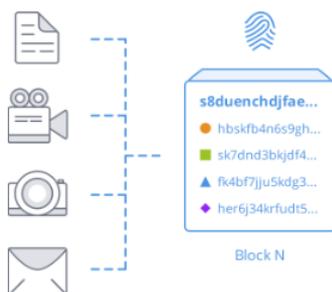


Acronis Notary

El primer producto de copia de seguridad para consumidores cuyo objetivo es usar la tecnología de la cadena de bloques para probar que un archivo es auténtico y que no ha cambiado desde que se añadió a la copia de seguridad.

¿Qué es la tecnología de la cadena de bloques?

Puede que haya escuchado hablar de blockchain en el contexto de la divisa digital llamada «bitcoin». Más allá del revuelo generado por el bitcoin, no es en absoluto la única aplicación útil de la tecnología de la cadena de bloques. Sin embargo, para comprender el resto de aplicaciones, se debe entender la cadena de bloques. Sencillamente, es una base de datos distribuida que conserva una lista, o cadena, de registros de transacciones de datos que crece sin cesar. Cada parte de su sistema descentralizado cuenta con una copia de la cadena de registros; no existe ninguna copia «oficial». Así, la información está protegida para que no se pueda manipular ni alterar.



«Huellas digitales» de los datos

Acronis Notary calcula una función hash criptográfica de la «huella digital» de cada archivo, única para cada uno. Este algoritmo de hash produce el mismo resultado si se le ofrece el mismo archivo de entrada siempre, independientemente de las circunstancias. Cualquier cambio, por pequeño que sea, en el archivo de entrada tiene como consecuencia una huella digital muy diferente. El algoritmo de hash está diseñado para trabajar en una sola dirección, lo que hace imposible determinar los archivos de entrada originales de los de salida.

Anclaje de los datos en la cadena de bloques

Tenga en cuenta que la cadena de bloques es un libro mayor que solo se puede adjuntar con un pedido de transacción que se distribuye por muchas entidades, cada una se queda con una copia idéntica de este. Cada registro del libro mayor tiene una marca de tiempo, es inalterable y se puede verificar de forma independiente.

Una función hash de toda la estructura que contenga las huellas digitales de los archivos se registra en la cadena de bloques. La autenticidad de esos archivos la puede confirmar de forma independiente cada entidad (aunque alguna no trabaje con Acronis) que tenga acceso a la cadena de bloques.

¿Cómo se puede usar Acronis Notary y por qué esto es tan importante?

Cuando hace una copia de seguridad de sus datos en discos locales o en la nube, espera correctamente que la solución de copia de seguridad actúe de forma fiel con esos archivos. La tecnología de Acronis Notary puede añadir un nivel de confianza a la autenticidad de sus datos. En el futuro, puede que quiera simplemente asegurarse de que un archivo no ha cambiado. O bien, puede que tenga, o alguien le ofrezca, un archivo y necesite validar si es auténtico, además de si no es diferente del de la copia de seguridad. Entre los casos prácticos se incluyen las copias de registros personales y patrimoniales, cadenas de pruebas para documentos exigidos por los tribunales y archivos a largo plazo que pueden ser objeto de varias auditorías legales y fiscales. En esta página, más adelante, encontrará otros ejemplos.



Acronis Notary crea un certificado para cada archivo certificado por notario. Este certificado conecta las funciones del archivo único con el registro permanente en la cadena de bloques. Esto le permite comprobar su autenticidad. Los certificados de Acronis Notary incluyen toda la información necesaria para verificar datos protegidos con el objetivo de que se puedan comprobar de manera independiente. Esta comprobación la puede realizar una persona o usar un equipo, e incluso la puede llevar a cabo un tercero, siempre que tenga acceso a la cadena de bloques.

Acronis Notary crea un certificado para cada archivo certificado por notario. Este certificado conecta las funciones del archivo único con el registro permanente en la cadena de bloques. Esto le permite comprobar su autenticidad. Los certificados de Acronis Notary incluyen toda la información necesaria para verificar datos protegidos con el objetivo de que se puedan comprobar de manera independiente. Esta comprobación la puede realizar una persona o usar un equipo, e incluso la puede llevar a cabo un tercero, siempre que tenga acceso a la cadena de bloques.