Blockchain-Based Product Authentication: Concepts, Architecture, Applications, and Limitations

Reza Ebrahimi

University-level overview of blockchain, traceability, smart contracts, distributed storage, and product verification

Abstract

Product authentication is increasingly important in digital commerce, where consumers, brands, marketplaces, and supply-chain participants need mechanisms for establishing whether a physical or digital product corresponds to a legitimate issuer or documented provenance. Blockchain technology has been proposed as one component of such systems because distributed ledgers can provide persistent, independently verifiable records and can make subsequent alteration of recorded events detectable. However, blockchain does not by itself establish that the physical product described by a record is genuine. Effective authentication therefore requires a combination of trusted identification, traceability data, cryptographic verification, appropriate data storage, and clearly defined issuer responsibilities. This article examines the technical foundations of blockchain-based product authentication, including distributed ledgers, smart contracts, content-addressed storage, traceability structures, digital signatures, and verification workflows. It also considers applications in e-commerce, luxury goods, collectibles, warranties, and supply-chain environments, while discussing limitations involving data quality, key management, privacy, scalability, interoperability, and the distinction between authenticity of a record and authenticity of a physical object.

1. Introduction

Product authentication refers to processes used to determine whether a product, certificate, transaction, or provenance claim can reasonably be associated with an authorized source. Conventional approaches include serial numbers, certificates of authenticity, holograms, centralized databases, QR codes, RFID systems, and inspection by authorized organizations. These approaches can be effective, but their security properties depend heavily on the design and governance of the issuing organization and on the ability to protect records from unauthorized modification or duplication.

The growth of e-commerce and digitally mediated supply chains has increased the importance of verifiable product information. A consumer may purchase an item without interacting directly with its manufacturer, while later owners, resellers, insurers, or service providers may also need evidence concerning provenance. Blockchain-based approaches seek to address part of this problem by creating records whose history can be independently inspected and whose subsequent alteration can be detected.

Research by Gao et al. (2022), for example, describes a product authentication architecture combining blockchain, a traceability structure, IPFS-based storage, smart contracts, and consumer review information. Their approach illustrates a broader architectural principle: the blockchain can maintain references and verification-related data while larger or private information is maintained outside the ledger.

2. What Blockchain Contributes to Product Authentication

A blockchain is a distributed ledger maintained through a network of participating nodes according to a consensus mechanism. For authentication applications, its principal contribution is not that it automatically identifies genuine physical products, but that it can provide a persistent record against which later claims can be compared.

An issuer can record a certificate identifier, product identifier, timestamp, issuer address, or cryptographic hash on a blockchain. A verifier can subsequently compare information associated with the product with the information represented by the blockchain record. If the relevant cryptographic values match, the verifier can establish that the checked data corresponds to the recorded data. This is different from proving that the original data was truthful: blockchain preserves and exposes a record, but it cannot independently determine whether an issuer entered false information.

This distinction is fundamental. Blockchain can strengthen the integrity and verifiability of an authentication record, while the credibility of the initial product information depends on the issuer, the data-collection process, physical identification mechanisms, and governance surrounding the system.

3. Smart Contracts

Smart contracts are programs deployed on blockchain networks that execute predefined rules. In a product-authentication system, a smart contract can provide functions for registering certificates, associating identifiers with issuers, recording status changes, and implementing rules concerning verification, transfer, freezing, or revocation.

Gao et al. (2022) demonstrate this model through platform- and consumer-oriented authentication operations. Their proposed traceability structure contains identifiers and attributes representing production, transaction, circulation, and consumer-review information. Smart-contract operations can then retrieve or compare these attributes during an authentication procedure.

The use of smart contracts can reduce dependence on a single application server for the integrity of the recorded rules. Nevertheless, smart contracts introduce requirements including secure software development, correct access control, careful management of privileged operations, and mechanisms for dealing with erroneous or compromised inputs.

4. On-Chain and Off-Chain Data

Storing every product document directly on a blockchain is often inefficient or inappropriate. Ledgers may have limited storage capacity, transaction costs can increase with data volume, and sensitive information may not be suitable for public disclosure. Consequently, many architectures use a hybrid model in which the blockchain stores compact verification information while detailed records are maintained elsewhere.

The 2022 study by Gao et al. uses IPFS as an off-chain storage component. IPFS identifies content through a content identifier derived from the content, allowing a verifier to check whether retrieved information corresponds to the referenced content. In their architecture, encrypted traceability information and consumer reviews are stored through IPFS, while blockchain records provide references and verification-related values.

This architecture demonstrates an important design principle: the blockchain and distributed storage system serve different functions. The blockchain can provide durable verification metadata, while off-chain storage can handle larger information objects. Encryption and access controls may additionally be required when the underlying information is private.

5. Traceability and Product Identity

A product-authentication system requires a reliable method for connecting a physical product to a digital record. This may involve serial numbers, QR codes, NFC tags, RFID, secure labels, embedded identifiers, digital certificates, or combinations of these technologies.

Traceability extends this concept by recording relevant events across a product's lifecycle. Depending on the application, events can include manufacture, inspection, transfer, distribution, sale, ownership change, warranty service, and return. A standardized traceability structure can organize these events so that different participants can interpret the information consistently.

However, a digital record remains dependent on the integrity of the physical-to-digital binding. If an attacker can copy a QR code or transfer a digital identifier to a counterfeit product, the existence of a valid blockchain record does not necessarily establish that the physical object being inspected is the original object. Strong authentication therefore benefits from tamper-resistant identifiers and procedures that make duplication or unauthorized transfer more difficult.

6. Verification Workflow

A general blockchain-based authentication workflow can be represented as follows:

1. An authorized issuer creates a product identity and associated certificate.
2. Relevant product or provenance information is collected and, where appropriate, encrypted.
3. A cryptographic hash or other compact verification value is recorded on a blockchain.
4. Detailed documents may be stored through an off-chain or distributed storage system.
5. The customer or verifier accesses the certificate through a QR code, identifier, web interface, or other mechanism.
6. The verification system retrieves the relevant blockchain record and compares the supplied information with the recorded cryptographic values.
7. The system presents the verification result together with appropriate information about the issuer and certificate status.

A verification result should be communicated carefully. A successful cryptographic match establishes correspondence with the recorded data; it does not necessarily establish every claim made about the physical product. The interface should therefore distinguish between statements such as “certificate issued by X,” “record has not been altered,” and broader claims such as “the physical product is genuine.”

7. Applications

Blockchain-based authentication can be applied to high-value and trust-sensitive categories such as luxury goods, watches, jewellery, collectibles, limited editions, artworks, premium accessories, and products for which provenance affects resale value. It may also support warranty administration, authorized resale, service histories, and business-to-business supply-chain documentation.

In e-commerce, authentication records can be associated with orders or products and made available to customers after purchase. Such systems can potentially reduce reliance on static PDF certificates or records that exist only within a merchant's database. For secondary markets, a persistent certificate can provide additional evidence that a particular item was associated with an authorized issuer, although the certificate should not be treated as conclusive proof without appropriate physical verification.

8. Privacy and Security Considerations

Authentication systems frequently process information that may be commercially sensitive or personally identifiable. Public blockchains are generally unsuitable for storing unnecessary private information directly on-chain. A privacy-conscious architecture can instead store hashes, references, or other minimal verification data on-chain while retaining sensitive records under appropriate access controls.

Cryptographic key management is equally important. If an issuer loses control of a signing key, an attacker may be able to create apparently legitimate records. Systems therefore require secure key storage, role separation, revocation procedures, monitoring, and recovery mechanisms. Smart-contract vulnerabilities can also affect certificate issuance or status management.

9. Limitations

Blockchain does not eliminate counterfeit products, guarantee truthful data entry, or replace physical inspection. Its principal strength is the integrity and auditability of records after they have been created. The reliability of the overall authentication process therefore depends on the entire chain of trust—from product identification and data collection to issuer authorization, blockchain recording, storage, and final inspection.

Other limitations include transaction costs, network dependence, interoperability between blockchain platforms, long-term availability of off-chain data, user experience, wallet management, regulatory requirements, and the governance of certificate revocation. Hybrid architectures can reduce some technical limitations, but they also introduce dependencies on external infrastructure.

10. Research and Industry Direction

Research has explored blockchain-based product authentication through different combinations of traceability, smart contracts, distributed storage, encryption, and consumer feedback. Gao et al. (2022) describe one such architecture and report experimental measurements concerning request failures and access times in their test environment. Their study also acknowledges limitations concerning decentralization and the exploratory nature of blockchain applications.

Future systems can increasingly combine blockchain records with secure physical identifiers, decentralized identifiers, digital signatures, privacy-preserving cryptography, and interoperable product-data standards. Such combinations may provide stronger links between physical objects and digital records while reducing the amount of sensitive information exposed publicly.

11. Conclusion

Blockchain-based product authentication is best understood as a verification architecture rather than a standalone anti-counterfeiting technology. A blockchain can provide persistent, independently inspectable records; smart contracts can automate authentication rules; content-addressed or distributed storage can accommodate larger information objects; and traceability structures can organize lifecycle information. Together, these components can strengthen the integrity and auditability of product certificates.

At the same time, successful authentication depends on the credibility of the issuer, the integrity of the product-identification mechanism, secure key management, appropriate privacy controls, and reliable governance. The central technical distinction is therefore between proving that a digital record corresponds to a recorded issuer and proving that a physical product is genuine. Blockchain can

materially support the former and contribute to the latter, but it does not independently solve the entire authenticity problem.

References

Gao, X., Zhang, W., Zhao, B., Zhang, J., Wang, J., & Gao, Y. (2022). Product Authentication Technology Integrating Blockchain and Traceability Structure. Electronics, 11(20), 3314. https://doi.org/10.3390/electronics11203314

Blockchain Review. (2026). WooChainPro Review: The Practical Blockchain Plugin Bringing Real Product Authentication to WordPress and WooCommerce. September 27, 2026. https://blockchainreview.org/wcp-wordpress-blockchain-certification-plugin/