Cryptowerk

Ensuring Data Authenticity with Cryptowerk

Public Blockchain Verification

Introduction

In an era of rapid digital transformation, ensuring the authenticity and integrity of data is more critical than ever. Cryptowerk specializes in providing public blockchain-based data integrity solutions, enabling organizations to verify the authenticity of their digital assets at scale. By creating an immutable, verifiable record of data, Cryptowerk ensures that any tampering or unauthorized alterations can be detected promptly.

Cryptowerk's Approach to Data Verification

Cryptowerk's flagship service, **Cryptowerk Horizon**, employs its proprietary **RealitySeal** technology to create an unalterable proof of data authenticity. This is achieved through **digital fingerprinting**—generating unique **cryptographic hashes** of data, which are then securely anchored via a patented mechanism onto **public blockchains**. This ensures that the original data is not shared but that each unique RealitySeal can be verified against the recorded hash, providing **irrefutable and mathematical proof** of its authenticity.

Comparison: Digital Signatures vs. Blockchain-Verified Data Hashes

Digital Signatures

Digital signatures authenticate both the sender's identity and the authorship of the data. They function as a cryptographic mechanism equivalent to a handwritten signature, ensuring **non-repudiation**.

Key Features:

- Ensures authenticity of the sender.
- Provides proof of data authorship or ownership
- Requires **public-key infrastructure (PKI)** for key management.

Blockchain-Verified Data Authenticity

A **data hash** is a cryptographic fingerprint of data that is stored via a proprietary system on a public **blockchain ledger** to provide a tamper-proof record. For each hash a RealitySeal is returned to the sender. Unlike digital signatures, blockchain-based verification does not confirm the sender's identity but provides **immutable proof** of the data's existence and state at a specific time, including possible metadata.

Process:

1. **Hashing the Data**: The original data is processed through a cryptographic hash function, creating a unique hash. The original data are not shared.
2. **Storing the Hash on the Blockchain**: The Cryptowerk system accumulated multiple hashes to a superhash which is recorded onto a **public blockchain**, ensuring it cannot be altered. For each hash a RealitySeal is returned to the sender.
3. **Verification**: To verify integrity, the original data is hashed again and compared to the stored RealitySeal.

Key Features:

- **Immutable proof** of data authenticity.
- Ensures data remains unchanged over time.
- Independent verification without requiring **trusted third parties**.

Key Distinctions

Feature	Digital Signatures	Blockchain-Verified Data Authenticity
Functionality	Verifies sender identity & authorship	Ensures data authenticity & integrity and existence
Use Cases	Legal documents, content licensing	Supply chain tracking, evidence authentication, AI input & output data validation
Complexity	Requires key management & PKI	Requires blockchain access

Cryptowerk’s RealitySeal Technology

Cryptowerk’s **RealitySeal** technology enhances blockchain-based verification by “**compressing” and optimizing data hashing**, making it highly scalable for enterprise applications.

How It Works:

1. **Digital Fingerprinting**: The data owner generates **hashes of data and metadata**.
2. **Blockchain Anchoring**: Cryptowerk receives only hashes via a REST API. A **master fingerprint** is generated stored on multiple public and private blockchains.
3. For each hash a unique **RealitySeal** is returned to the sender.
4. **Tamper-Proof Verification**: Users can instantly verify the authenticity of data by comparing a regenerated hash with the RealitySeal
5. **Such verification can be done independently of Cryptowerk or** using Cryptowerk’s APIs.

Advantages of RealitySeal:

- **Scalability**: Handles millions of verifications per second.
- **Redundancy**: Can use multiple **distributed ledgers** (public blockchains) for increased security.
- **Cost-Effective**: Blockchain transaction costs are almost irrelevant as each blockchain transaction consists of millions of hashes.
- **Compliance-Ready**: Meets legal and regulatory standards, including **GDPR**.

Use Case examples

Journalism & Investigative Reporting

- **Whistleblower Protection**: Ensures confidentiality of sources and evidence.
- **Court-Admissible Evidence**: Blockchain-verified documents to become legally recognized.
- **Fake News Prevention**: Prevents tampering of articles and multimedia content.

Cyber Insurance & Fraud Prevention

- **Claims Validation**: Provides **tamper-proof** logs of cyber incidents.
- **Regulatory Compliance**: Auditable compliance reporting.

AI & Machine Learning

- **AI Model Provenance**: Verifies the **state and integrity** of AI training data.
- **Decision Transparency**: Ensures AI-generated outcomes are **authentic and reproducible**.

Enterprise Data Security

- **Supply Chain Verification**: Ensures the integrity of material chains and transactions.
- **Regulatory Compliance**: Helps organizations meet **audit and compliance** requirements.

Conclusion

Cryptowerk's **Data Integrity solution** based on **public blockchain verification** technology is a game-changer in **data authenticity**. By leveraging its patented **RealitySeal** technology and **immutable public blockchain records**, organizations can ensure that their **digital assets remain tamper-proof, auditable, and verifiable**.

Contact:

CRYPTOWERK Corp.

CEO: Dirk Kanngiesser

dirk.kanngiesser@cryptowerk.com

www.cryptowerk.com