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

Acronis Notary™ is a new, innovative service based on blockchain technology. But before we move into that, let's define what a blockchain is. It can be known to some due to its usage in Bitcoin currency, but it's a lot more than just bitcoin technology and it can be used in a much wider set of scenarios, such as for data protection. Many industries have already started to use blockchain or are actively looking into it. 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.

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

- Immutable data storage
- Secure time-stamping
- Public audit

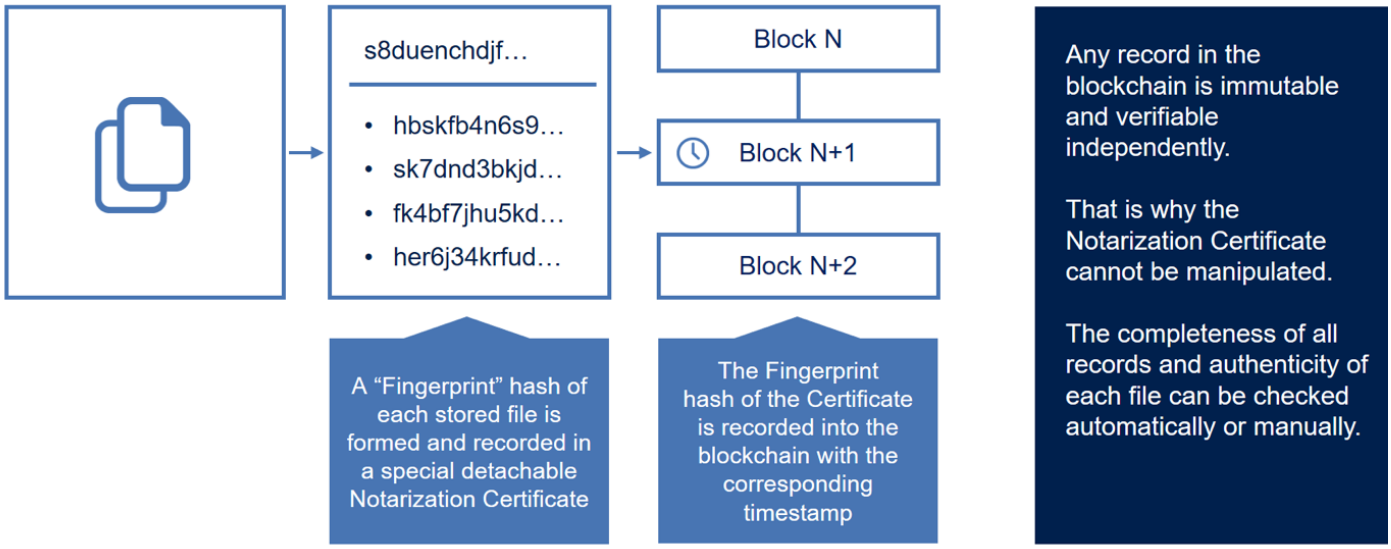
Acronis Notary service: How does it work?

Acronis 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 Notary service. The Notary service then calculates a single hash by using the received file hashes, and then sends the new hash to the Etherium (Blockchain-based distributed computing platform). The Notary service provides a certificate and

ACRONIS ESIGN

Notary is actually a foundation for another Acronis service within consumer product line called eSign. It is an easy to use web interface which 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 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 Notary, creating a secure trail of the signatures in the blockchain.

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



YOUR GUARANTEE THAT FILES ARE STILL

Acronis Notary protects any data from tampering and deleting because data immutability is algorithmically protected by the 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 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.

technical details about how to verify the certificate to the user of Acronis Backup Cloud. Then, whenever that file is reflected in an Acronis True Image user interface, the file is shown as notarized by Acronis. This ensures that a user can be assured that the file that is being stored is in fact 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 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 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 agreement
- Permission slips

- Financial documents
- Insurance documents
- Liability waiver
- Healthcare documents
- Research papers
- Certificate of product authenticity
- Nondisclosure agreements
- Offer letters
- Confidentiality agreements
- Independent contractor agreements

Let's look at few easy examples of Acronis 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 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 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 Notary. After a period of time, she decides to sell the diamond. A buyer can use Acronis 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 Notary technology, you compare a "new" document with the original document's certificate or just present original certificate to prove your document timestamp and authenticity.

Acronis

For additional information, please visit **www.acronis.com**