International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 06 | June - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Blockchain-Powered Product Authentication and Counterfeit Detection Using QR Code Technology

Ms K. Ashwini, Gudikati Ashok, T. Uttej, K. Rakhi
Assistant Professor, Department of Computer Science and Engineering
, Geethanjali College of Engineering and Technology, Hyderabad,India
Final Year, Department of Computer Science and Engineering,
Geethanjali College of Engineering and Technology, Hyderabad,India

***Abstract*—** The trend of counterfeit or replica products is becoming an issue in several industries including pharmaceuticals, fashion, electronics, etc. Because of this, a secure and transparent way to check the authenticity of these types of products is required. The system proposed in this paper implements product authentication, based on blockchain technology and QR code technology for instant verification of the legitimacy of a product. The system allows manufacturers to register their products on a secure and tamper-proof blockchain ledger. Once registered, each item is assigned a unique QR code. For shoppers or retailers wanting confirmation and disclosure on a product, scanning the QR code displays legitimacy, confirmed against the blockchain ledger. The system has a role based access control model, allowing secure interaction between manufacturers, retailers and admins. The QR code scanner app also provides scan history, re-verify, and review functionality for users that want to leave feedback about the verification practice. We believe this software approach provides full transparency, effective traceability, and trust, greatly reducing the chance or risk of counterfeit product, or replica product distribution in the supply chain.

***Keywords*—**Blockchain, Product Authentication, QR Code, Counterfeit Detection, Supply Chain, Traceability, Role-Based Access

I. INTRODUCTION

The rising presence of counterfeit goods has become a serious problem in sectors like seeds, pharmaceuticals, electronics, and consumer goods. Counterfeit goods negatively influence not just consumer safety but also billions of dollars in losses and brand degradation every year. Traditional anti-counterfeit methods are not effective, as the protection mechanisms, holograms and barcodes, are easily altered or replicated.

Blockchain has emerged as a disruptive solution that can provide data integrity, decentralization, and transparency. As an immutable ledger, it is very effective at tracking the origin and flow of goods from the point-of-origin to the end-user. When combined with existing QR technologies for ease of use, blockchain creates an efficient and scalable solution, allowing end-users to easily verify a product's authenticity by scanning the product.

Recent investigations and deployments of blockchain-based traceability systems have primarily lacked user-level participation or do not provide real-time re-verifications and feedback on products. To account for these limitations, this contribution proposes a hybrid solution leveraging blockchain inspired data in storage, which is combined with a role-based QR verification component. Using this solution, manufacturers can enter product details and generate unique QR codes for their products. Retailers and consumers can do a real-time scan and independently verify their true authenticity. Re-verification, verification logging, and user feedback ensures increase transparency and trust that is active and present in the system.

In today's supply chain, where products often pass through several stakeholders before reaching the end consumer, product authenticity must be established and verified at each stage of the supply chain. Counterfeiters will look for any loophole in the distribution channels to sell counterfeits that visually resemble the original product. Current centralized verification systems are also vulnerable to tampering, lack and transparency and rely on trust of a sole authority. By decentralizing the verification process, and enabling each stakeholder (manufacturers, retailers, consumers) the ability to independently verify using QR codes, the proposed offering provides a secure form of data verification at each level within the distribution channel.

II. RELATED WORK

Counterfeit detection has gained increasing significance over the last few years, particularly as there are global threats emerging in supply chains. Traditional solutions have generally included using barcodes, holograms, and RFID-based systems where fraud is concerned. Unfortunately established solutions still have limitations including data tampering, data duplication or central control. With the advancements in blockchain technology, researchers are now looking to leverage the unique capabilities of blockchain technology to provide tamper-proof and decentralised protection of product information, supporting the rest of the supply chain in terms of end-to-end traceability.

Recent indications of research have highlighted blockchain-based authentication systems, featuring smart contracts and QR codes. Some models have enabled secure tracking of products and fraud tampering protection; however, these systems do not highlight end-consumer visible functionality, including, re-verification, product ratings systems or retrievable record scan history. Rather than presenting yet another solution, this work combines blockchain concepts with role-based access and QR verification. The end result allows for data registration (product data) from manufacturers, product authenticity verification from retailers (in real-time using a scan), and feedback/referral from end-users — resulting in an overall improved system with transparency for all users and longitudinal participation for counterfeiting prevention.

III. BACKGROUND AND OBJECTIVES

The increased threat of counterfeit products within global products, including pharmaceuticals, electronics, and consumer goods, has highlighted the need for increased and accessible verification processes. Previous verification processes to supply chain verification, including barcodes, RFIDs, and holograms, are susceptible to copying, lack end-to-end transparency or the use of engagement, are subject to centralized risk in the form of manipulated data, and limited staleway access.

To alleviate, this paper identifies a blockchain-based product verification system in conjunction with QR code product codes. This system would allow manufacturers to identify and register their products, produce unique QR code products to facilitate real-time product verification by retailers and end consumers. However, the system provides role-based access along with scan tracking and accessibility for re-verification and user feedback capabilities to instil increased transparency, authenticity, and traceability throughout a product life cycle.

IV. METHODOLOGY AND PARAMETERS

Methodology:

A. **System Overview** – The proposed blockchain-based product authentication system is based on secure product registration, dynamic QR code generation, and real-time verification, on a centralized database, following blockchain principles to ensure data immutability, transparency, and traceability. The system has three modules in total: Manufacturer, Retailer, and Admin. Each role has limited access and privileges to provide a secure storage and role-based functionality of the data.

B. **Manufacturer Module** – Manufacturers are authenticated users who can register products by filling up relevant details such as product name, category, product ID, batch number, and manufacturing date. Upon submission, each product is given a dynamically generated QR code. The QR codes are connected with product records. Manufacturers also receive a dashboard showing their registered product entries with status indicators.

C. **Retailer Verification Module** – The retailers are provided with a login site to verify the genuineness of the products by scanning or uploading the related QR code. The QR code read and compares the information that is embedded within the QR code with the records in the system. When the information compare the product is validated as genuine. When mismatches and unknown products are scanned, the system alerts as such. Day and time of each verification is stored in the system.

D. **Administrator Role** – The administrator manages the entire system, such as user accounts, product records, and verification logs. Admins have the ability to approve or block manufacturers or retailers, track feedback, and examine overall scan activity. They are the highest authority in the system and can delete any suspicious or duplicate entries. Admin-level visibility encompasses verification history, feedback summaries, and suspicious scan alerts.

E. **QR Code Generation and Encoding** - QR codes are created through programming in Python. One of the libraries example is the qrcode library. The QR codes produced encode important product information that cannot be altered after it has been created. Such information that can be encoded includes the unique product ID, manufacturer name, the batch of product, and manufacturing date. The QR code image file type (PNG) is saved and referenced in the database against the product record. Once QR codes are created, they are basically tamper-proof, are assigned a one-to-one relationship with its original record.

F. **Product Verification Workflow –** When the QR code is scanned in a product, the system will read the encoded attributes for attributes and compare them against records in the database. If a match is found, the product is flagged as verified. It will log the attempt at verification, timestamp the date and time of that scan, as well as the name of the retailer who performed the scan. The code can also be scanned multiple times, with history of the scan events retained. This is so that there is a record of the scan for traceability and for security audits.

G. **Database Design and Data Integrity –** The application employs SQLite to store product records, user information, scan logs, and feedback. Tables are normalized to eliminate redundancy and provide consistency. Foreign key constraints are employed to associate products with manufacturers and scan events with retailers. After a product is registered, its fundamental fields are immutable, simulating the non-editable aspect of blockchain records.

H. **Security Considerations -** User access is role-based, and the QR data is safely encrypted to prevent tampering. By creating QR image on the server-side rather than user-changeable, we limit the opportunity of tampering. If an admin receives a scan of a blocked product or invalid QR code has been recorded, the admin receives a notification. All information about products is read-only after it is registered, helping preserve trust around the product data.

I. **Interface Design and Workflow Navigation -** The user interface is simple and clear. There is minimal training for manufacturers and retailers, with advanced filters, logs, and user management functions in the admin dashboard. UI flow is also optimized to cut down on repetitive actions and guide users from login to verification.

J. **Scalability and Extensibility -** The system is built using Django, enabling easy scalability by connecting to larger databases such as PostgreSQL or cloud-source QR APIs. Other modules, such as email notifications or block-chain wallet integration, can be added at a later date. The modular construction ensures that features can grow into viable additions without compromising the integrity of the core system.

K. **User Interaction and Real-World Deployment -** The system deployed is accessible using web browsers and tested for device compatibility. Retailers are able to check products at points of sale, and manufacturers are able to control products from anywhere. The web-based interface provides low barriers to entry and enables integration into real-world supply chains with minimal infrastructure requirements.

Parameters:

The proposed system incorporates various parameters throughout the product registration, verification, logging, and feedback processes.

Some of those parameters are:

1. **Product ID** – Product ID is a system-generate unique alphanumeric code given to every product while registering. This serves as the master key of the product's data entry within the blockchain-based ledger. This is also encoded in the corresponding QR code and thus becomes an integral part while scanning and authentication. Its uniqueness prevents any two products from being confused with each other. In blockchain terminology, this ID is an immutable link to the original registration block.

2. **Manufacturer Name** – This parameter is used to store the registered name of the producer who enters the product into the system. This parameter guarantees traceability and responsibility by associating every product with its rightful maker. This linking is crucial in avoiding impersonation or duplication of brand identity. At product verification, the system reads and displays this information, assuring end-users that the product comes from a certified origin.

3. **Batch Number** – The Batch Number is another level of classification and comes into play to aggregate products produced under the same cycle of production. The batch number is critical in aiding targeted product recalls, performing quality auditing, and analyzing inventories. The batch number is incorporated within the QR code to facilitate easy confirmation and ensure that both consumers as well as supply chain members can confirm that the product is from a valid production batch.

4. **Product Category** – The Product Category specifies the wider categorization under which a product belongs—e.g., pharmaceuticals, electronics, fashion, or consumer goods. Categorization facilitates system scalability and supports role-based filtering and analytics, allowing administrators and manufacturers to more easily monitor trends, anomalies, and distribution patterns within various verticals. The parameter can also be utilized to customize AI-driven fraud detection models by product type.

5. **Manufacturing Date** – The Manufacturing Date captures the precise date the product was manufactured. The time-critical parameter is key to ensuring product freshness, tracking inventory, and identifying expired products within the supply chain. The date is embedded in the QR code digitally and, upon scanning, assists the system in ascertaining if the product remains within its effective usage period. It also facilitates time-based analysis for lifecycle and shelf-life estimates.

6. **QR Code Image** – An image file that holds dynamically generated product data in the form of encodes. A digital fingerprint for the product, which is placed on the server and associated with the corresponding product entry. A QR code would have to correlate its product record in order to be labeled authentic.

7. **Verification Timestamp** – Each time a QR code embedded within a product is scanned, the system registers a Verification Timestamp, which reflects the specific date and time of the scan. Having a timestamp list is useful for auditing purposes, so that administrators can watch verification evidence trends and identify unusual activity, such as excessive scanning or scanning from unfamiliar geolocations. The timestamp data is used in statistical reporting and to identify other signs of fraudulent or suspicious activity.

8. **Retailer ID** – The Retailer ID is a unique number assigned to retailers or verification agents who complete the scan and verification processes. This aspect is tied to scan logs so that all verification processes can be accounted for by user. It increases accountability and can help determine access control policies in the system. In the case of abuse or inaccurate reporting the Retailer ID is key for tracing the activity back to its origin.

9. **Scan Status** – Indicates the result of an attempt to verify. Can have values such as "Verified," "Invalid," or "Blocked." This parameter indicates if the scanned product succeeded in the verification test or was blocked by the system. Optional comments provided by the retailer while scanning an item. Observations such as quality, suspect pack or scan might be noted here as feedback. Comments are preserved in conjunction with the scan history and can be accessed by admin to look for mistakes and refine the system.records how many times a product has ever been verified. This can detect malicious behavior like heavy scanning on a single item and aids the fraud detection engines.

10. **Product Status** – Records if a product is active, blocked, or has expired. The admins can modify this status by hand if a product is proven to be a fake or under any disputes.

V. EXISTING SYSTEM

Today's systems for counterfeit detection are still based on traditional methods such as barcodes, holograms, RFID tags, and centralized databases. While these methods can provide a certain level of product tracking, they are grossly deficient; barcodes and holograms are easy to duplicate or modify, while RFID-based methods are more robust but require specific equipment to verify. Centralized databases present various vulnerabilities as they are a single point of failure, and act as a prominent attack vector as unauthorized people can tamper with the data and can lead to un-trustworthy or suspicious records for the product over its lifecycle.

Most of these systems involve supply chain intermediaries to verify the provenance of products, which provide little or, no transparency to the consumer, let alone the user. Additionally, these systems usually lack features such as scan history, feedback features, role-based traceability features, and the like, which affects the users' ability to detect suspicious patterns of

behavior and to communicate themselves at many levels of users.

VI. PROPOSED SYSTEM

The system proposes a blockchain-like, role-based product authentication platform that utilizes QR code technology for real-time validation. Product manufacturers can register products via a secure portal, providing important product information like batch number, manufacturing date, and category. A special QR code is created for each product and tied to its database entry. This QR code becomes the digital identity of the product and is utilized for verification during the supply chain.

The authenticity of a product can be confirmed by scanning the QR code through a web interface. The system reads the details, compares it with the recorded data, and provides the status of verification in real-time. Every scan gets recorded with a timestamp and an ID of the retailer to keep the record traceable. The users are also asked to give feedback after every verification, and it gets stored and read by the admin.

The platform features a secure admin dashboard for managing user activity, product listings, scan history, and feedback. Admins are able to mark or block products, approve or deny user access, and scan pattern review for identifying anomalies. This decentralized model of interaction coupled with a tamper-resistant data path provides transparency, trust, and greater security against counterfeit products throughout the supply chain.

VII. SYSTEM ARCHITECTURE

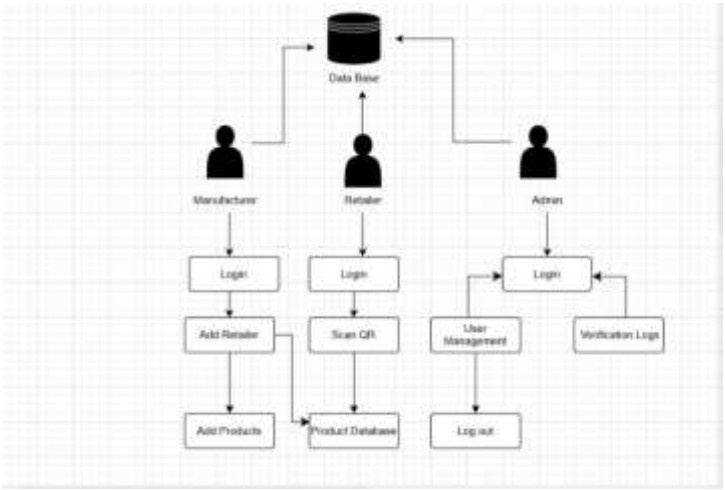

Fig 1: System Architecture.

The system architecture of the proposed system is based on modular and role-based design with three key components: Manufacturer Module, Retailer Module, and Admin Module. These are interfaced with each other by a central application developed using Django, which takes care of authentication, QR code generation, processing of data, and verification logic. The manufacturer adds products, which are stored in the database along with a generated uniquely QR code. The QR code is scanned by the retailers to authenticate the product, and the system checks the data against current entries. Every scan is recorded with a timestamp and user ID to facilitate re-verification and tracing. The admin has overall control to track system activity, manage users, and monitor feedback. The design provides for an unbroken data flow among modules, secure data storage, role-based access, and user interaction via a responsive web interface.

VIII. RESULTS AND DISCUSSION

Fig 2: Adding products details

The proposed system was successfully developed and tested for product authentication using QR codes and a role-based structure. Manufacturers could register products and create unique QR codes, whereas retailers authenticated product genuineness by scanning in real-time. Each scan was logged with timestamping, and retailer feedback was stored and retrieved for admin checking. The admin dashboard gave complete insight into scan history, listed products flagged, and user activity. The system efficiently detected counterfeit attempts by recognizing invalid QR data, and its modularity ensured secure, accurate, and traceable product validation for all user roles.

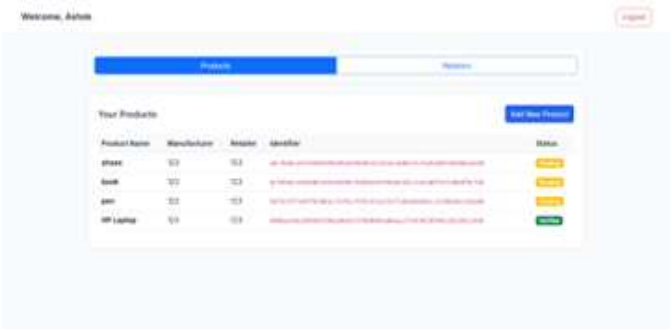

Fig 3: Product details with verification status

Fig 4: QR Scanner for product verification

One of the observations made in testing was how responsive,the system was in processing multiple verification requests at the same time and obtain near-immediate results.

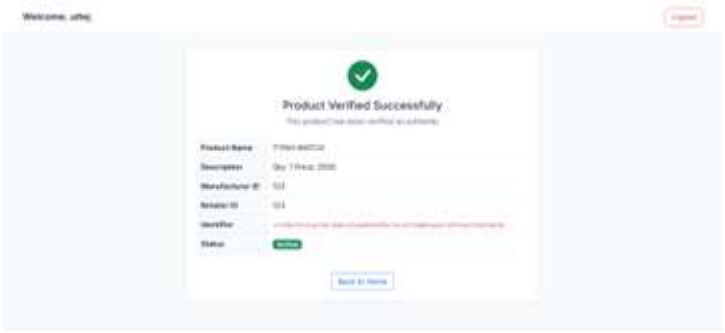

Fig 5: Product verification by scanning the QR

IX. FUTURE SCOPE

While the current implementation sufficiently addresses the primary concerns of product authentication and counterfeiting prevention, the system could certainly be further developed in other areas. By adding a decentralized blockchain ledger (e.g., Ethereum or Hyperledger), true immutability can be guaranteed and any use of centralized data storage can be eliminated. This change would improve security and provide more trustless interactions among supply chain actors.

In addition, moving to cloud-based infrastructure would enable improved scalability and availability, enabling the system to support high-volume, multi-location deployments. Subsequent versions of the platform could include mobile applications to support end-users, distributors, and quality inspectors to conduct instant QR code verification with handheld devices.

In addition, advanced fraud detection functions with machine learning could be incorporated to continually scan for behavior analysis, find anomalies, and automatically observe questionable activity. Logistics API integration, real-time alerts, multilingual interfaces, and periodic auditing of the blockchain could all facilitate adoption outside of the local geography. These developments would not only enhance security and efficiency but also broaden the system's applicability across industries such as pharmaceuticals, electronics, and luxury items.

Another upgrade entails the embedding of smart contracts to automate imperative verification and supply chain functions. Smart contracts could completely automate the verification of product registration postings, the verification of legitimate transactions between manufacturers and retailers, and the recording of verification updates with little to no manual input. Smart contracts would also prevent human error by creating efficiencies, and record only authorized data on the blockchain-- thus enhancing the visibility and trust of all parties.As the technology environment continues to advance, embedding newer innovations such as zero-knowledge proofs and digital watermarking may provide more robust privacy and anti-tampering measures. Zero-knowledge proofs would enable authenticity verification without revealing sensitive product information, vital in industries such as defense and pharmaceuticals. On a similar note, digital watermarking incorporated in product images or labels may serve as a second layer of verification that is tamper-proof and machine-verifiable. By remaining adaptive and receptive to these innovative technologies, the system will continue to be relevant and effective in the dynamic struggle against fake goods.

X. CONCLUSION

The proposed product authentication system based on a blockchain solution provides a practical and scalable answer to the quickly accelerating challenge of counterfeit products throughout supply chains; in part, by enabling secure product registration, to dynamic QR code production, and real-time validation with a role-based access approach that conserves data integrity, trust, transparency and traceability. It adeptly imitates critical blockchain properties like immutability and distributed trust in a lightweight web-friendly context. It demonstrated continuous effectiveness of performance viability in product authentication, scan history logging and administrative oversight via structured logging and role-based permissions. Its modularity, small footprint and ease of use and deployment make it especially desirable for small and medium enterprises. Its customizable aspect also opens up future opportunities for complete integration with blockchain ledgers, a mobile-based product verification, fraud detection based on machine learning, and a hosted cloud enabling scalability. With these attributes, the platform's future maturation can lead to a viable and effective end-to-end anti-counterfeiting solution, one that brings transparency and trust into global supply chains. So, the product experience is about deploying not just a technology platform, but also adding to the momentum of a safer, more transparent, and ethically intentioned commercial space.As consumers and companies become aware of authenticity in products, frameworks such as that proposed will assist in renewing trust in the supply chain. The intersection of blockchain, automation and data analytics represents a significant leap forward in counterfeiting prevention — from being conceived as an episodic task, it has become an intelligent and real-time process that recycles itself over the entire product lifecycle.

REFERENCES

[1] Tambe, T., & Chitkala, S. "Fake Product Detection using Blockchain," *IEEE Access*, vol. 8, pp. 107654-107661, 2020.

[2] Won-Shik, K., & Sondawale, I. "Detection of Counterfeit Products using Blockchain," *International Research Journal of Modernization in Engineering Technology and Science*, vol. 4, no. 5, pp. 876-881, May 2022.

[3] Product Identification in Retail Stores by Combining Faster R-CNN And Recurrent Neural Network by Rajib Ghosh (June 2023).

[4] Faisal Jamil, Lei Hang, KyuHyung Kim and DoHyeun Kim "A Novel Medical Blockchain Model for Drug Supply Chain Integrity Management in a Smart Hospital". MDPI Electronics 2019, 8,505, 2019.

[5] Brilliant Earth & Everledger. "Tracking Diamonds: Blockchain for Transparency," *Vogue Business*, Nov. 2018.

[6] Fake Product Identification System Using Blockchain by Anil Pawar, A. Quadri, meenaz Kolyal (2022).

[7] Fraud Detection: A Review on Blockchain by Anuska Rakshit, Shriya Kumar (2022).

[8] Aditya, K., & Gautam, H. "Combating Counterfeit Goods: A Blockchain-Enabled QR Code Authentication System," *JETIR*, vol. 10, no. 8, pp. 8671-8678, Aug. 2023.

[9] Ghodekar Prachi Shrikant, Pokharkar " Traceability and detection of counterfeit medicine supply chain through Blockchain " Nov 2019.

[10] Improving Fake Product Detection Using Ai- Based Technology by Eduard Daoud, Dang Vu Nguyen Hai, Hung Nguyen (April 2020).

[11] Kavita Kumari Kavita Sain and Olivier "CFDD (Counter Feit Drug Detection) using Blockchain in the Pharmaceutical Industry". IJERT Dec 2019.

[12] Deep Learning Approach for Cosmetic Product Detection and Classification by Se-Won Kim, Sang- Woong Lee (January 2021).

[13] Fake Product Detection Using Deep Learning Object Detection Models Eduard Daoud, Dang Vu, Hung Nguyen and Martin Gaedke (October 2020).

[14] Blockchain Applications in Supply Chain Transactions by Christian F. Durach, Till Blesik, Maximilian Von Diring, Markus Bick (March 2020).

[15] Detection of Counterfeit Cosmetic Products Using Image Processing and Text Extraction by Siddharth Mehta, Prajakta Divekar, Aditi Kolambekar & Amol Deshpande (2020).

[16] Kim, H. M., & Laskowski, M. (2018). “Toward an Ontology-Driven Blockchain Design for Supply Chain Provenance.” *Intelligent Systems in Accounting, Finance and Management*, 25(1), 18–27.

[17] Bhargava, B., et al. (2020). “Blockchain for Compliance and Integrity in the Pharmaceutical Supply Chain.” *Journal of the American Medical Informatics Association (JAMIA)*, 27(3), 394–400.

[18] Christidis, K., & Devetsikiotis, M. (2016). “Blockchains and Smart Contracts for the Internet of Things.” *IEEE Access*, 4, 2292–2303.

[19] Ray, P. P., Dash, D., & Salah, K. (2020). “Blockchain for IoT-Based Healthcare: Background, Consensus, Platforms, and Use Cases.” *IEEE Systems Journal*, 15(1), 85–94.

[20] Patil, P., & Shetty, S. (2021). “Counterfeit Detection Using Blockchain and QR Codes: A Multi-Layered Security Approach.” *International Journal of Computer Applications*, 183(21), 12–16.