Ensuring Data Authenticity

When handling sensitive data, such as financial transactions, we need to ensure the data is one-hundred percent authentic. That is, we need to make sure that the data was produced and updated only by authorized persons or systems, that it has not been altered afterward, and that we can fully audit what happened to it.

Traditional Approaches

Traditionally, sensitive data such as financial transactions is protected through a series of measures such as user authentication and access controls to ensure only legitimate users and systems can read and update the data, performing regular backups and archives to make copies of that data at regular intervals, and signing data with cryptographic signatures to prove its authenticity. Many advanced systems will also implement journals to record activity on separate storage for analysis and safekeeping. We can also gain confidence that data is valid and was not altered after the fact by comparing current data with backups and archives, by verifying digital signatures, and by checking journals for suspicious activity. These processes are complex to set up and operate. Blockchain may be an easier alternative that combines ledgers with digital signatures and some form of proof-of-work to certify data is authentic, but it can often be extremely power-hungry, and lead to significantly more storage and processing as the data in the ledger normally needs to be replicated and organized in external databases to be of practical use.

COSNIM automatically records all data activity providing full data certification and auditing tools directly and securely from live storage.

COSNIM Technology

Due to COSNIM's unique design, all data creation, updates, and deletions are automatically recorded, tracked, and sealed by Time-Travel with full historical access, without resorting to backups, copies, journals, or ledgers as traditional technologies. This unique behaviour, when combined with other COSNIM features, can form an extremely powerful data certification and auditing tool, as described below.

Immutability

All COSNIM capsules can be stored directly on immutable storage, even for live storage, which ensures that data cannot be physically altered after it has been produced. This not only protects it against ransomware but also from all unauthorized alterations. Capsule immutability does not, however, mean

that data itself cannot be updated; it simply means that updates will have to be recorded in other capsules, fully tracked by Time-Travel. As long as capsules remain in immutable storage, there is a physical guarantee that past data cannot be altered. Contrary to many other storage technologies, capsules stored on immutable storage continue to be fully active members of data storage and participate in all activities, even if some of their contents have since been updated.

Audits

Because Time-Travel records absolutely all data modifications, it implicitly forms a security audit. That is, every single change made to data is automatically retraceable through Time-Travel and is readily available directly through the filesystem. Audit information contains everything an auditor might be interested in, including precise dates and times when the activity occurred, data attributes, which data fragments were altered, along with direct access to both before and after images of each file and data fragment. When combined with immutable storage, signatures, or hashes, COSNIM audits become extremely reliable proof of all update activity, without the use of separate journals or ledgers.

> Automatic digital signatures, hashes and immutable storage provide additional proof of the data and related audit information.

Digital Signatures

Data produced by a user may also be signed with the user's unique private key to prove who has created, updated, or deleted precise pieces of data. These signatures are based on cryptographic hashes computed from the data that was modified and are stored directly in the Continuum and capsules alongside the data and metadata, making them readily accessible. Signatures can be checked automatically as data is read back or verified separately by making a request to COSNIM. They can be used to further ensure that data has not been altered, in addition to or in lieu of immutable storage.

Signature Cascades

Because of the way signatures are computed and data is organized in COSNIM, digital signatures also indirectly sign Time-Travel information that is part of the Continuum's mesh. When subsequent data is updated and signed, this indirectly also signs other related data at the same time. With many signatures, the entire Continuum ends up as a large web of inter-related signatures, driven by Time-Travel, de facto signing the state of the entire Continuum. When many different user signatures are in use, a bad actor that would attempt to nefariously alter past data would not only need to re-sign the altered data with the private key of the user that produced the original data, but would also need the private keys of all other users that had indirectly signed the Continuum in cascades afterward. This cascade of different

signatures can provide solid proof of the data's authenticity, without the complexity and resources of traditional ledgers or proof-of-work authentication solutions.

Hashes and Continuum Authentication

The same way signatures can sign data in cascades to authenticate each other, so can hashes. Cryptographic hashes are much smaller and faster to compute than signatures, yet, still fully authenticate data, albeit without the proof of who produced it. By configuring automatic hashes on some key (or all) data elements, hashes end up authenticating each other in cascades, and eventually, the entire Continuum and all its Time-Travel points, making past alterations impossible to hide.

As a result, a single hash can de facto authenticate the entire Continuum and all Time-Travel points that previously existed at any given time. Extracted hashes can be stored in a safe place, given to a third party for safekeeping, or simply disclosed publicly. They can later be used to re-verify that the data that is being read has not been altered. Contrary to chained hashes, COSNIM's hash cascades do not need to re-read all of the data and will continue to authenticate reliably even after updates and deletions.

COSNIM certifies current and past archival data with extreme simplicity, and no extra copies.

Archival

Data often needs to be archived for regulatory purposes. This is normally done by making a special copy of the data and saving it in separate, secure storage. In COSNIM, with Time-Travel, data can be archived and locked automatically in place simply by protecting it from storage reclaims. This in effect preserves the data as a fully secure archive without having separate physical copies. Moreover, when combined with digital signatures, cryptographic hashes, or immutable storage, archived data can also be fully certified as authentic. Of course, since the archive is still part of the Continuum, it's always readily available, directly from the filesystem, as if it were live data, independently of where capsules are physically stored.

With Time-Travel and fully integrated services, COSNIM provides advanced data authentication, auditing, and archiving capabilities, right from within the filesystem.

Https://www.cosnim.com
info@cosnim.com
+1 888 212-3527