CryptoWerk

SEAL YOUR DATA

Ensure system integrity, reduce fraud and provide data authenticity

INDUSTRY SOLUTIONS FOR:

AEROSPACE & DEFENSE • AUTOMOTIVE • PHARMA • SOFTWARE • UTILITIES

SAP® Certified
Built on SAP Cloud Platform

TABLE OF CONTENTS

Summary

New business models based on digital trust are crucial to future growth. Because these efforts require the secure handling of massive amounts of data, system integrity, data authenticity and fraud prevention are a top priority for CEOs and business leaders in nearly every industry.

Fraud costs millions of lives and hundreds of billions of dollars and touches every industry sector. The statistics are staggering. More than one million people die each year from counterfeit drugs. Fraudulent goods are a $1.8 trillion-dollar industry. Almost 7% of a company's profit is lost to internal fraud and data manipulation. By 2020, 50% of organizations will have suffered damage caused by fraudulent software. Data records are falsified or tampered with every day.

Cryptowerk helps companies detect and defeat fraud by creating a tamper-evident chain of custody of "digital moments," building trust into every product, process and transaction. Cryptowerk Seal digitally seals documents and data at the time-of-entry. Companies can then give access to validated parties to verify that the sealed data hasn't been tampered with and matches the underlying physical or digital assets.

Using Cryptowerk Seal, organizations can:

- Prove data was in a specific state at a specific point in time.
- Create a tamper-evident record of up to a million digital moments per second with connectors for many distributed ledgersboth public and private.
- Secure your data with an electronic fingerprint without the need to ever see the data itself, based on the decentralization and immutability of blockchains.
- Slash costs and increase the scalability of public blockchains, such as Bitcoin and Ethereum.
- Write to multiple distributed ledgers in parallel for added security.
- Future-proof your applications with the ability to switch blockchains without reprogramming.
- Scale easily with an enterprise-grade, SAP Cloud Certified solution.

Cryptowerk Seal integrates easily into existing environments, connecting to cloud services like Amazon, Microsoft Azure and Google, along with enterprise applications, databases and document repositories. It also supports new applications for digitally notarizing documents, images and software. Benefits for the Cryptowerk-powered organization include:

- Improved data reliability for analytics and decision-making
- Improved customer and partner trust
- Reduced audit costs
- Easier compliance with industry regulations
- Reduced security and reputational risk

Cryptowerk's SAP-Certified solution provides companies with blockchain-powered data integrity solutions to digitally notarize their data, creating a digital hash, or "fingerprint," of the data that can be stored as an immutable proof of authenticity on any public or private blockchain. The original data stays private and is never transferred to Cryptowerk. This approach also solves the throughput and cost limitations of public blockchains, making them practical for use in enterprise-grade high data volume applications.

Cryptowerk Seal enables data interoperability between the disparate network of applications and application languages used by various participating organizations. It connects with any public, private or hybrid blockchain, or multiple blockchains. Blockchains can even be switched out with no loss of data or system downtime. There is no need to change end-user application interfaces to create a tamper-evident record of data. Cryptowerk Seal also enables faster, cheaper processing through specialized compression algorithms, providing true Big Data enterprise scalability.

Introduction

Because of the importance of digital data to today's successful organizations, digital fraud prevention and anti-data manipulation security is a top priority for CEOs, CFOs and business leaders in nearly every industry. Many of these organizations must also meet industry regulatory and legal compliance requirements for data integrity. Blockchains and other distributed ledger technologies create an unalterable transaction record that maintains and records data in a way that gives stakeholders the ability to detect data manipulation. and to ensure that the data and information they are using to track processes and to make vital decisions is accurate.

Anti-fraud applications for blockchains include:

- Provide greater, more secure supply chain processes by attaching digital tokens to parts and "notarizing" supply chain data with a digital seal. This creates digital "fingerprints" that can be compared to the original data to verify authenticity between all parties in the chain, improving information transfer and logistics coordination, detecting counterfeit items, and reducing leakage and errors in ordering and inventory cataloging.
- Verify system integrity, and the integrity and quality of code, by providing a tamper-evident record of applications and code at any moment in time, improving security, trust and transparency.
- Turbo-charge any application requiring data integrity in days—not weeks—with the power of blockchain sealing, without requiring specialized blockchain expertise.
- Allow pharmaceutical companies to secure systems that can detect when counterfeit or inferior drugs enter the supply chain. Prevent those components from ever making it to the retail shelf—saving money and lives.
- Empower consumers to more confidently make decisions about what they purchase (such as a fair-trade item, organic food or a luxury brand) based on the transparency and immutability that blockchain technology provides in proving provenance.
- Capture and verify digital moments from the time a vehicle or aircraft is being manufactured, sold, maintained and operated. Combat fraud, comply with new industry and government requirements, and drive new innovations such as driverless cars and intelligent digital displays.

Unfortunately, often enhancing applications with blockchains comes with economic and technical challenges—notably the lack of interoperability, ease of integration with existing systems and making them future-proof. There are competing and emerging distributed ledger technologies with varying levels of adoption in various industries that are mostly incompatible. The myriad of enterprise applications and legacy systems add to integration complexity. In addition, if an enterprise is using public blockchains, such as Bitcoin Blockchain or Ethereum, transactions are often costly and throughput is limited. At this stage of evolution, implementing distributed ledger technologies poses a high risk for companies based on uncertain regulation, missing standards, and technical limitations.

Cryptowerk Seal is a blockchain-enabled solution that automatically verifies the authenticity and integrity of your digital moments, up to one million times per second. Whether it's a product's ID code, the data generated by a process or a digital transaction, Cryptowerk Seal creates a tamper-evident chain of custody that seals your data at the time of entry, creating a digital fingerprint that helps you detect and deter fraud. Blockchains are emerging as a game-changing technology well-suited for this task, and combating fraud is a top priority of CFOs, CTOs and CIOs driving digital business initiatives.

Cryptowerk's patent-pending technology makes blockchains practical for high performance, enterprise applications, providing a scalable, future-proof platform for your digital transformation initiatives.

SECURE: Cryptowerk's SmartStamp™ hashing technology lets you instantly verify, store and share only "digital fingerprints" of transactions. Your sensitive data stays private. In addition, Cryptowerk Seal allows you to leverage both public and private blockchains for additional security and redundancy.

ENTERPRISE GRADE AND SAP-CERTIFIED: Cryptowerk Seal is certified and proven in high-volume enterprise implementations with some of SAP's largest customers, and is available now on the SAP App Center, and from Cryptowerk and its partners.

ANY BLOCKCHAIN: Cryptowerk's REST API makes it easy to integrate your application with any public, private or hybrid blockchain, with no downtime or special blockchain expertise required. As technologies change, you can take advantage of the latest innovations without recoding, making your solution future-proof.

EXTREME SCALABILITY: Built for complex, high-volume applications, Cryptowerk Seal accelerates blockchain transactions up to 80,000 times faster, while decreasing blockchain transaction costs to a fraction of their typical cost.

FLEXIBLE: Cryptowerk Seal is available on-cloud, on-premise and on-chip, meeting the strict requirements of the most heavily regulated industries. Your data remains completely portable to any blockchain.

Blockchain Overview

A blockchain is a shared, immutable ledger for recording and tracking digital assets in a network. Their decentralized, open and cryptographic nature allow people to trust each other and transact peer-to-peer. To put it another way, think of a blockchain as a distributed database, with no central administration. It's called a "blockchain" because of the way it stores data—in bundles of data called "blocks" that record and confirm the time and sequence of transactions. These blocks are then linked together to form a chain. Each block contains a time-stamped batch of recent valid transactions, and the hash of the previous block.

The previous block hash links the blocks together and prevents any block from being altered or inserting a block between two existing blocks. Each subsequent block strengthens the verification of the previous block and the entire blockchain. This distributed, duplicated, peer-validation method renders the blockchain tamper-evident. Also, blockchain-powered databases have extreme fault tolerance because of their built-in redundancy. Every node processes every transaction, so no individual node is critical to the database as a whole. Because nodes connect to each other peer-to-peer, many communication links can fail before the system collapses.

Why are blockchains secure?

Traditional databases are controlled by a single entity, which makes them easier to alter. Contrast this with blockchains, which store data in a linked chain across a network of non-trusting parties, without requiring a central administrator—eliminating the risks that come with holding data in a central place. Blockchain transactions inherently contain both proof of validity and proof of authorization, instead of using centralized application logic to enforce those constraints. Transactions are verified and processed independently by multiple "nodes," with the blockchain acting as a consensus mechanism to ensure that those nodes stay in sync. Store your data on the blockchain, and it is immutable.

What are public and private keys?

A "public key" is a long, randomly-generated string of numbers that serve as a user's address on the blockchain. Digital assets that are sent across the network from a user get recorded as belonging to that address. Because blockchain security methods use encryption technology to protect digital assets, you need some way of accessing them. A "private key" is a code that gives the owner access to the digital assets held behind a virtual door. You can only access the digital asset by providing the private key.

Why are public blockchains slow?

Centralized databases only process transactions once (or twice). In a blockchain, transactions must be handled independently by every node in the network. "Miners" group transactions into "blocks" which are added to the "blockchain"—the shared historical record of all transactions. Block sizes are limited, which means transactions that exceed the capacity for a block get stuck in a queue waiting for the next block.

In today's most prominent blockchains, ensuring that nodes in the network reach consensus takes a considerable effort of predetermined average time—in the case of Bitcoin, ten minutes. Because of its distributed, peer-to-peer nature, blockchain-based transactions can only complete when everyone updates their respective ledgers—a process that can take hours. For example, on Bitcoin, a transaction is only considered confirmed if it has been added to a block six blocks ago. You can see how if the blocks get stacked

up in queues, this can take quite some time. Also, consensus mechanisms can involve significant back-and-forth communication, using forks and rollbacks, or other costly methods. A limited number of transactions per block together with the predetermined time per block predetermines the maximum throughput, typically below 30 transactions per second, for everything, worldwide. With blockchain use rapidly multiplying, these delays will only increase.

Cryptowerk Seal uses a patent-pending compression algorithm to fit more data into each block, by orders of magnitude, speeding up throughput and reducing costs. Contrast this to other solutions, which often jeopardize security for throughput by decreasing the number of nodes, posting only consolidated transactions, or changing the proof-of-work mechanism. In addition, Cryptowerk Seal is compatible with any consensus mechanism and can also handle off-chain data.

Cryptowerk Seal

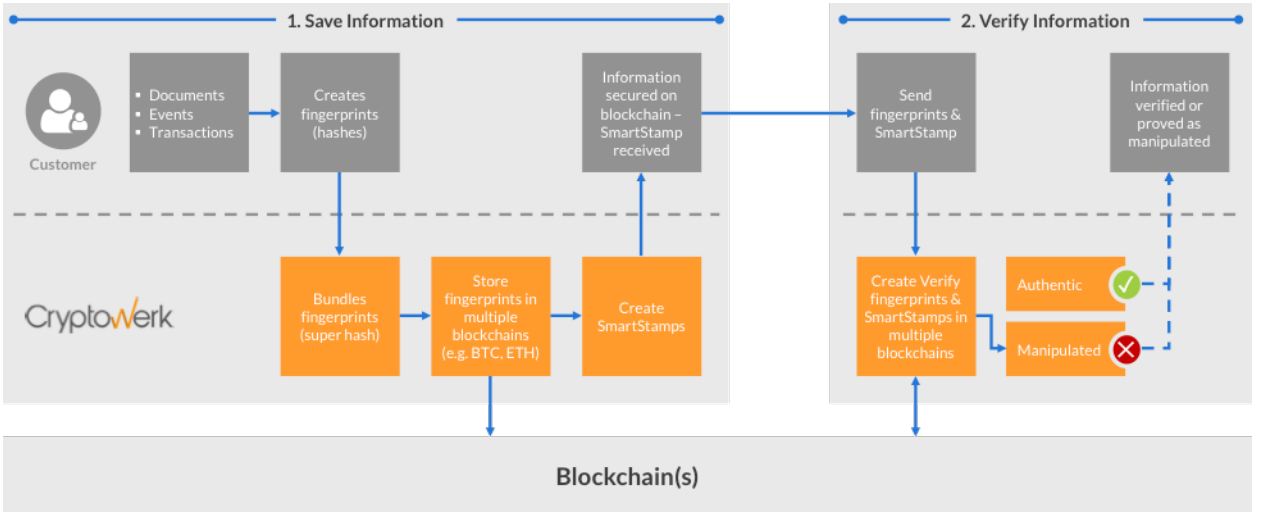
Cryptowerk Seal makes it easy and affordable for enterprise organizations to integrate the benefits of blockchain into their enterprise applications. Cryptowerk Seal easily connects to any blockchain, and even allows you to switch between blockchains transparently and easily. Cryptowerk's blockchain-powered software digitally seals your data, creating a digital hash, or "fingerprint," of the data that can be stored as an immutable proof of authenticity on any public or private blockchain. The original data stays private and is never transferred to Cryptowerk. This approach also solves the throughput and cost limitations of public blockchains, making them practical for use in enterprise-grade, high data volume applications.

Interoperability, Scalability, Portability and Control

Any application. Any blockchain. Cryptowerk makes the connection. Crytpowerk Seal powers data interoperability between the disparate network of applications and application languages used by various participating organizations. The Cryptowerk solution has a set of standard interfaces and web services, enabling developers to easily work with various blockchain platforms (and even cutting edge next-generation consensus mechanisms) and even store transactions simultaneously in different blockchain platforms. Having a single API that is easily programmable to results in faster time-to-deployment and the ability to leverage blockchain technology without requiring expensive, specialized knowledge or expertise.

- **Improves Public Blockchain Scalability:** Cryptowerk Seal enables faster, cheaper processing when using public blockchains through specialized compression algorithms, providing true Big Data enterprise scalability.
- **Portability and Control:** Organizations are in full control of their data. Because Cryptowerk Seal stores hashes in a blockchain, there is no sensitive data submitted. This means enterprises can easily stop using blockchain technology or move to another blockchain platform without deleting data. The hashes stay in the blockchain, but the underlying data will be where the organization wants it to be.

Cryptowerk's Data Integrity Solution Architecture



Cryptowerk Seal consists of:

- The Cryptowerk Engine
- The Cryptowerk REST API, used for inserting and retrieving data to and from the engine
- A Universal Blockchain Connector that provides the ability to utilize any or multiple blockchains

Cryptowerk Seal also supports client-specific/industry-specific APIs, such as the SAP Pharma API that talks to the Cryptowerk API. The SAP Pharma API is included in Cryptowerk Seal for SAP. A connector to SAP HANA is also available.

Storing hashes of transactions into one or more blockchains

Cryptowerk Seal does not store original customer data in blockchains. This provides the highest possible security, efficiency, and ease of implementation. To submit information to Cryptowerk, customers hash any digital asset such as a performed transaction or file and send it to our server. Customers can also attach identifying metadata in addition to the hash.

Once Cryptowerk receives the hash, a ticket number is sent back to the customer which confirms receipt. Cryptowerk Seal bundles the collected hashes from all customers and creates a single bundle hash (the "anchor"). Cryptowerk Seal then submits the anchor to one or more blockchains as desired by the customer. Once a blockchain confirms a particular transaction, Cryptowerk returns one SmartStamp™ for each original hash on demand. SmartStamps allow customers to demonstrate irrefutable proof of existence and authenticity directly in respective blockchains.

Validating transactions via ticket number

A customer first sends a ticket number to the Cryptowerk system. Based on the ticket number, the associated anchor is identified and sent to the blockchain server for validation. If the position of the anchor in the blockchain is correctly returned, the Cryptowerk server generates a SmartStamp, which is the key to prove authenticity of a transaction or document and sends it back to the customer. Each SmartStamp consists of a

calculation instruction, the hashed transaction or document, and the anchor (hash of bundled transactions). (Note that if you are submitting a document to multiple blockchains, there is one SmartStamp issued per blockchain.) At this point, for even greater security, the ticket number, anchor and SmartStamp are currently removed from the Cryptowerk database. In turn, customers can then send the SmartStamp to their partners or clients to verify authenticity of a transaction or document by themselves.

Things to Keep in Mind When Starting a Blockchain Project

Don't do blockchain just to "do blockchain"

Don't jump on the bandwagon just to implement a "blockchain project." Look for areas where you need to add trust, security and data authenticity to an untrusted environment.

Don't expect current blockchain technologies to be the end of your journey

There are over 70 different blockchain platform technologies available—and tomorrow's "blockchain" might not even be a blockchain at all. Also, blockchain lacks the maturity and standards to promise interoperability among competing ledgers and platforms. Be prepared for integration challenges between blockchain technologies and legacy environments. You should choose a solution that is flexible enough to accommodate a rapidly changing technology stack with little or no reprogramming required on your part. Previous technology "winners" (e.g., social, mobile, etc.) appeared after the original incumbents laid the groundwork. The dominant technology today might not be the dominant technology in 12 months. Don't assume the technology you're using today will offer longevity and be aware that the best option doesn't even exist yet. Consider technology options that will offer flexibility to adapt. Cryptowerk insulates you from these types of problems by continually adding and updating its suite of blockchain connectors.

Don't forget to incorporate a learning process and disseminate knowledge

Begin experimenting with blockchain and establish test-and-learn constructs. Lessons regarding platforms, new business models, and products are vital to future success. Make sure that even contracted-out projects include heavy in-house IT involvement and establish a system to transfer knowledge and skills learned. Be sure that learnings are recorded and communicated to senior executives.

Follow a Structured Blockchain Project Process

Industry Specific Use Cases for Blockchain

Blockchain and other distributed ledgers are most useful for business processes involving multiple parties where there is less than complete trust among them. Organizations should consider using blockchain when one or more participants have an incentive to alter transactions, or when an application requires absolute data security against accidental or malicious tampering, both from within and outside the network.

Aerospace & Defense

Aerospace companies need to ensure that their products are safe and reliable while reducing costs. There are many use cases for blockchain technology in aerospace systems, and in data integrity and fraud prevention efforts. For example:

- Know when counterfeit or inferior parts enter the supply chain and prevent those components from ever making it into an airplane by enhancing track-and-trace solutions with the ability to create twinned digital tokens for parts and tracing transactions between all parties in the chain.
- Add an extra layer of security and accountability for better participation in the Government-Industry Data Exchange Program (GIDEP) and for following SAE AS5553 recommendations on Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition.
- Tamper-proof SAP Integrated Business Planning (IBP) deployments, securing inputs of key data used for supply planning and inventory optimization.
- Reduce insurance claims risk and improve regulatory compliance by providing an irrefutable, iron-clad record of all maintenance performed on an airplane and the provenance of all parts on that plane.
- Instantly verify the identity, experience, and training of flight and maintenance personnel—even when those personnel change companies.
- Track the entire lifecycle of parts—even when parts have been swapped between airplanes or airlines—allowing the original provenance, transfers, and entire maintenance cycle of a single component to be reviewed in its entirety.
- Optimize maintenance by allowing OEMs, airlines, and MRO teams to analyze how specific parts perform over time and under different conditions through a secure, shared digital ledger of flight events and potential and scheduled maintenance.

Automotive

Automotive industry leaders are looking for new ways to combat fraud, comply with new industry and government requirements, and drive new innovations such as driverless cars and intelligent digital displays. They need the ability to swiftly capture and verify digital moments from the time the car is being manufactured, throughout the supply chain, and even after the car is sold. Cryptowerk's Automotive industry solution verifies digital moments at scale, helping auto companies around the globe solve these complex challenges.

- Secure and validate automotive supply chain processes by attaching digital tokens to parts and digitally notarize supply chain data with a digital seal, creating digital "fingerprints" that can be compared to the original data to verify authenticity between all parties in the chain, improving information transfer and logistics coordination, detecting counterfeit items, and reducing leakage and errors in ordering and inventory cataloging.

- Verify the integrity and quality of the code automotive manufacturers use in self-driving and other integrated software by providing a tamper-proof record of applications and code at any moment in time, improving security, trust and transparency throughout the software development and distribution process.
- Capture and verify digital moments from the time a vehicle is being manufactured, sold, maintained, and operated to combat fraud and comply with industry and government requirements.
- Seal sensor data, vehicle operation data, and other data collected from real-time maintenance, manual and self-driving operations, and accidents for audit and litigation situations.

Pharmaceuticals

Pharma companies are being challenged to prove their products are authentic, safe and reliable, while reducing supply chain costs.

- More easily and securely comply with regulations like DSCSA and EU regulations by enabling pharma companies to more securely attach metadata to transactions, enhancing their ability to communicate information up and down the supply chain.
- Reduce leakage, counterfeiting, and theft by enhancing track-and-trace solutions with an unalterable digital record of each item's movement through the manufacturing and logistics chain.

Two leading pharmaceutical companies successfully ran a fast-track POC with SAP and Cryptowerk. The goal: to much more efficiently detect counterfeits and irrefutably document compliance at scale. The POC also demonstrates its applicability for ultimately tracking and tracing billions of items throughout their supply chains. SAP integrated Cryptowerk's Enterprise Blockchain Enablement Kit with the SAP Advanced Track and Trace solution, including its mobile component, to deliver a solution to the problem. Working closely with its pharmaceutical customers, SAP in partnership with Cryptowerk was able to rapidly deliver a solution in just a few weeks with the following benefits:

- Full compliance with DSCSA sellable returns verifications
- Instant verification of the authenticity of returned items
- No replication of manufacturer data required for wholesaler source of truth provided to all parties, including regulators
- Minimum complexity, maximum security
- Scalable to consumer scanning at point of dispense

Software

Since data integrity and fraud prevention are so important to build into software products, providers of applications like supply chain, provenance, systems operations, and other applications need to be able to both provide an extra data integrity layer to their applications and validate the code they use.

- Provide a tamper-proof record of third-party and open code used, and models, applications and code developed at any moment in time, improving security, trust and transparency throughout the software development and distribution process.

- Enable data authenticity checks of file systems and databases
- Turbo-charge any application requiring data integrity in days – not weeks -- with the power of blockchain sealing without requiring specialized blockchain expertise.

Utilities

The utility industry is changing faster than ever before. Emerging technologies and trends are creating a network in which electricity can flow among a wide variety of points, even from consumers. Utilities must comply with new regulatory requirements, continue to improve operational efficiency and look for new high-margin revenue opportunities. Cryptowerk's blockchain-enabled utility solutions address these opportunities securely and efficiently.

- Prevent fraud and manipulation of data from oil field exploration, production, and other operations.
- Register and validate customer usage data from SmartMeters and other sensors.
- Seal and validate data from green energy producing assets, such as wind and solar farms, for insurance, bond issuance, credits, and green certification purposes.

Conclusion

Blockchains and other distributed ledger technologies are highly useful in fraud prevention and digital transformation efforts, especially in highly regulated industries. They create a tamper-evident transaction record that maintains and records data in a way that allows multiple stakeholders to share access to the same data and information confidently and securely.

Blockchain is useful for sealing data from business processes involving multiple parties where there are multiple writers, many transaction interactions, and significant disintermediation, such as a supply chain. Although attempting to build a blockchain deployment from scratch can often be expensive and complicated, Cryptowerk Seal makes blockchain-based digital transformation frictionless.

Cryptowerk Seal enables true interoperability. It works with existing applications and processes—meaning organizations don't need to change your existing infrastructure and systems. You can add the benefits of blockchain today with no downtime. And organization can switch blockchains with minimal effort and no data loss.

Cryptowerk

SEAL YOUR DATA

About Cryptowerk

Cryptowerk envisions a future where trust is built into every product, process and transaction. To make that vision a reality, Cryptowerk powers solutions that make it possible for organizations to seal their data at massive scale, creating a tamper-evident chain of custody of your digital moments. Cryptowerk solutions help organizations in multiple industries drive digital transformation, including aerospace and defense, automotive, pharmaceuticals, software and utilities. Headquartered in Silicon Valley, Cryptowerk was founded by former SAP executives, experts in cryptography, and seasoned enterprise software professionals.

CRYPTOWERK
585 BROADWAY ST.
REDWOOD CITY, CA 94063
WWW.CRYPTOWERK.COM

Cryptowerk