International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 04 | April - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

A Decentralized Blockchain Architecture for Counterfeit Product Detection Using Cryptographic Verification Techniques

P. Bhanuchand[1], R Meghanadh[2], CH .Yashwanth[3], T. Madhavi[4], T. Mohana[5]

[1]*Assistant Professor, Department of CSE(CB), Bapatla Engineering College, Bapatla 522101, AP,India*

[2]*Student, Department of CSE(CB),Bapatla Engineering College, Bapatla 522101,AP, India*

[3]*Student, Department of CSE(CB), Bapatla Engineering College, Bapatla 522101, AP, India*

[4]*Student, Department of CSE(CB), Bapatla Engineering College, Bapatla 522101, AP, India*

[5]*Student, Department of CSE(CB), Bapatla Engineering College, Bapatla 522101, AP, India*

Abstract - The rapid expansion of global supply chains has intensified the prevalence of counterfeit products, posing significant risks to consumer safety and brand credibility. Conventional identification mechanisms, including QR codes and RFID systems, suffer from vulnerabilities such as duplication, limited transparency, and high implementation costs. This paper presents a decentralized architecture leveraging blockchain technology integrated with cryptographic verification techniques to ensure secure product authentication and traceability. The proposed system records each transaction within an immutable distributed ledger, enabling transparent and tamper-resistant data management. Smart contracts facilitate automated validation of product information across different supply chain stages, from manufacturing to end-user verification. Additionally, QR code integration provides a user-friendly interface for authenticity checks. Experimental analysis demonstrates enhanced reliability, improved transparency, and effective counterfeit detection compared to traditional approaches. The framework offers a scalable and trustworthy solution for securing modern supply chain ecosystems against fraudulent activities.

Key Words: Blockchain, Counterfeit Detection, Supply Chain Security, Cryptographic Verification, Smart, Contracts, Decentralized Architecture, Product Traceability, QR Code Authentication, Distributed, Ledger Technology

1. INTRODUCTION

The rapid evolution of global trade and digital commerce has significantly increased the complexity of supply chain networks, making them more vulnerable to counterfeit infiltration. Counterfeit products not only undermine brand reputation but also pose serious risks to consumer safety and economic stability. Industries such as pharmaceuticals, electronics, and luxury goods are particularly affected, where even minor compromises in authenticity can lead to severe consequences. Despite the adoption of various identification and tracking technologies, ensuring product integrity across multiple stakeholders remains a persistent challenge.

Traditional anti-counterfeiting mechanisms, including QR codes and Radio Frequency Identification (RFID), provide basic traceability but fail to guarantee security due to their susceptibility to duplication and unauthorized replication. Moreover, centralized data management systems introduce risks related to data manipulation, lack of transparency, and single points of failure. These limitations highlight the necessity for a more resilient and trustworthy solution.

Blockchain technology has emerged as a transformative paradigm capable of addressing these challenges through decentralization, immutability, and transparency. By maintaining a distributed ledger of transactions, blockchain ensures that once data is recorded, it cannot be altered without consensus, thereby preserving data integrity. The integration of cryptographic techniques further enhances security by safeguarding transactions and verifying authenticity at each stage of the supply chain.

In this paper, a decentralized blockchain-based architecture is proposed to detect and prevent counterfeit products. The system incorporates smart contracts for automated validation, QR code-based identification for user interaction, and end-to-end traceability from manufacturer to consumer. This approach not only strengthens security but also improves transparency and trust among all participants in the supply chain ecosystem.

The remainder of this paper is organized as follows: Section II discusses the problem definition, Section III reviews existing systems, Section IV presents the proposed methodology, followed by implementation, results, and conclusion in subsequent sections.

2. LITERATURE SURVEY

The problem of counterfeit product detection in supply chains has been extensively explored using various technological approaches, including identification systems, centralized databases, and emerging decentralized frameworks. This section reviews the most relevant contributions and highlights their limitations.

Early approaches primarily relied on QR code-based identification systems, where product information is encoded and accessed through scanning. These systems offer simplicity and low deployment cost; however, studies indicate that QR codes are highly susceptible to duplication and unauthorized reproduction, which limits their effectiveness in ensuring product authenticity.

To overcome these issues, Radio Frequency Identification (RFID) technology was introduced to enable automated and wireless tracking of products. Research demonstrates that RFID enhances traceability and operational efficiency. Nevertheless, RFID tags can be cloned or tampered with, and the associated infrastructure cost remains a significant drawback for large-scale implementation.

Recent advancements have incorporated Artificial Intelligence (AI) and machine learning techniques to detect counterfeit products based on pattern recognition and anomaly detection. While these methods improve detection accuracy, they often require extensive training datasets, high computational resources, and do not inherently provide data immutability or transparency.

With the advent of decentralized technologies, blockchain-based solutions have gained considerable attention. Blockchain Technology enables secure, transparent, and immutable record-keeping without relying on a central authority. Smart Contracts further enhance system automation by enforcing predefined rules for transaction validation. Studies suggest that blockchain significantly improves supply chain transparency and reduces the risk of data manipulation.

Additionally, the application of Cryptography ensures confidentiality, integrity, and authentication of transactions across the network. Combining cryptographic hashing with blockchain storage creates a tamper-resistant system capable of detecting inconsistencies in product data.

Despite these advancements, existing blockchain-based models still face challenges related to scalability, latency, and integration with legacy systems. Therefore, there is a need for an optimized architecture that integrates blockchain with efficient identification mechanisms such as QR codes while maintaining security and usability.

The proposed system addresses these gaps by combining decentralized ledger technology, cryptographic verification, and user-friendly authentication to deliver a comprehensive and secure counterfeit detection framework.

3. Existing System

Conventional counterfeit detection frameworks within supply chain environments primarily depend on physical tagging mechanisms, centralized data repositories, and semi-automated tracking solutions. These systems provide foundational traceability; however, they exhibit significant vulnerabilities in terms of security, scalability, and data integrity.

3.1 QR Code-Based Systems

Quick Response (QR) code mechanisms are extensively utilized for product identification and consumer-level verification. Each item is embedded with a machine-readable code that links to product-specific metadata. Despite their low deployment cost and ease of implementation, QR codes lack intrinsic security features. The absence of cryptographic binding between the code and the product allows adversaries to duplicate or reprint codes on counterfeit items. Furthermore, these systems often rely on centralized backends, which weakens validation authenticity and increases susceptibility to data spoofing.

3.2 RFID-Based Systems

Radio Frequency Identification (RFID) technology facilitates contactless product tracking through embedded electronic tags and readers. This approach enhances inventory visibility and operational efficiency across logistics networks. However, RFID systems are prone to tag cloning, signal interference, and unauthorized scanning attacks. Additionally, the requirement for specialized hardware infrastructure and maintenance introduces substantial economic overhead, limiting scalability in cost-sensitive supply chain deployments.

3.3 Centralized Database Systems

Many legacy systems utilize centralized database architectures to maintain product lifecycle information. While these systems offer controlled access and structured data management, they inherently suffer from architectural weaknesses such as single points of failure and vulnerability to insider attacks. Data stored in centralized servers can be altered, deleted, or compromised without transparent auditability, thereby undermining trust among stakeholders.

3.4 AI-Based Detection Systems

Artificial Intelligence (AI) and machine learning-based approaches have been introduced to identify counterfeit products using visual inspection, feature extraction, and anomaly detection algorithms. Although these systems improve detection accuracy under controlled conditions, they require extensive training datasets and high computational resources. More importantly, AI-based systems operate as analytical layers and do not inherently ensure secure data storage, immutability, or end-to-end traceability within the supply chain.

3.5 Limitations of Existing Systems

The predominant limitations of current counterfeit detection mechanisms include:

Lack of cryptographic security and resistance to duplication
Inadequate end-to-end traceability across distributed stakeholders
Limited transparency due to centralized control models
High infrastructure and operational expenditure
Exposure to data manipulation, cloning, and replay attacks

These shortcomings collectively restrict the reliability and robustness of existing systems, particularly in large-scale and multi-entity supply chain ecosystems.

4. Proposed Methodology

This paper proposes a decentralized blockchain-based framework integrated with cryptographic validation mechanisms to detect and prevent counterfeit products across the supply chain. The architecture ensures data immutability, transparency, and secure product traceability from the manufacturing stage to end-user verification.

4.1 System Overview

The proposed system operates as a distributed application (DApp) built on a blockchain network, where each product is uniquely registered and tracked through successive supply chain stages. Every transaction associated with a product is recorded as a block, forming an immutable ledger that cannot be altered retroactively. The system incorporates QR code-based identification linked with blockchain records to facilitate user interaction and verification.

4.2 Architectural Components

The system consists of three primary entities:
Manufacturer: Initializes product registration by generating a unique product identifier and embedding it into a QR code. The corresponding product data is securely stored on the blockchain.
Supplier (Distributor/Retailer): Updates product movement and ownership details at each transition stage. These updates are appended to the blockchain as verified transactions.
Customer: Scans the QR code to retrieve the complete product history and verify authenticity through blockchain validation.
4.3 Blockchain Integration
The blockchain serves as a distributed ledger where each transaction is cryptographically secured using hashing algorithms. Each block contains:

Product ID
Timestamp
Transaction details
Previous block hash

This chaining mechanism ensures tamper resistance, as any modification in a block would invalidate the entire chain.

4.4 Smart Contract Mechanism

Smart contracts are deployed to automate the validation and execution of supply chain transactions. These contracts enforce predefined rules such as:
Authentic product registration
Authorized participant interaction
Sequential update of product lifecycle events
This eliminates the need for intermediaries and ensures trustless execution.

4.5 Cryptographic Security

The system utilizes cryptographic techniques to ensure:
Data Integrity: Hash functions prevent unauthorized modification
Authentication: Digital signatures validate participant identity
Confidentiality: Secure transaction handling within the network
Each transaction is verified before being added to the blockchain, preventing fraudulent entries.

4.6 Product Verification Process

- Product is registered by the manufacturer with a unique ID
- QR code is generated and attached to the product
- Each supply chain interaction updates the blockchain
- Customer scans QR code using an application
- System retrieves blockchain data and validates authenticity
- Any mismatch in records indicates a counterfeit product

4.7 Advantages of Proposed Method

Eliminates single point of failure through decentralization
Ensures immutable and transparent data storage
Provides real-time product traceability
Enhances trust among stakeholders
Reduces counterfeit risks significantly

5. Hardware & Software Requirements

The successful implementation of the proposed blockchain-based counterfeit detection system requires a combination of appropriate hardware infrastructure and software tools to ensure efficient execution, secure data handling, and seamless user interaction.

5.1 Hardware Requirements

The system does not demand specialized high-end hardware; however, the following configuration is recommended for optimal performance:
Processor: Intel Core i5 or higher / AMD equivalent
RAM: Minimum 8 GB (16 GB recommended for blockchain operations)
Storage: 256 GB SSD or higher for faster data access and blockchain synchronization
Network: Stable internet connectivity for blockchain transactions and distributed access
User Devices: Smartphone or desktop system with QR code scanning capability

5.2 Software Requirements

The proposed system is developed using modern decentralized application technologies and requires the following software components:
Operating System: Windows / Linux / macOS
Frontend Technologies: HTML, CSS, JavaScript (for user interface development)
Backend Environment: Node.js for server-side processing
Blockchain Platform: Ethereum or similar blockchain framework
Smart Contract Language: Solidity
Development Framework: Truffle / Hardhat for smart contract deployment and testing
Web3 Integration: Web3.js or Ethers.js for blockchain interaction
Wallet Integration: MetaMask for transaction authentication and account management
Database: IPFS or MongoDB for off-chain data storage
QR Code Generator: Library or API for generating and scanning QR codes

5.3 System Requirements

Category	Requirement
Hardware	i5 Processor, 8GB RAM, SSD Storage
Platform	Ethereum Blockchain
Programming	JavaScript, Solidity
Frameworks	Node.js, Truffle/Hardhat
Tools	MetaMask, Web3.js
Interface	Web-based Application

The proposed system utilizes widely available hardware and modern software frameworks, ensuring cost-effective deployment and scalability. The integration of blockchain tools and web technologies enables the development of a secure and efficient decentralized application for counterfeit detection.

6. System Architecture

The system architecture of the proposed blockchain-based counterfeit product detection framework is designed as a decentralized, secure, and traceable model that integrates cryptographic hashing, blockchain storage, and QR-based verification. The architecture is divided into three major layers: Data Generation Layer, Blockchain Layer, and Verification Layer, ensuring end-to-end product authentication.

Fig.1 : System Architecture of the proposed system

6.1 Data Generation Layer (Manufacturer Phase)

The process begins at the manufacturer level, where product details such as product name, batch number, manufacturing date, and other metadata are entered into the system. A unique Product ID (PID) is generated for each item to ensure distinct identification.

This product information is then processed using a cryptographic hashing algorithm (SHA-256), which converts the data into a fixed-length hash value. This hash acts as a digital fingerprint of the product, ensuring data integrity and preventing unauthorized modification.

6.2 Blockchain Layer (Secure Storage & Tracking)

The generated hash value, along with product details, is stored in the blockchain as a transaction block. Each block contains:

Product ID
Hash value
Timestamp
Previous block reference

This structure ensures immutability and tamper resistance, as any change in data would alter the hash and break the chain.
A QR code is generated containing the Product ID, which serves as a reference key to access blockchain data. As the product moves through the supply chain (manufacturer → distributor → retailer), each transaction is recorded in the blockchain, creating a transparent and traceable history.

6.3 Supply Chain Interaction Layer

- At every stage of product movement:
- Supply chain participants update product status
- Each update is verified and appended to the blockchain
- The system maintains a continuous and chronological record of product flow
- This ensures real-time visibility and accountability across all stakeholders.

6.4 Verification Layer (Customer Phase)

When the product reaches the end user, the verification process is initiated:
The user scans the QR code or enters the Product ID
The system retrieves stored product data from the blockchain
A new hash is generated from the scanned/input data
The newly generated hash is compared with the stored hash

6.5 Authentication Mechanism

If both hash values match:

- The product is verified as genuine

If hash values do not match:

- The product is identified as counterfeit

This comparison ensures data authenticity, integrity, and non-repudiation.

6.6 Output Layer

The final verification result is displayed to the user in a clear format:
Genuine Product
Counterfeit Product
This provides a user-friendly interface for instant decision-making.

6.7 Architectural Advantages

- Ensures end-to-end traceability
- Provides tamper-proof data storage
- Eliminates dependency on centralized authorities
- Enables real-time product authentication
- Strengthens trust among supply chain participants

The proposed system architecture effectively integrates blockchain, cryptographic hashing, and QR-based identification to establish a secure, transparent, and decentralized counterfeit detection mechanism. It ensures that every product can be authenticated reliably, thereby minimizing fraud and enhancing supply chain integrity.

7. System Design and Methodology

The proposed system is designed as a decentralized, modular, and secure framework that integrates blockchain infrastructure with cryptographic validation to ensure reliable counterfeit detection. The design emphasizes data integrity, transparency, and scalability, while the methodology outlines the step-by-step operational workflow of the system.

7.1 System Design

The system follows a layered and modular architecture, enabling efficient interaction between different components. It consists of the following key modules:

1. Product Registration Module

- Managed by the manufacturer
- Captures product metadata such as product name, batch number, and manufacturing details
- Generates a unique Product ID (PID) for each item
- Initiates blockchain entry for the product

2. Cryptographic Processing Module

- Applies SHA-256 hashing algorithm to product data
- Produces a unique hash value acting as a digital signature
- Ensures data integrity and resistance to tampering

3. Blockchain Storage Module

- Stores product details and hash values in a distributed ledger
- Each transaction is recorded as a block linked via hash pointers
- Guarantees immutability, transparency, and decentralization

4. QR Code Generation Module

- Generates a QR code mapped to the Product ID
- Serves as an interface between physical products and digital records
- Enables quick access to blockchain data

5. Supply Chain Management Module

- Tracks product movement across multiple stakeholders
- Updates transaction records at each stage (manufacturer → distributor → retailer)
- Maintains continuous product lifecycle history

6. Verification Module

- Allows customers to scan QR codes or enter Product ID
- Retrieves stored blockchain data
- Performs hash comparison for authenticity verification

7. User Interface Module

- Provides an interactive platform for all stakeholders
- Displays product details and verification results
- Ensures ease of use and accessibility

7.2 Methodology

The system operates through a structured workflow to ensure secure product tracking and verification:

Step 1: Product Initialization
Manufacturer registers the product in the system
Unique Product ID is generated
Step 2: Data Encryption
Product details are processed using SHA-256 hashing
A secure hash value is generated
Step 3: Blockchain Entry
Product data and hash are stored as a block in the blockchain
Timestamp and previous hash ensure chain integrity
Step 4: QR Code Assignment
QR code is generated containing the Product ID
Attached to the physical product
Step 5: Supply Chain Updates
Each stakeholder updates product movement
Transactions are recorded in blockchain sequentially
Step 6: Product Verification
Customer scans QR code
System retrieves stored blockchain data
Step 7: Hash Comparison
New hash is generated from scanned data
Compared with stored hash
Step 8: Authentication Result
Match → Genuine Product
Mismatch → Counterfeit Product

7.3 Design Characteristics

Decentralized Control: Eliminates reliance on a central authority
Immutability: Ensures data cannot be altered once recorded
Traceability**: Provides complete product lifecycle visibility**
Security: Utilizes cryptographic validation mechanisms
Scalability: Supports expansion across large supply chain networks

The system design and methodology collectively establish a robust, secure, and transparent framework for counterfeit detection. By integrating blockchain technology with cryptographic techniques and QR-based interaction, the proposed system ensures reliable product authentication and enhances trust across the supply chain ecosystem.

8. Workflow Implementation

The workflow implementation represents the complete operational sequence of the blockchain-based counterfeit detection system, derived from the system flow diagram. It involves four major entities—manufacturer, supplier, retailer, and customer—interacting through a decentralized blockchain network. The workflow ensures secure product registration, continuous tracking, and reliable verification using cryptographic validation and blockchain transactions.

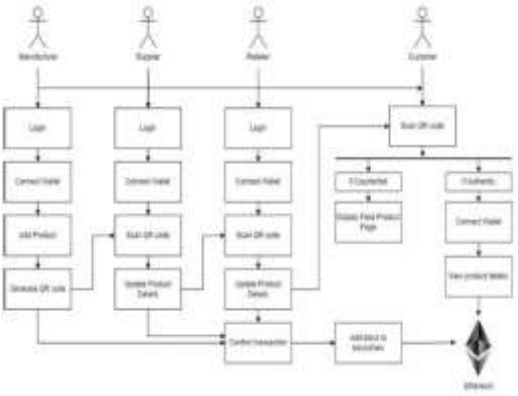

Fig.2 : System Workflow diagram

8.1 Workflow Description Based on System Flow

The process begins with product creation at the manufacturer level and progresses through multiple supply chain stages, including supplier and retailer interactions, before reaching the end customer. At each stage, transactions are authenticated using blockchain connectivity and wallet-based verification. This ensures that every update is securely recorded, maintaining transparency and preventing unauthorized modifications throughout the product lifecycle.

8.2 Step-by-Step Workflow Implementation

Step 1: Manufacturer Initialization

The workflow initiates when the manufacturer logs into the system and establishes a connection with the blockchain network using a digital wallet such as MetaMask. The manufacturer inputs essential product details, including name, batch number, and manufacturing specifications. The system then generates a unique Product ID (PID) for each item and creates a corresponding QR code, which is attached to the product for future identification and tracking.

Step 2: Product Registration on Blockchain

After data entry, the product information undergoes validation and is prepared for blockchain storage. A transaction is initiated, and the product details are recorded as a block in the blockchain ledger. This step establishes the origin of the product within the system and ensures that its initial state is securely stored and immutable.

Step 3: Supplier Interaction

When the product reaches the supplier, the supplier logs into the system and connects their digital wallet for authentication. The supplier scans the QR code attached to the product to retrieve its stored information from the blockchain. Relevant updates, such as transportation or handling details, are added to the system. Once verified, the supplier confirms the transaction, which is then recorded in the blockchain.

Step 4: Retailer Interaction

At the retailer stage, a similar process is followed. The retailer logs in, connects their wallet, and scans the QR code of the received product. The retailer updates the product status, such as inventory entry or readiness for sale. After confirming the update, the transaction is validated and prepared for blockchain storage.

Step 5: Blockchain Transaction Confirmation

Each update performed by supply chain participants, including suppliers and retailers, is verified using smart contracts. Once validated, the transaction is appended to the blockchain as a new block. This continuous addition of blocks ensures immutable tracking, meaning that the product's history cannot be altered or tampered with at any stage.

Step 6: Customer Verification Process

When the product reaches the customer, the verification process begins. The customer scans the QR code using a mobile or web application. The system then retrieves the complete product data and transaction history from the blockchain network for validation.

Step 7: Authenticity Check

The system performs an authenticity check by validating the retrieved data against stored blockchain records. If the data is consistent and matches the recorded history, the product is confirmed as genuine. In such cases, the system may request wallet authentication and display complete product details along with its transaction history. If inconsistencies or missing records are detected, the system identifies the product as counterfeit and redirects the user to a fake product alert interface.

Step 8: Result Display

Finally, the system presents the verification outcome to the user in a clear and understandable format. If the product is authentic, it displays a confirmation indicating a genuine product. If not, it alerts the user that the product is counterfeit, ensuring informed decision-making.

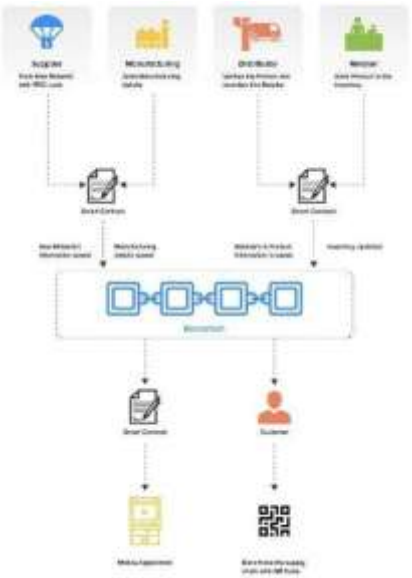

Fig.3 : User case diagram

8.3 Workflow Characteristics

The workflow is designed with role-based access control, ensuring that each participant-manufacturer, supplier, retailer, and customer-has specific functionalities. Blockchain validation guarantees that every action is authenticated and recorded securely. Wallet-based authentication enhances security by verifying user identity. The system ensures complete traceability by maintaining a detailed record of the product's journey, while its tamper-resistant nature prevents unauthorized modifications once data is stored.

9. RESULTS AND USER INTERFACE ANALYSIS

The developed blockchain-based application provides a functional interface for counterfeit product detection. The system offers two primary operations: product registration by manufacturers and verification by customers. During registration, manufacturers input essential details such as product ID, name, batch number, manufacturing date, and company information. Once submitted, the product is securely recorded on the blockchain through smart contracts, ensuring immutability and transparency. On the customer side, the verification module allows users to scan or enter product details to instantly retrieve its blockchain-stored history, thereby confirming authenticity.

9.1 User Interface

Fig.4 : User Interface

The backend connectivity is established using a local Hardhat environment, with Web3 integration and a deployed smart contract address, demonstrating successful blockchain interaction. This interface validates the project's objective of enabling secure product tracking and counterfeit detection in real time.

9.2 Inputs Product Details

In this stage, the manufacturer enters product details such as ID, name, batch number, date of manufacture, and company information. For example, the product "IPHONE" with batch number 457 was registered on 16-04-2026. Once submitted, the data is stored securely on the blockchain through smart contracts, ensuring immutability and authenticity. This step highlights how the system uniquely records each product to prevent duplication and counterfeiting.

Fig.5: Inputs products details

9.3 Product details

After entering the product information, the system successfully registers the item on the blockchain. The interface confirms this by displaying a transaction hash, which serves as a unique proof of registration. For example, the product "IPHONE" with batch number 457 was recorded along with manufacturer details, and the blockchain generated a secure transaction ID. This immutable record ensures that the product's authenticity can be traced at any point in the supply chain. The backend connection through Hardhat and the deployed smart contract validates that the registration process is fully integrated with blockchain technology.

Fig.6: Products details

The verification module confirms that the registered product is genuine. When the product ID is entered, the system retrieves blockchain-stored details such as product name, batch number, manufacturing date, manufacturer address, and ownership information. The interface displays the status as "Genuine (registered)" along with a QR code encoding the product ID, enabling quick validation by customers. The transaction history and actor details are securely linked to the deployed smart contract, ensuring transparency and traceability across the supply chain. This result demonstrates the system's ability to authenticate products and prevent counterfeit entries.

Fig.7: Product Counterfelt Detection

9.4 Counterfeit products result

When an unregistered product ID is entered, the system immediately flags it as counterfeit. The interface displays the message "Not found (possible counterfeit)", confirming that the product does not exist in the blockchain registry. This outcome demonstrates the effectiveness of the verification module in distinguishing genuine items from fake ones. By cross-checking product IDs against immutable blockchain records, the system ensures that only registered products can be validated, thereby preventing fraudulent entries into the supply chain.

Fig.8: Counterfeit products result

The developed system incorporates a web-based user interface designed to facilitate seamless interaction between users and the underlying blockchain infrastructure. The interface, as illustrated in the implementation results, provides a structured and intuitive environment for product registration and verification within the counterfeit detection framework.

The interface is titled "Product Counterfeit Detection" and operates as a blockchain-backed product registry deployed on a local development network. It includes two primary functional sections—registration and verification—accessible through dedicated navigation options. The presented screen focuses on the manufacturer registration module, which serves as the entry point for product data initialization.

The registration panel is organized into clearly defined input fields, including Product ID, Product Name, Batch Number, Manufacturing Date, and Manufacturer Details. These fields enable the manufacturer to input essential product metadata in

a structured format. The inclusion of a date selector ensures standardized input for manufacturing information, while the manufacturer details field captures organizational credentials such as company name, address, and contact information.

A prominent "Register on Blockchain" action button is provided to initiate the transaction process. Upon activation, the system communicates with the blockchain backend through a local node, invoking the deployed smart contract responsible for storing product data. The interface displays backend connectivity details, including the local host address and smart contract identifier, indicating successful integration with the blockchain environment.

The design adopts a modern, minimalistic layout with a dark-themed background, improving readability and user focus. Input fields are centrally aligned, enhancing accessibility and reducing user interaction complexity. The interface ensures that all required data is collected before submission, thereby minimizing input errors and improving data consistency.

Overall, the user interface demonstrates efficient integration between frontend components and blockchain services, enabling secure product registration with minimal user effort. It plays a crucial role in ensuring usability, accuracy, and reliability of the system, thereby contributing to effective counterfeit detection and product authentication.

10. CONCLUSION

This paper presented a blockchain-based counterfeit product detection system that addresses the limitations of conventional supply chain verification mechanisms. By leveraging a decentralized architecture combined with cryptographic hashing and QR code-based identification, the proposed system ensures secure, transparent, and tamper-resistant product tracking from the manufacturer to the end consumer.

The integration of smart contracts enables automated validation of transactions, eliminating dependency on centralized authorities and reducing the risk of data manipulation. Each product is uniquely identified and recorded on the blockchain, allowing real-time traceability and reliable authentication at every stage of the supply chain. The implementation results demonstrate that the system effectively detects counterfeit products by identifying inconsistencies in product data and transaction history.

Furthermore, the proposed framework enhances trust among stakeholders by providing immutable records and user-friendly verification through QR scanning. Although challenges such as scalability and transaction latency exist, the system offers a robust foundation for secure supply chain management.

In conclusion, the proposed approach significantly improves counterfeit detection capabilities and establishes a scalable and trustworthy solution for modern supply chain ecosystems.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.
Available: https://bitcoin.org/bitcoin.pdf

[2] M. Swan, Blockchain: Blueprint for a New Economy, O'Reilly Media, 2015.
Available:
https://www.oreilly.com/library/view/blockchain/9781491920487/

[3] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," IEEE Access, vol. 4, 2016, pp. 2292–2303.
Available: https://ieeexplore.ieee.org/document/7467408

[4] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology:
Architecture, Consensus, and Future Trends," IEEE International Congress on Big Data, 2017.

[5] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in Internet of Things: Challenges and
Solutions," IEEE Internet of Things Journal, 2017.

[6] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain Technology:
Beyond Bitcoin," Applied Innovation Review, 2016.

[7] T. Tian, "An Agri-food Supply Chain Traceability System for China Based on RFID &
Blockchain Technology," IEEE International Conference, 2016.

[8] H. Hasan and K. Salah, "Blockchain-Based Solution for Proof of Delivery of Physical
Assets," IEEE Access, vol. 6, 2018, pp. 45565–45577.

[9] F. Casino, T. K. Dasaklis, and C. Patsakis, "A Systematic Literature Review of Blockchain
Based Applications: Current Status and Future Directions," Telematics and Informatics, 2019.

[10] Y. Lu, "Blockchain and the Related Issues: A Review of Current Research Topics,"
Journal of Management Analytics, 2018.

[11] D. Tapscott and A. Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin
is Changing Money, Penguin, 2016.

[12] G. Wood, "Ethereum: A Secure Decentralized Generalized Transaction Ledger,"
Ethereum Project Yellow Paper, 2014.

[13] NIST, "Secure Hash Standard (SHS)," Federal Information Processing Standards
Publication, 2015.