Acronis Cyber Notary: a new way to prove data authenticity via Blockchain

Acronis Cyber Notary™ is a new, innovative service based on blockchain technology. But before we move into that, let's define what a blockchain is. Some know it in relation to Bitcoin but it can be used in a much wider set of scenarios, including data protection. Many industries have already started to use blockchain or are actively looking into its applications. For example, cloud storage, art and ownership, anti-counterfeiting, governance, Internet of Things, and digital identity.

BUT WHAT IS BLOCKCHAIN, ACTUALLY?

A blockchain is a distributed database that maintains a continuously growing list of records that are secured from tampering and revision. It consists of data-structure blocks that may contain data or programs, with each block holding batches of individual transactions, and the results of any blockchain executables. Every node in a decentralized system has a copy of the blockchain.

No centralized "official" copy exists and no user is "trusted" more than any other. The blockchain resides across a network of computers (nodes). Whenever new transactions occur, the blockchain is authenticated across this distributed network, before the transaction can be included as the next block on the chain.

So the consensus of nodes is required to add the block into the blockchain. The blockchain creates trust because a complete copy of the chain, which shows every transaction, is held by the entire network. If someone attempts to cheat the system, they can be easily identified.

ACRONIS ASIGN

Acronis Cyber Notary is actually the foudation for another service within our consumer product line called Acronis ASign. It is an easy-to-use web interface that allows you to digitally sign documents without having to print, sign, and scan them.

It supports sending documents to multiple signatories at the same time which results in a PDF file with all the details on the file and audit trail including timestamps. The hash of this PDF is computed and goes to Acronis Cyber Notary, creating a secure trail of the signatures in the blockchain.

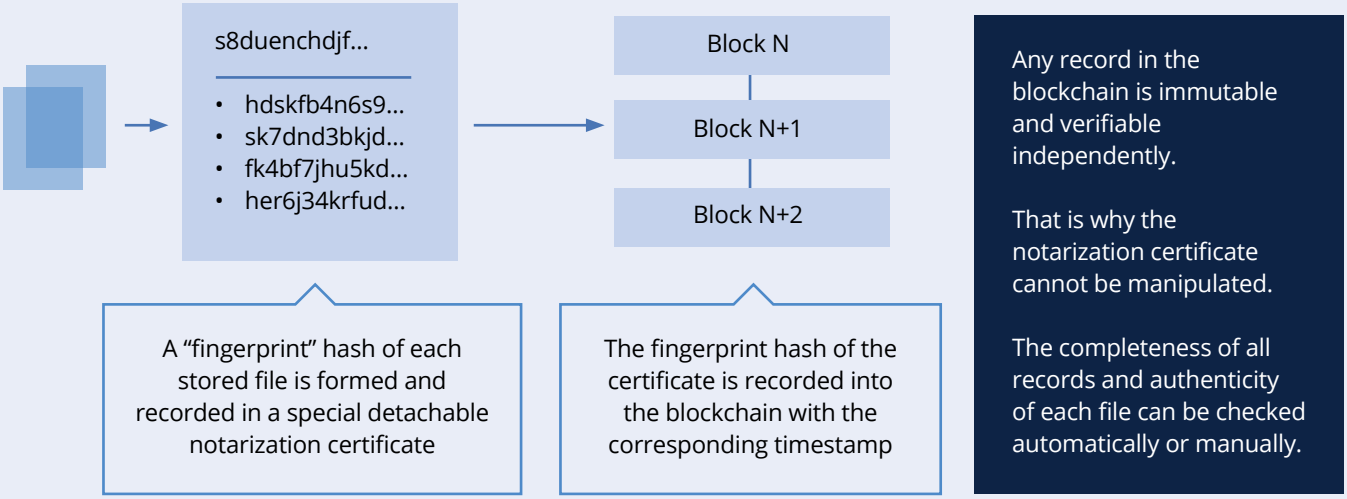
At the moment you can only sign files stored in your Acronis Cyber Cloud Storage backup. This is done for security and authenticity reasons.

To summarize, a blockchain is an append-only database with transaction order and the following data protection properties:

- Immutable data storage
- Secure timestamping
- Public audit

ACRONIS CYBER NOTARY SERVICE: HOW DOES IT WORK?

Acronis Cyber Notary is the universal solution for timestamping and fingerprinting any data objects and streams. It is impractical to store big chunks of data in a blockchain, which is why Acronis products will only send file/backup hashes to the Acronis Cyber Notary service.



YOUR GUARANTEE THAT FILES ARE STILL EXACTLY THE SAME

Acronis Cyber Notary protects any data from tampering and deletion because data immutability is algorithmically protected by blockchain technology and can be verified independently.

A carefully designed service architecture ensures the high throughput necessary for a wide range of industrial solutions. Because of this, Acronis Cyber Notary can be installed as a proxy on any existing data stream and requires no changes in the existing processes or infrastructure. More than that, it can be deployed either in the cloud or on-premises.

The Acronis Cyber Notary service then calculates a single hash by using the received file hashes and then sends the new hash to a blockchain-based computing platform. Acronis users then have a choice: either use the well known public blockchain Ethereum or use the permissioned Zero-Trust Consortium ledger.

WHAT IS THE ZERO-TRUST CONSORTIUM (ZTC)

Acronis was a founding member of ZTC at the end of 2018 along with vChain Inc, Chainstack Inc, and others. The Zero-Trust Consortium is an independent, community-led membership group whose purpose is to support the usage of a fast, private permissioned blockchain, free of per-transaction fees, for software vendors, by software vendors. The Zero-Trust Consortium could acquire over 30 members within the first 14 months of its existence, to run blockchain nodes distributed across the globe.

The current issue in the blockchain industry is that existing blockchains are too expensive (on a per-transaction fee basis) and too slow to allow software vendors to create zero-trust solutions that use such public blockchains. At the same time, having a distributed, uncontrolled, fast (i.e. near real-time) and free permissioned blockchain has the potential to disrupt today's incumbent software solutions with new approaches where the customers and users do not need to extend trust based on certificates, public/private keys schemes, or reputation only.

Pioneering the approach, the Zero-Trust Consortium operates a permissioned blockchain that can be publicly read. This means capturing the best of both worlds: no transaction costs, high throughput, and low latency while being open to public scrutiny. The Zero-Trust Consortium serves as the host and center of administrative, off-chain governance and user support for the Zero-Trust Permissioned Blockchain environment. This includes the open-source software developed as part of the Zero-Trust project and, when appropriate and feasible, software developed by additional follow-on research and development projects, and members of the Zero-Trust user community.

INNOVATIVE TECHNOLOGY

The Zero-Trust Consortium does not use an in-house developed blockchain protocol but uses an Ethereum-based blockchain building upon the Parity project. Parity has been built for mission-critical use by service providers and exchanges in need of fast synchronization and maximum uptime. Parity Ethereum provides the core infrastructure essential for speedy and reliable services.

This allows users to achieve much better transaction speeds compared to other blockchain ledgers, as can be seen in the table below:

	Bitcoin	Ethereum	ZTC Blockchain
Throughput	~400 TX/ min	~800 TX/ min	~60,000 TX/min
Confirmation time	Up to hours	Minutes	Instant
Block creation time	~10 min	~15 sec	5 sec

The Zero-Trust Consortium, for instance, currently uses the Aura consensus algorithm, which iterates over the list of authority nodes, the ValidatorSet. At each turn, there is one leading authority node that will fetch all transactions broadcasted, verify them, and broadcast them in a newly proposed block. Once 51% of the authorities have validated this proposed block it will be written to the blockchain. Additionally, most blockchain ledgers charge businesses a transaction price for each use. The Zero-Trust Consortium does not. Based on customer preference in terms of performance and price, they can choose between two blockchain validation options in their Acronis Cyber Notary enabled product.

NOTARY CERTIFICATE

After the hash is sent to the ledger of choice, the Acronis Cyber Notary service provides a certificate and technical details about how to verify the certificate to the user of Acronis Cyber Cloud.

Then, whenever that file is reflected in an Acronis products user interface, the file is shown as notarized by Acronis. This ensures that a user can be assured that the file being stored is identical, on a bit-by-bit basis, with what was backed up and stored in the cloud—whether it was a few hours ago or a few months ago. Acronis Cyber Notary technology can protect any data in any industry.

Common use cases include:

- Proof of document ownership, including real-life and digital-work attribution. It works very well for protection of intellectual property and, for example, certifying who created, accessed, or modified a document.
- Certification that a document existed.
- Time-stamping is critical for digital contracts, research data, medical records, evidence, petitions, purchase orders, etc. Users can seamlessly and irrefutably prove the exact moment data in a document existed, for legal, compliance, and business purposes. Users also can create a registry of digitized copies of paper documents, proving their existence at a certain time.

- Proof of Integrity. For example, the ability to demonstrate that data has not been tampered with.
- Facilitation of sales and trading of digital assets or real objects, and digital rights management.
- Users can digitally trace the document and find information about the file/document movement.
- Proof of the product's authenticity. It goes even further when we talk about usage for Acronis Cyber Notary and blockchain for business: chain-of-evidence for court documents, police video or security camera footage, long-term archiving that could be subject to IT audits, and 'consortium' data storage where multiple entities or individuals need to securely store and exchange massive amounts of data and information.

If we are talking about an individual user's documents, these are examples of what they may need to sign and notarize:

- Rental/lease agreements
- Sales contracts or asset purchase agreements
- Loan agreements
- Permission slips
- Financial documents
- Insurance documents
- Liability waivers
- Healthcare documents
- Research papers
- Certificates of product authenticity
- Nondisclosure agreements
- Offer letters
- Confidentiality agreements
- Independent contractor agreements

A few examples of Acronis Cyber Notary usage:

- **Sally** is a composer and she has been skeptical about publishing her work on the internet. Using blockchain certification as a tool for copyright protection can change her mind. Sally can create a protected backup of a folder that contains her work. Once the backup is completed, she can obtain a registration certificate with cryptographic evidence that protects her copyright. The record is permanent and immutable. Sally can prove that her piece of art existed at a certain time in the past, was authored by her, and claim her ownership for it.
- **Bill** is a lawyer, and he needs to prove to a judge and jury that a file in his possession can be proven to have been in existence on a certain date/time. Using Acronis Cyber Notary, Bill can tie the file in his possession to data on an Ethereum blockchain, which mathematically proves the existence of the file.
- **Emily** bought a certified diamond and notarized the certificate and the invoice by using Acronis Cyber Notary. After a period of time, she decides to sell the diamond. A buyer can use Acronis Cyber Notary to verify the initial certificate. Once a buyer is confident about the original certificate, he can then compare certification with a stone by using a third-party's professional evaluation.
- **Roger** has an archive of paid bills that he keeps in electronic form. He keeps all bills in the notarized backup. One day, Roger receives an overdue notice for a bill that he paid two years ago. The record in blockchain is permanent and immutable. Roger can prove that this bill was sent by mistake.

As you can see, in all cases using Acronis Cyber Notary technology, you compare a "new" document with the original document's certificate or just present the original certificate to prove your document timestamp and authenticity.

Acronis

Learn more at
www.acronis.com