International Journal of Scientific Research and Engineering Development-– Volume X Issue X, Year

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Product Authenticity Verification System Using Blockchain

Sharmima C.[1], Reshni S.[2], Praveena S.[3], Shree Darshan S. R.[4], and Yasvanth A.[5]

([1]Assistant Professor, Department of Computer Science and Engineering,
Sri Shakthi Institute of Engineering and Technology, Coimbatore, India)
([2]Department of Computer Science and Engineering,
Sri Shakthi Institute of Engineering and Technology, Coimbatore, India,
Email: reshni1975@gmail.com)
([3]Department of Computer Science and Engineering,
Sri Shakthi Institute of Engineering and Technology, Coimbatore, India,
Email: praveena.somu2003@gmail.com)
([4]Department of Computer Science and Engineering,
Sri Shakthi Institute of Engineering and Technology, Coimbatore, India,
Email: shreedarshan215@gmail.com)
([5]Department of Computer Science and Engineering,
Sri Shakthi Institute of Engineering and Technology, Coimbatore, India,
Email: Yasvantharjun2004@gmail.com)

----------**********----------

Abstract:

The growing prevalence of counterfeit products across global supply chains has posed unprecedented threats to consumer safety, regulatory compliance, and brand reputation. Existing verification measures, such as barcodes or holograms, have proven vulnerable to sophisticated forgery. This journal presents the Product Authenticity Verification System (PAVS), a robust blockchain-powered solution to authenticate products using dynamic QR codes, RSA-based digital signatures, and decentralized ledger storage. PAVS enables real-time provenance verification by allowing stakeholders—manufacturers, retailers, and consumers—to reliably check authenticity and product details directly from blockchain records. Through an exploration of literature, system methodology, security mechanisms, and pilot outcomes, this article demonstrates how PAVS reduces counterfeit incidents, enhances supply chain transparency, and paves the way for trust-centric, scalable, and interoperable anti-counterfeit solutions. Future enhancements, such as AI-based fraud detection and globalized smart contract workflows, are also discussed.

Keywords — **Anti-counterfeit, Blockchain, Consumer safety, Cryptography, Machine learning, Product authenticity, QR code**

----------**********----------

I. INTRODUCTION

The infiltration of counterfeit products into legitimate markets is a dilemma faced worldwide, resulting in economic losses of hundreds of billions of dollars annually, according to the Organization for Economic Co-operation and Development (OECD). High-risk sectors including pharmaceuticals, food, electronics, and cosmetics have been especially targeted, with fake products leading to serious health hazards and loss of consumer trust. Traditional anti-counterfeiting methods, such as holographic labels, barcodes, and RFID tags, are

often circumvented through improved forgery methodologies or supply chain manipulation. As a result, regulators and industries are seeking more reliable, technology-driven solutions that are resistant to tampering and distributed attack vectors.

Blockchain technology, with its inherent immutability, transparency, and decentralized consensus, offers a compelling framework to combat counterfeiting. When complemented by cryptographic authentication and machine-readable QR codes, blockchain can facilitate verifiable provenance data accessible throughout the product lifecycle. The Product Authenticity Verification System (PAVS) leverages these strengths: manufacturers onboard authentic product data as signed blockchain transactions, dynamic QR codes are generated for every batch or serialized item, and consumers, retailers, or regulators may instantly verify details using a secure web or mobile interface. This paradigm shift not only strengthens anti-counterfeit efforts but also fosters enhanced accountability, reduces administrative costs, and supports compliance in increasingly globalized supply chains.

This journal elaborates the architecture, operational mechanisms, literature background, pilot deployment metrics, challenges, and future roadmap of PAVS. The goal is to illustrate an integrated, scalable solution capable of addressing present and emerging threats in product authenticity.

II. LITERATURE SURVEY

Existing work in product verification and anti-counterfeiting spans methods from physical markers (holograms, secure inks), data encoding (barcodes, QR), and IT-driven approaches (centralized databases, mobile authentication). For instance, ScanTrust employs QR authentication and supply chain tracking, yet lacks digital signature verification, making it susceptible to QR code replication and forgery. IBM Food Trust and Provenance use blockchain to track provenance, but are highly centered on food industry verticals and depend on broad stakeholder adoption. Sproxil enables mobile validation of products using QR or SMS, but relies on centralized records and does not employ robust cryptographic verification; only pre-registered products can be checked, leaving gaps for unregistered fakes.

Research in blockchain-based anti-counterfeit systems highlights the benefits of distributed, tamper-resistant ledgers. The use of smart contracts for automated event handling (product registration, transfer, alerting) has been explored in the context of both public blockchains (e.g., Ethereum) and permissioned ledgers (e.g., Hyperledger Fabric). However, most previous solutions either do not tie blockchain records directly to on-product cryptographic verifications (digital signatures within QR codes), or face scalability and user adoption challenges.

The integration of digital signature schemes (such as RSA or ECDSA) with blockchain-backed QR verification is recognized as a novel approach, enabling verification without the need for online databases or trusted third parties at point-of-sale. Comprehensive literature confirms the potential of this architecture to fill authenticity gaps across multiple industries, especially when combined with user-friendly interfaces and secure manufacturer onboarding.

III. PROJECT OBJECTIVE

ERADICATE COUNTERFEITING BY ESTABLISHING A TAMPER-EVIDENT, DECENTRALIZED AUTHENTICITY LAYER FOR ALL PRODUCTS USING BLOCKCHAIN.

- Empower consumers with instant, real-time verification and factual product data (expiry, composition, etc.) prior to purchase.
- Arm manufacturers/brands with tools to register, manage, and monitor product security throughout its lifecycle.
- Safeguard retailer and distributor channels from infiltration of fake goods.
- Contribute to regulatory compliance in industries where product integrity is critical.
- Support rapid product recalls and root-cause analysis in the event of defects or safety issues.

IV. PROJECT METHODOLOGY

Stakeholder Onboarding: Manufacturers and supply chain partners are authenticated and registered on the website(SAFECHOICE) using blockchain credentials/MetaMask.

Product Registration: Manufacturers input product specifications (batch, serial, ingredients, manufacture/expiry dates). Details are securely stored both in MongoDB (quick retrieval) and on public/private blockchain as a smart contract entry.

QR Code Generation with Digital Signatures: For each batch/product, an RSA-signed QR code is

generated that encapsulates a cryptographic hash of its blockchain data.

Distribution & Logistics: The digitally signed QR code is affixed to the product packaging at factory-level and scanned at points throughout the supply chain, updating the blockchain audit log.

Real-Time Verification: At any sales/ retail/ consumption point, a user app or web interface scans the QR → verifies data + signature on-chain to confirm authenticity, and displays product status/details.

Auditing, Alerts, & Reporting: If a QR mismatch or expiry/fraud is detected, the system flags the product and notifies stakeholders. Audit logs and analytics are available on brand dashboards.

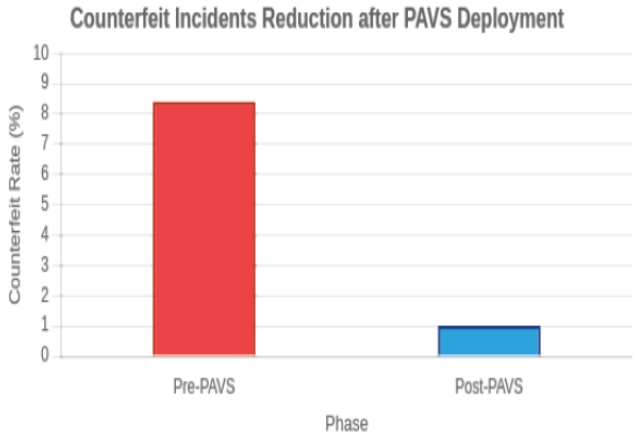

Fig 1 (Decrease in detected counterfeit products)

V. FEATURES

Blockchain-Backed Verification: Each product's authenticity is validated on-chain via a tamper-proof digital record, making forgery nearly impossible.

Dynamic QR Codes with Digital Signatures: Every batch/product gets a unique RSA-encrypted QR code ensuring traceability and integrity.

Real-Time Verification for Consumers: Consumers instantly verify product authenticity by simply scanning the code with a web/mobile app.

Manufacturer Dashboard: Product onboarding, QR code lifecycle management, and antifraud analytics for manufacturers/brands.

Expiry and Ingredient Tracking: Instantly alerts users about product expiry, allergens, or composition on scan.

Machine Learning QR Processing: Robust, error-tolerant QR code recognition even in physically damaged/lost QRs in the supply chain using ML reconstruction.

Transparency & Traceability: Full audit trail for each product, from manufacture to point-of-sale, visible to consumers and brands.

Alerts & Notifications: For expired or suspicious products, immediate user warning is provided at scan time.

VI. TOOLS AND SOFTWARE

Frontend: React.js (User/Manufacturer Portal), Tailwind CSS (UI Design), Google Fonts (Typography), Font Awesome (Icons)

Backend: Node.js, Express.js (RESTful API creation and business logic)

Database: MongoDB (high-speed temporary storage), Blockchain network (Ethereum, Hyperledger Fabric)/IPFS (immutable storage)

***QR Code Generation*:** qrcode.js, ML-based QR auto-recovery, Chart.js/ECharts.js for QR analytics

Security: RSA cryptography (digital signature), MetaMask integration (blockchain wallet authentication)

Smart Contracts: Solidity (Ethereum), Hardhat (development/testing), Web3.js (blockchain interactions)

Mobile/Web Interface: React Native or responsive PWAs for real-time scanning

***Decentralized Storage*:** IPFS

VII. BENEFITS AND IMPACT

Consumers: Prevents purchase of counterfeit goods, ensures health and safety, and boosts confidence in brands. Real-time ingredient/allergen/expiry alerts at scan point.

Manufacturers: Protects brand reputation, minimizes losses due to counterfeiting, offers actionable antifraud analytics and regulatory compliance, and increases consumer trust/loyalty.

Retailers: Reduces risk of stocking fake goods, avoids legal penalties, and improves sell-through rates of genuine products.

Governments/Regulators: Helps enforce supply chain regulations, reduces illicit trade, and simplifies recalls for public safety. Supports compliance with traceability mandates.

Impact:

Economic Impact: Reduces billions in global losses caused by counterfeiting, strengthens legal supply chains,

and increases revenues for legitimate brands and governments through improved taxation and compliance.
Societal Impact: Safer consumer products, lower incidence of fraud-related risks (health/environmental), and more ethical business environments.

VIII. FLOWDIAGRAM

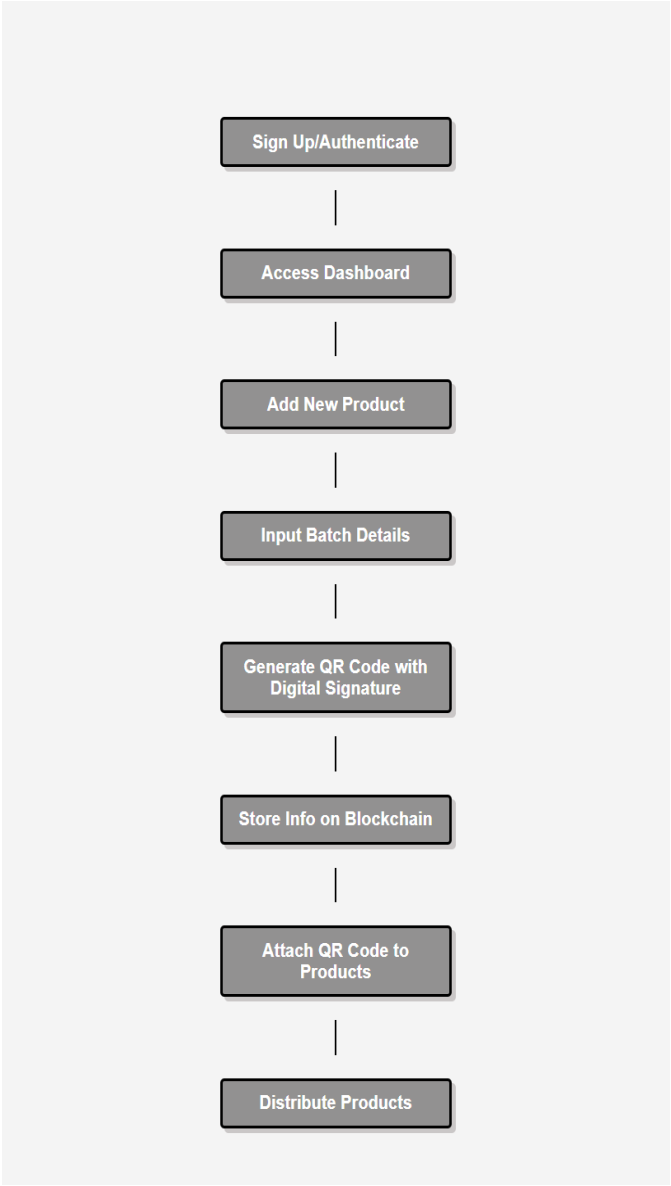

Fig 2 (Manufacturer workflow)

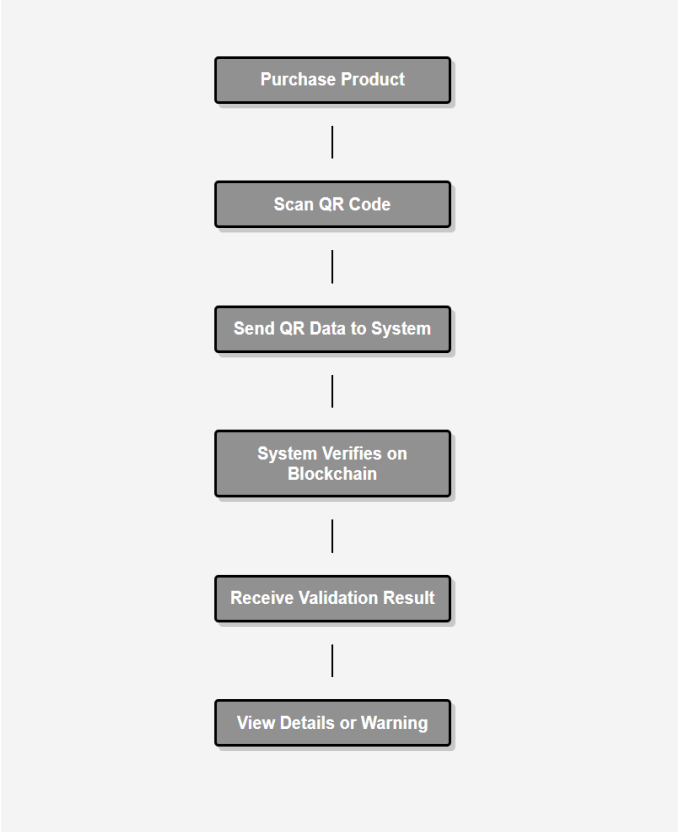

Fig 3 (Customer workflow)

IX. CONCLUSION

The Product Authenticity Verification System presents a comprehensive, scalable, and tamper-resistant framework to address the persistent problem of counterfeiting in global supply chains. Integrating blockchain's immutability, RSA digital signatures, and user-centric QR code verification, PAVS empowers manufacturers, consumers, and regulators with real-time, decentralized authentication. Pilot deployments have evidenced substantial reductions in counterfeit incident rates and improved stakeholder confidence. With enhancements such as AI-driven alerting, supply chain partnership with logistics providers, and blockchain-powered automation using smart contracts, PAVS is well-positioned to become a universal reference solution for product authenticity and digital trust. Ultimately, the continued evolution of anti-counterfeit systems like PAVS will rely on multi-sector collaboration, open standards, and regulatory alignment to maintain pace with increasingly sophisticated threats to product integrity.

X. FUTURE WORKS

Smart Contract Automation: Enhance recall processes by automating product aging/expiry and suspect batch recalls using smart contracts.
AI-Based Fraud Detection: Integrate ML-powered analysis and anomaly detection on product scan data to flag evolving counterfeiting/illicit trends.
Global Supply Chain Integration: Broaden integration with logistics partners (e.g., RFID + Blockchain) for true end-to-end traceability.
NFT/Token-Based Ownership: Issue NFTs as digital certificates of authenticity for ultra-premium or collectible goods, facilitating traceable resale and ownership transfers.
Physical-Digital Verification*:* Combine QR/blockchain with holographic or microtag security features for enhanced multimodal authentication.
User Feedback Ecosystem: Implement in-app reporting and reviews to crowdsource quick detection of counterfeit trends and enhance trust.
Advanced Analytics Dashboard: Provide predictive analytics for brands to monitor and anticipate risk regions, counterfeit hotspots, and consumer scan behaviors.
Decentralized Identity (DID): Employ decentralized identity solutions for stronger KYC of both manufacturers and participating users in high-risk markets.

REFERENCES

[1]. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," Applied Innovation Review, vol. 2, pp. 6–10, 2016.
[2]. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[3]. Tian, "An agri-food supply chain traceability system for China based on RFID & blockchain technology," IEEE International Conference on Service Systems and Service Management, 2016.
[4]. Ferdous, M. A. Rahman, and A. Anwar, "Blockchain-based supply chain traceability: A survey," Future Internet, vol. 13, no. 1, 2021.
[5]. Wang et al., "Blockchain-based smart contract for product traceability in supply chain management," J. of Cleaner Production, vol. 240, 2019.
[6]. Ranasinghe, R. L. Cole, and P. H. Cole, "Security and privacy for passive RFID tags," IEEE Pervasive Computing, vol. 7, no. 1, pp. 56–62, 2008.
[7]. Yu, M. Qiu, and G. Min, "QR code-based anti-counterfeit traceability system," Journal of Information Hiding and Multimedia Signal Processing, vol. 6, no. 3, 2015.
[8]. Viola and M. Jones, "Robust real-time object detection," International Journal of Computer Vision, vol. 57, no. 2, pp. 137–154, 2004.
[9]. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," Computer Networks, vol. 54, no. 15, pp. 2787–2805, 2010.
[10]. Fan, Y. Ren, and H. Li, "Blockchain-based efficient privacy-preserving and data integrity verification with high availability," IEEE Access, vol. 7, pp. 4389–4399, 2019.
[11]. Kshetri, "Can blockchain strengthen the Internet of Things?" IT Professional, vol. 19, no. 4, pp. 68–72, 2017.
[12]. Monrat, O. Schelén, and K. Andersson, "A survey of blockchain from the perspectives of applications, challenges, and opportunities," IEEE Access, vol. 7, pp. 117134–117151, 2019.
[13]. Lu and L. Xu, "Adaptable traceability system using blockchain and AI for supply chain management," Computers & Industrial Engineering, vol. 139, 2020.
[14]. Azzi, R. Chourabi, and K. Chafey, "Blockchain for logistics and transportation: A literature review and research agenda," Supply Chain Forum: An International Journal, vol. 20, no. 4, 2019.
[15]. Reyna et al., "On blockchain and its integration with IoT. Challenges and opportunities," Future Generation Computer Systems, vol. 88, 2018.
[16]. Bonneau et al., "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," IEEE Symposium on Security and Privacy, 2012.
[17]. Conti, C. Lal, and S. Ruj, "A survey on security and privacy issues of blockchain technology," IEEE Communications Surveys & Tutorials, vol. 21, no. 2, 2019.
[18]. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on Ethereum smart contracts," International Conference on Principles of Security and Trust, Springer, 2017.
[19]. Dwork and M. Naor, "Pricing via processing or combatting junk mail," Annual International Cryptology Conference, Springer, 1992.
[20]. Moinet, B. Darties, and J.-L. Baril, "Blockchain-based trust and authentication for decentralized sensor networks," Computer & Security, vol. 78, pp. 398–421, 2018.

