, and tamper-resistant authentication mechanisms enabling con- sumers to independently verify product authenticity without excessive dependence on retail intermediaries or centralized authorities.

The fundamental research problem addressed by this in- vestigation is: *How can blockchain technology and QR code integration be architected to create a reliable counterfeit de- tection system that prevents data manipulation while ensuring accessibility for end-users?*

Objectives

The primary objectives guiding this research are:

- To develop a counterfeit detection framework leveraging blockchain distributed ledger technology and QR code authentication interfaces.
- To establish secure, transparent, and tamper-evident stor- age mechanisms for product specification data within blockchain infrastructure.
- To enable consumer-accessible product authenticity veri- fication through straightforward QR code scanning oper- ations.
- To prevent product identifier duplication and data manip- ulation, thereby establishing trust between manufacturers and consumers.

System Design and Methodology

A. *System Overview*

The architecture encompasses two principal stakeholder categories: manufacturers and consumers. The operational workflow proceeds as follows:

Product registration: Manufacturers input comprehen- sive product specifications including product identifica- tion, brand designation, model information, and detailed

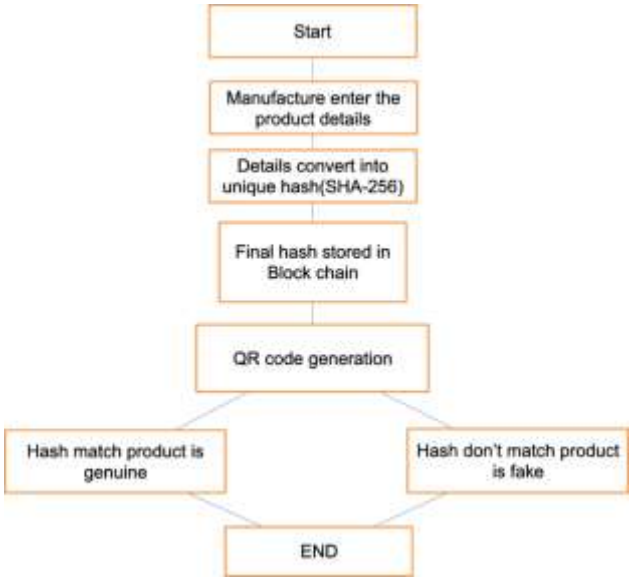

Fig. 1. System workflow for product registration and authentication verifica- tion.

component attributes (such as battery specifications, pro- cessor type, memory capacity, display characteristics).

Cryptographic hash generation: Each component specification undergoes cryptographic transformation us- ing SHA-256 hashing algorithms. These component- specific hashes are subsequently combined through hier- archical aggregation to compute a consolidated product hash.

Blockchain data persistence: The final product hash alongside product identification and auxiliary metadata are persistently stored within an Ethereum smart contract infrastructure.

QR code generation: A unique QR code encoding the product identifier, transaction hash, or blockchain refer- ence pointer is generated for each registered product.

Verification workflow: When consumers scan the QR code, the system retrieves corresponding on- chain data, recalculates the hash from current product details, and performs comparative analysis against the stored hash.

Authentication result: Hash correspondence indicates *Authentic* product status; hash discrepancy signals *Coun- terfeit* or *Tampered* product status.

B. *Merkle Tree-Based Cryptographic Aggregation*

To enhance security architecture, component-level hash val- ues undergo aggregation through Merkle tree data structures. Consider hash values H_1, H_2, H_3, H_4 representing crypto- graphic transformations of four component specifications (pro- cessor, display, memory, battery). Pairwise hash concatenation and subsequent hashing operations generate intermediate hash values H_{12} and H_{34}:

$$H_{12} = \text{SHA256}(H_1 \mid H_2), \quad (1)$$

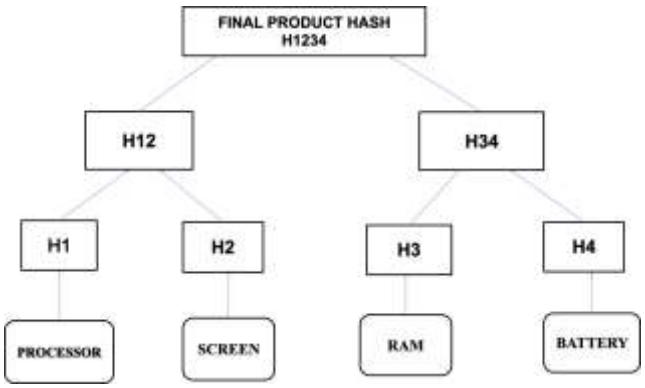

Fig. 2. Merkle tree structure demonstrating hierarchical hash aggregation into final product fingerprint.

$H_{34} = \text{SHA256}(H_3 \mid H_4)$. (2)

The final product hash (Merkle root) emerges from a final concatenation and hashing operation:

$H_{\text{root}} = \text{SHA256}(H_{12} \mid H_{34})$. (3)

Any modification to component specifications propagates through the hierarchical structure, altering the corresponding component hash and consequently the Merkle root, thereby enabling immediate tamper detection.

SYSTEM REQUIREMENTS

A. *Functional Requirements*

The system must satisfy the following functional specifica- tions:

- The platform shall provide manufacturer interfaces for product registration including product identification, brand information, model designation, and comprehen- sive component specifications.
- The system shall generate unique cryptographic hash values for each product through component-level hash aggregation.
- The platform shall persist final product hash values and associated metadata within blockchain infrastructure through smart contract interactions.
- The system shall generate unique QR code identifiers for each registered product entry.
- The platform shall provide consumer interfaces for QR code scanning and product authenticity verification.

B. *Non-Functional Requirements*

Security: Blockchain-persisted data must exhibit tamper- evident properties and resist unauthorized modification attempts.

Reliability: The verification system should deliver con- sistent and accurate authentication results across diverse operating conditions.

Performance: QR scanning operations and blockchain query latency should remain within acceptable response time thresholds for practical deployment.

Usability: User interfaces should demonstrate intuitive design principles and accessibility for both manufacturer and consumer stakeholders.

IMPLEMENTATION

A. *Blockchain Infrastructure Configuration*

The prototype implementation utilizes a local Ethereum blockchain network environment. Ganache serves as the local blockchain infrastructure for smart contract deployment and testing operations. Smart contracts are developed using the So- lidity programming language and managed through the Truffle development framework. Backend application-blockchain con- nectivity is established using the Web3.js JavaScript library.

B. *Backend Development*

The backend architecture is constructed using Node.js run- time environment and Express.js web framework. RESTful API endpoints facilitate product registration and verification operations. SHA-256 cryptographic hashing functions imple- ment component-level hashing and Merkle root computation.

Primary API endpoints include:

- `/api/registerProduct`: Accepts product and com- ponent specifications from manufacturers, computes the final cryptographic hash, persists data to blockchain in- frastructure, and returns QR code data.
- `/api/verifyProduct`: Accepts QR code data from consumers, retrieves corresponding blockchain records, recalculates hash values from supplied product details, and returns verification status.

C. *Frontend and QR Code Integration*

A web-based interface enables manufacturers to register products and access generated QR codes. QR code genera- tion leverages specialized libraries to create machine-readable codes suitable for product packaging integration.

Consumer-facing interfaces or mobile-responsive web appli- cations facilitate QR code scanning through device cameras or image upload mechanisms. Following scan operations, the application transmits code data to backend services for verification processing and displays authentication results to users.

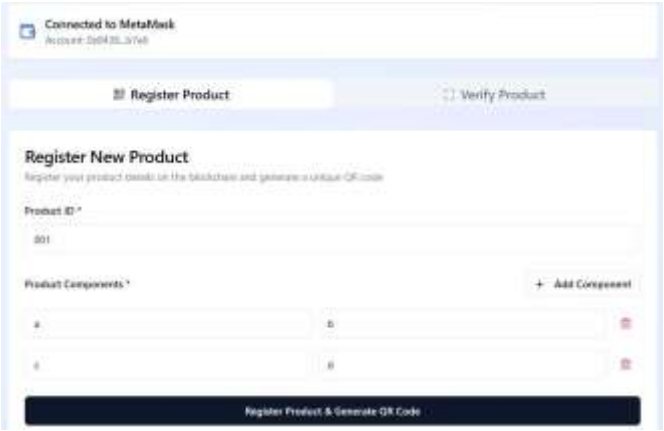

Fig. 3. Manufacturer interface demonstrating product registration and QR code generation workflow.

Fig. 4. Consumer interface displaying product authentication verification results.

RESULTS AND DISCUSSION

The system underwent comprehensive testing with multiple sample products registered through manufacturer interfaces. For each registered product, component specifications were input, cryptographic hashes were computed, data was persisted to blockchain infrastructure, and corresponding QR codes were generated.

During verification testing, scanning of legitimate QR codes for registered products resulted in successful hash recompu- tation and correct authentication as genuine products. When QR codes underwent unauthorized duplication or component specifications were locally modified, recomputed hash values failed to match on-chain stored hashes, and the system cor- rectly identified products as counterfeit or tampered.

The prototype demonstrates that local Ethereum network implementations provide adequate performance characteristics for practical deployment. Response time overhead primarily derives from blockchain read operations and cryptographic hash calculations, both remaining within acceptable latency thresholds for end-user applications.

CONCLUSION

This research presents a blockchain-based authentication framework for counterfeit product detection utilizing QR code technology. By storing product specifications as cryptographic hash values within Ethereum blockchain infrastructure and linking them to QR code interfaces, the system establishes a transparent and tamper-evident mechanism for authenticity verification. Consumers can readily validate product genuine- ness through pre-purchase QR code scanning.

The implementation of component-level hashing combined with Merkle tree aggregation enhances security posture and significantly complicates product identifier cloning or reuse attempts by adversaries. The system cultivates trust between manufacturers and consumers through data manipulation pre- vention and product duplication mitigation.

Future development directions include full supply chain integration where distributors and retailers similarly record transactions within blockchain infrastructure. Integration with native mobile applications, cloud-based blockchain services, and real-time analytics dashboards could further enhance sys- tem usability and scalability.

REFERENCES

1. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
2. M. Swan, *Blockchain: Blueprint for a New Economy*. O'Reilly Media, 2015.
3. Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in *Proc. 2017 IEEE International Congress on Big Data*, 2017, pp. 557– 564.
4. Guo, Y., Wang, S., Zeng, Z. (2021) IEEE Transactions on Industrial Informatics, 17(6), 4292-4300.
5. Wu, C., Wu, M. (2021) Journal of Manufacturing Systems, 59, 178-188.
6. M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain Technology: Beyond Bitcoin," *Applied Innovation Review*, no. 2, pp. 6– 10, 2016.
7. IBM Corporation, "IBM Blockchain Platform: Product Authenticity and Supply Chain Solutions." [Online]. Available: https://www.ibm.com/ blockchain/
8. Li, X., Liu, D., Liu, J. (2022). IEEE Transactions on Engineering Management.
9. Rathi, A., Agrawal, S. (2021). International Journal of Production Research.
10. Ethereum Foundation, "Ethereum Whitepaper." [Online]. Available: https://ethereum.org/en/whitepaper/