(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 890 933**

(51) Int. CI.:

H04L 29/06 (2006.01)
H04L 9/08 (2006.01)
H04L 9/32 (2006.01)
G06F 21/10 (2013.01)
G06F 21/16 (2013.01)
G06F 21/62 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **03.12.2018 E 18382884 (7)**

(97) Fecha y número de publicación de la concesión europea: **23.06.2021 EP 3664399**

(54) Título: **Procedimiento implementado por ordenador, sistema y programas de ordenador para la gestión y la conservación de ficheros digitales en licencias digitales**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.01.2022

(73) Titular/es:

BILDOSUND SL (100.0%)
C/ de Ganduxer, 52, 6 B
08021 Barcelona, ES

(72) Inventor/es:

NORDSTRÖM, VIKTOR;
MUÑOZ SOLÀ, VÍCTOR y
DE LA ROSA I ESTEVA, JOSÉ LUIS

(74) Agente/Representante:

TORNER LASALLE, Elisabet

DESCRIPCIÓN

Procedimiento implementado por ordenador, sistema y programas de ordenador para la gestión y la conservación de ficheros digitales en licencias digitales

Campo técnico

La presente invención está dirigida, en general, a la distribución de ficheros entre ordenadores en una red descentralizada. En particular, la invención versa acerca de un procedimiento implementado por ordenador, sistema y programas de ordenador para la gestión y la conservación de ficheros digitales en licencias digitales. Los ficheros digitales pueden hacer referencia a un objeto tridimensional, por ejemplo, o a otro tipo de objetos incluyendo objetos bidimensionales o tetradimensionales.

Antecedentes de la invención

Vivimos en una revolución de soluciones de plataformas en Internet que se convierten de servicios propios centralizados en unos abiertos descentralizados optimizados no solo con IA sino con registros de transacciones descentralizadas, en concreto cadena de bloques. Es un punto de encuentro de varios dominios, siendo un objeto clave del estudio el procesamiento, el almacenamiento y la conservación de datos de propiedad intelectual (PI), objetos de conocimiento y cualquier activo cuyo valor sea digno de conservación para el futuro.

Existe la necesidad de entornos favorables a la PI para mantener una IPP o conservación de la propiedad intelectual (por sus siglas en inglés) (valor y digital). En particular, la fabricación, más que el sector de construcción, utiliza diseños tridimensionales cuyos ficheros CAD se caracterizan por los mismos pros y contras de cualquier activo digital, dado que pueden ser transferidos con facilidad entre personas, haciendo que el robo de diseños sea más sencillo que nunca; además, el diseño es un procedimiento iterativo que implica muchas partes interesadas en el que los propietarios comparten su trabajo con otros, multiplicando las potenciales fugas mientras que la codificación de punto a punto y los usuarios autorizados no protegen legalmente a los propietarios contra un uso o explotación no autorizado de sus diseños, ni son prueba de su propiedad. Lo que será peor, la impresión tridimensional permitirá que se reproduzcan diseños robados en cualquier lugar y a una fracción del coste de fabricación: el robo de PI será más provechoso incluso que en la actualidad.

Aparte de eso, cualquier base de datos es modificada mediante “transacciones”, que contienen un conjunto de cambios a esa base de datos que deben tener éxito o fallar en su conjunto. En una base de datos centralizada normal, las transacciones son validadas por una única autoridad fiable. En cambio, en una base de datos compartida dirigida por cadena de bloques, las transacciones pueden ser validadas por cualquiera de los usuarios de esa cadena de bloques. Dado que estos usuarios no tienen (completamente) confianza mutua, la base de datos tiene que contener normas que restrinjan las transacciones llevadas a cabo. Una cadena de bloques permite que una base de datos sea compartida de forma directa y segura por entidades que no tienen confianza mutua, sin requerir un administrador central. Con contratos inteligentes uno afirma que todas las modificaciones a los datos de un contrato deben ser llevadas a cabo por este código. Para modificar los datos de un contrato, los usuarios de cadenas de bloques envían solicitudes a su código, que determina si deben atenderse esas solicitudes, y cómo hacerlo.

El mayor reto en el desarrollo de una cadena de bloques es la transparencia radical que proporciona. Por ejemplo, si 5 establecen una cadena de bloques conjuntamente, y dos llevan a cabo una transacción bilateral, esta será inmediatamente visible para los otros tres. Aunque existen diversas estrategias para mitigar este problema, ninguna supera la simplicidad y la eficacia de una base de datos centralizada en la que un administrador fiable tiene un control completo sobre quién puede ver qué.

Inicialmente, se pensó que los contratos inteligentes podrían solucionar este problema. El hecho de que cada contrato inteligente contiene su propia base de datos miniatura, sobre la que tiene un control completo, parece prometedor. Todas las operaciones de lectura y de escritura en esta base de datos son mediadas por el código del contrato, haciendo que sea imposible que un contrato lea los datos de otro directamente. Este acoplamiento estrecho entre datos y código es denominado encapsulación, y es la base del paradigma popular de programación orientada a objetos. Así, si un contrato inteligente no puede acceder a los datos de otro, ¿se ha solucionado el problema de la confidencialidad de la cadena de bloques? ¿Tiene sentido hablar de ocultar información en un contrato inteligente? Por desgracia, la respuesta es no. Debido a que, aunque un contrato inteligente no puede leer los datos de otro, esos datos siguen estando almacenados en cada nodo individual en la cadena. Para cada participante de la cadena de bloques, se encuentran en la memoria o en el disco de un sistema que ese participante controla completamente. Y no hay nada que impida que lean la información de su propio sistema, si escogen hacerlo ni cuando lo hagan.

Ocultar datos en un contrato inteligente es aproximadamente tan seguro como ocultarlos en el código HTML de una página Web. Está claro que los usuarios normales de la web no los verán, debido a que no son representados visualmente en su ventana del navegador. Pero todo lo que se requiere es que un navegador web añada una función de “Visualizar el código fuente” para que la información quede visible universalmente. De forma similar, para los datos ocultos en contratos inteligentes, todo lo que se requiere es que alguien modifique su soporte lógico de la cadena de bloques para representar visualmente el estado completo del contrato, y se pierde todo aspecto de confidencialidad. Un programador medio decente podría hacerlo en una hora aproximadamente.

Cualquiera que resulte ser la respuesta, la clave que hay que recordar es que los contratos inteligentes son simplemente un procedimiento para restringir las transacciones llevadas a cabo en una base de datos. Esto es indudablemente una cosa útil, y es esencial para hacer que esa base de datos sea segura para compartir.

Pero los contratos inteligentes no hacen nada más, y ciertamente no pueden escapar de las limitaciones de la base de datos en la que residen.

Una solicitud de patente conocida en la técnica es la EP-A1-3226165 que describe sistemas, procedimientos, dispositivos y otras técnicas para utilizar registros distribuidos, tales como una base de datos de cadenas de bloques, para facilitar la distribución y el uso seguro de ficheros de modelos tridimensionales en impresoras tridimensionales o sistemas CAD por una red informática. Un controlador de impresora tridimensional o el sistema CAD pueden acceder a un registro electrónico que identifica una pluralidad de ficheros de modelos tridimensionales que se han puesto a disposición para su distribución. La impresora o el sistema CAD puede obtener un fichero particular de modelo tridimensional y una clave secreta, estando codificado el fichero de modelo tridimensional en función de la clave secreta. La clave secreta puede ser decodificada utilizando una clave privada asociada con el dispositivo informático que se corresponde con la clave pública. Después de decodificar la clave secreta, el fichero particular de modelo tridimensional puede ser decodificado utilizando la clave secreta, y después de decodificar el fichero particular de modelo tridimensional, el fichero particular de modelo tridimensional puede ser ejecutado en la impresora para imprimir un objeto tridimensional físico o ser visualizado en un sistema CAD. Sin embargo, este procedimiento tiene el problema de no saber qué usuario accede al fichero tridimensional en un dispositivo dado; por lo tanto, este mecanismo no impide que el usuario tenga acceso al objeto digital tridimensional cuando el contrato inteligente decide que la licencia ha caducado temporalmente o numéricamente cambiando simplemente el dispositivo.

El documento CN108846297A proporciona un procedimiento para distribuir y recuperar datos en una red de cadenas de bloques con nodos del mismo nivel. El procedimiento comprende: codificar un fichero que contiene los datos con una clave privada; dividir el fichero codificado en bloques codificados, y dividir la clave privada en porciones privadas; distribuir los bloques y las porciones privadas a los nodos del mismo nivel; acceder al fichero según la solicitud de un cliente, recuperar los bloques codificados a través de un nodo del mismo nivel para reconstruir el fichero codificado, recuperar al menos algunas porciones privadas para reconstruir la clave privada, y decodificar el fichero codificado con la clave privada reconstruida; compartir, mediante los nodos del mismo nivel, la cadena de bloques para formar la red de cadenas de bloques; y enviar las porciones privadas a los nodos del mismo nivel a través del mensaje enviado por la red de cadenas de bloques, y solicitar y recuperar las porciones privadas a través del mensaje enviado en la red de cadenas de bloques.

El documento US10114969B1 da a conocer un sistema y un procedimiento que presentan una codificación segura habilitada por cadenas de bloques. La información y los ficheros de datos entrantes pueden ser codificados utilizando cualquier procedimiento preferido de codificación, luego divididos en segmentos, dándose a cada segmento de los cuales una clave irreversible y codificándose en una o más cadenas de bloques dependiendo del tamaño de los segmentos deseados. Se emplea un mecanismo de recuperación y de recombinación para localizar y decodificar rápidamente todos los segmentos de cada fichero de información, de modo que la cadena de bloques esté distribuida en múltiples servidores, incluyendo servidores basados en la nube. Tras una solicitud, los segmentos codificados de cadena de bloques también pueden ser compartidos entre múltiples usuarios sin poner en peligro la codificación del fichero de información.

Por lo tanto, son necesarias más soluciones para una gestión y una conservación de ficheros digitales en licencias digitales.

Descripción de la invención

Con ese fin, las realizaciones de la presente invención proporcionan, según un primer aspecto, un procedimiento implementado por ordenador para una gestión y una conservación de ficheros digitales en licencias digitales, que comprende:

dividir al menos una parte de un fichero digital en una pluralidad de testigos y distribuir cada testigo dividido en una pluralidad de nodos informáticos que participan en un sistema basado en un protocolo de cadenas de bloques, teniendo asociado cada nodo informático una clave pública, y teniendo el fichero digital asociado una primera clave aleatoria R_1 y estando sujeto a una licencia digital, por ejemplo, un contrato inteligente;

dividir la primera clave aleatoria R_1 asociada con el fichero digital en varias porciones Ri y distribuir cada porción dividida Ri a cada uno de los nodos informáticos;

barajar, aleatoriamente, la pluralidad de nodos informáticos y sus claves públicas asociadas, proporcionando una lista barajada de forma aleatoria de nodos informáticos y de testigos;

para cada nodo informático en la lista barajada de forma aleatoria de nodos informáticos y de testigos que codifican la porción dividida Ri con la clave pública del nodo, proporcionar una porción codificada de la primera clave aleatoria

Ri' y codificar el testigo recibido y una función de clave irreversible relacionada con la dirección del siguiente nodo informático en la cadena de bloques con una clave pública del nodo informático;

almacenar un testigo principal que se corresponde con un primer nodo informático de la cadena de bloques y su clave pública asociada en la licencia digital, pudiendo cambiar dicho primer nodo informático cada vez que se accede al fichero o cambiará con certeza cuando la licencia digital decida prohibir a ese nodo informático el acceso a futuros usos; y

generar una clave multicodificada *Ra* decodificando la porción codificada de la primera clave aleatoria *Ri'* del primer nodo informático con una clave privada del mismo, y utilizar la clave multicodificada generada *Ra* como la clave para recuperar el fichero digital.

Cada vez que un usuario solicita acceder a un fichero codificado con este mecanismo multifirma multitestigo, necesita solicitar las claves de todos los nodos en la clave multifirma en el orden exacto en el que fueron introducidos inicialmente, para obtener la clave que es necesaria para decodificar el fichero digital. Un nodo externo no podría ni siquiera reconstruir el orden exacto de los nodos requerido para la firma, dado que solo lo conocen los testigos. Por lo tanto, se tiene que conocer cuál es el primer nodo y posiblemente la secuencia exacta para acceder, de lo contrario el objeto digital no se desbloqueará. En cualquier caso, la fuerte protección es el hecho de que cada testigo tiene que aceptar la solicitud de decodificación para el siguiente.

En una realización, el fichero digital comprende un objeto tridimensional. Preferiblemente, el objeto tridimensional comprende una geometría dada y/u otros metadatos asociados tales como textura, animación y/o movimiento, entre otros. En otras realizaciones, el fichero digital puede comprender un objeto tetradimensional u otros tipos de ficheros tales como objetos bidimensionales, música, personajes o paisajes de juegos, obras de arte digitales, bases de datos, documentación en cualquier formato *.pdf* o de ofimática, modelos de utilidad e incluso licencias digitales o testigos de cualquier otro tipo a los definidos en la presente patente que contengan activos digitales en un sentido general.

En caso de que el fichero digital esté dividido a un nivel de geometría, los testigos son distribuidos, preferiblemente, a cada nodo informático con una cantidad de datos de la geometría del fichero digital, de manera que cada nodo informático reciba una cantidad similar, pero no necesariamente la misma, de datos, salvo que uno de los testigos también incluye los metadatos asociados del fichero digital.

Según el procedimiento propuesto, los testigos pueden ser divididos por igual o pueden tener distintos tamaños entre ellos. Además, el dispositivo informático puede ser uno de los nodos informáticos o, de forma alternativa, puede formar parte de un componente fiable.

El componente fiable gestiona claves secretas para acceder a la licencia digital y al objeto digital, de manera que se cuente con un cortafuegos adicional para imponer la ley de las licencias digitales cuando deciden cortar el acceso a los objetos digitales aparte de la defensa central general del algoritmo propuesto basado en testigos.

En una realización, el procedimiento comprende, además, publicar el fichero digital al:

- codificar la clave multicodificada *Ra* con una clave pública del componente fiable de un usuario que creó el fichero digital, obteniendo *Ra';*

- codificar el fichero digital con la primera clave aleatoria R_1, obteniendo Fr_1;

- codificar una clave irreversible de Fr_1 con la primera clave aleatoria R_1, obteniendo Hr_1;

- cargar la siguiente información a la licencia digital:

  - la clave multicodificada codificada *Ra';*
  - la clave irreversible codificada Hr_1;
  - dos claves públicas del usuario que creó el fichero digital y dicha clave pública del componente fiable; y
  - una marca de agua del fichero digital;

- cada vez que se accede al fichero digital, por ejemplo, para leerlo o editarlo, utilizar una clave privada del componente fiable del usuario que creó el fichero digital tridimensional para decodificar la clave multicodificada codificada *Ra',* obteniendo *Ra,* y una clave privada del usuario que creó el fichero digital para decodificar *Ra;* y

- decodificar la clave irreversible codificada Hr_1, obteniendo *H,* y buscar el fichero digital en un sistema de ficheros distribuidos, por ejemplo, un IPFS, y luego obtener el fichero digital después de que se decodifica este con la primera clave aleatoria R_1.

En otra realización, para editar el fichero digital, el procedimiento comprende, además:

- al editar al menos un nodo informático el fichero digital, codificar el fichero digital con una segunda clave aleatoria R_2, obteniendo Fr_2, y cargar, además, Fr_2 al sistema de ficheros distribuidos, y calcular una nueva clave irreversible que será codificada con R_2, obteniendo Hr_2;

- hacer una llamada a la licencia digital y:

obtener un mapa de claves irreversibles del fichero digital;

añadir la nueva clave irreversible a dicho mapa de claves irreversibles y una nueva marca de agua, comprendiendo dicho mapa de claves irreversibles distintos campos, y poner la anterior clave irreversible en un campo “pre” del mapa de claves irreversibles;

añadir la nueva marca de agua al mapa de claves irreversibles de marcas de agua; y

para cada nodo informático:

i. ir al mapa de claves irreversibles del nodo informático sustituyendo la clave irreversible vieja por la nueva;

ii. poner la nueva clave irreversible en un campo “sig” del fichero viejo;

iii. sustituir las claves públicas viejas por claves públicas nuevas; y

iv. actualizar un estado a “válido”.

Otras realizaciones de la invención que se divulgan en la presente memoria incluyen un sistema y programas de soporte lógico para llevar a cabo las etapas de realización y las operaciones del procedimiento resumidas anteriormente y divulgadas en detalle a continuación. Más en particular, un producto de programa de ordenador es una realización que tiene un medio legible por un ordenador que incluye instrucciones de programa de ordenador codificadas en el mismo que, cuando son ejecutadas en al menos un procesador en un sistema informático, provocan que el procesador lleve a cabo las operaciones indicadas en la presente memoria como realizaciones de la invención.

Por lo tanto, a diferencia de las soluciones predominantes, la invención propuesta actúa como un registro descentralizado público para proporcionar una única fuente unificada de datos, crear un registro de auditoría más claro y una coherencia entre entidades. La presente invención carga y descarga contenido de PI de valor en la cadena de bloques como una red descentralizada de almacenamiento que convierte la conservación de PI en un mercado algorítmico para conservar su valor. El mercado se ejecuta en una cadena de bloques con un testigo nativo de protocolo gestionado por mineros proporcionando almacenamiento, protección de la PI y conservación digital a clientes, posiblemente pero no necesariamente a un precio en una moneda virtual. En cambio, los clientes gastan las monedas en nodos para conservar, almacenar, minar e indexar objetos digitales y sus PI.

Finalmente, para empresas de fabricación que requieren una resolución definitiva para la protección de la PI de sus ficheros CAD, la presente invención es una plataforma basada en cadenas de bloques que dificulta la distribución no autorizada, prueba la propiedad, protege la reproducción no restringida de ficheros CAD y abre un nuevo paradigma de conservación de PI con consumidores como copropietarios mucho más allá del estado de la técnica.

Breve descripción de los dibujos

Se comprenderán más completamente las anteriores y otras ventajas y características a partir de la siguiente descripción detallada de realizaciones, con referencia a las figuras adjuntas, que deben ser consideradas de forma ilustrativa y no limitante, en las que:

La Fig. 1 ilustra de forma esquemática un ejemplo de la arquitectura propuesta.

La Fig. 2 ilustra de forma esquemática un ejemplo de la interacción de un usuario con un componente fiable.

La Fig. 3 es un diagrama de flujo que muestra una realización de un procedimiento para la gestión y la conservación de ficheros digitales en licencias digitales.

La Fig. 4 ilustra de forma esquemática un ejemplo del procedimiento de barajado.

La Fig. 5 es un diagrama de flujo que muestra el procedimiento para publicar el fichero digital, según una realización de la presente invención.

Descripción detallada de realizaciones preferidas

La presente invención proporciona un procedimiento, un sistema y programas de ordenador para la gestión y la conservación de ficheros digitales en licencias digitales, por ejemplo, contratos inteligentes. Los ficheros digitales, por ejemplo, objetos digitales tridimensionales, están basados en testigos, distribuidos mediante un sistema de ficheros distribuidos, por ejemplo un protocolo PIPFS, y gestionados mediante licencias digitales, por ejemplo, con contratos inteligentes, para su uso, actualización y garantía de los términos de licencia. En una implementación particular, se despliega la invención sobre Ethereum, lo que significa que los testigos con la división del objeto digital tridimensional serán testigos Ethereum y los testigos hablarán con los contratos inteligentes permitiendo que los propietarios de los objetos digitales sean compensados por sus derechos de PI, siendo una licencia.

La Fig. 1 muestra una realización de la arquitectura propuesta de la invención. El protocolo de la presente invención se ejecuta en cualquier plataforma de cadenas de bloques, por ejemplo, el IPFS para distribuir un almacenamiento de los ficheros (y los testigos divididos de los ficheros), y el Ethereum para ejecutar las licencias digitales (como contratos inteligentes). Por lo tanto, los algoritmos propuestos implementados sobre dichas dos plataformas se ejecutan posiblemente conectados con los componentes fiables, mediante servicios como una API, instalada en la visualización web, en la aplicación de los sistemas CAD/CAM, o en un soporte físico de fabricación o en las impresoras tridimensionales.

La Fig. 2 muestra una realización de la interacción de un usuario con un componente fiable (TC, por sus siglas en inglés). El componente fiable gestiona las claves secretas para acceder a las licencias digitales y a los objetos digitales, de forma que se incluya un cortafuegos adicional para imponer la ley de las licencias digitales cuando decidan cortar el acceso a los objetos digitales aparte de la defensa central general del algoritmo basado en testigos. El componente fiable añade una característica interesante, pero no esencial, de dificultad adicional de acceso al contenido, direcciones y licencias como contratos inteligentes en la cadena de bloques. El componente fiable añade la posibilidad de impedir cualquier acceso adicional al objeto digital tridimensional por parte de cualquier usuario que lo tuvo en el pasado.

Aquí se detalla un ejemplo de la estructura del contrato inteligente. El mapa de claves irreversibles de nodos contiene las direcciones de los nodos y su lista de ficheros (claves irreversibles codificadas). Además, el mapa de claves irreversibles comprende distintos campos; en particular, el nombre, la WM, pre, sig, estado, tipo, inic y usuarios.

Para cada fichero digital (clave irreversible codificada) el objeto contiene:

- Nombre descriptivo del fichero
- Marca de agua
- Anterior clave irreversible de fichero
- Siguiente clave irreversible de fichero
- Estado (válido o inválido)
- Tipo de fichero (formato)
- Info inic
  - Creado por
  - Fecha de creación
  - Primer acceso
- Lista de usuarios (direcciones)
- Mapa de claves irreversibles de usuarios con acceso al fichero, con:
  - Dirección del usuario
  - Clave pública del usuario
  - Clave pública del componente fiable
  - Clave R de codificación del fichero codificado
  - Permisos del usuario
    - Tipo (Admin, visualizar, editar, descargar)

- Hora (hasta día D, X horas desde el primer acceso)
- Uso (cargar X veces, editar X veces, descargar X veces)

Por ejemplo: derechos (editar, visualizar, reproducir, etc.) y condiciones (horas, veces, pago por uso, etc.)

Para cada marca de agua, la correspondiente clave irreversible de fichero codificada.

Con referencia ahora a la Fig. 3, se muestra un diagrama de flujo de un procedimiento para la gestión y la conservación de ficheros digitales en licencias digitales. Según esta realización, en la etapa 301, un usuario crea un fichero digital tridimensional con una geometría dada y, preferiblemente, otros metadatos asociados tales como textura, animación y/o movimiento. También pueden incluirse otros tipos de metadatos, por ejemplo, una descripción textual del fichero digital tridimensional.

En la etapa 302, un dispositivo informático que tiene al menos una memoria que incluye instrucciones de programa de ordenador y uno o más procesadores dividen una parte de todo el fichero digital, o una parte del mismo, en una pluralidad de testigos y distribuye cada testigo divido en una pluralidad de nodos informáticos 101, 102, 103, 104 que participan en un sistema basado en un protocolo de cadenas de bloques. El dispositivo informático puede ser parte de un componente fiable o puede ser uno de la pluralidad de nodos informáticos de cadenas de bloques. Cada nodo informático 101, 102, 103, 104 de cadenas de bloques tiene asociado una clave pública y el fichero digital tiene asociado una primera clave aleatoria R_1 y está sujeto a un contrato inteligente. Los testigos pueden tener todos el mismo tamaño o un tamaño distinto. En algunas implementaciones, en particular cuando se divide un fichero digital tridimensional a un nivel de geometría, todos los testigos se distribuyen a los nodos informáticos 101, 102, 103, 104 de cadenas de bloques con una cantidad de datos acerca de la geometría del fichero digital tridimensional excepto uno de los testigos que también incluye los metadatos asociados con el fichero digital tridimensional.

En la etapa 303, el dispositivo informático divide dicha primera clave aleatoria R_1 en varias porciones *Ri* y distribuye cada porción *Ri* a cada nodo informático 101, 102, 103, 104 de cadenas de bloques.

En la etapa 304, el dispositivo informático baraja de forma aleatoria (véase la Fig. 4) los nodos informáticos 101, 102, 103, 104 de cadena de bloques y sus claves públicas asociadas. De esta manera, se proporciona una lista barajada de forma aleatoria de nodos informáticos y de testigos.

En ese punto, en la etapa 305, cada nodo informático 101, 102, 103, 104 de cadenas de bloques codifica su porción *Ri* con la clave pública del nodo, proporcionando, de esta manera una primera clave aleatoria *Ri'* de la porción codificada y codifica, adicionalmente, el testigo recibido y una función de clave irreversible con la clave pública del nodo. La función de clave irreversible está relacionada con la dirección del siguiente nodo informático en la cadena de bloques.

En la etapa 306, el dispositivo informático almacena un testigo principal correspondiente al primer nodo informático de cadenas de bloques y su clave pública asociada en el contrato inteligente. Según el procedimiento, el primer nodo informático de cadenas de bloques cambia cada vez que se accede al fichero digital tridimensional.

En la etapa final 307, el dispositivo informático genera una clave multicodificada *Ra* decodificando la primera clave aleatoria *Ri'* de la porción codificada con una clave privada asociada a cada nodo informático 101, 102, 103, 104 de cadenas de bloques. Esta clave multicodificada *Ra* es la clave que tiene que ser utilizado para recuperar el fichero digital tridimensional.

Con referencia a la Fig. 4, en la misma se ilustra un ejemplo del procedimiento 304 de barajado mediante el cual se barajan los nodos informáticos 101, 102, 103, 104 de cadenas de bloques y sus claves públicas asociadas. Las Figuras 4A y 4B muestran la posición de los nodos informáticos 101, 102, 103, 104 de cadenas de bloques antes (Fig. 4A) y después (Fig. 4B) del procedimiento de barajado. En este caso particular, la licencia digital mantiene el testigo principal de la cadena de testigos del fichero digital tridimensional. Las Figuras 4C y 4D muestran la posición de los nodos informáticos 101, 102, 103, 104 de cadenas de bloques después y antes del procedimiento de barajado cuando la licencia digital se olvida del testigo principal de la cadena de testigos del fichero digital tridimensional. En este caso solo se accederá posiblemente a los nodos informáticos 101 y 104 (no a todo el fichero digital tridimensional ni a toda la clave Ra) dado que solo se podrá acceder a R4' y a R1'.

Con referencia a la Fig. 5, se ilustra un diagrama de flujo del procedimiento para publicar el fichero digital. Según esta realización, en la etapa 501, la clave multicodificada *Ra* es codificada con una clave pública del componente fiable del usuario que creó el fichero digital tridimensional, obteniendo *Ra'.* En la etapa 502, se codifica el fichero digital tridimensional con la primera clave aleatoria R_1, obteniendo Fr_1 y en la etapa 503 se codifica una clave irreversible de Fr_1 con la primera clave aleatoria R_1, obteniendo Hr_1.

En ese punto, etapa 504, se carga la siguiente información a la licencia digital:

- la clave multicodificada codificada *Ra';*

- la clave irreversible codificada Hr_1;

- dos claves públicas del usuario que creó el fichero digital tridimensional y dicha clave pública del componente fiable; y

- una marca de agua del fichero digital.

En la etapa 506, se abre el fichero digital tridimensional, así que, en la etapa 507, se utiliza una clave privada del componente fiable del usuario que creó el fichero digital tridimensional para decodificar la clave multicodificada codificada *Ra',* obteniendo *Ra,* y se utiliza la clave privada del usuario que creó el fichero digital tridimensional para decodificar *Ra* para obtener la primera clave aleatoria R_1.

En la etapa final 508, se decodifica la clave irreversible codificada Hr_1, obteniendo *H,* y se obtiene el fichero digital tridimensional después de buscarlo en un sistema 300 de ficheros distribuidos, tal como el IPFS y decodificarlo con la primera clave aleatoria R_1.

Según otra realización, en este caso no ilustrada, el procedimiento de editar el fichero digital tridimensional comprende, al editar al menos un nodo informático 101, 102, 103, 104 el fichero digital tridimensional, codificar el fichero digital tridimensional con una segunda clave aleatoria R_2, obteniendo Fr_2, y luego cargar Fr_2 en el sistema 300 de ficheros distribuidos y calcular una nueva clave irreversible que será codificada con R_2, obteniendo Hr_2.

Entonces, hacer una llamada a la licencia digital para almacenar la edición y:

- obtener el mapa de claves irreversibles viejo del fichero digital tridimensional;

- añadir la nueva clave irreversible al mapa de claves irreversibles de ficheros con los mismos usuarios, la nueva marca de agua del fichero y poner la clave irreversible vieja en el campo “pre”;

- añadir la nueva marca de agua del fichero al mapa de claves irreversibles de marcas de agua; y

- para cada nodo informático 101, 102, 103, 104:

v. ir al mapa de claves irreversibles del nodo informático sustituyendo la clave irreversible vieja por la nueva;

vi. poner la clave irreversible nueva en un campo “sig” del fichero viejo;

vii. sustituir las claves públicas viejas por claves públicas nuevas; y

viii. actualizar un estado a “válido”.

Se debería hacer notar que el orden de estas etapas es importante dado que la nueva versión del fichero digital tridimensional solo será utilizable cuando se ponga el estado a válido, por lo que, si se rompe el procedimiento (por ejemplo, el programa se paraliza, hay un corte de luz, se cuelga el ordenador) en cualquier etapa mientras se actualizan las claves irreversibles de fichero, el contrato inteligente no se corrompe.

Según otra realización, el procedimiento de auditoría del fichero digital tridimensional comprende calcular su marca de agua e investigar en el contrato inteligente si existe la marca de agua y obtener la clave irreversible de fichero codificada (si existe). Se podría obtener el historial del fichero digital tridimensional a partir de su marca de agua, pero no el propio fichero, dado que está codificado.

En otra realización más, si el contrato inteligente no es desbloqueado en el orden apropiado o se comienza con el primer usuario indebido, el fichero digital o su geometría nunca está completo, de forma que el objeto tridimensional tenga errores de cualquier magnitud en su reconstrucción o conservación utilizando información adicional almacenada en los testigos disponibles. La idea es evitar que cualquiera utilice un objeto tridimensional no contenido en la cadena de bloques y gestionado por una licencia digital apropiada, a no ser que pudieran resentirse los costes de fabricar o de integrar las piezas indebidas. En aquellos dominios en los que estos errores fuera de la cadena no son tan terribles, este mecanismo no es tan potente en comparación con aquellos en los que los modelos son costosos (varias decenas, centenas o millares de miles de dólares) y la demanda de calidad es del 100% como en la mayoría de las industrias de fabricación o CAM).

La idea es que el fichero digital sea una cadena de bloques de testigos, una *cadena de testigos*, en la que cada testigo conozca el siguiente testigo pero no el anterior. Así, descomponer el fichero digital en 100 testigos significa que la probabilidad de que un usuario tenga toda la *cadena de testigos* es solo 1/100, y cuanto más basado en testigos esté, menos probable es que un usuario llegue a tenerlos todos. Esta limitación se aplica en el momento de guardar el fichero digital fuera de la cadena de bloques. Por lo tanto, los testigos ausentes fuera de la cadena son la solución técnica. Además, multitestigo significa un mecanismo de nuevas autorizaciones: siempre que se transfiera, comparta o visualice el fichero digital, potencialmente todos los propietarios deben proporcionar (votar/firmar) la autorización. La

autorización podría ser automática y sencilla de obtener para todas las operaciones excepto para guardarlo fuera de la cadena. Por lo tanto, esta es otra forma de generar testigos de PI ausentes debido a que es probable que se eviten o pospongan autorizaciones manuales o automáticas, con la tentación de descargar el fichero digital fuera de la cadena. La cadena de testigos se denominará cadena3DDO, y tendrá un formato en el IPFS.

En otra realización más, alternativa o complementaria a la anterior, un subconjunto de testigos podría recomponer todo el fichero digital utilizando redundancia. Por lo tanto, no es tan terrible que haya un testigo ausente, dado que se podría recomponer el fichero digital de forma progresiva con cada vez más testigos, pero es improbable o no se prevé que sea reconstruido totalmente fuera de la cadena de bloques. Por lo tanto, por defecto, un fichero digital basado en testigos nunca es descargado FUERA de la cadena totalmente y siempre habrá testigos ausentes que podrían reconstruir el fichero digital con una baja probabilidad de estar completo, a pesar de que el fichero digital pudiera tener buen aspecto en muchos casos, pero no suficientemente bueno para los estándares de calidad de la industria de fabricación.

El mecanismo de redundancia podría ser similar al Parchive de fuente abierta. Los ficheros Par2 utilizan, en general, este sistema de denominación/extensión: nombrefichero.vol000+01.PAR2, nombrefichero.vol001+02.PAR2, nombrefichero.vol003+04.PAR2, nombrefichero.vol007+06.PAR2, etc. El +01, +02, etc. en el nombrefichero indica cuántos bloques/testigos contiene, y el vol000, vol001, vol003, etc. indica el número del primer bloque de recuperación en el fichero PAR2. Si un fichero de índice del fichero digital fuera de cadena indica que hay 4 bloques ausentes, la forma más sencilla de reparar los ficheros sería descargar el nombrefichero.vol003+04.PAR2 de los testigos ausentes y, debido a la redundancia, también es aceptable el nombrefichero.vol007+06.PAR2.

La especificación Par2 soporta hasta 32768 bloques fuente y hasta 65535 bloques de recuperación. Los ficheros introducidos son divididos en múltiples bloques de tamaño idéntico de forma que los ficheros de recuperación no necesiten tener el tamaño del fichero introducido más grande. En la presente invención la implementación podría ser testigos de bloques de tamaño idéntico o distinto para hacer que sea más difícil detectar cuál es la composición correcta para reconstruir el fichero digital original. Por lo tanto, los testigos de PI son almacenados de forma redundante en IPFS y, como se ha dicho, un fichero digital nunca contiene todos los testigos de la cadena de bloques (FUERA de cadena), pero no hay forma de conocer, *a priori*, cuál es el testigo ausente dado que siempre se descarga el código redundante.

El mecanismo para impedir que los testigos sean descargados fuera de la cadena podría ser múltiple: por defecto, es aleatorio, podría ser aleatorio cada vez, podría serlo mediante una decisión particular de cualquier propietario de cualquier testigo, podría serlo según una norma programable, podría ser todos los anteriores combinados. Cualquier posibilidad será válida, debido a que la novedad es que no hay forma de guardar fuera de cadena distinta que a través de la licencia digital, que siempre aplicará esta prevención de testigo ausente. Con este mecanismo, cuantos más testigos mejor para hacer que sea más difícil la detección y la reparación del testigo ausente.

El mecanismo de la presente realización es, que en el momento de descarga fuera de la cadena de bloques, será gestionado por el mismo contrato inteligente de licencia digital que sigue este mecanismo que aplicará, preferiblemente:

Para cada testigo Tp*i* = Dp*i* + datos redundantes Np*i*
Se descarga Dp*i* al destinatario T o podría ser saltado aleatoriamente, con una probabilidad p = {0, 1}, por ejemplo p=0,9
No hay indicio o evidencia de si se descarga un testigo Dp*i* o no en T o si solo es el código redundante Np*i.*
EndFor

Conteniendo T los datos de muchos Dp*i* y toda la redundancia Ni*i*, entonces, utilizando esta información, se reconstruye el fichero digital Dp. Cuanto menor sea p, más probable es que el fichero digital Dp reconstruido sea distinto de D.

Lo importante es haber regulado p con tal probabilidad de Dp sea tan similar a D, pero no perfectamente idéntico, de forma que cualquier intento por utilizar Dp como la única versión disponible fuera de la cadena de D pueda fallar probablemente, produciendo una impresión o fabricación imperfecta, costosa y perjudicial, a lo que nadie se arriesgaría. Adicionalmente, el algoritmo aleatorio de este procedimiento podría ser sustituido por un sistema de votación en el que cada testigo Tp*i* pertenece a un propietario distinto que podría prohibir, en cualquier momento, la descarga fuera de línea del fichero digital.

Como observación final, los dos mecanismos podrían aplicarse a la vez, de forma que si se intenta descargar el fichero digital D fuera de la cadena, entonces podría estar incompleto debido al testigo principal perdido de la cadena de testigos, y también podría haber ausentes algunos otros testigos.

La presente invención puede implementarse mediante soporte físico, soporte lógico, soporte lógico inalterable, soporte lógico personalizado, microcódigo, lenguajes descriptivos de soporte físico o cualquier combinación de los mismos.

Cuando se implementa en soporte lógico, soporte lógico inalterable, soporte lógico personalizado o microcódigo, el código o los segmentos de código del programa para llevar a cabo las tareas necesarias pueden ser almacenados en un medio no transitorio legible por ordenador tal como un medio de almacenamiento. Los procesadores pueden llevar a cabo las tareas descritas.

Aunque se ha descrito el contenido en un lenguaje específico a características estructurales y/o a hechos metodológicos, se debe comprender que el contenido definido en las reivindicaciones adjuntas no está limitado necesariamente a las características o a los hechos específicos descritos anteriormente. Más bien, las características y los hechos específicos descritos anteriormente son divulgados como formas ejemplares de implementar las reivindicaciones.

Lo anterior describe realizaciones de la presente invención y modificaciones, evidentes para los expertos en la técnica que pueden realizarse a la misma, sin alejarse del alcance de la presente invención.

El alcance de la presente invención está definido en el siguiente conjunto de reivindicaciones.

REIVINDICACIONES

1. Un procedimiento implementado por ordenador para la gestión y la conservación de ficheros digitales en licencias digitales, que comprende:

dividir, por medio de un dispositivo informático, al menos una parte de un fichero digital en una pluralidad de testigos y distribuir cada testigo dividido en una pluralidad de nodos informáticos (101, 102, 103, 104) que participan en un sistema basado en un protocolo de cadenas de bloques, teniendo asociado cada nodo informático (101, 102, 103, 104) una clave pública, y teniendo asociado cada fichero digital una primera clave aleatoria R_1 y estando sujeto a una licencia digital que incluye un contrato inteligente;

dividir, por medio del dispositivo informático, la primera clave aleatoria R_1 asociada con el fichero digital en una pluralidad de porciones *Ri* y distribuir cada porción dividida *Ri* a cada uno de dicha pluralidad de nodos informáticos (101, 102, 103, 104);

barajar, por medio del dispositivo informático (10), de forma aleatoria, la pluralidad de nodos informáticos (101, 102, 103, 104) y sus claves públicas asociadas, proporcionando una lista barajada de forma aleatoria de nodos informáticos y de testigos;

para cada nodo informático (101, 102, 103, 104) en la lista barajada de forma aleatoria de nodos informáticos y de testigos:

- codificar la porción dividida *Ri* con la clave pública del nodo, proporcionando una primera clave aleatoria *Ri'* de la porción codificada; y

- codificar el testigo recibido y una función de clave irreversible relacionados con una dirección del siguiente nodo informático en la cadena de bloques con una clave pública del nodo informático (101, 102, 103, 104);

almacenar, por medio del dispositivo informático, un testigo principal que se corresponde con un primer nodo informático de la cadena de bloques y su clave pública asociada en la licencia digital, cambiando dicho primer nodo informático cada vez que se accede al fichero digital; y

generar, por medio del dispositivo informático, una clave multicodificada *Ra* decodificando la primera clave aleatoria *Ri'* de la porción codificada del primer nodo informático con una clave privada del mismo, y utilizar la clave multicodificada generada *Ra* como la clave para recuperar el fichero digital.

2. El procedimiento implementado por ordenador de la reivindicación 1, en el que el fichero digital comprende un objeto tridimensional con una geometría dada y/u otros metadatos asociados, incluyendo textura, animación y/o movimiento.

3. El procedimiento implementado por ordenador de la reivindicación 2, en el que cada uno de la pluralidad de testigos divididos tiene un tamaño idéntico o uno distinto.

4. El procedimiento implementado por ordenador de la reivindicación 2, en el que, cuando el fichero digital está siendo dividido a un nivel de geometría, los testigos divididos se distribuyen en cada uno de la pluralidad de nodos informáticos (101, 102, 103, 104) con una cantidad de datos de la geometría del fichero digital, excepto un testigo que también incluye dichos metadatos asociados del fichero digital.

5. El procedimiento implementado por ordenador de la reivindicación 1, en el que se divide todo el fichero digital en una pluralidad de testigos.

6. El procedimiento implementado por ordenador de la reivindicación 1, que comprende, además, publicar el fichero digital al:

- codificar la clave multicodificada *Ra* con una clave pública del componente fiable de un usuario que creó el fichero digital, obteniendo *Ra';*

- codificar el fichero digital con la primera clave aleatoria R_1, obteniendo Fr_1;

- codificar una clave irreversible de Fr_1 con la primera clave aleatoria R_1, obteniendo Hr_1;

- cargar la siguiente información a la licencia digital:

- la clave multicodificada codificada *Ra';*

- la clave irreversible codificada Hr_1;

- dos claves públicas del usuario que creó el fichero digital y dicha clave pública del componente fiable; y

- una marca de agua del fichero digital;

- cada vez que se abre el fichero digital, utilizar una clave privada del componente fiable del usuario que creó el fichero digital para decodificar la clave multicodificada codificada *Ra',* obteniendo *Ra,* y la clave privada del usuario que creó el fichero digital para decodificar *Ra;* y

- decodificar la clave irreversible codificada Hr_1, obteniendo *H,* y buscar el fichero digital en un sistema de ficheros distribuidos (300) y luego obtener el fichero digital después de que se decodifique este con la primera clave aleatoria R_1.

7. El procedimiento implementado por ordenador de la reivindicación 1, que comprende, además:

- al editar al menos un nodo informático (101, 102, 103, 104) el fichero digital, codificar el fichero digital con una segunda clave aleatoria R_2, obteniendo Fr_2, y cargar, además, Fr_2 al sistema de ficheros distribuidos (300) y calcular una nueva clave irreversible que será codificada con R_2, obteniendo Hr_2;

- hacer una llamada a la licencia digital y:

- obtener un mapa de claves irreversibles del fichero digital;

- añadir la nueva clave irreversible a dicho mapa de claves irreversibles y una nueva marca de agua, comprendiendo dicho mapa de claves irreversibles distintos campos y poner la anterior clave irreversible en un campo “pre” del mapa de claves irreversibles;

- añadir la nueva marca de agua al mapa de claves irreversibles de marcas de agua; y

- para cada nodo informático (101, 102, 103, 104);

i. ir al mapa de claves irreversibles del nodo informático sustituyendo la clave irreversible vieja por la nueva;

ii. poner la nueva clave irreversible en un campo “sig” del fichero viejo;

iii. sustituir las claves públicas viejas por claves públicas nuevas; y

iv. actualizar un estado a “válido”.

8. El procedimiento implementado por ordenador de reivindicaciones anteriores, que comprende, además, almacenar la pluralidad de testigos divididos de forma redundante en el sistema de ficheros distribuidos (300).

9. El procedimiento implementado por ordenador de cualquiera de las reivindicaciones anteriores, en el que el dispositivo informático está incluido en uno de la pluralidad de nodos informáticos (101, 102, 103, 104) o forma parte del componente fiable (200).

10. Un sistema para la gestión y la conservación de ficheros digitales en licencias digitales, que comprende:

- al menos una memoria que incluye instrucciones de programa de ordenador; y

- uno o más procesadores, en donde las instrucciones de programa de ordenador, cuando son ejecutadas por los uno o más procesadores informáticos, provocan:

- dividir al menos una parte de un fichero digital en una pluralidad de testigos y distribuir cada testigo dividido en una pluralidad de nodos informáticos (101, 102, 103, 104) que participan en un sistema basado en un protocolo de cadenas de bloques, teniendo asociado cada nodo informático (101, 102, 103, 104) una clave pública, y teniendo asociado dicho fichero digital una primera clave aleatoria R_1 y estando sujeto a una licencia digital que incluye un contrato inteligente;

- dividir la primera clave aleatoria R_1 asociada con el fichero digital en una pluralidad de porciones *Ri* y distribuir cada porción dividida *Ri* a cada uno de dicha pluralidad de nodos informáticos (101, 102, 103, 104);

- barajar, de forma aleatoria, la pluralidad de nodos informáticos (101, 102, 103, 104) y sus claves públicas asociadas, proporcionando una lista barajada de forma aleatoria de nodos informáticos y de testigos; en el que cada nodo informático (101, 102, 103, 104) en la lista barajada de forma aleatoria de nodos informáticos y de testigos codifica la porción dividida *Ri* con la clave pública del nodo, proporcionando una primera clave aleatoria *Ri'* de la porción codificada, y codifica el testigo recibido y una función de clave irreversible relacionados con una dirección del siguiente nodo informático en la cadena de bloques con una clave pública del nodo informático (101, 102, 103, 104);

- almacenar un testigo principal que se corresponde con un primer nodo informático de la cadena de bloques y su clave pública asociada en la licencia digital, cambiando dicho primer nodo informático cada vez que se accede al fichero digital; y

- generar una clave multicodificada *Ra* decodificando la primera clave aleatoria *Ri'* de la porción codificada del primer nodo informático con una clave privada del mismo, y utilizar la clave multicodificada generada *Ra* como la clave para recuperar el fichero digital.

11. El sistema de la reivindicación 10, que comprende, además, una impresora tridimensional para crear el fichero digital con una geometría dada y/u otros metadatos asociados, incluyendo textura, animación y/o movimiento.

12. El sistema de la reivindicación 10 u 11, en el que los uno o más procesadores están incluidos en uno de la pluralidad de nodos informáticos (101, 102, 103, 104) o están incluidos en un dispositivo informático del componente fiable.

13. El sistema de la reivindicación 11, en el que las instrucciones de programa de ordenador, cuando son ejecutadas por los uno o más procesadores informáticos, provocan dicha división de la pluralidad de testigos con un tamaño idéntico o uno distinto.

14. El sistema de la reivindicación 11, en el que las instrucciones de programa de ordenador, cuando son ejecutadas por los uno o más procesadores informáticos, en dicha etapa a) provocan la división del fichero digital a un nivel de geometría, y la distribución de los testigos divididos en cada uno de la pluralidad de nodos informáticos (101, 102, 103, 104) con una cantidad de datos de la geometría del fichero digital excepto un testigo que también incluye dichos metadatos asociados del fichero digital.

15. Un medio no transitorio legible por ordenador que comprende de forma tangible instrucciones de programa de ordenador, que, cuando son ejecutadas por un procesador provoca que el procesador implemente el procedimiento de las reivindicaciones 1 a 9.

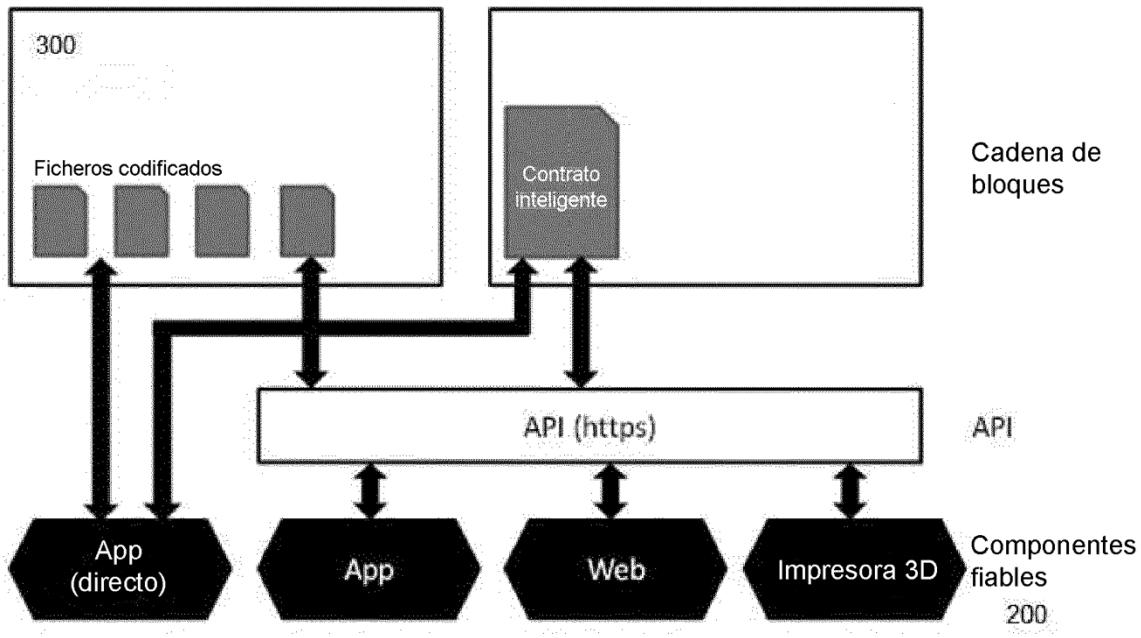
300
Ficheros codificados
Contrato inteligente
Cadena de bloques
API (https)
API
App (directo)
App
Web
Impresora 3D
Componentes fiables
200

Fig. 1

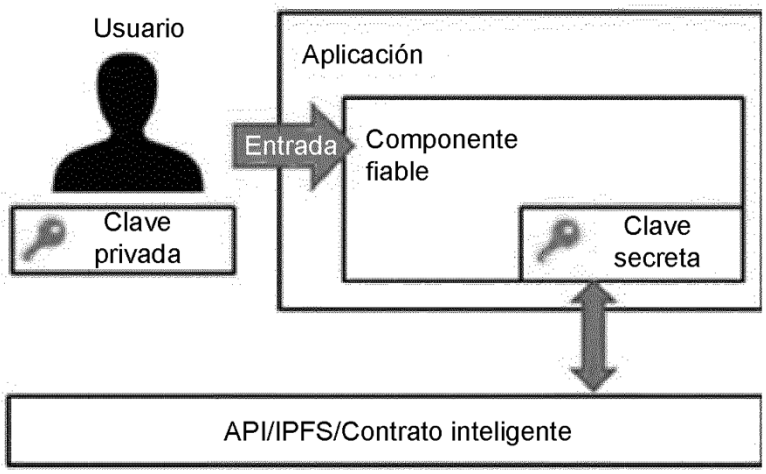
Usuario
Aplicación
Entrada
Componente fiable
Clave privada
Clave secreta
API/IPFS/Contrato inteligente

Fig. 2

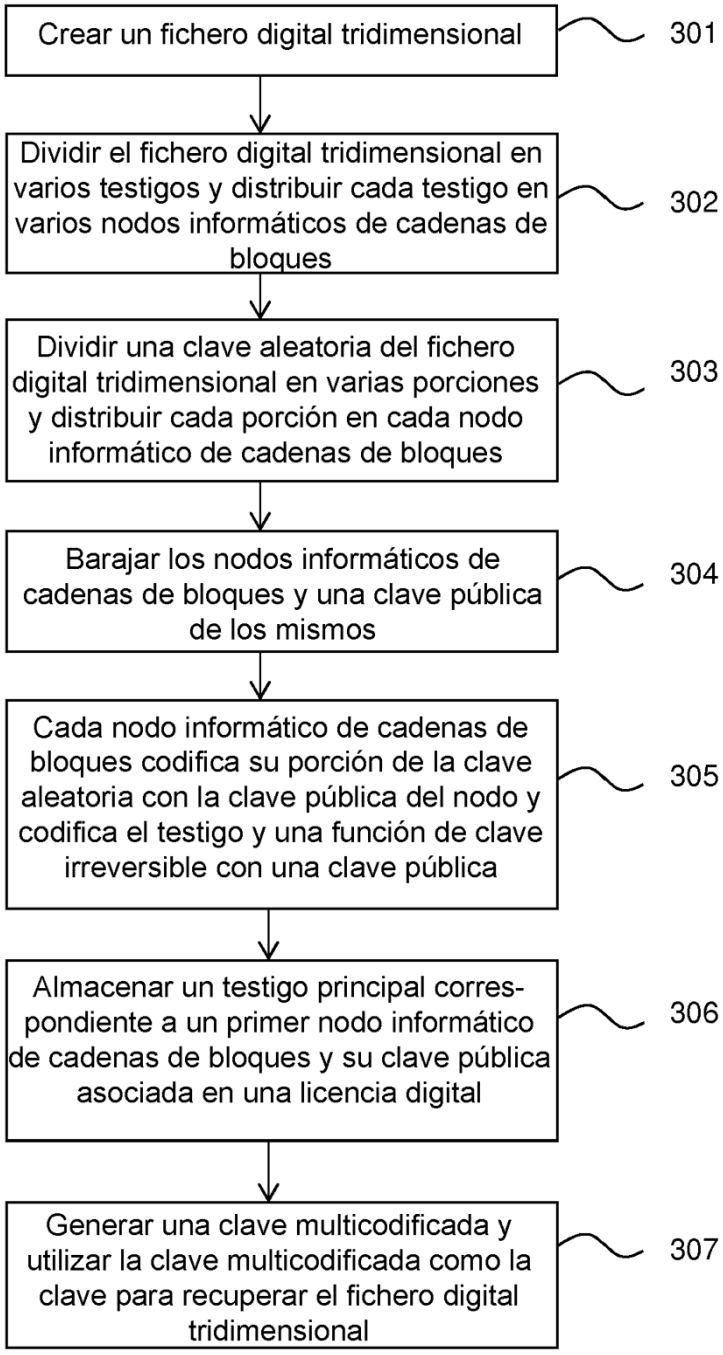
Crear un fichero digital tridimensional
301
Dividir el fichero digital tridimensional en varios testigos y distribuir cada testigo en varios nodos informáticos de cadenas de bloques
302
Dividir una clave aleatoria del fichero digital tridimensional en varias porciones y distribuir cada porción en cada nodo informático de cadenas de bloques
303
Barajar los nodos informáticos de cadenas de bloques y una clave pública de los mismos
304
Cada nodo informático de cadenas de bloques codifica su porción de la clave aleatoria con la clave pública del nodo y codifica el testigo y una función de clave irreversible con una clave pública
305
Almacenar un testigo principal correspondiente a un primer nodo informático de cadenas de bloques y su clave pública asociada en una licencia digital
306
Generar una clave multicodificada y utilizar la clave multicodificada como la clave para recuperar el fichero digital tridimensional
307

Fig. 3

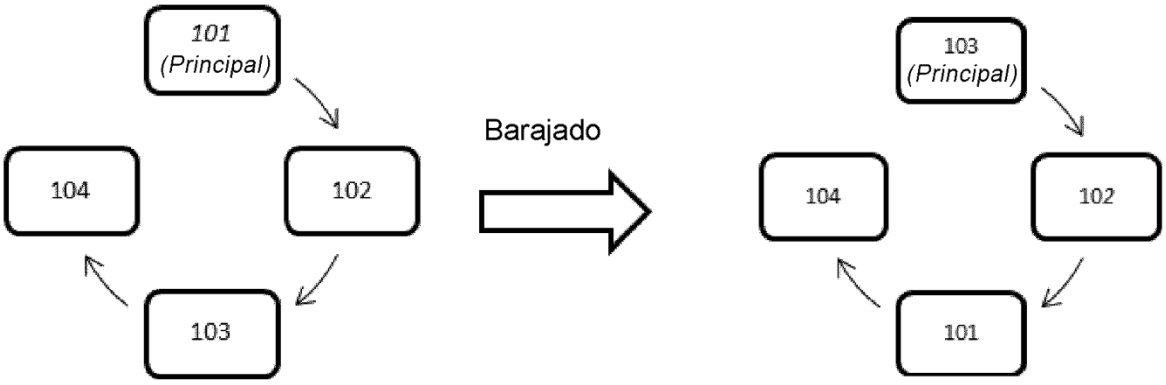

Fig. 4A

Fig. 4B

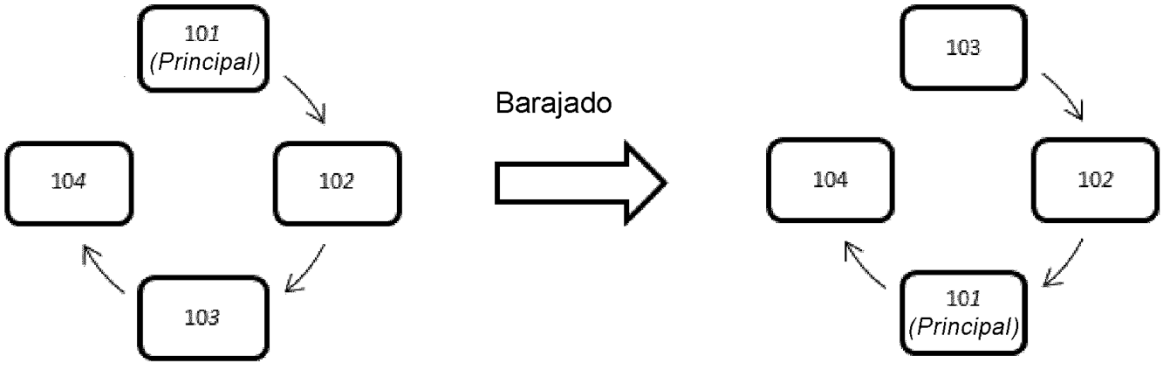

Fig. 4C

Fig. 4D

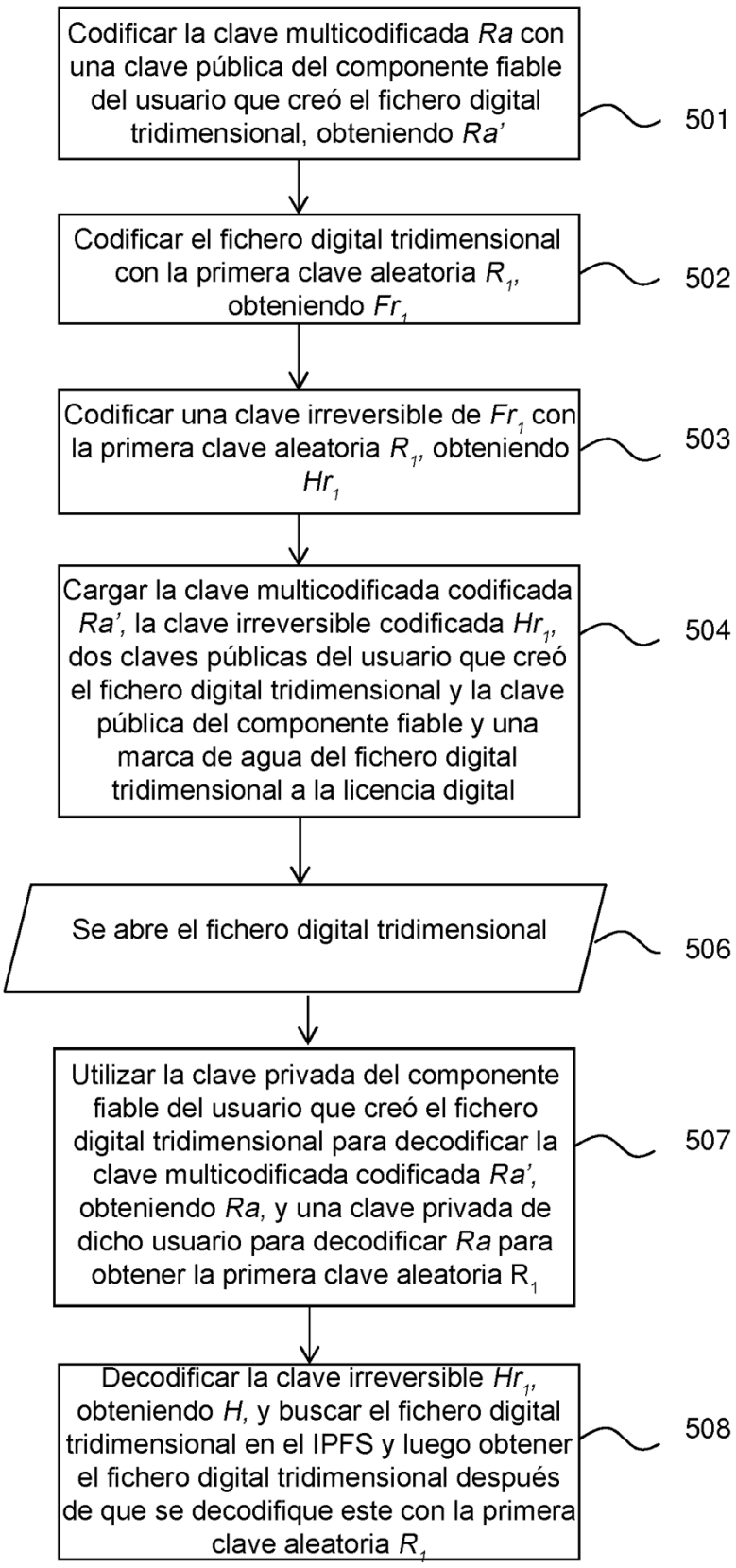
Codificar la clave multicodificada *Ra* con una clave pública del componente fiable del usuario que creó el fichero digital tridimensional, obteniendo *Ra'*
501
Codificar el fichero digital tridimensional con la primera clave aleatoria R_1, obteniendo Fr_1
502
Codificar una clave irreversible de Fr_1 con la primera clave aleatoria R_1, obteniendo Hr_1
503
Cargar la clave multicodificada codificada *Ra'*, la clave irreversible codificada Hr_1, dos claves públicas del usuario que creó el fichero digital tridimensional y la clave pública del componente fiable y una marca de agua del fichero digital tridimensional a la licencia digital
504
Se abre el fichero digital tridimensional
506
Utilizar la clave privada del componente fiable del usuario que creó el fichero digital tridimensional para decodificar la clave multicodificada codificada *Ra'*, obteniendo *Ra*, y una clave privada de dicho usuario para decodificar *Ra* para obtener la primera clave aleatoria R_1
507
Decodificar la clave irreversible Hr_1, obteniendo *H*, y buscar el fichero digital tridimensional en el IPFS y luego obtener el fichero digital tridimensional después de que se decodifique este con la primera clave aleatoria R_1
508

Fig. 5