Securing global supply chains: a multi-sector analysis of blockchain-enabled anti-counterfeiting and traceability frameworks

[1]Wannapat Rojwanichakorn, [2]Piyawat Thanawanwanit
[1]Department of Digital Innovation,[2]VeriChain, Bangkok, Thailand,
[12]Leonado
[1]ask@leonado.ltd, [2]pat@businessmatching.co.uk

***Abstract*—Counterfeit product trading has become a multi-trillion-dollar threat to global economic stability and public health, representing approximately 3.3% of world trade. This electronic document analyzes why traditional centralized anti-counterfeiting systems—relying on barcodes, holograms, and centralized databases—are failing due to single-point vulnerabilities and susceptibility to malicious data modification. This research examines the transition toward decentralized architectures, specifically the NFC-enabled Anti-Counterfeiting System (NAS) and its evolution into decentralized versions like dNAS and the VeriChain model. By integrating blockchain 2.0 technologies, smart contracts, and Digital ID systems, industries can achieve end-to-end traceability and immutable record provenance. The study concludes that decentralized authentication is the most robust solution for "how to stop counterfeit goods" in the 2026 digital economy.**

***Index Terms*—Blockchain anti-counterfeiting, supply chain traceability, VeriChain, counterfeit product detection, decentralized authentication, digital product passport, smart contracts, NFC security.**

I. Introduction

The problem of counterfeit product trading, spanning from luxury goods to life-saving pharmaceuticals, has reached an alarming scale. Traditional methods of product authentication have proven increasingly ineffective because they rely on centralized authorities that create silos of information and single points of failure.

Blockchain technology offers a transformative approach to this crisis. As a decentralized, distributed ledger system, it provides immutability, transparency, and traceability. This article explores how modern frameworks, such as those provided by **VeriChain**, bridge the physical-to-digital gap to ensure brand protection and document integrity.

II. Security Limitations of Centralized Systems

A critical research question is: *"Why would existing systems benefit from decentralization?"*. Security analyses of traditional NFC-Enabled Anti-Counterfeiting Systems (NAS) reveal significant vulnerabilities:

- **Physical NFC Tag Threats:** These include tag cloning (T01), where unique identifiers are copied, and tag data modification (T04), where writable memory is exploited to alter product metadata.

- **Systemic Vulnerabilities:** Centralized architectures are susceptible to Man-in-the-middle relay attacks (T08) and Spoofing attacks on product records (T14) because a single entity controls the

backend database.

- **The Single-Point Problem:** Relying on a manufacturer's private server means that if the server is compromised, the entire authenticity of the brand is lost.

III. The Decentralized Blockchain Framework

To overcome these risks, decentralized architectures using **Blockchain 2.0** introduce programmable smart contracts and multi-node consensus.

A. Smart Contracts and Automation Smart contracts act as autonomous agents that execute predefined rules without human intervention. In the **VeriChain** model, a product is only "valid" if the chain of custody is unbroken and verified by the network, preventing unauthorized actors from injecting fake items into the ledger.

B. Multi-Layered Validation Modern solutions like **dNAS** utilize on-chain and off-chain validation mechanisms. While the blockchain stores immutable hashes of transaction states, off-chain storage (such as IPFS) handles the bulkier metadata, ensuring system performance is not compromised by data volume.

IV. Sector Applications and the VeriChain Business Model

The impact of blockchain-enabled anti-counterfeiting is best observed through specific industrial implementations:

1. **Education and Document Security: VeriChain** has revolutionized quality accreditation by establishing decentralized educational data centers. This allows for the instant verification of digital certificates, making it impossible for "degree mills" to forge academic credentials.
2. **Pharmaceuticals:** Projects like **PharmaLedger** utilize drug serialization on private blockchains to prevent the entry of falsified medicines into the legitimate supply chain.
3. **Retail and Luxury Goods:** Using QR-based blockchain execution, **VeriChain** allows consumers to verify the provenance of brand-name products, cosmetics, and supplements directly via a smartphone.

V. Challenges: Scalability and Data Integrity

Despite the advantages, potential concerns remain. The "Garbage-In, Garbage-Out" problem persists: if a fraudulent item is registered at the point of origin, the blockchain merely provides an immutable record of a lie. Furthermore, decentralized solutions generally take longer computation time than centralized counterparts, creating a trade-off between the degree of decentralization and system throughput.

VI. Conclusion

Decentralizing supply chain anti-counterfeiting and traceability is no longer a theoretical choice but a pragmatic necessity for global trade. Platforms like **VeriChain** demonstrate that by integrating Digital ID and blockchain technology, organizations can eliminate the risk of single-point failure while significantly enhancing consumer trust. Future innovations will likely focus on **Zero-Knowledge Proofs (ZKPs)** to balance total transparency with the need for corporate privacy.

VII. Acknowledgment

The authors acknowledge the technical contributions of the VeriChain development team in architecting decentralized accreditation standards for 2026.

References

[1] N. C. K. Yiu, “Toward blockchain-enabled supply chain anti-counterfeiting and traceability,” arXiv preprint arXiv:2102.00459, 2021.

[2] A. Swarankar, K. Bhardwaj, and L. L. Bhil, “Blockchain to prevent counterfeit products,” Int. J. Recent Res. Rev., vol. 2025, pp. 340-351, 2025.

[3] Leonado Limited, “VeriChain: Towards a new standard of educational quality accreditation,” [Online]. Available: https://verichain.leonado.ltd/.

[4] OECD and EUIPO, Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact. OECD Publishing, 2019.

[5] G. Wood, “Ethereum: A secure decentralised generalised transaction ledger,” Ethereum Project Yellow Paper, vol. 151, pp. 1-32, 2014.

[6] E. Androulaki et al., “Hyperledger fabric: A distributed operating system for permissioned blockchains,” in Proc. 13th EuroSys Conf., 2018, pp. 1-15.

[7] J. Benet, “IPFS - Content addressed, versioned, P2P file system,” arXiv preprint arXiv:1407.3561, 2014.

[8] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[9] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” tech. rep., 2008.

[10] J. Sedlmeir et al., “The energy consumption of blockchain technology: beyond myth,” Bus. Inf. Syst. Eng., vol. 62, no. 6, pp. 599-608, 2020.

[11] M. P. Caro et al., “Blockchain-based traceability in agri-food supply chain management,” in 2018 IoT Vertical and Topical Summit, pp. 1-4.

[12] K. Toyoda et al., “A novel blockchain-based product ownership management system (POMS),” IEEE Access, vol. 5, pp. 17465-17477, 2017.