FEBRUARY 2023

REALITYSEAL BY CRYPTOWERK

PROOF, AT SCALE

INTRODUCTION

Proving data authenticity in the face of exponential growth in data production and manipulation is a daunting challenge, especially when considering the need to guarantee scalability, and compliance with increasingly stringent standards of proof.

We now live in a world where anyone can manipulate data and commit fraud from the supercomputers they are carrying in their pockets.

In this context, it is increasingly difficult for organizations to trust global institutions and Certificate Authorities to authenticate their data.

2030 IT STRATEGY
MANAGEABLE LEVELS OF FRAUD
TOLERANCE FOR ERROR IN PROCESS AUTOMATION
PREDICTABLE DATA GROWTH
TRUST IN INSTITUTIONS
TRUST IN CENTRALIZED CERTIFICATE AUTHORITIES

Photo by Valery Fedotov on Unsplash

For example, how can an insurer prove, without doubt, that data relating to a claim is the same data that was recorded at the point of incident? Or, how might a fan manufacturer prove the configuration of its air flow equipment to an investigation into the causes of an industrial accident? Or, how might an AI vendor prove the state of its models when the model makes a contentious decision?

In these scenarios we must remove any margin of doubt about data authenticity. With current methods this level of absolute proof is not possible.

Companies must proactively address this issue and plan for the potential consequences of fraud and data manipulation, as the potential damage will be catastrophic if they fail.

CURRENT SOLUTIONS ARE INADEQUATE

We can categorize current approaches to data authentication in three broad categories: manual methods, hashing, and signatures.

MANUAL METHODS

Notaries, signatories, trusted institutions and privileged users may be suitable for small-scale contract law applications where the volume of data is minimal and stakes (and profits) are high. However, these methods are not sufficient for automated data creation and decision making, as it is possible to generate hundreds of thousands of data points per second.

HASHING

Generating a hash value of data is a commonly used approach to ensure data authenticity and anonymous data verification. This process creates a unique, fixed-length digital representation of the data, also known as a "fingerprint" or "digest", which can be used to verify that the original data has not been tampered with or altered in any way.

For example:

Original data: `Jeff is riding on a camel`
Hash value: `34de09e610aec6389c248f7749663259fabe27c8ef4631d392e95b26337506f5`

Altered data: `Jeff is riding on a Camel`
Hash value: `8cfed49bcd1e14303d37e5c333c8014ab99db084ed8fa9e88cc4b5e228e81b41`

The example illustrates that even a small alteration in the original data results in a total change in the hash value. By possessing both the data and the corresponding original hash value, it is easy to confirm that the data is authentic and has not been tampered with.

However, to ensure that the original data remains verifiable at a later time it is essential to securely store the hash values in an immutable location, along with metadata that proves that the hash values being verified are those which correspond to the event in question. Without this, it is difficult to prove that original data was not replaced and re-hashed.

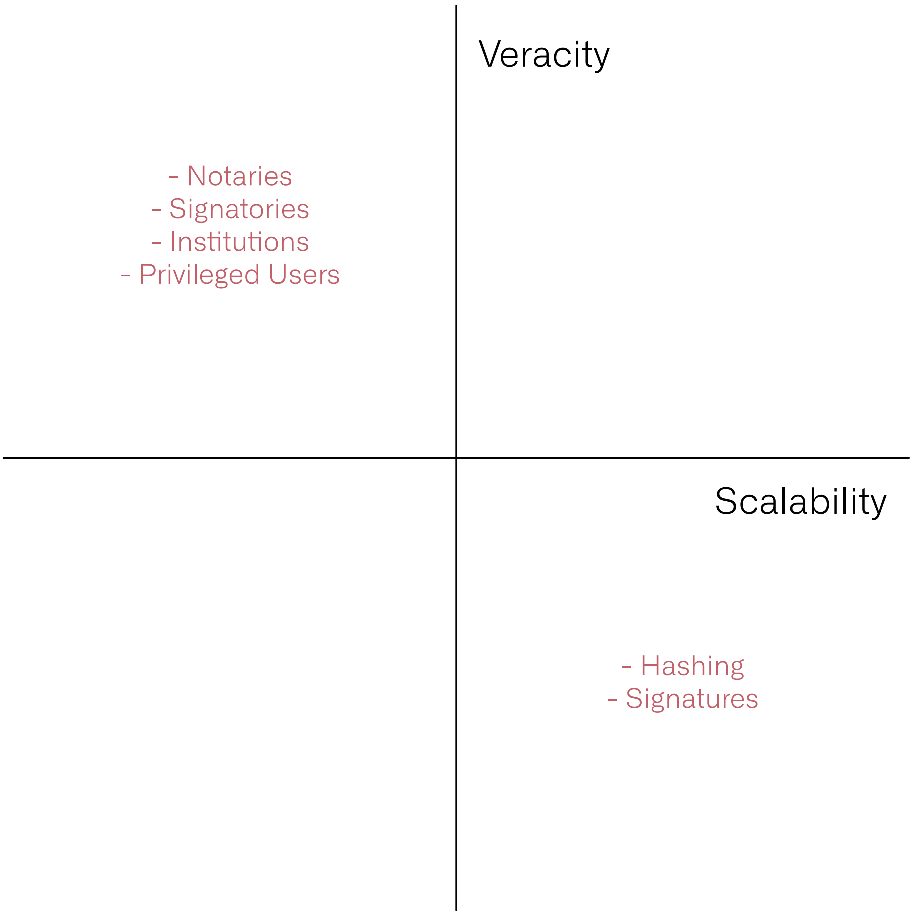
So, simple data hashing is insufficient.

SIGNATURES

The other common approach is to employ digital signatures and certificates, but while these are sufficient to prove ownership, they cannot prove that the data is not manipulated.

This problem is multiplied by the importance of the data, as the trustworthiness of an organization's private server or blockchain may be called into question by an adversary.

Furthermore, the centralized infrastructure required by these solutions renders them ineffective in an adversarial context, where entities such as organizations, governments, or even supranational bodies are not willing to trust each other. For instance, a data-hashing system operated by a US-government institution may not be trusted by the Chinese government, and vice-versa.



A NEW APPROACH

WHY DO WE NEED A NEW APPROACH?

Data sources, including robotics, AI, the Internet of Things, and cloud computing, have increased exponentially. This surge in data requires secure data exchange protocols to mitigate the risk of manipulation, tampering, or fraud, which is essential to ensure that decisions based upon that data can be trusted and verified.

Maintaining data authenticity is a critical challenge that requires scalability and rigorous standards of proof to be upheld and monitored continuously. For instance, an insurance company must be able to demonstrate that the records related to a claim have not been altered during the chain of custody since the incident occurred. Similarly, an IoT company must be able to demonstrate that the controller software distributed in millions of devices remained up-to-date and unaltered when sensor failures resulted in catastrophic damage. Additionally, an AI provider must establish proof of the data used to train an AI model after a controversial decision is made by the model.

Organizations must guarantee the authenticity and accuracy of the data to avoid potential risks such as legal claims and harm to their reputation. Any solution must be able to handle a large volume of data, be accessible to all users, and provide a high degree of trustworthiness, even if evidence of authenticity must be presented in a court of law.

THE CHALLENGES OF IMPLEMENTING A NEW APPROACH

The implementation of a new approach is challenged by the distributed ledger (blockchain), due to its slow writing speed and incompatibility with industrial applications, thus hindering the potential to reap the benefits of its immutability.

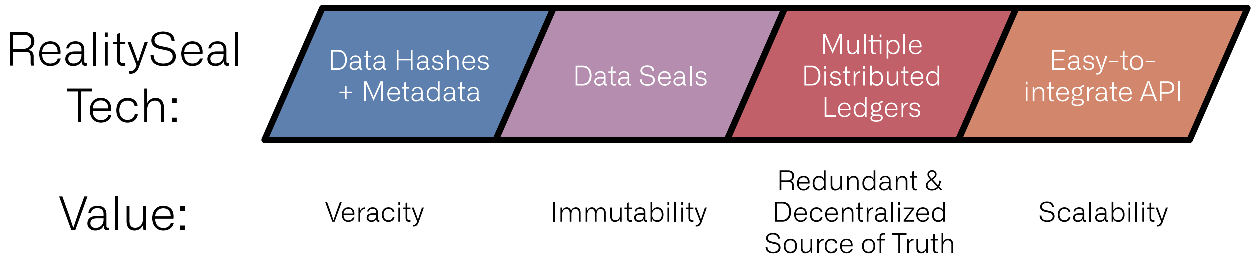
To overcome this challenge, organizations and developers must focus on developing and deploying blockchain-based solutions that are optimized for industrial applications. This can be done by leveraging existing blockchain technologies and protocols, such as Hyperledger Fabric, Ethereum, and Corda, that are specifically designed for enterprise use cases. But this alone will not solve the scalability challenge.

The reluctance to adopt blockchain technology also remains a challenge, due in no small part cryptocurrency market crash in 2022 which created a negative perception of the underlying technology to the general public.

To overcome this challenge, organizations should focus on educating their stakeholders about the potential of blockchain technology, and the ways in which it can be used to improve existing processes and create new opportunities. They should also emphasize the potential for blockchain to increase transparency and security, and explain the differences between blockchain and cryptocurrency. Finally, the term "*distributed ledger*" is a better description of the technology without the negative connotation of "*blockchain*".

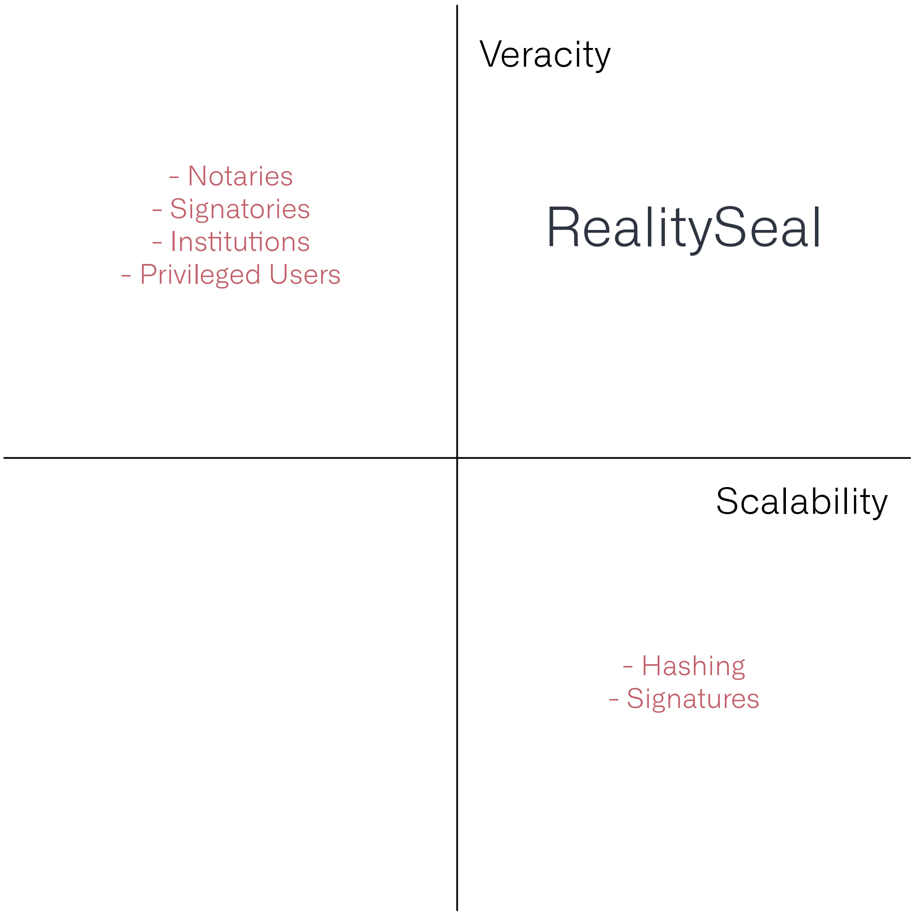
REALITYSEAL

CryptoWerk's unique RealitySeal data seal is more than a cryptographic hash, as it also contains any desired metadata, and can process data hashes at unprecedented speeds. We use proprietary compression technologies to write an almost limitless amount of RealitySeals to distributed ledgers, thereby solving the problem of slow writing speeds. This new technology is scalable and able to provide ultimate proof-of-truth in a high-standard truth environment, such as a courtroom. RealitySeal provides an affordable API that is easy to integrate into existing data flows and processes, and can establish decentralized redundancy by utilizing multiple distributed ledgers instead of a single blockchain proof.



This is particularly important in situations where trust is implausible as RealitySeals can be simultaneously written to multiple ledgers hosted by adversarial institutions or governments. This eliminates the need to establish trust between those institutions in order to ensure the accuracy of the data.

This technology enables multiple industries, including insurance, medical, manufacturing, and forensics, can confidently transform their data into irrefutable facts at a large scale. In comparison to other technologies, RealitySeal is easy to implement, scalable, decentralized, and is robust under adversarial scrutiny.



Veracity

- Notaries
- Signatories
- Institutions
- Privileged Users

RealitySeal

Scalability

- Hashing
- Signatures

Comparison

	CRYPTOWERK	HASHING	SIGNATURES
Attesting Authorship			✅
Immutability	✅		✅
Timestamp	✅		
Proof of Existence	✅		
Does not require trusted authority	✅	✅	
Permits private notarization	✅	✅	✅
Proof of causality	✅		
Certificate Authority not required	✅	✅	
Does not require private key	✅	✅	
Decentralized ledger for attestation	✅		

USE CASES FOR REALITYSEAL

SUPPLY CHAIN MANAGEMENT

Create an immutable record of products as they move through the supply chain. This can be used to track the origin of goods, as well as ensure that they have not been tampered with.

DATA MANAGEMENT

Anchor data such as documents, images, and videos onto a public ledger, making them tamper-proof and easily verifiable. This can be useful for organizations that need to ensure the authenticity of important documents, such as certificates or legal agreements.

IOT

Seamlessly write data from IoT devices onto a blockchain, in real time. This can be used to create an immutable record of the device's activity and ensure that it has not been tampered with.

FRAUD DETECTION & FORENSIC INVESTIGATION

Detect and prevent fraud by creating an immutable record of transactions, and pinpointing erroneous events in chains-of-custody.

ASSET MANAGEMENT

Write digital assets such as stock certificates, bonds, and other financial instruments onto a public blockchain, providing a tamper-proof record of ownership.

HEALTHCARE

Secure private patient data such as medical records, test results, and prescriptions onto a blockchain, eliminating the need for multiple conflicting standards and enabling zero-touch communication between healthcare providers.

REAL ESTATE

Reduce the risk of fraud by creating permanent records for deeds, mortgages, ownership transfer, and related documents.

GOVERNMENT

Government agencies can reduce the risk of fraud while supporting democratized data access by writing tamper-proof RealitySeals for important documents such as voter registration records, birth certificates, and land titles onto a public ledger, providing secure and verifiable access to this information.

LEGAL AND COMPLIANCE:

RealitySeal can be used to create provable tamper-proof records of legal documents, financial transactions, and other sensitive information to meet regulatory compliance.