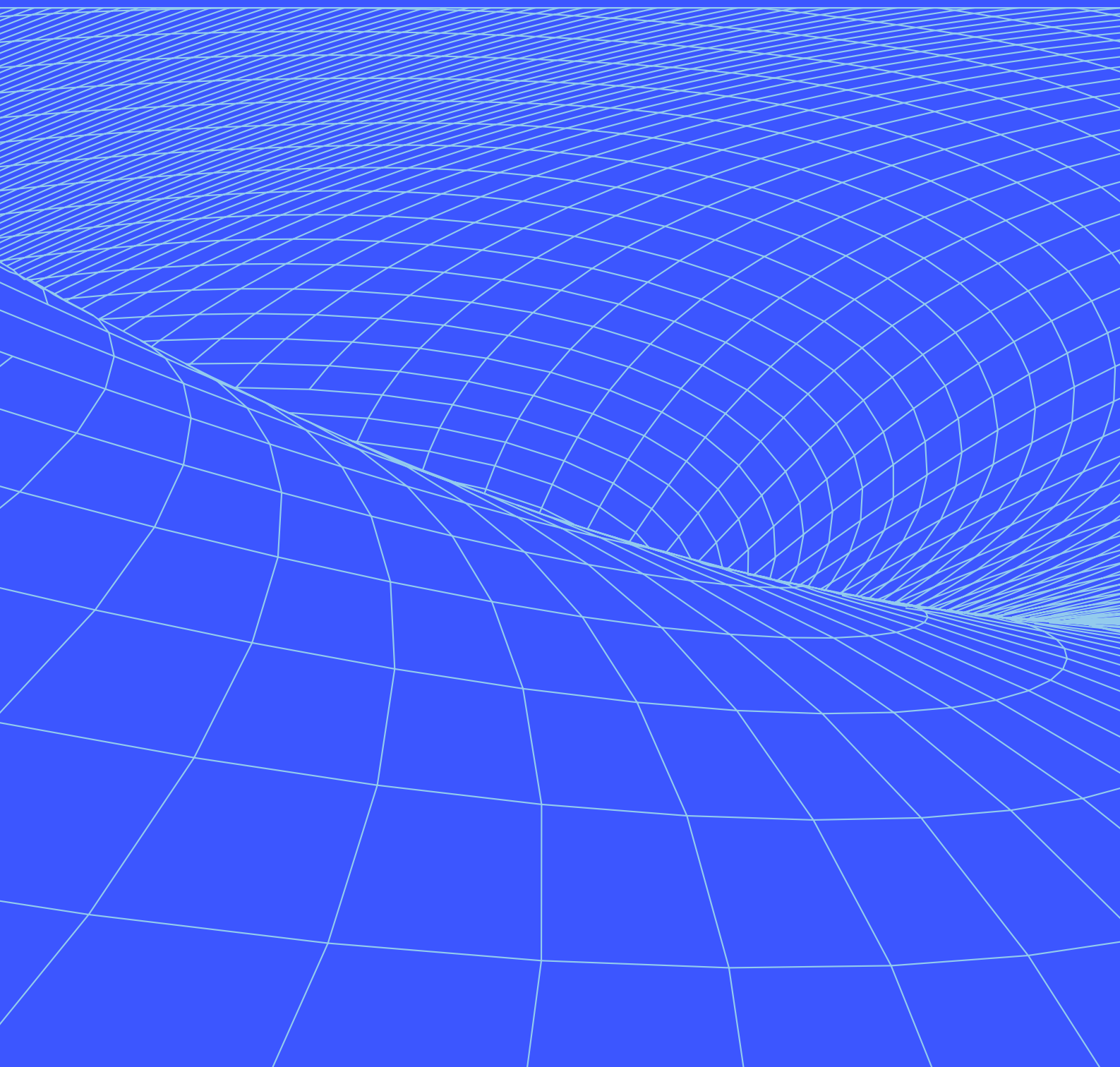
Xordex[Hashentic]

Smart UID tags for real things



Global counterfeiting crisis

$1.7T
estimated value of the global counterfeiting market /2023/

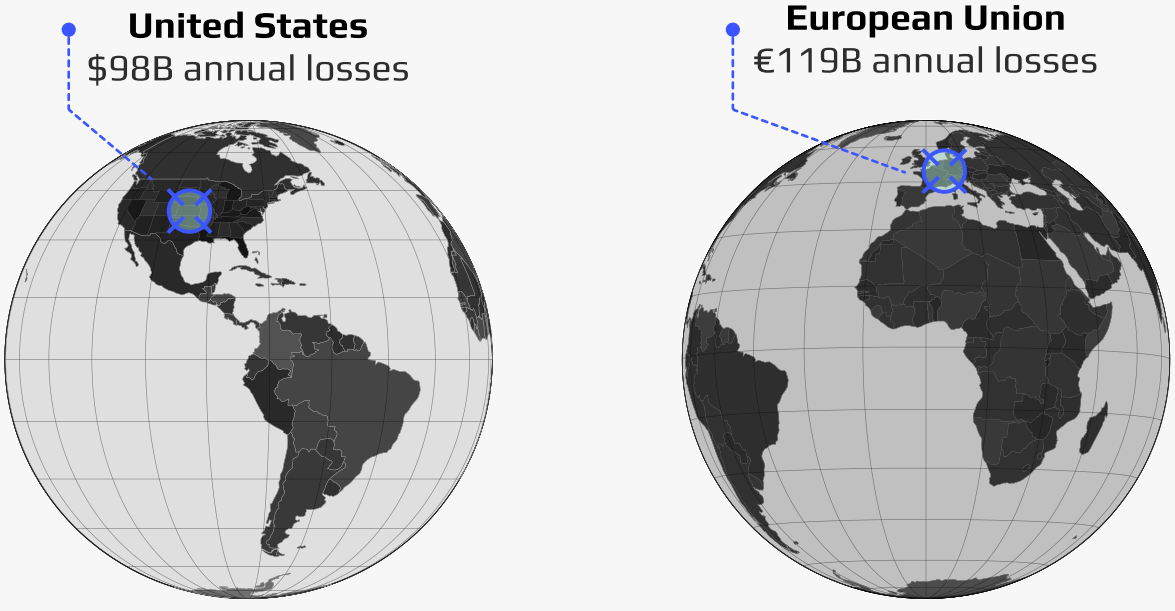
$174B
in lost tax revenue globally

5.4M
jobs at risk from counterfeit products

1in20
dollars will be spent on counterfeits if action is not taken by 2030.

Economic Losses from Counterfeit Goods by Region

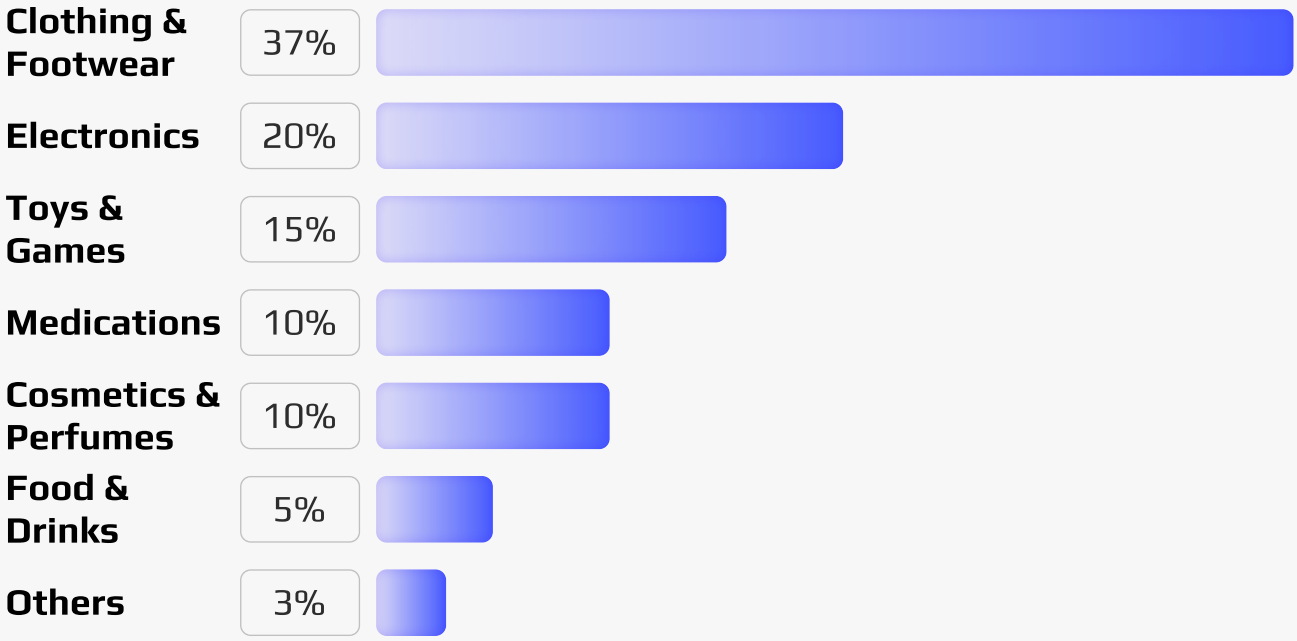
/2023/



SOURCE: WORLDMETRICS.ORG

Global Counterfeit Goods Distribution by Category

/2023/



The expansion of the illicit market poses significant risks to all participants in the legal economy:

Government
The expansion of the black market reduces tax revenues, as legitimate businesses lose profits and economic activity declines.

Manufacturers
Customer dissatisfaction caused by counterfeit goods damages brand reputation, leading to lower loyalty and a decline in sales.

Consumers
Beyond financial and emotional harm, counterfeit products pose serious risks to consumer health and safety.

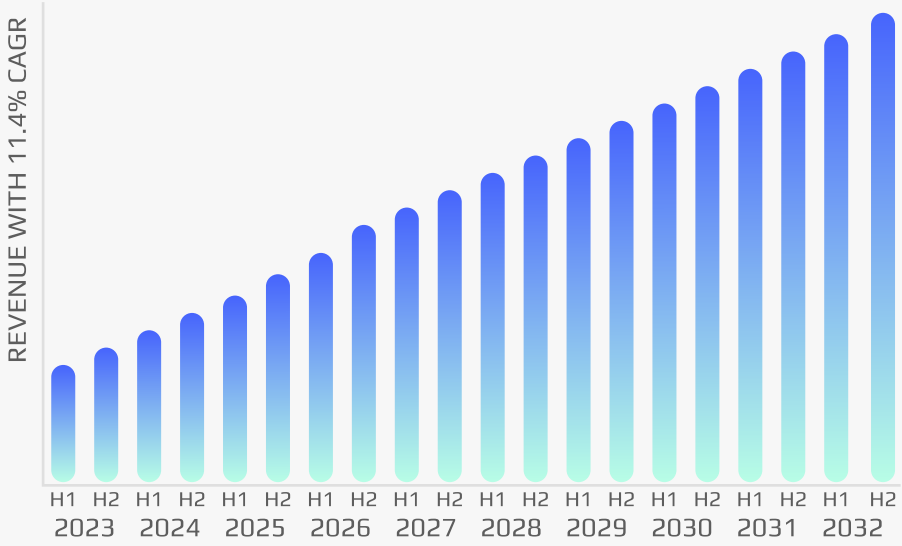
SOURCE: WORLDMETRICS.ORG, COMMISSION.EUROPA.EU

Anti-Counterfeiting Technology Market Growth

/2023-2032/

$146.92B
market size in 2023

$381.97B
expected market size by 2032



Trend

The demand for anti-counterfeiting solutions is rapidly accelerating across industries due to rising threats of product fraud, stricter regulations, and consumer expectations for transparency. Authentication technologies (NFC tags, blockchain verification, serialization, and AI-based analytics) are becoming standard components in modern supply chains. Key growth drivers:

1. Surge in counterfeit activity across high-risk sectors: medicines, electronics, luxury goods
2. Expansion of e-commerce, where brand protection is harder to enforce
3. Government mandates around serialization, digital identities
4. Brand owners prioritizing consumer trust, anti-fraud capabilities

SOURCE: ZION MARKET RESEARCH

Smart tags for real things

Our solution is a blockchain-based authentication system that uses NFC technology to verify the authenticity of physical goods — seamlessly, securely, and at scale.

The entire system runs on Xordex — a modular blockchain engine designed for enterprise use. Each client can deploy their own private blockchain instance, tailored to their needs. Optional integrations include loyalty programs, supply chain visibility, and regulatory compliance tools.

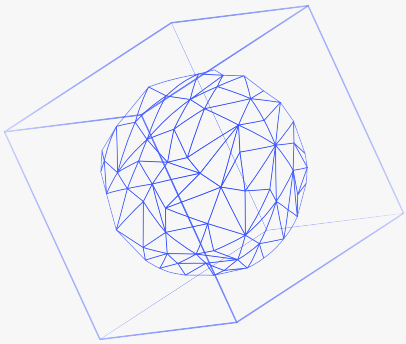
Deployment is flexible: Xordex supports both on-premises installations and fully hosted SaaS solutions. Every implementation is customized — from tag choice to backend logic — to align with the customer's existing infrastructure and business goals.

Our blockchain engine is the basis of everything

#1.0 A Modern, scalable & modular architecture

Xordex is a high-performance blockchain engine designed with scalability and modularity in mind. It operates through a trio of specialized node types — hub, validator, and composer — each fulfilling a unique role in transaction handling, consensus, and data orchestration.

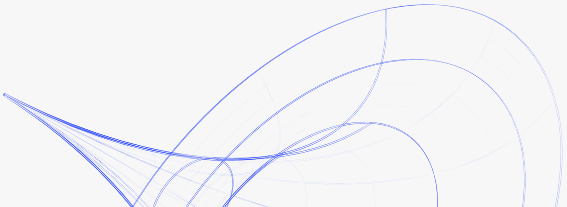
Every node runs as a lightweight container (in Docker) with its own PostgreSQL database, which guarantees data integrity, scalability, and seamless deployment across environments.



#2.0 Customizable & plug-and-play ecosystem

With a rich library of pluggable services — from authentication solutions and KYC to tools for tracking supply chains and implementing loyalty programs — Xordex enables businesses to tailor their blockchain network to specific use cases.

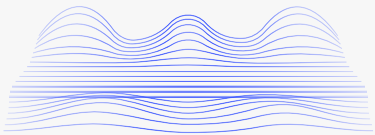
This modular approach empowers rapid development without sacrificing flexibility, allowing for fine-tuned control over network behavior and functionality.



#3.0 Flexible consensus mechanisms

Businesses can choose the most appropriate consensus method depending on their specific needs for speed, decentralization, and trust. Xordex supports Proof of Authority (PoA) by default and offers options for Proof of Stake (PoS), Proof of Work (PoW), and Delegated Proof of Stake (DPoS).

With customizable network parameters — fees, token emissions, denominations, and more — the engine is adaptable to a wide range of industries and user bases, ensuring scalability.

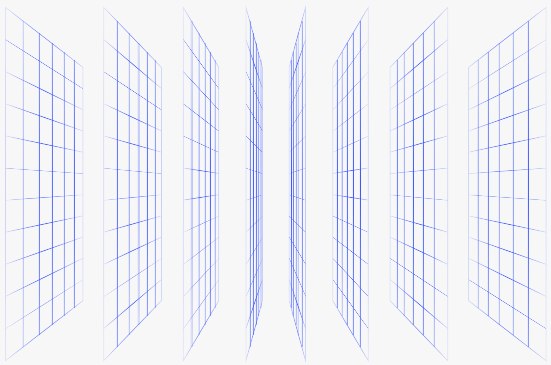


Our blockchain is the basis of everything

#4.0 High-level security & transparency

Security is at the core of the Xordex design. With robust ECDSA encryption, SHA-512 hashing, and granular access control, Xordex ensures high-grade protection across the stack.

The built-in block explorer provides real-time visibility into transactions, the validator model and public APIs ensure network integrity, trustworthiness, and protection against malicious behavior.

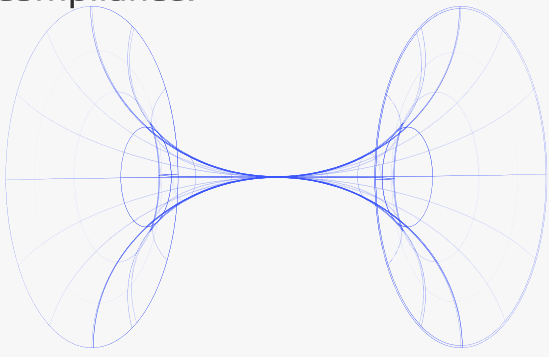


#5.0 Engineered for fast deployment, automation

With full automation based on Ansible, Xordex dramatically shortens time-to-launch. A built-in SDK, preconfigured wallets, and RESTful APIs accelerate integration.

From genesis block creation to live network operation, every step can be automated and version-controlled — making it ideal for workflows and minimizing human error in mission-critical environments.

The solution is available as SaaS or can be deployed on-premises, giving businesses full control over infrastructure and compliance.



Cutting-Edge System

- Verification of tagged products using any NFC-enabled smartphone.
- Flexible tag standards — from cost-effective NTAG213/215 to highly secure NTAG424, including support for proprietary tag formats.
- Data from the tag leads to an immutable blockchain record or transaction that proves product origin, integrity, and status.
- Scalable across industries and suitable for any product category — electronics, perishables, cosmetics, fashion, and more.

Protection for Manufacturers

- Counterfeit reduction contributes to stronger brand positioning and improved profitability.
- A private, fully controlled blockchain network can be deployed using Xordex's flexible, modular engine.
- Available deployment models: on-premises or cloud-based (SaaS).
- Loyalty systems, supply chain tracking, and compliance modules can be seamlessly integrated into a customized blockchain network.

Trust & Safety for Consumers

- No apps needed — simply tap the product with a smartphone to verify authenticity.
- Instant, effortless, and free authenticity confirmation.
- Consumers can check product information anytime, anywhere.
- Helps protect consumer health, safety, and trust.

Phase: 1. Encoding

1.1 Secure Key Generation

During the initial encoding phase, each NFC tag is assigned a cryptographic key used for future authentication. This key is generated using a high-entropy, cryptographically secure random number generator (CSPRNG), ensuring both unpredictability and resistance to duplication.

For basic tags (NTAG213/215), this key is written into a protected memory area of the tag itself, typically using NXP's password protection scheme.

For advanced tags (NTAG424), the key is never written into the tag's memory. Instead, the tag uses an internal secure element to perform cryptographic operations (CMAC) without exposing the key, while the matching key remains securely stored on our backend.

1.2 Secure Key Storage & Isolation

All encryption keys are securely stored on our backend infrastructure, regardless of tag type. This storage environment uses industry-grade security practices, including hardware-backed encryption, access control policies, and audit trails.

Especially for NTAG424 tags, where authentication relies on server-side CMAC verification, our architecture ensures full key isolation and guarantees that keys are never exposed or stored on the tag in a readable form.

1.3 Token Generation (UID, CMAC)

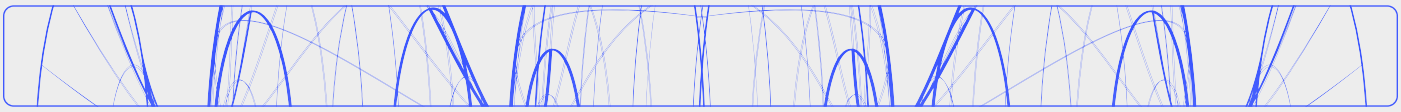
When an NFC tag is scanned, its internal logic uses a stored key (or a derived shared secret) to generate a secure authentication token. For standard tags like NTAG213 or NTAG215, this is typically a static UID. For advanced tags such as NTAG424, a dynamic CMAC is generated using a challenge-response mechanism.

In both cases, a cryptographic hash function (SHA-512) may be applied to enhance token integrity and prevent reverse engineering. The resulting token is then validated against the corresponding blockchain record, confirming both product authenticity and data integrity.

Phase: 2. Scanning

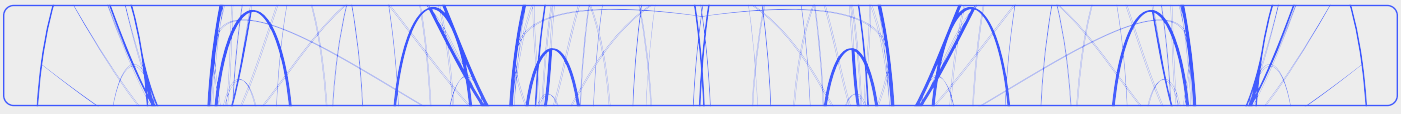
2.1 NFC Activation & Tag Interaction

The verification process begins when a consumer enables NFC on their smartphone and brings it close to the embedded NFC tag—typically placed on the product or its packaging. Most modern devices detect the tag automatically within 1–3 cm, with no need for a separate app. This effortless interaction initiates the authentication sequence in real time.



2.2 Automatic Redirect via Secure Identifier

Once scanned, the NFC tag transmits a pre-encoded URL to the device. This URL includes a unique identifier—either a static UID (for tags like NTAG213/215) or a dynamic CMAC (for secure tags like NTAG424)—appended as a query parameter. The redirection is instant and seamless, routing the user to a secure verification endpoint hosted on our platform.



2.3 Real-Time Verification & Dynamic Content Delivery

At the destination URL, the platform verifies the identifier against the blockchain record and displays the authentication result: genuine or invalid. The same page can also be dynamically configured to deliver personalized content, product data, or marketing experiences, adapting based on context, location, or scan history.

Phase: 3. Verification

3.1 UID and CMAC Verification via Blockchain Records

Once a tag is scanned, the platform receives either a static UID (for standard tags like NTAG213/215) or a dynamic CMAC (for secure tags like NTAG424). For standard tags, the UID is validated by matching it against the product's corresponding record stored on the blockchain. For NTAG424, the platform uses the pre-stored cryptographic key to verify the CMAC via challenge-response validation, ensuring the token was generated by a genuine tag and not forged.

This confirms:

- Tag authenticity
- Resistance to cloning or spoofing
- Match with the original blockchain-anchored identity

3.2 Real-Time Verification Result

Upon successful verification, the user is shown a secure results page indicating the product's authenticity status. This page may also include personalized data: origin, certifications, metadata, or branded content — all tied to the specific product and scan event.

3.3 Immutable Proof via Blockchain Anchoring

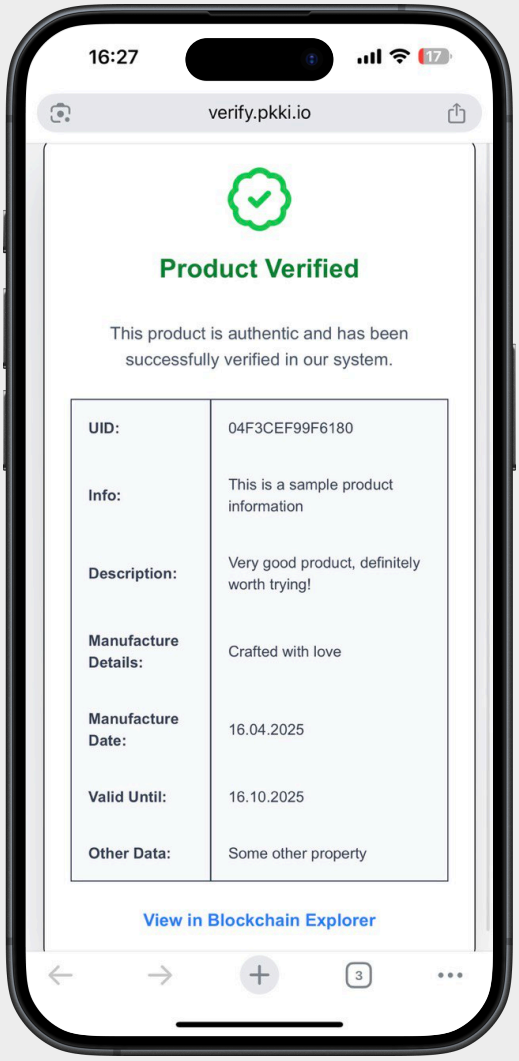
Each verification event is cryptographically anchored to the Xordex blockchain. A unique hash of the verification data is recorded on-chain and linked to the product ID.

The verification page includes a direct link to the Xordex blockchain explorer, allowing any stakeholder to independently verify:

- The blockchain transaction hash
- The timestamp and block number
- Proof of data immutability and integrity

This ensures a transparent, tamper-proof, and auditable product journey — from tag creation to scan and validation.

User Journey



- Enable NFC
- Scan the product tag
- Open the authentication page in any browser
- View the result
- If the product is authentic, the user will see detailed information and a link to the Xordex Blockchain Explorer

Let's talk!

VISIT OUR WEBSITE →

Xordex[Hashentic]