IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026

DOI: 10.17148/IJARCCE.2026.154259

Blockchain-Based Anti-Counterfeit Product Identification System: A Comprehensive Survey

Alam Basha N[1], Avinash V K[2], B K Raghavendra[3], Dandiya Mohammad Kaif[4], Dr. Muhibur Rahman T R[5]

6th Sem B.E.(CS&E), Ballari Institute of Technology and Management (BITM), Ballari, Karnataka – 583104, India[1-4]

Associate Professor, Department of Computer Science and Engineering, Ballari Institute of Technology and Management (BITM), Ballari, Karnataka – 583104, India[5]

Abstract: Counterfeit products pose a significant and growing threat to global supply chains, resulting in substantial financial losses, diminished brand equity, and risks to consumer health and safety. Conventional authentication mechanisms depend on centralized databases that remain susceptible to unauthorized alteration and offer limited transparency to downstream stakeholders. Blockchain technology has emerged as a compelling countermeasure, owing to its decentralized architecture, cryptographic security, and append-only immutability. This paper presents a complete survey of blockchain-based anti-counterfeit systems, with particular emphasis on QR code integration, smart contract deployment, and end-to-end product traceability. Let me tell you, a structured fourtier taxonomy is proposed to classify existing systems according to their functional sophistication, from basic barcode verification to fully integrated supply chain solutions. The truth is, critical performance dimensions, including security assurance, scalability, implementation cost, and end-user usability, are examined in depth. A comparative analysis of fifteen representative studies highlights their respective strengths and limitations. The survey further identifies persistent research gaps, including the absence of holistic system integration, susceptibility of QR codes to physical cloning, and constraints on large-scale throughput. Prospective research directions are outlined to guide the development of more strong, scalable, and user-accessible anti-counterfeit solutions.

Keywords: Blockchain; Counterfeit Detection; QR Code; Supply Chain; Smart Contracts; Traceability; Product Authentication; Decentralized Systems.

I. INTRODUCTION

Counterfeit goods represent one of the most pervasive and economically damaging challenges in contemporary global commerce, affecting a broad spectrum of industries including pharmaceuticals, electronics, luxury goods, and agricultural products. Beyond their direct economic ramifications, estimated at hundreds of billions of dollars annually, fraudulent products frequently expose consumers to serious safety risks, particularly in healthcare and food sectors [1], [2]. The scale and sophistication of counterfeiting operations have grown substantially with globalization, making traditional authentication approaches increasingly inadequate.

Conventional product authentication frameworks depend on centralized databases administered by individual organizations or regulatory bodies. While operationally straightforward, these systems are inherently vulnerable to internal manipulation, single-point failures, and coordinated cyberattacks. The absence of a shared, tamper-resistant ledger further undermines trust among geographically dispersed supply chain stakeholders [3]. plus, the opacity of centralized systems limits the ability of downstream participants, including end consumers, to independently verify product provenance.

Blockchain technology directly addresses these shortcomings by providing a distributed, append-only record that's computationally infeasible to alter retroactively. When combined with QR codes or RFID-based identifiers, blockchain enables end-users to verify product authenticity at the point of consumption without relying on any central authority. This survey systematically examines the environment of blockchain-based anti-counterfeit systems, evaluates their performance characteristics across multiple dimensions, and proposes a structured classification framework to organize the existing literature. The overarching objective is to synthesize current knowledge, facilitate comparative evaluation, and identify open challenges that merit focused future research.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026

DOI: 10.17148/IJARCCE.2026.154259

Four principal contributions structure this analysis: (1) a four-tier taxonomy classifying AI anti-counterfeit systems by functional depth; (2) a curated review of fifteen representative studies drawn from IEEE Xplore, Springer, and related venues; (3) cross-paper comparative tables examining methodology, performance, and limitations; and (4) a gap analysis identifying unresolved challenges and directions for future investigation.

II. THEORETICAL BACKGROUND

The truth is, before comparing specific systems, it's useful to establish the formal scaffolding common to most blockchain-based anti-counterfeit approaches. The following subsections lay out the key modelling and evaluation primitives used across the reviewed literature.

A. Blockchain Data Model

A blockchain is a chronologically ordered sequence of cryptographically linked blocks. Each block is formally defined as: $Block = \{ Data, Hash, Previous\ Hash \}$ (1)

Each product transaction recorded on the chain takes the form:

$T = \{ Product\ ID, Owner, Timestamp \}$ (2)

This structure guarantees immutability and auditability: any retroactive modification of a block invalidates the hashes of all subsequent blocks, rendering tampering immediately detectable. The combination of decentralization and cryptographic linkage provides a trust foundation that no centralized system can replicate [4], [5].

B. Smart Contract Verification Model

Smart contracts automate the authentication decision through pre-programmed conditional logic. The verification function is expressed as:

$Verification = f(Product\ ID, Stored\ Data)$ (3)

The output of this function determines product status:

$If\ f = match \rightarrow Genuine;\quad Else \rightarrow Counterfeit$ (4)

By encoding authentication logic directly in the contract, the system eliminates reliance on human intermediaries and substantially reduces the probability of authentication fraud. Smart contracts also generate immutable execution logs, providing an auditable trail for regulatory compliance [6], [7].

C. QR Code Encoding Scheme

Each product in the system is assigned a unique identifier that's encoded into a machine-readable QR code:

$QR = Encode(Product\ ID)$ (5)

Upon consumer scanning, the encoded identifier is transmitted to the blockchain smart contract for real-time validation against the stored record. This mechanism provides a low-cost, hardware-agnostic verification interface accessible via any smartphone [12]. The primary vulnerability of this scheme is physical QR code replication, which is addressed in the research gap analysis.

D. Classification Performance Metrics

System detection efficacy is evaluated using standard binary classification metrics derived from the confusion matrix:

$Accuracy = (TP + TN) / (TP + TN + FP + FN)$ (6)

$Precision = TP / (TP + FP)$ (7)

$Recall = TP / (TP + FN)$ (8)

Let me tell you, in anti-counterfeit contexts, recall is often prioritized, failing to flag a counterfeit product (false negative) carries substantially higher risk than a false alarm. System designers must calibrate this trade-off based on the cost asymmetry of each application domain.

E. System Response Time

End-to-end verification latency is decomposed as:

$Tresponse = Tprocessing + Tverification$ (9)

Where $Tprocessing$ covers QR decoding and data normalization, and $Tverification$ is the blockchain query and smart contract execution time. Minimizing both components is essential for seamless user experience in high-throughput retail and logistics environments [9], [11].

III. FOUR-TIER TAXONOMY

Reviewing anti-counterfeit systems without an organizing framework makes rigorous comparison difficult. We propose classifying existing blockchain-based systems into four tiers, ordered by functional sophistication and integration depth.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026

DOI: 10.17148/IJARCCE.2026.154259

The taxonomy was derived inductively from the reviewed literature rather than imposed from a prior theoretical model. Table I presents the complete classification.

TABLE I: FOUR-TIER TAXONOMY OF BLOCKCHAIN-BASED ANTI-COUNTERFEIT SYSTEMS

Tier	System Type	Key Characteristics	Primary Limitations
1	Basic Verification Systems (QR / Barcode)	Centralized storage; low deployment cost; simple scan-and-verify workflow; no blockchain integration	Highly susceptible to replication; single point of failure; no tamper evidence
2	Blockchain-Based Systems	Decentralized immutable ledger; cryptographic product identity; tamper-proof audit trail	No end-to-end supply chain tracking; limited real-time capability
3	Supply Chain Tracking Systems	Ownership transfer logging; multi-stakeholder transparency; logistics event anchoring	High architectural complexity; significant deployment cost
4	Integrated AntiCounterfeit Systems (Proposed Tier)	QR + blockchain + tracking unified; real-time consumer verification; full lifecycle visibility	Scalability and implementation cost challenges; no mature production deployment

Tier 1 systems represent the most common form in practice: standard QR or barcode labels paired with centralized lookup databases. they're cost-effective and straightforward to deploy, but their centralized architecture and susceptibility to label replication make them inadequate as standalone solutions.

Tier 2 introduces blockchain as the storage and verification backend, establishing immutable product records and eliminating single points of failure. But, these systems typically cover only verification, they don't track ownership changes or supply chain events.

Tier 3 extends the architecture to include full supply chain traceability: ownership transfer events, multi-stakeholder access control, and logistics anchoring. This tier corresponds to the majority of sophisticated academic proposals reviewed in Section IV.

Tier 4 represents the fully integrated paradigm that unifies all prior capabilities within a single, real-time, consumer-accessible platform. No reviewed paper has yet achieved this level in its entirety, an observation that directly motivates the research gap analysis presented in Section VI.

IV. LITERATURE REVIEW

The fifteen papers reviewed here were drawn from IEEE Xplore, Springer, ScienceDirect, and related venues. Selection criteria required that each paper report at least one concrete system implementation or quantitative performance outcome, or in the case of survey-type works, provide substantial comparative evidence rather than purely conceptual description. Table II presents the complete review summary

TABLE II: LITERATURE REVIEW SUMMARY

Sl.	Author(s)	Year & Title	Method / Technique	Key Findings	Venue & Index
1	Nagarkar et al.	2024 -Fake Products Identification Using Blockchain	Blockchain ledger, QR verification, hash-based product records	Significant reduction in fake product circulation; immutable record-keeping improved stakeholder trust	Int. Conf. Emerging Trends Comput. Sci., 2024
2	Pathan et al.	Let me tell you, 2024 counterfeit product detection using blockchain technology	Decentralized blockchain, consensus-based validation, product	Demonstrated measurable improvement in counterfeit detection rates across pilot supply chains	J. Distrib. Ledger Technol., 2024

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026
DOI: 10.17148/IJARCCE.2026.154259

			ID hashing		
3	Saraswathi et al.	2024 -Combating Counterfeit Products with Blockchain	Transparent distributed ledger, stakeholder access control	Enhanced supply chain transparency; multi-party trust established without centralized authority	IEEE Access, 2024
Sl.	**Author(s)**	**Year & Title**	**Method / Technique**	**Key Findings**	**Venue & Index**
4	Toyoda et al.	2017 -POMS: Product Ownership Management System	Blockchain ownership transfer, event-triggered smart records	Provable ownership chain from manufacturer to consumer; applicable across diverse product categories	IEEE Access, vol. 5, 2017
5	Casino et al.	2019 -Systematic Literature Review of Blockchain Applications	thorough literature synthesis, domain taxonomy	Established foundational design principles; identified scalability and privacy as dominant open problems	Telemat. Informat., vol. 36, 2019
6	Kordestani et al.	2023 -Smart Contract Diffusion in Pharmaceutical Blockchain	Smart contracts, compliance automation, audit trail generation	Automated compliance reduced manual oversight; audit trail generation strengthened regulatory reporting	J. Bus. Res., vol. 163, 2023
7	Lo et al.	2023 -Blockchain Anti-Counterfeit Product Identification System	QR-blockchain coupling, authentication protocol, Layer 2 scaling	Reliable end-user authentication via mobile scan; Layer 2 reduced verification latency significantly	IEEE Trans. Consum. Electron., 2023
8	Wang & Li	2022 -Cross-Border ECommerce Traceability via Blockchain	Cross-chain interoperability, distributed traceability framework	Multi-jurisdiction traceability achieved; regulatory compliance integrated into transaction flow	Comput. Ind. Eng., vol. 168, 2022
9	Zhang & Kumar	2023 -IoT + Blockchain Dynamic Supervision for Supply Chains	IoT sensor data, blockchain anchoring, real-time event logging	Continuous monitoring of physical goods enabled; tamper events detected and logged automatically	IEEE Internet Things J., vol. 10, 2023
10	Anjum & Dutta	2022 -Identifying Counterfeit Products Using Blockchain	Decentralized fraud detection, supply chain event hashing	Fraud patterns identified earlier compared to centralized baselines; falsepositive rate acceptable	Electron. Commer. Res. Appl., 2022
11	Mohammed et al.	2024 -On-Chain/Off-Chain Traceability Architecture	Hybrid onchain/off-chain storage, throughput optimization	Storage costs reduced substantially; throughput scaled under high transaction load without accuracy loss	Future Gener. Comput. Syst., 2024
12	TE-FOOD Team	2020 -Food Supply Chain Traceability with QR and Blockchain	QR code labeling, blockchain anchoring, consumer-facing app	Farm-to-consumer visibility demonstrated at pilot scale; consumer scan adoption rate above expectations	TE-FOOD White Paper, 2020
13	Gucci & Louis Vuitton	2024 -Luxury Brand AntiCounterfeiting via QR and	NFC chip + QR dual-layer tagging, Aura Blockchain	Grey-market diversion measurably reduced; brand	Aura Blockchain Consortium Report, 2024

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026

DOI: 10.17148/IJARCCE.2026.154259

		NFC Tags	Consortium	provenance verifiable by end consumers globally	
14	Lo et al.	2023 -Blockchain + Layer 2 for Jewellery Certification	Layer 2 blockchain, certificate hashing, jewellery provenance ledger	Authentication cost per item reduced; certification forgery rendered computationally infeasible	IEEE Trans. Consum. Electron., 2023
15	Alzahrani & Bulusu	2020 -Anti-Counterfeiting Blockchain with Decentralised Consensus	Dynamic consensus protocol, decentralized node validation	Consensus latency improved over standard PoW; resilient to singlenode compromise scenarios	IEEE Access, 2020

Note: QR = Quick Response code. POMS = Product Ownership Management System. NFC = Near Field Communication. PoW = Proof of Work. IoT = Internet of Things.

V. COMPARATIVE ANALYSIS

Table III presents a structured cross-paper comparison examining each reviewed system across six performance dimensions: security assurance, scalability, real-time verification capability, degree of decentralization, and primary limitation.

TABLE III: COMPARATIVE ANALYSIS OF REVIEWED ANTI-COUNTERFEIT SYSTEMS

Sl.	Paper / System	Protocol / Technique	Security	Scalability	Real-Time	Decentral.	Limitations
1	Nagarkar et al. [1]	Blockchain ledger, QR verification	High	Medium	No	Yes	No supply-chain tracking module
2	Pathan et al. [2]	Consensus validation, hash-based ID	High	Medium	Partial	Yes	No consumer-facing interface
3	Saraswathi et al. [3]	Transparent distributed ledger	High	Medium	No	Yes	No smart contract automation
4	Toyoda et al. [4]	POMS ownership transfer chain	High	Low	No	Yes	Limited to postsupply-chain phase
5	Casino et al. [5]	Literature synthesis, domain taxonomy	N/A	N/A	N/A	N/A	No empirical system implementation
6	Kordestani et al. [6]	Smart contracts, compliance automation	High	Medium	Partial	Yes	Pharmaceuticalspecific; not generalized
7	Lo et al. [7]	QR-blockchain, Layer 2 scaling	High	High	Yes	Yes	No drug/product interaction module
8	Wang & Li [8]	Cross-chain interoperability framework	High	High	Partial	Yes	Complex crossjurisdiction deployment
9	Zhang & Kumar [9]	IoT sensor + blockchain anchoring	High	Medium	Yes	Yes	High infrastructure cost
10	Anjum & Dutta [10]	Decentralized fraud detection hashing	High	Low	No	Yes	Static snapshot; no rolling update
11	Mohammed et al. [11]	On-chain/off-chain hybrid storage	High	High	Partial	Yes	Off-chain segment introduces trust gap
12	TE-FOOD [12]	QR labeling, consumer-facing app	Medium	High	Yes	Partial	QR codes susceptible to cloning

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026
DOI: 10.17148/IJARCCE.2026.154259

13	Gucci & LV [13]	NFC + QR dual-layer, Aura Consortium	High	Medium	Yes	Yes	Proprietary; limited open-source access
14	Lo et al. [14]	Layer 2, jewellery provenance ledger	High	High	Partial	Yes	Domain-specific; not generalized
15	Alzahrani & Bulusu [15]	Dynamic consensus, decentralized nodes	High	Medium	Partial	Yes	Consensus overhead at large node count

Note: Decentral. = Decentralized architecture. Real-Time = Supports real-time consumer verification. N/A = Not applicable (survey/conceptual paper).

VI. RESEARCH GAPS

The survey reveals consistent patterns of omission across the reviewed body of work. By the way, seven gaps are identified below, ordered roughly from the most practically urgent to the more systemic.

Gap 1 — No Fully Integrated Platform: Every reviewed system addresses a subset of required functionality. Systems with strong authentication lack supply chain tracking; systems with tracking lack consumer-facing real-time verification. The composite system, QR authentication, blockchain anchoring, ownership traceability, and live consumer verification within one unified platform, has not been built. This is the most immediately actionable gap.

Gap 2 —QR Code Cloning Vulnerability: Standard printed QR codes can be physically reproduced and affixed to counterfeit products, undermining the entire verification chain. No reviewed system incorporates cryptographically secure physical identifiers such as Physical Unclonable Functions (PUFs) or NFC chips with challenge-response authentication as a systematic solution.

Gap 3 — Limited Real-Time Verification: Blockchain consensus latency and smart contract execution overhead prevent most reviewed systems from delivering sub-second verification responses at scale. Layer 2 solutions exist but haven't been systematically evaluated across diverse supply chain workloads.

Gap 4 — High Implementation Cost: Deployment costs, particularly for IoT integration and on-chain storage, remain prohibitive for small and medium-sized enterprises, limiting adoption to large-cap companies with established technology infrastructure.

Gap 5 — Scalability Constraints: Most public blockchain implementations exhibit throughput degradation as transaction volumes increase. Hybrid on-chain/off-chain architectures partially address this but introduce new trust and consistency challenges.

Gap 6 — Lack of User-Friendly Interfaces: End-user verification interfaces in academic proposals are typically designed for technically proficient users. Consumer-facing deployments require intuitive mobile experiences with minimal friction, a design dimension largely absent from the reviewed literature.

Gap 7 — No AI-Based Fraud Detection: Machine learning anomaly detection hasn't been integrated into any mainstream blockchain authentication framework. AI-driven pattern recognition across transaction histories could proactively identify coordinated counterfeiting attacks before they reach consumers.

VII. CONCLUSION

This survey examined fifteen peer-reviewed studies and industry implementations on blockchain-based anti-counterfeit systems, spanning foundational work from 2017 through recent publications in 2024. The reviewed literature demonstrates that blockchain technology, particularly when combined with QR code or NFC identifiers and smart contract automation, provides a structurally sound foundation for product authentication. Its core properties of decentralization, immutability, and transparent auditability directly mitigate the vulnerabilities inherent in legacy centralized systems.

At the same time, the review makes visible a gap that individual papers naturally obscure: no existing system simultaneously addresses security, scalability, real-time usability, and economic feasibility within an integrated architecture. The proposed four-tier taxonomy makes this gap concrete. Tiers 1 through 3 are populated with validated work; Tier 4 remains largely theoretical. The specific missing components are identifiable, cryptographically secure physical identifiers, Layer 2 real-time verification, AI anomaly detection, and consumer-optimized interfaces, and none represents an unsolved fundamental research problem in isolation. The gap is more architectural and integrative than algorithmic.

The research direction of highest value from this point isn't further incremental refinement of individual components, but rather systematic work on integration: how to assemble validated building blocks into a deployment-grade platform that's simultaneously secure, scalable, usable, and economically viable for adoption across enterprise scales.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026
DOI: 10.17148/IJARCCE.2026.154259

REFERENCES

[1] N. Nagarkar, P. Punekar, S. Sheikh, and A. Dumbere, "Fake Products Identification Using Blockchain," in Proc. Int. Conf. Emerging Trends Comput. Sci., 2024.
[2] S. Pathan, S. Salunke, and S. Nagvekar , "Counterfeit Product Detection Using Blockchain Technology," J. Distrib. Ledger Technol., vol. 3, no. 1, pp. 45–58, 2024.
[3] S. Saraswathi, S. Suresh, and R. Gandhi, "Combating Counterfeit Products with Blockchain," IEEE Access, vol. 12, pp. 11234– 11247, 2024.
[4] 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.
[5] F. Casino, T. K. Dasaklis, and C. Patsakis, "A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification and Open Issues," Telemat. Informat., vol. 36, pp. 55–81, 2019.
[6] M. Kordestani, A. Oghazi, and P. Sahamkhadam, "Smart Contract Diffusion and Adoption in Pharmaceutical Blockchain Supply Chains," J. Bus. Res., vol. 163, p. 113988, 2023.
[7] Y. Lo, M. Khalil, and A. Fahad, "Blockchain-Based Anti-Counterfeit Product Identification and Authentication System," IEEE Trans. Consum. Electron., vol. 69, no. 2, pp. 312–322, 2023.
[8] X. Wang and Y. Li, "Cross-Border E-Commerce Product Traceability via Blockchain: A Framework and Implementation," Comput. Ind. Eng., vol. 168, p. 108078, 2022.
[9] Y. Zhang and R. Kumar, "IoT- and Blockchain-Integrated Dynamic Supervision Model for Supply Chain Anti-Counterfeiting," IEEE Internet Things J., vol. 10, no. 5, pp. 4321–4335, 2023.
[10] A. Anjum and S. Dutta, "Identifying Counterfeit Products Using Blockchain in a Transparent Supply Chain Network," Electron. Commer. Res. Appl., vol. 55, p. 101180, 2022.
[11] A. Mohammed, M. Al-Rakhami, and H. AlSalman, "On-Chain/Off-Chain Hybrid Traceability Architecture for Supply Chain Management," Future Gener. Comput. Syst., vol. 152, pp. 78–92, 2024.
[12] TE-FOOD Team, "Food Supply Chain Traceability with QR Codes and Blockchain," TE-FOOD White Paper, 2020. [Online]. Available: https://te-food.com
[13] Aura Blockchain Consortium, "Luxury Brand Anti-Counterfeiting via QR and NFC Blockchain Tags," Industry Report, Aura Blockchain Consortium, 2024.
[14] R. Vaidya, A. Tembhurnikar, C. Mohite, S. Puri, S. Kulkarni, and A. Buchade, "Blockchain and Layer 2 Scaling for Jewellery Certification and Authentication," IEEE Trans. Consum. Electron., vol. 69, no. 3, pp. 401–412, 2023.
[15] S. Alzahrani and N. Bulusu, "Anti-Counterfeiting with Blockchain Using Decentralised Dynamic Consensus," IEEE Access, vol. 8, pp. 97013–97027, 2020.

