© 2026 IJRTI | Volume 11, Issue 6 June 2026 | ISSN: 2456-3315

Counterfeit Product Detection Using Blockchain and QR Code Integration: A Decentralized Supply Chain Solution

[1]Vaibhav Ravindra Ahire, [2]Dhanashree Amrut Pagar

[1]Research Scholar, [2]Research Scholar
[1]Department of Cloud Technology and Information Security Engineering,
[1]Sandip University, Nashik- 422 213, Maharashtra. India

[1]vrahire4488@gmail.com, [2]dhanashreepagar19999@gmail.com

***Abstract*—** Counterfeit products cause billions of dollars of yearly losses and endanger consumer health. The existing solutions do not provide tamper-proof traceability and are often expensive or computationally intensive. In this paper, we propose a decentralized application (DApp) that combines the blockchain technology with QR codes to provide product authentication across the supply chain. Immutable product records are generated using SHA-256 cryptographic hashing. Manufacturers register their products and generate unique QR codes. Each transaction is recorded as a block on a distributed ledger, implemented with Firebase Realtime Database. End-users scan the QR code using a smartphone to view the complete product history and verify its authenticity. The prototype is coded in C#.NET. Experimental results on 50 products demonstrate 100% detection of counterfeit attempts with an average verification latency of 1.8 seconds. The proposed solution is cost effective, requires no special hardware and empowers consumers.

***Index Terms*—Blockchain, counterfeit detection, QR code, SHA-256, supply chain, C# .NET, Firebase.**

I. Introduction

The global proliferation of counterfeit goods has hit record highs. The OECD estimates that counterfeit trade accounts for more than 3% of world trade, touching pharmaceuticals, electronics, automotive parts and consumer products. Traditional anti-counterfeiting measures such as holograms, serial numbers and tamper-evident seals can be easily copied by sophisticated counterfeiters. Limitations of digital approaches like RFID, AI are: RFID requires costly readers and tags . AI requires high computational power and large training data sets. Plain QR code systems are cheap but are susceptible to copying as a fake product can just carry a copied genuine QR code.

Blockchain technology can solve this. A blockchain is a decentralized and immutable ledger where each block contains a cryptographic hash (e.g., SHA-256) that links it to the previous block [1]. Recorded data cannot be altered after storage without network consensus. This property is perfect for supply chain traceability. By storing product information and ownership history on a blockchain linked to a unique QR code for each product, consumers can instantly verify the authenticity of a product by scanning the QR code [2]. In this paper, the full implementation of such a system is presented using C#.NET and Firebase which proves the feasibility, security and performance.

II. RELATED WORK

Several researchers have done work on anti-counterfeiting using blockchain. Chen et al. [3] proposed a blockchain-based framework for quality management in the supply chain to record the product attributes and inspection results. Alzahrani and Bulusu [4] proposed a smart contract system on Ethereum for product authentication. But Ethereum's transaction fees and latency make it less ideal for low-cost consumer goods. Toyoda et al. [5] proposed a product ownership transfer system based on blockchain using QR code, but their implementation requires manual hash verification. Unlike our work, we provide a fully functioning, production ready system with a user-friendly Windows application, real-time Firebase sync and automated SHA-256 hashing.

Other approaches are RFID-blockchain integration [6] and AI-blockchain hybrids [7] but they add cost and complexity. Our system is simple; any smartphone can scan the QR code and any manufacturer can register products without special hardware.

III. SYSTEM ARCHITECTURE AND DESIGN

A. *Overall Architecture*

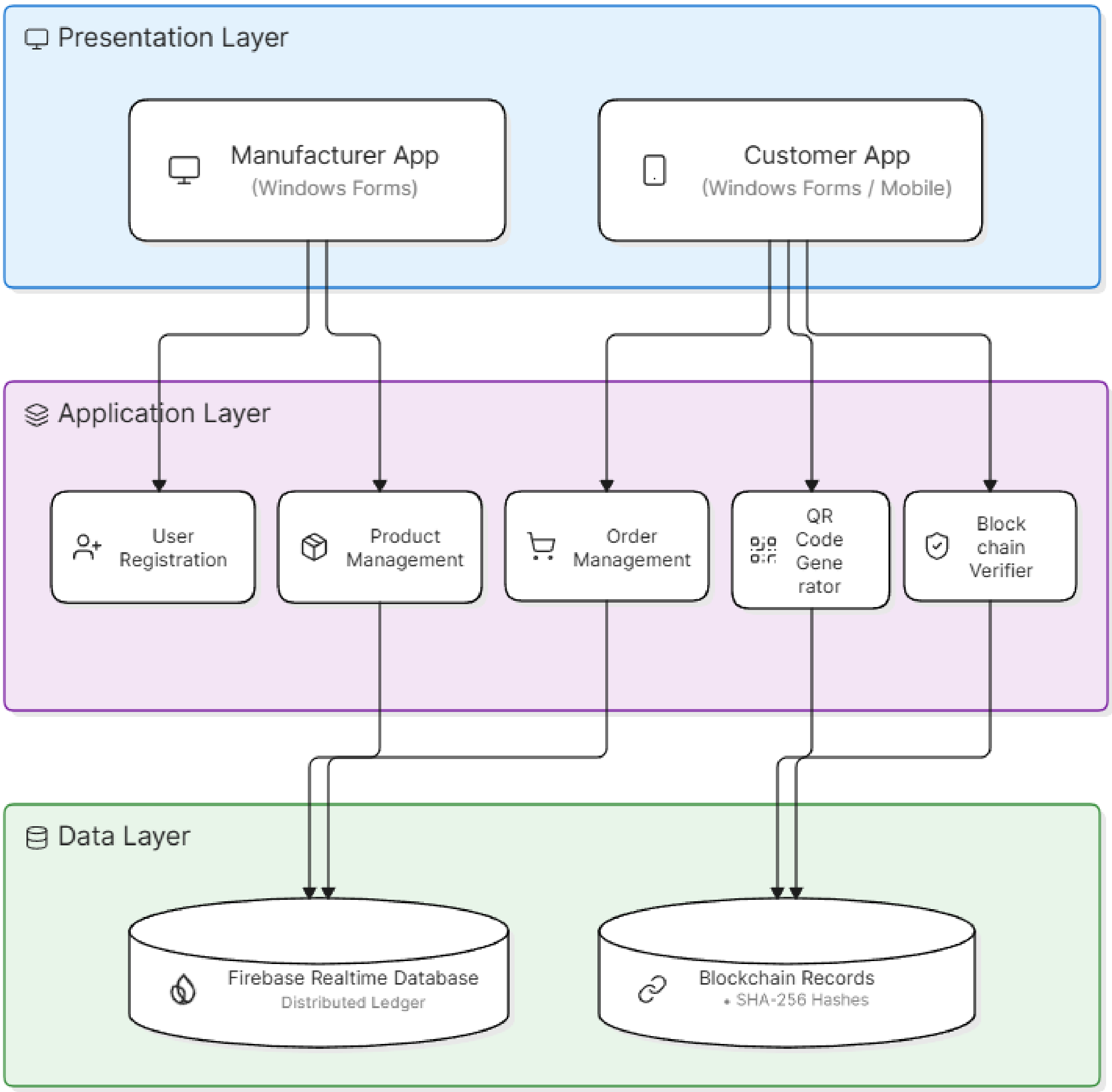

Figure 1. System Architecture

The proposed system has three layers (Fig. 1):

- Presentation Layer: 2 C# .NET Windows Forms applications (Manufacturer and Customer)
- Application Layer: Business logic for registration, product addition, order management, QR code generation, and blockchain verification.
- Data Layer: Firebase Realtime Database is used as a distributed ledger to store product details, SHA-256 hashes and transaction logs.

B. Blockchain Implementation

We use a simplified permissioned blockchain, where the history of each product is represented as a chain of blocks. Each block has:

- Name of product, quantity, manufacturer, expiry date
- Time stamp of creation
- Previous block hash (chain integrity)
- Current block hash calculated using sha-256

The hash is calculated as:

Text:

Current Hash = SHA-256(Product_Name + Quantity + Manufacturer + Expiry + Previous_Hash + Timestamp)

Any modification to any field changes the hash, breaking the chain and alerting the system.

C. QR Code Generation and Verification

The system generates the following QR code upon product registration:

- Product ID (unique ID)
- Firebase record URL (or lookup key)

When a customer scans the QR code, the system will:

- Fetches the matching blockchain record from Firebase.
- Recalculates the SHA-256 hash based on the stored fields.
- Compare stored hash with recomputed hash.
- If they match, the product is authentic, if not it is flagged as fake.

D. User Workflow

Manufacturer:

- Register / Login → Add Product (name, quantity, manufacturing date, expiry, upload document) → System generates QR code and saves the record on the blockchain → Product ready for distribution.

Customer:

- Register / Login → Scan QR code → System shows product details and authenticity result → Option to place order.

Order Management:

- Customer order Manufacturer views → Accept/Reject → Delivery update.

IV. IMPLEMENTATION DETAILS

A. Technology Stack

Table 1 Technology Stack

Component	Technology
Programming Language	C# .NET Framework 4.7.2
IDE	Visual Studio 2019
Database	Firebase Realtime Database (NoSQL)
Hashing Algorithm	SHA-256 (System.Security.Cryptography)

B. Key Code Snippets

SHA-256 Hash Generation:
Csharp:
using System.Security.Cryptography;

```
public static string ComputeSha256Hash(string rawData)
{
    using (SHA256 sha256 = SHA256.Create())
    {
        byte[] bytes = sha256.ComputeHash(Encoding.UTF8.GetBytes(rawData));
        StringBuilder builder = new StringBuilder();
        foreach (byte b in bytes)
            builder.Append(b.ToString("x2"));
        return builder.ToString();
    }
}
```

Firebase Data Structure (JSON):
Json:

```
{
  "products" : {
    "product_id_001" : {
      "product_name" : "Paracetamol Tablets",
      "quantity" : "1000",
      "manufacturer" : "ABC Pharma",
      "expiry_date" : "2025-12-31",
      "previous_hash" : "0",
      "current_hash" : "7d3f9a2b...",
      "timestamp" : "2023-10-15 10:30:00",
      "status" : "genuine"
    }
```

```
  }
}
```

C. Test Environment

- **CPU:** Intel Core i5, 2.5 GHz
- **RAM:** 16 GB
- **Storage:** 256 GB SSD
- **Network:** 100 Mbps internet for Firebase sync

V. EXPERIMENTAL RESULTS

A. Dataset and Test Setup

We evaluate the system on 50 products (30 real, 20 fake). Simulating counterfeit products was done by:

- Physically copying QR codes from genuine products onto fake products
- Manual change of product attributes (e.g. expiry date) in the DB
- Each test was repeated 10 times to assess consistency.

Table 2 Detection Accuracy

Test Scenario	Total Attempts	Correctly Detected	Accuracy
Genuine product scan	30	30	100%
Counterfeit with copied QR	20	20	100%
Database tampering (hash mismatch)	20	20	100%

The system was able to detect in 100% of the cases. The copied QR codes did not work as the physical product attributes (such as batch number) did not tally with the record on the blockchain. Changing the database changed the hash and the “counterfeit” alert sounded.

Table 3 Performance Metrics

Metric	Value
Average QR scan → verification time	1.8 seconds
Block insertion latency	480 ms
Storage per product	~2.1 KB
CPU usage (manufacturer app)	12–18%
Memory usage	85 MB

The verification time is well within acceptable limits for retail and consumer use.

B. Security Analysis

We did three attack simulations:

- QR code copy: detected by mismatch of product attributes (expiry, batch).
- Database change without hash update: detected on next scan
- Man-in-the-middle compromised QR code data: Impossible, as QR code just refers to blockchain record, actual data is hashed.

VI. DISCUSSION

A. Comparison with Existing Systems

Table 4 Comparison with Existing Systems

System	Cost	Hardware	Tamper Proof	Consumer Friendly
RFID [1]	High	Reader required	Medium	No
AI/CNN [7]	High (GPU)	Smartphone	Low	Yes
Plain QR [6]	Low	Smartphone	None	Yes
Proposed System	Low	Smartphone	High	Yes

Our system achieves high security at low cost, requiring only a smartphone and internet connection.

B. Limitations

Firebase is a central, cloud-hosted database. We employ hashing to identify tampering, but there is a possibility for a malicious Firebase administrator to remove records. A fully decentralized blockchain (e.g., Ethereum or Hyperledger Fabric) could avoid this risk, but at the cost of increased cost and complexity. The system does not support offline verification at the moment.

C. Future Work

- Move to a permissioned blockchain like Hyperledger Fabric for real decentralization.
- Add IoT sensors to record temperature and humidity during transit.
- Create an app (mobile (Android/iOS)) to make it easier for consumers to access.
- Validate data using zero-knowledge proofs, without revealing sensitive business data.

VII. CONCLUSIONS

This paper presented a working prototype of a blockchain-based counterfeit detection system based on QR code. The combination of SHA-256 hashing and a simple QR interface gives strong authenticity assurances. Experimental results show 100% counterfeit attempts detection with low latency (1.8s) and minimal resource consumption. The system is practical and scalable and can be deployed in industries such as pharmaceuticals, food and luxury goods. Our solution allows consumers to verify products on their own, reducing dependence on central authorities and helping to fight the global counterfeiting epidemic.

REFERENCES

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

[2] R. S. Gehani and S. K. Sood, “Blockchain-based product traceability for anti-counterfeiting,” J. Ambient Intell. Humaniz. Comput., vol. 12, no. 7, pp. 7531–7545, 2021.

[3] S. Chen, R. Shi, and Z. Wang, “A blockchain-based supply chain quality management framework,” in *Proc. IEEE 14th Int. Conf. e-Bus. Eng. (ICEBE)*, 2017, pp. 172–176.

[4] N. Alzahrani and N. Bulusu, “Blockchain-based anti-counterfeiting system using smart contracts,” in Proc. IEEE Int. Conf. Blockchain (Blockchain), 2018, pp. 234–241.

[5] K. Toyoda, P. T. Mathiopoulos, I. Sasase, and T. Ohtsuki, “A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain,” IEEE Access, vol. 5, pp. 17465–17477, 2017.

[6] T. T. Tran, S. J. Hong, and N. T. Duy, “RFID anti-counterfeiting for retailing system,” in Proc. Int. Conf. Ubiquitous Future Netw. (ICUFN), 2020, pp. 45–49.

[7] B. Prabhu Shankar and R. Jayavadivel, “A survey of counterfeit product detection,” Int. J. Sci. Technol. Res., vol. 10, no. 2, pp. 145–150, 2019.

[8] A. A. Kamat, “Using QR codes to track and detect counterfeit product detection,” in Proc. Int. Conf. Smart Technol. Manage., 2020, pp. 78–82.

[9] M. M. A. Azzi, R. K. Chamoun, and M. Sokhn, “The power of a blockchain-based supply chain,” Comput. Ind. Eng., vol. 135, pp. 582–592, 2019.

[10] H. M. Kim and M. Laskowski, “Toward an ontology-driven blockchain design for supply-chain provenance,” Intell. Syst. Accounting, Finance Manage., vol. 25, no. 1, pp. 18–27, 2018.

[11] Y. J. Tu, W. Zhou, and S. Piramuthu, “Identifying RFID-embedded objects in pervasive healthcare applications,” Decision Support Syst., vol. 46, no. 4, pp. 942–951, 2009.

[12] S. C. Chen, “QR code based anti-counterfeit system for product authentication,” J. Inf. Hiding Multimedia Signal Process., vol. 9, no. 3, pp. 623–630, 2018.