WHITE PAPER - KATENAE

“Blockchain de negocio legitimada notarialmente”

INTRODUCCIÓN

La tecnología blockchain es esencialmente una base de datos distribuida entre diversos miembros donde los registros o transacciones que ejecutan los participantes son compartidos de manera automática y pública, de tal manera que estos son verificados y consensuados por la mayoría de participantes de la red.

Bajo esta premisa, Katenae ha desarrollado un software que permite la verificación de objetos digitales (fotografía, documentos, archivos .pdf, fichero de texto, etc.) los cuales son registrados en una red blockchain privada, y cuyo valor principal es que la información contenida en dicha red no puede ser modificada o eliminada por sus participantes.

La Blockchain privada de Katenae contiene un registro cierto y verificable de cada una de las transacciones realizadas, convertidas en los denominados “Itemblocks”. La función principal de la tecnología blockchain de Katenae es establecer un sistema de registro, permitiendo a sus usuarios obtener un certificado de trazabilidad y no alteración.

Este documento pretende describir la tecnología blockchain desarrollada por Katenae, sus aplicaciones, así como las oportunidades de negocio que puede aportar a su compañía.

ÍNDICE

Katenae

El servicio que ofrece Katenae permite a las empresas certificar la autenticidad de los documentos digitales (u objetos digitales) que tu empresa genera, estableciendo en el momento en el que se han creado (sello de tiempo) y asegurando que no han sido manipulados o alterados.

Esta plataforma de registro y evidencia en blockchain proporciona a nuestros clientes una forma segura y fiable de verificar la existencia de cualquier documento con una fecha determinada, con el fin de probar su autenticidad, así como de crear una evidencia del proceso que pueda ser utilizada en caso de disputa.

La plataforma ofrece una serie de ventajas, como integridad, disponibilidad, confidencialidad y escalabilidad de los datos.

El reto a la hora de implementar una solución de blockchain para la conservación de pruebas radica en que, mientras que blockchain pública como Bitcoin o Ethereum están diseñados para ser un sistema abierto y transparente, los requisitos para la conservación de pruebas de todos nuestros clientes requieren los más estrictos controles de confidencialidad e integridad.

Para resolver este problema, Katenae ha implementado una solución basada en una blockchain privada, de esta forma, Katenae permite obtener todas las ventajas de blockchain (seguridad, fiabilidad, inmutabilidad) sin sacrificar la confidencialidad de la información.

¿Qué es una blockchain privada?

Una blockchain privada está gestionada por una entidad centralizada, en este caso Katenae, y su uso está restringido a aquellos a los que se les ha concedido acceso. En otras palabras, una blockchain privada es un ecosistema cerrado que no está abierto a la participación pública. Los participantes deben obtener primero la autorización de la autoridad centralizada antes de poder utilizar la blockchain privada.

¿Cuáles son las principales características de una blockchain privada?

- Acceso: Las blockchains privadas están centralizadas, lo que significa que los usuarios necesitan permiso para acceder a la blockchain (aunque los miembros de la cadena pueden negociar el nivel de descentralización que puede tener la red).
- Identidad: Los usuarios de la blockchain privada no pueden comprobar los registros de la cadena, ni autorizarlos hasta que no se les conceda el acceso por parte de la entidad central. Esto significa que cada participante en la cadena de bloques puede ser fácilmente identificado.

- Velocidad: Las transacciones en las blockchains privadas son mucho más rápidas que en las blockchains públicas debido a su naturaleza centralizada.
- Coste: Dado que el consenso o aceptación del bloque es dado por la autoridad central, no es necesario compensar a los participantes terceros que realizan esa labor, como son los mineros en redes públicas.
- Gobernanza: La autoridad central de la blockchain privada establece las reglas que deben seguir los usuarios de la blockchain.
- Seguridad: Una blockchain privada es más vulnerable a los hackeos porque está centralizada y puede ser objeto de ataques más fácilmente. Una cadena de bloques privada con una única autoridad centralizada también crea un único punto de fallo.

Notarización

Como hemos indicado anteriormente, existen dos características que pueden afectar la integridad y la seguridad de una red privada, como son el acceso restringido y la centralización del sistema.

En el primer ejemplo, si una base de datos de blockchain es completamente opaca para los clientes (es decir, no tienen acceso a los datos del blockchain), el aspecto de la seguridad de la tecnología disminuye, dado que no existen numerosas figuras que puedan determinar si ha existido un problema en el consenso (ya sea por factor humano, o por el propio incorrecto funcionamiento del blockchain privado). En cuanto a la centralización, en ausencia de otros usuarios, en caso de un ataque que afecte al nodo principal, la propia red podría verse afectada en su totalidad.

Con el objetivo de garantizar la inmutabilidad de los registros y evitar que un ataque pudiese afectar a la integridad de los mismos, Katenae ha conseguido incluir satisfactoria entre sus servicios el ser la primera Blockchain legitimada notarialmente bajo acta notarial.

Si nos atenemos a lo que indica el Reglamento Notarial, un acta notarial es un documento público que tiene como objetivo constatar los hechos o percepciones que se presenten a un notario, siempre que por sus actos no puedan calificarse de actos o contratos.

Por tanto, un acta notarial es el reflejo documental y fehaciente solicitado por Katenae, sobre los hash, o itemblocks, que se han incluido en la blockchain privada creada en a través de nuestra plataforma durante una periodicidad determinada.

La notarización de dicha cadena permite verificar de forma segura el hash generado, el cual se encuentra asociado a los objetos digitales que los usuarios han podido certificar a través de Katenae. De esta manera, en caso de disputa, los usuarios cuentan con el acta notarial que verifique la integridad, autenticidad, propiedad y tiempo de creación de los archivos que han sido previamente notarizados.

El valor de un acta notarial reside en que prueba de manera incontestable el hecho que constituye su objeto, sin que sea discutible ni siquiera en sede judicial, salvo querella de falsedad. El acta notarial permite constituir pruebas que podrán ser utilizadas en el ámbito judicial, administrativo o privado.

Katenae pone a disposición de sus clientes las actas notariales correspondientes a los registros realizados en la blockchain para su uso en caso de disputa.

Características de la red

A continuación enumeramos un conjunto de características básicas que se encuentran presentes en la red privada desarrollada por Katenae.

1. Inmutabilidad: una vez que una transacción se ha consignado en la cadena de bloques, no puede ser modificada ni eliminada. Esto, por extensión, requiere que todas las transacciones sean totalmente verificables mediante técnicas criptográficas.

2. Privacidad: las transacciones deben poder ocultarse a todos, excepto a las partes involucradas.

3. Escalabilidad: capaz de mantener un alto rendimiento a medida que aumenta el número de nodos, hasta cientos, sino miles, de nodos.

4. Identificación criptográfica: la creación del hash a partir del objeto digital que se quiere autenticar se realiza utilizando tecnología criptográfica, de tal manera que la transacción pueda ser almacenable y reproducible de manera segura.

Tipos de nodos

Una red blockchain está compuesta de diversos tipos de nodos, los cuales realizan diferentes funciones basadas en los requisitos de la blockchain, algunas de las tareas básicas que puede realizar son:

- Facilitar la comunicación: Los nodos permiten a los usuarios acceder a la blockchain e interactuar con ella con el objeto de ver las transacciones que se producen en la red, ver los detalles de la transacción y verificar los registros.

- Aceptar o rechazar una transacción: Los nodos se utilizan para añadir nuevos bloques a la red y sincronizar sus datos, manteniendo la copia de la cadena, en el caso del nodo full. Para aprobar finalmente que un bloque se añade a la cadena, el nodo full debe lograr el consenso.
- Procesar una transacción: Una vez aprobada, la transacción es procesada para que sea incluida en la cadena.
- Almacenar bloques: Los nodos mantienen la red y ayudan a hacerla crecer. Cada bloque de datos se añade al almacenamiento de un nodo.

Los nodos de la red blockchain de Katenae se clasifican en función de sus funciones:

Nodo completo

El trabajo principal del nodo completo de Katenea es confirmar cada lote de transacciones de la red (o bloques) y la ejecución del blockchain.

Los nodos completos son responsables de mantener todos los registros de transacciones en la red de blockchain. Se consideran los servidores de la blockchain donde se almacenan y mantienen los datos.

Nodos ligero

Katenae pone a disposición de sus clientes la posibilidad de mantener un nodo ligero que permite una copia de la cadena actualizada en todo momento para su verificación por parte del poseedor del nodo.

Criptografía

La criptografía es el método por el cual a través de desarrollos técnicos y protocolos se evita que un tercero acceda y tenga conocimiento de los datos privados durante un proceso de comunicación.

En blockchain, la criptografía puede ser fundamentalmente de tres formas diferentes, simétrica, asimétrica o mediante funciones hash.

Katenae mantiene una tecnología de encriptación a través de técnicas hash, por las cuales se genera un valor de una longitud fija (SHA-512) a partir del texto plano del objeto digital.

¿Cómo funciona el “hasheo” del objeto digital?

Primeramente, debemos hacer referencia al carácter inalterable y seguro de la blockchain privada de Katenae, derivado de las técnicas de encriptación empleadas por esta. En este sentido, debe señalarse que en nuestra red, la información se encuentra escrita en “bloques” conectados a su predecesor en la cadena a través de un código de identificación hash, que en nuestro sistema se denomina “itemblock”.

Así, dichos bloques incluyen no solo su itemblock sino también el de su predecesor, quedando unidos entre sí en razón de dicho elemento identificador. La alteración fraudulenta de la información contenida en un bloque implicaría una modificación del itemblock existente, lo que resultaría en una modificación sencillamente advertida por Katenae o cualquiera de sus usuarios, los cuales podrán denunciar su modificación.

El hecho de que tanto los usuarios de la red, como cualquier tercero ajeno a la misma tenga acceso para verificar una transacción, complica enormemente la eliminación o perturbación de tales datos.

En la red privada de Katenae, el usuario debe seleccionar un objeto digital (documento, video, archivo, etc.) para su encriptación. Una vez subido, este archivo es procesado vía API para obtener el SHA-512, que es una conversión en un solo sentido del archivo a una cadena de valores aleatorios de 64 bytes o hash.

Una vez generado, el sistema posteriormente realiza de manera automática la encriptación SHA-256 de los metadatos de la transacción, es decir, la fecha y hora de subida, el usuario que lo realiza y la IP desde donde se está realizando, así como el stack o proyecto, generado un hash de 32 bytes.

La unión de estos dos hashes determinará el “hash completo” o también denominado “itemblock”. Por tanto, todo objeto incluido en el sistema pasará una doble encriptación de los datos relativos a la transacción, utilizando sistemas automáticos para ellos.

De este modo, el itemblock queda registrado de forma permanente en la blockchain privada de Katenae y vinculado a un lugar exacto en la cadena.

SHA-512 + SHA256 = Itemblock

Es necesario indicar que cada bloque puede contener hasta 50 itemblocks registrados en la red de Katenae. Los bloques se componen del código del nodo, el número del bloque, la fecha de apertura y cierre, el hash del bloque anterior, el hash del cierre del bloque

Verificación

En caso de que un usuario desease realizar una verificación sobre el objeto digital, la cadena de bloques generada o el certificado, Katenae a través de su página web https://katenae.com pone a disposición de cualquiera la posibilidad de realizar las comprobaciones pertinentes.

De esta manera, tanto el usuario de Katenae, como sus clientes o proveedores, podrán tener acceso de manera online y en tiempo real sobre el registro realizado, o la integridad de la blockchain privada.

Mylegalinbox, despacho de abogados especializado en nuevas tecnologías y blockchain, ha asistido a Katenae en la preparación y asesoramiento legal de este White Paper. En caso de consulta, no dude en ponerse en contacto con nosotros a través de la dirección de correo electrónico info@mylegalinbox.com