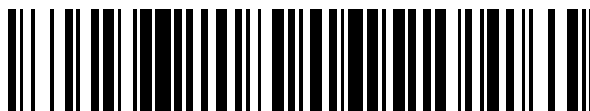


19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 847 170**

51 Int. Cl.:

H04L 9/00

(2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **24.09.2018** **PCT/US2018/052429**

87 Fecha y número de publicación internacional: **04.04.2019** **WO19067357**

96 Fecha de presentación y número de la solicitud europea: **24.09.2018** **E 18786143 (0)**

97 Fecha y número de publicación de la concesión europea: **04.11.2020** **EP 3673608**

54 Título: **Método de almacenamiento de datos, método de consulta de datos y aparatos**

30 Prioridad:

29.09.2017 CN 201710910293

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

02.08.2021

73 Titular/es:

ADVANCED NEW TECHNOLOGIES CO., LTD.
(100.0%)

Cayman Corporate Centre, 27 Hospital Road
George Town, Grand Cayman KY1-9008, KY

72 Inventor/es:

WU, HAO

74 Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

ES 2 847 170 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Método de almacenamiento de datos, método de consulta de datos y aparatos

5 Antecedentes

- En la era de la información, los datos tienen valores. Por ejemplo, si un banco pudiera adquirir registros de compra de vivienda de un cliente en un centro de venta de viviendas, el banco podría evaluar mejor el crédito del cliente; Si el centro de ventas de viviendas puede adquirir las calificaciones crediticias de los clientes del banco, entonces se podrían emplear diferentes estrategias de ventas para diferentes clientes. En el ejemplo anterior, aparentemente existe una demanda para compartir los datos de los demás entre el banco y el centro de venta de viviendas. De hecho, cada vez más instituciones desean compartir datos a medida que el valor de los datos se vuelve cada vez más significativo.
- En la actualidad, se suele utilizar una plataforma de intercambio de datos como intermediario. Por un lado, la plataforma de intercambio de datos recibe y almacena datos cargados por varias instituciones y, por otro lado, la plataforma de intercambio de datos brinda servicios de consulta de datos a las instituciones. Además, como no todas las instituciones pueden tener permiso para consultar todos los datos en la plataforma de intercambio de datos (por ejemplo, una institución sin una licencia financiera no puede consultar legalmente los datos cargados por instituciones financieras; para otro ejemplo, una institución puede firmar un acuerdo solo con algunas otras instituciones para consultar los datos cargados de cada uno), la plataforma de intercambio de datos debe configurar un permiso de acceso para cada institución, de modo que la consulta de datos por parte de cada institución en la plataforma de intercambio de datos cumple con las normas legales o acuerdos entre instituciones. El intercambio de datos entre instituciones se realiza de esa manera.
- Sobre la base de la técnica anterior, se desea desarrollar métodos de almacenamiento de datos y métodos de consulta de datos más seguros y eficientes.
- El documento US 2016/261690 A1 da a conocer sistemas y métodos que facilitan la comunicación de mensajes a un número enormemente escalable de dispositivos, independientemente de un recurso centralizado. El documento WO 2017/007806 A1 desvela un sistema de comercio de valores que utiliza un libro mayor de cadena de bloques distribuido para realizar transacciones de valores.
- "El sistema de distribución de contenido digital basado en cadena de bloques" (Kishigami Junichi et al, quinta conferencia internacional IEEE 2015 sobre big data y computación en la nube, 26 de agosto de 2015, páginas 187-190) desvela un sistema de distribución de contenido digital basado en cadena de bloques.

Sumario

- La invención proporciona un método de almacenamiento de datos, un sistema y un método de consulta de datos como se establece en las reivindicaciones adjuntas. También se describe en el presente documento un método de almacenamiento de datos, un método de consulta de datos y aparatos para resolver los problemas de que los métodos de acceso a datos existentes no pueden garantizar la seguridad de los datos y tienen una baja eficiencia de consulta de datos.
- Para resolver los problemas técnicos anteriores, las realizaciones de la presente descripción se logran de la siguiente manera:
- Un método de almacenamiento de datos según algunas realizaciones de la presente descripción comprende: enviar, mediante un nodo de cadena de bloques asociado a una cadena de bloques, datos a un dispositivo de cifrado para hacer que el dispositivo de cifrado cifre los datos y devuelva los datos cifrados al nodo de cadena de bloques; recibir los datos cifrados devueltos por el dispositivo de cifrado; enviar los datos cifrados a otros nodos de cadena de bloques asociados a la cadena de bloques para hacer que los otros nodos de cadena de bloques almacenen los datos cifrados en la cadena de bloques después de realizar la verificación de consenso sobre los datos cifrados con éxito.
- Un método de cifrado de datos de acuerdo con algunas realizaciones de la presente descripción comprende: recibir, mediante un dispositivo de cifrado, datos enviados por un nodo de cadena de bloques; cifrar una parte de los datos; devolver los datos cifrados al nodo de cadena de bloques para hacer que el nodo de cadena de bloques envíe los datos cifrados a otros nodos de cadena de bloques para la verificación del consenso y luego hacer que cada uno de los otros nodos de cadena de bloques almacene los datos cifrados en la cadena de bloques después de realizar la verificación de consenso en los datos cifrados con éxito.
- Un método de consulta de datos de acuerdo con algunas realizaciones de la presente descripción comprende: determinar, mediante un nodo de cadena de bloques asociado a una cadena de bloques, los datos que se van a consultar en datos cifrados almacenados en la cadena de bloques; determinar, a través de un contrato inteligente, si

el nodo de cadena de bloques tiene permiso para descifrar los datos que se van a consultar; si el nodo de cadena de bloques tiene el permiso, enviar los datos que se van a consultar a un dispositivo de cifrado a través del contrato inteligente para hacer que el dispositivo de cifrado descifre los datos que se van a consultar y devuelva los datos obtenidos del descifrado al nodo de cadena de bloques; si el nodo de cadena de bloques no tiene el permiso, se niega a enviar los datos para ser consultados al dispositivo de cifrado. Un contrato inteligente es un protocolo informático destinado a facilitar, verificar o hacer cumplir digitalmente la negociación o el cumplimiento de un contrato. Los contratos inteligentes permiten la realización de transacciones creíbles sin terceros. Estas transacciones pueden ser rastreables e irreversibles.

Un aparato de almacenamiento de datos según algunas realizaciones de la presente descripción comprende: un primer módulo de envío configurado para enviar datos a un dispositivo de cifrado para hacer que el dispositivo de cifrado cifre los datos y devuelva los datos cifrados al nodo de cadena de bloques; un módulo de recepción configurado para recibir los datos cifrados devueltos por el dispositivo de cifrado; un segundo módulo de envío configurado para enviar los datos cifrados a otros nodos de cadena de bloques para hacer que cada uno de los otros nodos de cadena de bloques almacene los datos cifrados en la cadena de bloques después de realizar la verificación de consenso sobre los datos cifrados con éxito.

Un aparato de cifrado de datos según algunas realizaciones de la presente descripción comprende: un módulo de recepción configurado para recibir datos enviados por un nodo de cadena de bloques asociado a una cadena de bloques; un módulo de cifrado configurado para cifrar una parte de los datos; un módulo de retorno configurado para devolver los datos cifrados al nodo de cadena de bloques para hacer que el nodo de cadena de bloques envíe los datos cifrados a otros nodos de cadena de bloques asociados a la cadena de bloques para la verificación del consenso y luego haga que cada uno de los otros nodos de cadena de bloques almacene los datos cifrados en la cadena de bloques después de realizar la verificación de consenso en los datos cifrados con éxito.

Un aparato de consulta de datos implementado por un nodo de cadena de bloques asociado a una cadena de bloques de acuerdo con algunas realizaciones de la presente descripción comprende: un módulo de determinación configurado para determinar los datos a consultar en datos cifrados almacenados en la cadena de bloques; un módulo de determinación y procesamiento configurado para determinar, a través de un contrato inteligente, si el aparato tiene permiso para descifrar los datos que se van a consultar; si el nodo de cadena de bloques tiene el permiso, enviar los datos que se van a consultar a un dispositivo de cifrado a través del contrato inteligente para hacer que el dispositivo de cifrado descifre los datos que se van a consultar y devuelva los datos obtenidos del descifrado al aparato; si el nodo de cadena de bloques no tiene el permiso, rechazar el envío de los datos que se van a consultar al dispositivo de cifrado.

Un dispositivo de almacenamiento de datos implementado en un nodo de cadena de bloques asociado a una cadena de bloques de acuerdo con algunas realizaciones de la presente descripción comprende uno o más procesadores y memorias, en donde las memorias almacenan programas, y está configurado para ejecutar los siguientes pasos por uno o más procesadores: enviar datos a un dispositivo de cifrado para hacer que el dispositivo de cifrado cifre los datos y devuelva los datos cifrados al nodo de cadena de bloques; recibir los datos cifrados devueltos por el dispositivo de cifrado; enviar los datos cifrados a otros nodos de cadena de bloques asociados a la cadena de bloques para hacer que cada uno de los otros nodos de cadena de bloques almacene los datos cifrados en la cadena de bloques después de realizar la verificación de consenso sobre los datos cifrados con éxito.

Un dispositivo de cifrado de datos de acuerdo con algunas realizaciones de la presente descripción comprende uno o más procesadores y memorias, en donde las memorias almacenan programas, y está configurado para ejecutar los siguientes pasos por uno o más procesadores: recibir datos enviados por un nodo de cadena de bloques asociado a una cadena de bloques; cifrar una parte de los datos; devolver los datos cifrados al nodo de cadena de bloques para hacer que el nodo de cadena de bloques envíe los datos cifrados a otros nodos de cadena de bloques asociados a la cadena de bloques para la verificación del consenso y luego hacer que cada uno de los otros nodos de cadena de bloques almacene los datos cifrados en la cadena de bloques después de realizar la verificación del consenso en los datos cifrados con éxito.

Según otro aspecto, un sistema implementable como un nodo de cadena de bloques asociado a una cadena de bloques comprende un procesador y un medio de almacenamiento no transitorio legible por ordenador que almacena instrucciones que, cuando son ejecutadas por el procesador, hacen que el procesador realice un método de almacenamiento de datos, el método que comprende: enviar datos a un dispositivo de cifrado para hacer que el dispositivo de cifrado cifre los datos y devuelva los datos cifrados al nodo de cadena de bloques; recibir los datos cifrados devueltos por el dispositivo de cifrado; y enviar los datos cifrados a otros nodos de cadena de bloques asociados a la cadena de bloques para hacer que cada uno de los otros nodos de cadena de bloques almacene los datos cifrados en la cadena de bloques después de realizar la verificación de consenso sobre los datos cifrados con éxito.

En algunas realizaciones, el método comprende además: determinar un primer valor correspondiente a los datos a través de un contrato inteligente, utilizándose el primer valor para representar un valor añadido en una cuenta del nodo de cadena de bloques; y enviar el propio identificador de nodo del nodo de cadena de bloques y el primer valor a

otros nodos de cadena de bloques para hacer que el identificador de nodo y el primer valor se almacenen en la cadena de bloques después de una verificación de consenso sobre el identificador de nodo y el primer valor por los nodos de cadena de bloques pasados.

- 5 En algunas realizaciones, se hace que el dispositivo de cifrado cifre una parte de los datos.

En algunas realizaciones, el método comprende además: determinar, mediante uno de los nodos de cadena de bloques asociados a la cadena de bloques, los datos que se van a consultar en los datos cifrados almacenados en la cadena de bloques; determinar, mediante un contrato inteligente, si el único nodo de cadena de bloques tiene permiso para descifrar los datos que se van a consultar; si el único nodo de cadena de bloques tiene permiso, enviar los datos a consultar a un dispositivo de cifrado a través del contrato inteligente para hacer que el dispositivo de cifrado descifre los datos a consultar y devuelva los datos obtenidos del descifrado al único nodo de cadena de bloques; y si el único nodo de cadena de bloques no tiene el permiso, rechazara enviar los datos para ser consultados al dispositivo de cifrado.

En algunas realizaciones, cada dato cifrado almacenado en la cadena de bloques comprende una parte no cifrada; y la determinación, por uno de los nodos de cadena de bloques, los datos que se van a consultar en datos cifrados almacenados en una cadena de bloques comprende: determinar, por el nodo de una cadena de bloques, una condición de consulta de datos; determinar, a través del contrato inteligente y de acuerdo con la condición de consulta de datos, si la parte no cifrada comprendida en cada dato cifrado almacenado en la cadena de bloques satisface la condición de consulta de datos; si se satisface la condición de consulta de datos, usar los datos cifrados que contienen la parte no cifrada que satisface la condición de consulta de datos como datos a consultar; y si no se satisface la condición de consulta de datos, no utilizar ningún dato cifrado como datos a consultar.

En algunas realizaciones, cuando el único nodo de cadena de bloques tiene permiso para descifrar los datos que se van a consultar, el método comprende además: determinar, a través del contrato inteligente, un segundo valor correspondiente a los datos devueltos por el dispositivo de cifrado, utilizándose el segundo valor para representar un valor deducido de una cuenta del único nodo de cadena de bloques; y enviar, a través del contrato inteligente, el identificador de nodo de un nodo de cadena de bloques y el segundo valor a otros nodos de cadena de bloques asociados a la cadena de bloques para hacer que cada uno de los otros nodos de cadena de bloques almacene el identificador de nodo y el segundo valor en la cadena de bloques después de realizar la verificación del consenso en el identificador de nodo y el segundo valor con éxito.

En algunas realizaciones, cuando el único nodo de cadena de bloques tiene permiso para descifrar los datos que se van a consultar, el método comprende además: determinar, a través del contrato inteligente, un tercer valor correspondiente a los datos y los identificadores de nodo de otros nodos de cadena de bloques que comparten los datos, el tercer valor se utiliza para representar un valor añadido en las cuentas de los otros nodos de cadena de bloques que comparten los datos; y enviar, a través del contrato inteligente, los identificadores de nodo determinados y el tercer valor a los otros nodos de cadena de bloques para hacer que cada uno de los otros nodos de cadena de bloques almacene los identificadores de nodos determinados y el tercer valor en la cadena de bloques después de realizar la verificación de consenso en el nodo determinado identificadores y el tercer valor con éxito.

En algunas realizaciones, el método comprende además: enviar, por uno de los nodos de cadena de bloques asociados a una cadena de bloques, una solicitud de recarga a un dispositivo de recarga para hacer que el dispositivo de recarga determine un certificado de recarga de acuerdo con la solicitud de recarga y devuelva el certificado de recarga al único nodo de cadena de bloques; comprendiendo el certificado de recarga un cuarto valor y siendo usado el cuarto valor se usa para representar un valor añadido en una cuenta del único nodo de cadena de bloques; y enviar el identificador de nodo de un nodo de cadena de bloques y el certificado de recarga a otros nodos de cadena de bloques asociados a la cadena de bloques para hacer que cada uno de los otros nodos de cadena de bloques almacene el identificador de nodo y el cuarto valor en la cadena de bloques después de realizar la verificación de consenso en el identificador de nodo y el certificado de recarga con éxito.

Según otro aspecto, un medio de almacenamiento no transitorio legible por ordenado almacena instrucciones que, cuando son ejecutadas por un procesador de un nodo cadena de bloques, hacen que el procesador realice un método de almacenamiento de datos, comprendiendo el método: enviar datos a un dispositivo de cifrado para provocar el dispositivo de cifrado para cifrar los datos y devolver los datos cifrados al nodo de cadena de bloques; recibir los datos cifrados devueltos por el dispositivo de cifrado; y enviar los datos cifrados a otros nodos de cadena de bloques para hacer que cada uno de los otros nodos de cadena de bloques almacene los datos cifrados en la cadena de bloques después de realizar la verificación de consenso sobre los datos cifrados con éxito.

Un dispositivo de consulta de datos según algunas realizaciones de la presente descripción comprende uno o más procesadores y memorias. Las memorias almacenan programas que, cuando son ejecutados por uno o más procesadores, hacen que el dispositivo de consulta de datos realice las siguientes etapas: determinar los datos a consultar en datos cifrados almacenados en una cadena de bloques; determinar, a través de un contrato inteligente, si el nodo de cadena de bloques tiene permiso para descifrar los datos que se van a consultar; si el nodo de cadena de bloques tiene el permiso, enviar los datos que se van a consultar a un dispositivo de cifrado a través del contrato

inteligente para hacer que el dispositivo de cifrado descifre los datos que se van a consultar y devuelva los datos obtenidos del descifrado al nodo de cadena de bloques; si el nodo de cadena de bloques no tiene el permiso, se niega a enviar los datos para ser consultados al dispositivo de cifrado.

5 A partir de las soluciones técnicas anteriores de acuerdo con las realizaciones de la presente descripción, puede verse que se forma una red cadena de bloques con cada institución actuando como un nodo de cadena de bloques en algunas realizaciones de la presente descripción. Por un lado, cualquier nodo de cadena de bloques puede enviar sus propios datos a un dispositivo de cifrado para el cifrado, recibir datos cifrados retornados por el dispositivo de cifrado y luego transmitir los datos cifrados a otros nodos de cadena de bloques para hacer que cada uno de los
10 otros nodos de cadena de bloques almacene los datos cifrados. datos en la cadena de bloques después de realizar la verificación de consenso sobre los datos cifrados con éxito; por otro lado, con un contrato inteligente preestablecido en la cadena de bloques, los datos cifrados dentro del alcance del permiso de consulta del nodo de cadena de bloques se pueden enviar al dispositivo de cifrado para el descifrado, es decir, el nodo de cadena de bloques puede consultar datos dentro de su permiso. De acuerdo con algunas realizaciones de la presente
15 descripción, en primer lugar, los datos compartidos por los nodos de cadena de bloques se almacenan de manera distribuida en una cadena de bloques mantenida por los nodos de cadena de bloques y, en consecuencia, es difícil manipular los datos almacenados en la cadena de bloques, lo que conduce a una alta seguridad; En segundo lugar, los datos se cifran antes de ser almacenados en la cadena de bloques y si un nodo de cadena de bloques desea adquirir datos, debe verificar su permiso a través de un contrato inteligente, y se enviarán los datos cifrados que el
20 nodo de cadena de bloques tiene permiso para adquirir a un dispositivo de cifrado para el descifrado y finalmente serán devueltos al nodo cadena de bloques; en tercer lugar, cada nodo de cadena de bloques puede adquirir rápidamente datos de la cadena de bloques mantenida por sí misma, lo que mejora la eficiencia de la adquisición de datos.

25 Breve descripción de los dibujos

Para describir más claramente las soluciones técnicas de la presente descripción o la técnica anterior, los dibujos adjuntos que se utilizarán en la descripción de las realizaciones o la técnica anterior se describirán brevemente a continuación. Apparently, los dibujos adjuntos que se describen a continuación son simplemente algunas
30 realizaciones de la presente descripción. Un experto en la técnica puede obtener además otros dibujos según estos dibujos sin esfuerzo inventivo.

La figura 1 es un diagrama de flujo de un método de almacenamiento de datos según algunas realizaciones de la presente descripción;
35 la figura 2 es un diagrama de flujo de un método de cifrado de datos según algunas realizaciones de la presente descripción;
la figura 3 es un diagrama de flujo de un método de consulta de datos según algunas realizaciones de la presente descripción;
la figura 4 es un diagrama esquemático de una arquitectura de un sistema de consulta y almacenamiento de
40 datos de acuerdo con algunas realizaciones de la presente descripción;
la figura 5 es un diagrama esquemático de un aparato de almacenamiento de datos según algunas realizaciones de la presente descripción;
la figura 6 es un diagrama esquemático de un aparato de cifrado de datos según algunas realizaciones de la presente descripción;
45 la figura 7 es un diagrama esquemático de un aparato de consulta de datos según algunas realizaciones de la presente descripción;
la figura 8 es un diagrama esquemático de un dispositivo de almacenamiento de datos según algunas realizaciones de la presente descripción;
la figura 9 es un diagrama esquemático de un dispositivo de cifrado según algunas realizaciones de la presente
50 descripción;
la figura 10 es un diagrama esquemático de un dispositivo de consulta de datos según algunas realizaciones de la presente descripción.

Descripción detallada

55 Como se describe en los antecedentes, una plataforma de intercambio de datos existente puede, por un lado, recibir y almacenar datos cargados por varias instituciones y, por otro lado, proporcionar servicios de consulta de datos a las instituciones. Sin embargo, tal forma tiene dos problemas: uno, dado que los datos compartidos por las instituciones son almacenados por una plataforma centralizada de intercambio de datos, los datos consultados por
60 las instituciones desde la plataforma ya no serían fiables si alguien manipula maliciosamente los datos almacenados en la plataforma; en segundo lugar, la plataforma de intercambio de datos a menudo recibe simultáneamente solicitudes de consulta de datos enviadas desde múltiples instituciones, mientras que la plataforma de intercambio de datos tiene una capacidad limitada para procesar solicitudes de consulta de datos (es necesario realizar la verificación de permisos en cada institución que solicita la consulta de datos). Como tal, algunas instituciones necesitan esperar en una cola, la consulta de datos lleva un tiempo relativamente largo y la eficiencia de la consulta de datos es baja.

En algunas realizaciones de la presente descripción, en primer lugar, se forma una red de cadena de bloques con cada institución actuando como un nodo de cadena de bloques y los datos compartidos por los nodos de cadena de bloques se pueden almacenar, después de pasar la verificación de consenso por los nodos de cadena de bloques, en la cadena de bloques mantenida, respectivamente, por los nodos de cadena de bloques. De esa manera, sería difícil alterar o perder los datos almacenados en la cadena de bloques. En segundo lugar, si un nodo de cadena de bloques desea consultar datos compartidos por otros nodos de cadena de bloques, el nodo de cadena de bloques puede simplemente consultar los datos almacenados en la cadena de bloques mantenida por sí misma (los datos almacenados en la cadena de bloques mantenida por los nodos de cadena de bloques están sincronizados) y la eficiencia de consulta de datos se puede mejorar. En tercer lugar, para administrar el permiso de consulta de datos de los nodos de cadena de bloques, los datos se cifran mediante un dispositivo de cifrado antes de almacenarse en la cadena de bloques. Cualquier nodo de cadena de bloques puede adquirir los datos cifrados directamente desde cadena de bloques. Una vez que el nodo de cadena de bloques pasa una verificación de permisos sobre sí misma a través de un contrato inteligente, los datos cifrados se enviarán al dispositivo de cifrado para su descifrado y el nodo de cadena de bloques finalmente recibirá los datos de texto sin formato devueltos por el dispositivo de cifrado.

Para permitir que un experto en la técnica comprenda mejor las soluciones técnicas de la presente solicitud, las soluciones técnicas en las realizaciones de la presente descripción se describirán clara y completamente a continuación con referencia a los dibujos adjuntos en una o más realizaciones de la presente descripción. Aparentemente, las realizaciones descritas son simplemente algunas, en lugar de todas, las realizaciones de la presente descripción. Todas las demás realizaciones que pueda obtener un experto en la técnica sin esfuerzo inventivo sobre la base de las realizaciones de la presente descripción estarán dentro del alcance de la presente descripción.

Las soluciones técnicas en las realizaciones de la presente descripción se describirán con detalle a continuación con referencia a los dibujos adjuntos.

La figura 1 es un diagrama de flujo de un método de almacenamiento de datos según algunas realizaciones de la presente descripción, que comprende las etapas siguientes:

S100: enviar, mediante un nodo cadena de bloques asociado a una cadena de bloques, datos a un dispositivo de cifrado.

El flujo mostrado en la figura 1 es un flujo en el que un nodo de cadena de bloques almacena sus propios datos en una cadena de bloques (es decir, un flujo de datos compartidos).

En algunas realizaciones de la presente descripción, el nodo de cadena de bloques puede ser un servidor o un terminal, y en un ejemplo, puede ser un servidor de una institución que comparte sus propios datos (en la descripción siguiente, el nodo de cadena de bloques también puede ser un servidor de una institución que solicita consultar datos). Por ejemplo, si una empresa de alquiler de viviendas desea compartir una lista negra de clientes con retrasos con el alquiler con otras instituciones, un servidor de la empresa de alquiler de viviendas puede acceder a una cadena de bloques como un nodo de cadena de bloques y enviar la lista negra a un dispositivo de cifrado.

En algunas realizaciones de la presente descripción, el dispositivo de cifrado no es un nodo de cadena de bloques, sino un dispositivo para realizar el cifrado y descifrado de datos y proporcionar servicios públicos a todos los nodos de cadena de bloques. En algunas realizaciones, el dispositivo de cifrado puede utilizar un algoritmo de cifrado simétrico para cifrar los datos recibidos y descifrar los datos cifrados recibidos.

Cabe señalar que, como dispositivo de terceros, el dispositivo de cifrado tiene la función de utilizar un algoritmo de cifrado particular para cifrar los datos recibidos y de utilizar un algoritmo de descifrado simétrico al algoritmo de cifrado para descifrar los datos cifrados recibidos, mientras que ningún nodo de cadena de bloques es capaz de aprender el algoritmo de cifrado que utiliza el dispositivo de cifrado para cifrar y descifrar. En otras palabras, ningún nodo de cadena de bloques puede realizar el descifrado sin permiso de los datos cifrados almacenados en la cadena de bloques y mantenidos por sí mismo.

En resumen, si un nodo de cadena de bloques desea compartir sus propios datos en algunas realizaciones de la presente descripción, el nodo de cadena de bloques puede enviar los datos a un dispositivo cifrado para hacer que el dispositivo de cifrado cifre los datos recibidos y devuelva los datos cifrados al nodo de cadena de bloques.

S102: recibir los datos cifrados devueltos por el dispositivo de cifrado.

S104: enviar los datos cifrados a otros nodos de cadena de bloques asociados a la cadena de bloques.

Una vez que un nodo de cadena de bloques ha enviado los datos cifrados a otros nodos de cadena de bloques, los nodos de cadena de bloques pueden realizar una verificación de consenso sobre los datos cifrados. Si se pasa la verificación de consenso, los nodos de cadena de bloques guardan los datos cifrados en la cadena de bloques.

En algunas realizaciones, la verificación de consenso realizada sobre los datos cifrados es en realidad para realizar la verificación de consenso, de acuerdo con una firma de un nodo de cadena de bloques, sobre si se han manipulado o no una identidad y los datos cifrados del nodo de cadena de bloques. En un ejemplo, el nodo de cadena de bloques genera un resumen de los datos cifrados de acuerdo con los datos cifrados, genera una firma de acuerdo con el resumen mediante el uso de un algoritmo de firma (una clave privada del nodo de cadena de bloques) y luego envía los datos cifrados y la firma a otros nodos de cadena de bloques. Cada uno de los otros nodos de cadena de bloques que reciben los datos cifrados y la firma, por un lado, utilizará una clave pública del nodo de cadena de bloques para descifrar la firma (si el descifrado tiene éxito, indica que la firma realmente es generada por el nodo de cadena de bloques usando su clave privada) para obtener el resumen; por otro lado, generará un resumen según los datos cifrados recibidos y comparará el resumen obtenido del descifrado y el resumen generado. Si el resultado de la comparación es consistente, indica que los datos cifrados no han sido manipulados durante el proceso de transmisión. El método de verificación de consenso anterior es una verificación de legitimidad común en el campo de las tecnologías cadena de bloques y no se describirá con más detalle.

La razón por la que es necesario enviar datos cifrados (en lugar de datos originales) a otros nodos de cadena de bloques es porque un nodo de cadena de bloques no necesariamente tiene permiso para consultar todos los datos compartidos por otros nodos de cadena de bloques. Para controlar los permisos de consulta de datos de los nodos de cadena de bloques, los datos compartidos por un nodo de cadena de bloques deben cifrarse antes de que puedan transmitirse a otros nodos de cadena de bloques. En otras palabras, si los datos compartidos por un nodo de cadena de bloques se envían directamente a otros nodos de cadena de bloques sin cifrado, entonces todos los demás nodos de cadena de bloques adquieren los datos compartidos por el nodo de cadena de bloques y no será posible realizar el control de permisos, que se describirán con más detalle a continuación.

La figura 2 es un diagrama de flujo de un método de cifrado de datos según algunas realizaciones de la presente descripción, que comprende las etapas siguientes:

S200: recibir, mediante un dispositivo de cifrado, los datos enviados por un nodo cadena de bloques.

S202: cifrar una parte de los datos.

S204: devolver los datos cifrados al nodo cadena de bloques.

En algunas realizaciones de la presente descripción, el dispositivo de cifrado recibe datos enviados por un nodo de cadena de bloques y luego solo cifra una parte de los datos. Esto se debe a que, además de los datos que tienen el valor de compartir, los datos compartidos por un nodo de cadena de bloques generalmente comprenden además información explicativa (por ejemplo, categorías de datos, fuentes, resúmenes y similares). Por ejemplo, con respecto a los datos de una lista negra de clientes en mora con el alquiler compartido por una empresa de alquiler de viviendas, los nombres de los clientes, la información de contacto y los números de identificación en la lista negra son los datos con valor, mientras que el nombre y el código de la institución de la empresa de alquiler de viviendas son información explicativa.

Por lo tanto, hay algunos datos en los datos compartidos por un nodo de cadena de bloques que tienen que ser confidenciales con otros nodos de cadena de bloques. Por lo tanto, el dispositivo de cifrado solo necesita cifrar una parte de los datos recibidos. Además, cifrar una parte de los datos facilita la consulta de datos por parte de los nodos de cadena de bloques, que se describirá más adelante. Para facilitar la descripción, la parte cifrada de cada dato cifrado se denominará datos de transacción y la parte no cifrada de cada dato cifrado se denominará en lo sucesivo datos que no son de transacción.

Al recibir los datos cifrados, el nodo de cadena de bloques puede ejecutar la etapa S104 anterior, es decir, enviar los datos cifrados a otros nodos de cadena de bloques asociados a la cadena de bloques para la verificación del consenso y luego hacer que cada uno de los otros nodos de cadena de bloques almacene los datos cifrados en la cadena de bloques después de realizar la verificación de consenso en los datos cifrados con éxito.

La figura 3 es un diagrama de flujo de un método de adquisición de datos según algunas realizaciones de la presente descripción, que comprende las etapas siguientes:

S300: determinar, mediante un nodo de cadena de bloques (por ejemplo, uno de los nodos de cadena de bloques asociados a una cadena de bloques), los datos que se van a consultar en datos cifrados almacenados en una cadena de bloques.

El flujo mostrado en la figura 3 es un flujo en el que un nodo de cadena de bloques consulta los datos en una cadena de bloques y los datos consultados por un nodo de cadena de bloques a menudo son almacenados por otros nodos de cadena de bloques en la cadena de bloques en el flujo que se muestra en la figura 1.

En algunas realizaciones de la presente descripción, si los datos cifrados almacenados en la cadena de bloques están parcialmente cifrados (los datos cifrados se pueden obtener a través del flujo que se muestra en la figura 2), entonces, un nodo de cadena de bloques que desee consultar los datos puede seleccionar datos que quiere

consultar (a los que se hace referencia en este documento como datos que se van a consultar) de acuerdo con la parte no cifrada de cada dato cifrado (datos que no son de transacción) almacenados en la cadena de bloques. Aparentemente, los datos de la transacción en los datos que se van a consultar están cifrados y los datos que el nodo de cadena de bloques desea consultar se obtendrán solo después del cifrado por un dispositivo de cifrado.

Además, el nodo de cadena de bloques también puede determinar una condición de consulta de datos; determinar, a través de un contrato inteligente y según la condición de consulta de datos, si la parte no cifrada comprendida en cada dato cifrado almacenado en la cadena de bloques satisface la condición de consulta de datos; si se satisface la condición de consulta de datos, utilizar los datos cifrados como los datos cifrados a consultar; si no se cumple la condición de consulta de datos, no utilizar los datos cifrados como los datos cifrados a consultar. En algunas realizaciones, la condición de consulta de datos puede ser una palabra clave comprendida en los datos a consultar según lo determinado por el nodo de cadena de bloques, la fuente de datos, el campo al que pertenecen los datos y similares. Por ejemplo, si un banco desea adquirir los registros de compra de vivienda de un cliente, el banco puede realizar una búsqueda con una palabra clave "registro de compra de vivienda", que puede recuperar datos que no son transacciones que contienen la palabra clave anterior y los datos cifrados que comprenden los datos de no transacción recuperados son los datos que se van a consultar.

Se sabe en el campo de las tecnologías cadena de bloques que un contrato inteligente puede ser esencialmente un código que se puede activar y ejecutar. Por lo general, está preestablecido en una cadena de bloques y es difícil manipular un contrato inteligente almacenado en una cadena de bloques. Por lo tanto, el contrato inteligente se puede utilizar para ejecutar una lógica de código preestablecida y los nodos de cadena de bloques no interfieren en el proceso de ejecución. En algunas realizaciones de la presente descripción, un contrato inteligente se usa en una pluralidad de etapas diferentes para ejecutar diferentes lógicas de código, en el que las diferentes lógicas de código pueden ser ejecutadas por diferentes contratos inteligentes o por el mismo contrato inteligente, que no está limitado en el presente documento. En resumen, el papel de un contrato inteligente es garantizar que las cadena de bloques ejecuten lógicas de código preestablecidas y evitar que las cadena de bloques funcionen con maldad.

S302: determinar, mediante un contrato inteligente, si el nodo de cadena de bloques tiene permiso o no para descifrar los datos que se van a consultar; si el nodo de cadena de bloques tiene el permiso, continuar con la etapa S304; si el nodo de cadena de bloques no tiene el permiso, se procede a la etapa S306.

En algunas realizaciones de la presente descripción, la información de atributos de los datos que se van a consultar se puede determinar a través de un contrato inteligente de acuerdo con los datos que no son de transacción incluidos en los datos que se van a consultar, y luego se determina si la información de atributos que tiene el nodo de cadena de bloques un permiso para consultar comprende información de atributos de los datos que se van a consultar; si es así, el nodo de cadena de bloques tiene permiso para descifrar los datos que se van a consultar; de lo contrario, el nodo de cadena de bloques no tiene permiso para descifrar los datos que se van a consultar.

En algunas realizaciones, la información de atributos de los datos que se van a consultar puede ser información tal como la fuente de los datos que se van a consultar, la categoría de los datos y similares, todos los cuales se pueden determinar de acuerdo con los datos que no son de transacción incluidos en los datos que se van a consultar. La información de atributos que el nodo cadena de bloques tiene permiso para consultar es información de atributos de datos preestablecidos que el nodo de cadena de bloques tiene permiso para consultar.

S304: enviar los datos a consultar a un dispositivo de cifrado a través del contrato inteligente.

Si el nodo de cadena de bloques tiene permiso para descifrar los datos que se van a consultar, el nodo de cadena de bloques puede enviar los datos a consultar a un dispositivo de cifrado a través del contrato inteligente para hacer que el dispositivo de cifrado descifre los datos que se consultarán y devuelva los datos obtenidos de el descifrado al nodo de cadena de bloques. Como tal, el nodo de cadena de bloques obtiene los datos de texto sin formato que desea.

S306: rechazar el envío de los datos a consultar al dispositivo de cifrado.

Según el método de almacenamiento de datos mostrado en la figura 1 y el método de cifrado de datos mostrado en la figura 2 y el método de consulta de datos mostrado en la figura 3, se puede ver que, en primer lugar, los datos compartidos por los nodos de cadena de bloques se almacenan de manera distribuida en una cadena de bloques mantenida respectivamente por los nodos de cadena de bloques y, en consecuencia, es difícil manipular los datos almacenados en la cadena de bloques, lo que conduce a una alta seguridad; en segundo lugar, los datos se cifran antes de almacenarse en la cadena de bloques, y si un nodo de cadena de bloques desea adquirir datos, su permiso debe verificarse a través de un contrato inteligente, y los datos cifrados que el nodo de cadena de bloques tiene permiso para adquirir se enviarán a un dispositivo de cifrado para descifrar y finalmente se devolverán al nodo de cadena de bloques; en tercer lugar, cada nodo de cadena de bloques puede consultar rápidamente datos de la cadena de bloques mantenida por sí misma, lo que mejora la eficiencia de la consulta de datos.

Además, para alentar a las instituciones a compartir datos, se puede introducir un mecanismo de intercambio de

datos en los flujos que se muestran en la figura 1 y la figura 3.

En un ejemplo, cuando un nodo de cadena de bloques comparte datos en el flujo mostrado en la figura 1, el nodo de cadena de bloques puede determinar un primer valor correspondiente a los datos a través de un contrato inteligente y luego enviar el identificador del nodo del nodo de cadena de bloques y el primer valor a otros nodos de cadena de bloques para hacer que el identificador de nodo y el primer valor se almacenen en la cadena de bloques después de haber pasado una verificación de consenso sobre el identificador de nodo y el primer valor de los nodos de cadena de bloques.

En algunas realizaciones, el primer valor puede usarse para representar un valor añadido en la cuenta del nodo de cadena de bloques. En otras palabras, el primer valor es en realidad un premio obtenido por el nodo cadena de bloques por compartir los datos. El primer valor debe determinarse mediante un contrato inteligente para evitar que un nodo cadena de bloques fabrique el primer valor sin autorización. Diferentes datos pueden corresponder a diferentes primeros valores, que pueden predeterminarse en el contrato inteligente según las necesidades.

Cabe destacar que, en el flujo mostrado en la figura 1, un nodo de cadena de bloques también puede determinar el primer valor antes de enviar los datos cifrados a otros nodos de cadena de bloques para la verificación del consenso y, a continuación, transmitir su propio identificador de nodo, el primer valor y los datos cifrados juntos a otros nodos de cadena de bloques para la verificación del consenso. En resumen, además de los datos compartidos, un identificador de nodo del nodo de cadena de bloques que comparte datos y el primer valor también se puede almacenar en una cadena de bloques como evidencia y para su publicación si pasan la verificación del consenso, lo que equivale a un aumento de saldo de la cuenta del nodo de cadena de bloques. El nodo de cadena de bloques puede usar el saldo de su cuenta para el consumo para intercambiar datos compartidos por otros nodos de cadena de bloques. Como tales, los nodos de cadena de bloques en una red de cadena de bloques forman un mecanismo comercial que fomenta el intercambio de datos.

De manera correspondiente, cuando un nodo de cadena de bloques desea adquirir datos compartidos por otros nodos de cadena de bloques en el flujo mostrado en la figura 3, el nodo de cadena de bloques puede determinar, a través de un contrato inteligente, un segundo valor correspondiente a los datos; enviar el identificador de nodo del nodo de cadena de bloques y el segundo valor a otros nodos de cadena de bloques para hacer que cada uno de los otros nodos de cadena de bloques almacene el identificador de nodo y el segundo valor en la cadena de bloques después de realizar la verificación de consenso en el identificador de nodo y el segundo valor con éxito.

En algunas realizaciones, el segundo valor puede usarse para representar un valor deducido de la cuenta del nodo de cadena de bloques. En otras palabras, el segundo valor se puede considerar como gastos para consultar los datos por el nodo de cadena de bloques. El segundo valor correspondiente a los datos también debe determinarse mediante un contrato inteligente. Los gastos realizados por el nodo de cadena de bloques se pueden deducir del saldo de su cuenta. El nodo de cadena de bloques puede transmitir su propio identificador de nodo y el segundo valor a otros nodos de cadena de bloques para la verificación del consenso. Si se pasa la verificación del consenso, el identificador de nodo del nodo de cadena de bloques que adquiere los datos y el segundo valor también se almacenarán en una cadena de bloques como evidencia y para su publicación.

Por tanto, una cadena de bloques no solo almacena datos compartidos por instituciones, sino que también publica registros de premios o gastos de las instituciones. Al verificar los registros de transacciones en la cadena de bloques, se puede determinar un saldo de cuenta para cada institución.

Además, el nodo de cadena de bloques que adquiere los datos puede determinar, a través de un contrato inteligente, un tercer valor correspondiente a los datos y los identificadores de nodo de otros nodos de cadena de bloques que comparten los datos; a continuación, envía los identificadores de nodo determinados y el tercer valor a otros nodos de cadena de bloques para hacer que cada uno de los otros nodos de cadena de bloques almacene los identificadores de nodos determinados y el tercer valor en la cadena de bloques después de realizar la verificación del consenso en los identificadores de nodos determinados y el tercer valor con éxito.

En algunas realizaciones, el tercer valor puede usarse para representar un valor añadido en las cuentas de otros nodos de cadena de bloques que comparten los datos. En otras palabras, el tercer valor puede considerarse como un premio para un nodo de cadena de bloques porque se consultan los datos compartidos por el nodo de cadena de bloques.

En algunas realizaciones de la presente descripción, además, el nodo de cadena de bloques puede enviar una solicitud de recarga a un dispositivo de recarga para hacer que el dispositivo de recarga determine un certificado de recarga de acuerdo con la solicitud de recarga y devuelva el certificado de recarga al nodo de cadena de bloques; el certificado de recarga comprende un cuarto valor y el cuarto valor puede usarse para representar un valor añadido en la cuenta del nodo de cadena de bloques; el nodo de cadena de bloques puede enviar su propio identificador de nodo y el certificado de recarga a otros nodos de cadena de bloques para hacer que cada uno de los otros nodos de cadena de bloques almacene el identificador de nodo y el cuarto valor en la cadena de bloques después de realizar la verificación del consenso en el identificador de nodo y el certificado de recarga con éxito.

En algunas realizaciones, el nodo de cadena de bloques puede enviar el cuarto valor a otros nodos de cadena de bloques para hacer que cada uno de los otros nodos de cadena de bloques compare el cuarto valor recibido y el cuarto valor contenido en el certificado de recarga; si son consistentes, se pasa la verificación. También es factible que el nodo de cadena de bloques no envíe el cuarto valor a otros nodos de cadena de bloques y los nodos de cadena de bloques pueden almacenar directamente el cuarto valor contenido en el certificado de recarga en la cadena de bloques.

Para poder continuar adquiriendo datos cuando un nodo de cadena de bloques no tiene suficiente saldo en su cuenta, el nodo de cadena de bloques puede recargar su cuenta, y el resultado de la recarga también se puede almacenar en una cadena de bloques como evidencia después de pasar la verificación del consenso realizada por los nodos de cadena de bloques.

En algunas realizaciones, el dispositivo de recarga no es un nodo de cadena de bloques, sino que es un dispositivo responsable de procesar y resolver una solicitud de recarga de un nodo de cadena de bloques y emitir un certificado de recarga.

La figura 4 es un diagrama esquemático de una arquitectura de un sistema de consulta y almacenamiento de datos de acuerdo con algunas realizaciones de la presente descripción. Como se muestra en la figura 4, los servidores de las instituciones A a C actúan como nodos de cadena de bloques y forman una red de cadena de bloques. El servidor de cada institución mantiene una cadena de bloques y el servidor de cada institución puede compartir datos en la cadena de bloques o consultar datos de la cadena de bloques. En la arquitectura mostrada en la figura 4, además, hay un dispositivo de cifrado de terceros y un dispositivo de recarga. El dispositivo de cifrado está configurado para cifrar y descifrar datos para evitar que una institución descifre datos en la cadena de bloques sin autorización; el dispositivo de recarga está configurado para emitir un certificado de recarga al servidor de una institución que compra el cuarto valor.

Según el método de almacenamiento de datos mostrado en la figura 1, algunas realizaciones de la presente descripción proporcionan correspondientemente un aparato de almacenamiento de datos, como se muestra en la figura 5, que comprende:

- un primer módulo 501 de envío configurado para enviar datos a un dispositivo de cifrado para hacer que el dispositivo de cifrado cifre los datos recibidos y devuelva los datos cifrados al nodo de cadena de bloques;
- un módulo 502 de recepción configurado para recibir los datos cifrados devueltos por el dispositivo de cifrado;
- un segundo módulo 503 de envío configurado para enviar los datos cifrados a otros nodos de cadena de bloques para hacer que cada uno de los otros nodos de cadena de bloques almacene los datos cifrados en la cadena de bloques después de realizar la verificación del consenso sobre los datos cifrados con éxito.

El aparato comprende además: un módulo 504 de procesamiento configurado para determinar un primer valor correspondiente a los datos a través de un contrato inteligente, utilizándose el primer valor para representar un valor añadido en la cuenta del aparato; enviar su propio identificador de nodo y el primer valor a otros nodos de cadena de bloques para hacer que el identificador de nodo y el primer valor se almacenen en el cadena de bloques después de una verificación de consenso sobre el identificador de nodo y el primer valor de los nodos de cadena de bloques que han pasado.

Los diversos módulos y unidades del aparato de almacenamiento de datos pueden implementarse como instrucciones de software. Es decir, el aparato de almacenamiento de datos puede comprender un procesador y un medio de almacenamiento no transitorio legible por ordenador que almacena instrucciones que, cuando son ejecutadas por el procesador, hacen que el aparato de almacenamiento de datos realice varias etapas y métodos de los módulos y unidades descritos anteriormente. En algunas realizaciones, el aparato de almacenamiento de datos puede incluir un ordenador, un servidor, un teléfono móvil, una libreta, etc. En algunas realizaciones, el aparato de almacenamiento de datos puede actuar como un nodo de cadena de bloques.

Según el método de cifrado de datos mostrado en la figura 2, algunas realizaciones de la presente descripción proporcionan correspondientemente un aparato de cifrado de datos, como se muestra en la figura 6, que comprende:

- un módulo 601 de recepción configurado para recibir datos enviados por un nodo de cadena de bloques;
- un módulo 602 de cifrado configurado para cifrar una parte de los datos;
- un módulo 603 de retorno configurado para devolver los datos cifrados al nodo de cadena de bloques para hacer que el nodo de cadena de bloques envíe los datos cifrados a otros nodos de cadena de bloques para la verificación del consenso y luego hacer que cada uno de los otros nodos de cadena de bloques almacene los datos cifrados en la cadena de bloques después de realizar verificación del consenso sobre los datos cifrados con éxito.

Los diversos módulos y unidades del aparato de cifrado de datos pueden implementarse como instrucciones de software. Es decir, el aparato de cifrado de datos puede comprender un procesador y un medio de almacenamiento

no transitorio legible por ordenador que almacena instrucciones que, cuando son ejecutadas por el procesador, hacen que el aparato de cifrado de datos realice varias etapas y métodos de los módulos y unidades descritos anteriormente. En algunas realizaciones, el aparato de cifrado de datos puede incluir un ordenador, un servidor, un teléfono móvil, una libreta, etc.

5 Según el método de consulta de datos mostrado en la figura 3, algunas realizaciones de la presente descripción proporcionan correspondientemente un aparato de cifrado de datos, como se muestra en la figura 7, que comprende:

- 10 un módulo 701 de determinación configurado para determinar datos a consultar en datos cifrados almacenados en una cadena de bloques;
- un módulo 702 de determinación y procesamiento configurado para determinar, a través de un contrato inteligente, si el aparato tiene permiso para descifrar los datos que se van a consultar; si el nodo de cadena de bloques tiene el permiso, enviar los datos que se van a consultar a un dispositivo de cifrado a través del contrato inteligente para hacer que el dispositivo de cifrado descifre los datos que se van a consultar y devuelva los datos
- 15 obtenidos del descifrado al aparato; si el nodo de cadena de bloques no tiene el permiso, rechazar el envío de los datos que se van a consultar al dispositivo de cifrado.

Cada dato cifrado almacenado en la cadena de bloques comprende una parte no cifrada.

- 20 El módulo 701 de determinación está configurado para determinar una condición de consulta de datos; determinar, a través de un contrato inteligente y según la condición de consulta de datos, si la parte no cifrada comprendida en cada dato cifrado almacenado en la cadena de bloques satisface la condición de consulta de datos; si se cumple la condición de consulta de datos, utilizar los datos cifrados como datos a consultar; si no se cumple la condición de consulta de datos, no utilizar los datos cifrados como datos a consultar.

- 25 El aparato comprende además: un primer módulo 703 de procesamiento configurado para, cuando el nodo de cadena de bloques tiene permiso para descifrar los datos que se van a consultar, determinar, a través de un contrato inteligente, un segundo valor correspondiente a los datos devueltos por el dispositivo de cifrado, utilizándose el segundo valor para representar un valor deducido de la cuenta del nodo de cadena de bloques; enviar, a través del contrato inteligente, el identificador de nodo del nodo de cadena de bloques y el segundo valor a otros nodos de
- 30 cadena de bloques para hacer que cada uno de los otros nodos de cadena de bloques almacene el identificador de nodo y el segundo valor en la cadena de bloques después de realizar la verificación del consenso en el identificador de nodo y el segundo valor con éxito.

- 35 El aparato comprende además: un segundo módulo 704 de procesamiento configurado para, cuando el nodo de cadena de bloques tiene permiso para descifrar los datos que se van a consultar, determinar, a través de un contrato inteligente, un tercer valor correspondiente a los datos y los identificadores de nodo de otros nodos de cadena de bloques que comparten los datos, utilizándose el tercer valor para representar un valor añadido en las cuentas de otros nodos de cadena de bloques que comparten los datos; enviar, a través del contrato inteligente, los
- 40 identificadores de nodo determinados y el tercer valor a otros nodos de cadena de bloques para hacer que cada uno de los otros nodos de cadena de bloques almacene los identificadores de nodos determinados y el tercer valor en la cadena de bloques después de realizar la verificación del consenso en los identificadores de nodos determinados y el tercer valor con éxito.

- 45 El aparato comprende además: un tercer módulo 705 de procesamiento configurado para enviar una solicitud de recarga a un dispositivo de recarga para hacer que el dispositivo de recarga determine un certificado de recarga de acuerdo con la solicitud de recarga y devuelva el certificado de recarga al nodo de cadena de bloques; comprendiendo el certificado de recarga un cuarto valor y utilizándose el cuarto valor para representar un valor
- 50 añadido en la cuenta del nodo de cadena de bloques; enviar su propio identificador de nodo y el certificado de recarga a otros nodos de cadena de bloques para hacer que cada uno de los otros nodos de cadena de bloques almacene el identificador de nodo y el cuarto valor en la cadena de bloques después de realizar la verificación del consenso en el identificador de nodo y el certificado de recarga con éxito.

- Los diversos módulos y unidades del aparato de consulta de datos pueden implementarse como instrucciones de
- 55 software. Es decir, el aparato de consulta de datos puede comprender un procesador y un medio de almacenamiento no transitorio legible por ordenador que almacena instrucciones que, cuando son ejecutadas por el procesador, hacen que el aparato de consulta de datos realice varias etapas y métodos de los módulos y unidades descritos anteriormente. En algunas realizaciones, el aparato de consulta de datos puede incluir un ordenador, un servidor, un teléfono móvil, una libreta, etc. En algunas realizaciones, el aparato de almacenamiento de datos puede actuar como
- 60 un nodo de cadena de bloques.

- Según el método de almacenamiento de datos mostrado en la figura 1, algunas realizaciones de la presente descripción proporcionan de forma correspondiente un dispositivo de almacenamiento de datos mostrado en la figura
- 8, que comprende uno o más procesadores y memorias, en el que las memorias almacenan programas y están
- 65 configuradas para ejecutar las siguientes etapas por uno o más procesadores:

enviar datos a un dispositivo de cifrado para hacer que el dispositivo de cifrado cifre los datos recibidos y devuelva los datos cifrados al nodo de cadena de bloques; recibir los datos cifrados devueltos por el dispositivo de cifrado;

- 5 enviar los datos cifrados a otros nodos de cadena de bloques para hacer que cada uno de los otros nodos de cadena de bloques almacene los datos cifrados en la cadena de bloques después de realizar la verificación de consenso sobre los datos cifrados con éxito.

Según el método de almacenamiento de datos mostrado en la figura 1, algunas realizaciones de la presente descripción proporcionan de forma correspondiente un dispositivo de almacenamiento de datos mostrado en la figura 9, que comprende uno o más procesadores y memorias, en el que las memorias almacenan programas y están configuradas para ejecutar las siguientes etapas por uno o más procesadores:

- 15 recibir datos enviados por un nodo de cadena de bloques;
cifrar una parte de los datos;
devolver los datos cifrados al nodo de cadena de bloques para hacer que el nodo de cadena de bloques envíe los datos cifrados a otros nodos de cadena de bloques para la verificación del consenso y luego hacer que cada uno de los otros nodos de cadena de bloques almacene los datos cifrados en la cadena de bloques después de realizar la verificación de consenso en los datos cifrados con éxito.

- 20 Según el método de consulta de datos mostrado en la figura 2, algunas realizaciones de la presente descripción proporcionan de forma correspondiente un dispositivo de consulta de datos mostrado en la figura 10, que comprende uno o más procesadores y memorias, en el que las memorias almacenan programas y están configuradas para ejecutar las siguientes etapas por uno o más procesadores:

- 25 determinar los datos a consultar en datos cifrados almacenados en una cadena de bloques;
determinar, a través de un contrato inteligente, si el nodo de cadena de bloques tiene permiso para descifrar los datos que se van a consultar;
si el nodo de cadena de bloques tiene el permiso, enviar los datos que se van a consultar a un dispositivo de cifrado a través del contrato inteligente para hacer que el dispositivo de cifrado descifre los datos que se van a consultar y devuelva los datos obtenidos del descifrado al nodo de cadena de bloques;
30 si el nodo de cadena de bloques no tiene el permiso, se niega a enviar los datos para ser consultados al dispositivo de cifrado.

- 35 Las realizaciones en la presente descripción se describen de una manera progresiva con cada realización enfocada en las diferencias de otras realizaciones y las realizaciones pueden ser referenciadas mutuamente para partes idénticas o similares. Para los dispositivos mostrados en las figuras 8-10, en particular, la descripción de los mismos es relativamente simple ya que son sustancialmente similares a las realizaciones del método. Se puede hacer referencia a la descripción de las realizaciones del método para partes relacionadas del mismo.

- 40 En la década de 1990, una mejora de una tecnología se puede diferenciar en una mejora de hardware (por ejemplo, una mejora de la estructura de un circuito, tal como un diodo, un transistor, un interruptor, y similares) o una mejora de software (una mejora de un flujo de un método). Sin embargo, con el desarrollo tecnológico, muchas de las mejoras actuales de los flujos de métodos pueden considerarse mejoras directas de las estructuras de hardware. Los diseñadores casi siempre obtienen una estructura de circuito de hardware correspondiente
45 programando un flujo de método mejorado en un circuito de hardware. Por lo tanto, no se puede concluir que no se pueda realizar una mejora en el flujo de un método con un módulo de hardware. Por ejemplo, el dispositivo lógico programable (PLD) (por ejemplo, la matriz de puertas programables en campo (FPGA)) es un circuito integrado tal que sus funciones lógicas las determina un usuario mediante la programación del dispositivo. Un diseñador programa por sí mismo para "integrar" un sistema digital en una pieza de PLD, sin necesidad de pedirle a un fabricante de chips que diseñe y fabrique un chip IC exclusivo. En la actualidad, además, este tipo de programación se ha implementado principalmente a través de software de "compilador lógico", en lugar de fabricar manualmente los chips IC. El software del compilador lógico es similar a un compilador de software utilizado para el desarrollo y la escritura de programas, mientras que se debe utilizar un lenguaje de programación particular para escribir códigos fuente antes de la compilación, que se conoce como lenguaje de descripción de hardware (HDL). No hay solo uno,
50 sino muchos tipos de HDL, tales como ABEL (lenguaje de expresiones booleanas avanzadas), AHDL (lenguaje de descripción de hardware Altera), Confluence, CUPL (lenguaje de programación de la Universidad de Cornell), HDCal, JHDL (lenguaje de descripción de hardware Java), Lava, Lola, MyHDL, PALASM, RHDH (lenguaje de descripción de hardware Ruby). Los que se utilizan con más frecuencia en este momento incluyen VHDL (lenguaje de descripción de hardware de circuitos integrados de muy alta velocidad) y Verilog. Un experto en la técnica también debería saber que sería muy fácil obtener un circuito de hardware para implementar un flujo de método lógico utilizando los HDL anteriores para llevar a cabo una ligera programación lógica en el flujo de método y programarlo en un IC.

- 65 Un controlador puede implementarse de cualquier manera adecuada. Por ejemplo, un controlador puede estar en, por ejemplo, una forma de microprocesador o procesador, así como un medio legible por ordenador que almacena códigos de programa legibles por ordenador (por ejemplo, software o firmware) capaces de ser ejecutados por el

(micro)procesador, una puerta lógica, un interruptor, un circuito integrado de aplicación específica (ASIC), un controlador lógico programable y un microcontrolador integrado. Los ejemplos del controlador incluyen, pero sin limitaciones, los siguientes microcontroladores: ARC 625D, Atmel AT91SAM, Microchip PIC18F26K20 y Silicone Labs C8051F320. Un controlador de memoria puede implementarse además como parte de una lógica de control de una memoria. Un experto en la técnica también debería ser consciente de que, además de que un controlador se implementa en una forma de códigos de programa legibles por ordenador, es totalmente factible realizar la programación lógica en las etapas de un método para permitir que un controlador implemente las mismas funciones en forma de puerta lógica, interruptor, ASIC, controlador lógico programable y microcontrolador integrado. Por lo tanto, dicho controlador puede considerarse como una parte de hardware, mientras que los aparatos comprendidos en él y configurados para llevar a cabo diversas funciones también pueden considerarse como una estructura dentro de la parte de hardware. Como alternativa, los aparatos configurados para lograr diversas funciones pueden incluso considerarse como módulos de software para implementar un método y una estructura dentro de una parte de hardware.

El sistema, aparato, módulo o unidad descrito en las realizaciones anteriores puede implementarse, por ejemplo, mediante un chip o entidad de ordenador, o implementarse mediante un producto que tiene una función. Un dispositivo de implementación típico es un ordenador. En un ejemplo, un ordenador puede ser, por ejemplo, un ordenador personal, un ordenador portátil, un teléfono móvil, un teléfono con cámara, un teléfono inteligente, un asistente digital personal, un reproductor multimedia, un dispositivo de navegación, un dispositivo de correo electrónico, un consola de juegos, una tableta, un dispositivo portátil o una combinación de cualquier dispositivo en estos dispositivos.

Por conveniencia de la descripción, el aparato anterior se divide en varias unidades de acuerdo con las funciones para la descripción. Las funciones de las unidades pueden implementarse en una o más piezas de software y/o hardware cuando se implementa la presente descripción.

Un experto en la técnica debe entender que las realizaciones de la presente invención pueden proporcionarse como un método, un sistema o un producto de programa informático. Por lo tanto, la presente invención puede implementarse como una realización completa de hardware, una realización completa de software o una realización que combine software y hardware. Además, la presente invención puede estar en forma de un producto de programa informático implementado en uno o más medios de almacenamiento usables por ordenador (que incluyen, pero sin limitación, una memoria de disco magnético, CD-ROM, una memoria óptica, y similares) que comprende códigos de programa usables por ordenador.

La presente invención se describe con referencia a diagramas de flujo y/o diagramas de bloques del método, dispositivo (sistema), y producto de programa informático de acuerdo con las realizaciones de la presente invención. Puede usarse una instrucción de programa informático para implementar cada proceso y/o bloque en los diagramas de flujo y/o diagramas de bloques y una combinación de procesos y/o bloques en los diagramas de flujo y/o diagramas de bloques. Estas instrucciones de programa informático pueden proporcionarse para un ordenador de uso general, un ordenador de fin especial, un procesador embebido, o un procesador de otros dispositivos de procesamiento de datos programables para generar una máquina, que hace que las instrucciones ejecutadas por un ordenador o un procesador de otros dispositivos de procesamiento de datos programables generen un aparato para implementar una función especificada en uno o más procesos en los diagramas de flujo y/o en uno o más bloques en los diagramas de bloques.

Estas instrucciones de programa informático pueden almacenarse también en una memoria legible por ordenador que puede dar instrucciones a un ordenador u otros dispositivos de procesamiento de datos programables para funcionar de una manera particular, de modo que las instrucciones almacenadas en la memoria legible por ordenador generen un artículo fabricado que incluye un aparato de instrucción. El aparato de instrucción implementa una función especificada en uno o más procesos en los diagramas de flujo y/o en uno o más bloques en los diagramas de bloques.

Estas instrucciones de programa informático pueden cargarse también en un ordenador u otros dispositivos de procesamiento de datos programables para hacer que una serie de etapas operacionales en el ordenador u otros dispositivos programables generen procesamiento implementado por ordenador. Por lo tanto, las instrucciones ejecutadas en el ordenador u otros dispositivos programables proporcionan etapas para implementar una función especificada en uno o más procesos en los diagramas de flujo y/o en uno o más bloques en los diagramas de bloques.

En una configuración típica, el dispositivo informático incluye uno o más procesadores (CPU), interfaces de entrada/salida, interfaces de red y una memoria.

La memoria puede incluir un medio legible por ordenador, tal como una memoria volátil, una Memoria de Acceso Aleatorio (RAM), y/o una memoria no volátil, por ejemplo, una Memoria de Sólo Lectura (ROM) o una RAM flash. La memoria es un ejemplo de un medio legible por ordenador.

Medios legibles por ordenador incluyen medios permanentes, volátiles, móviles e inmóviles, que pueden implementar almacenamiento de información a través de cualquier método o tecnología. La información pueden ser instrucciones legibles por ordenador, estructuras de datos, módulos de programa u otros datos. Los ejemplos de medios de almacenamiento de ordenadores incluyen, pero sin limitaciones, RAM de cambio de fase (PRAM), RAM estáticas (SRAM), RAM dinámicas (DRAM), otros tipos de memorias de acceso aleatorio (RAM), memorias de solo lectura (ROM), memorias de solo lectura programables y borrables eléctricamente (EEPROM), memorias flash u otras tecnologías de memoria, memorias de disco compacto de solo lectura (CD-ROM), discos versátiles digitales (DVD) u otras memorias ópticas, casetes, memorias de casete y disco u otros dispositivos de memoria magnética, o cualquier otro medio que no sea de transmisión que pueda usarse para almacenar información accesible a un dispositivo de computación. De acuerdo con las definiciones en el presente documento, el medio legible por ordenador no incluye medios transitorios, tales como señales de datos moduladas y portadoras.

Debe indicarse adicionalmente que los términos "que incluye", "que comprende", o cualesquiera otras variantes de los mismos se pretende que abarquen una inclusión no exclusiva, que hacen un proceso, método, producto o dispositivo que comprende una serie de elementos que no comprenden únicamente estos elementos, sino que también comprenden otros elementos que no están claramente enumerados, o comprenden adicionalmente elementos que son inherentes al proceso, método, producto o dispositivo. Cuando no hay ninguna restricción adicional, los elementos definidos por la declaración "que comprende uno ..." no excluyen que un proceso, método, producto básico o dispositivo que comprende los elementos anteriores comprenda además elementos idénticos adicionales.

Un experto en la materia debe entender que las realizaciones de la presente invención pueden proporcionarse como un método, un sistema o un producto de programa informático. Por lo tanto, la presente descripción puede implementarse como una realización de hardware completa, una realización de software completa o una realización que combina software y hardware. Además, la presente descripción puede estar en forma de un producto de programa informático implementado en uno o más medios de almacenamiento usables por ordenador (que incluyen, pero sin limitación, una memoria de disco magnético, CD-ROM, una memoria óptica, etc.) que comprende códigos de programa usables por ordenador.

La presente descripción puede describirse en un contexto regular de una instrucción ejecutable por ordenador que es ejecutada por un ordenador, tal como un módulo de programa. Generalmente, el módulo de programa comprende una rutina, un programa, un objeto, un componente, una estructura de datos y similares para ejecutar una tarea particular o implementar un tipo de datos abstracto particular. La presente descripción también se puede poner en práctica en entornos informáticos distribuidos. En estos entornos informáticos distribuidos, los dispositivos de procesamiento remoto conectados a través de redes de comunicación realizan tareas. En los entornos informáticos distribuidos, un módulo de programa puede estar ubicado en un medio de almacenamiento informático local y remoto, incluidos los dispositivos de almacenamiento.

Anteriormente solo se han descrito realizaciones de la presente descripción que no se utilizan para limitar la presente descripción. Para un experto en la técnica, la presente descripción puede tener varias modificaciones y cambios.

REIVINDICACIONES

1. Un método de almacenamiento de datos, que comprende:

- 5 enviar (S 100), mediante un primer nodo de cadena de bloques asociado a una cadena de bloques, datos a un dispositivo de cifrado para hacer que el dispositivo de cifrado cifre los datos y devuelva los datos cifrados al nodo de cadena de bloques;
recibir (S102), mediante el primer nodo de cadena de bloques, los datos cifrados devueltos por el dispositivo de cifrado;
- 10 enviar (S104), mediante el primer nodo de cadena de bloques, los datos cifrados a otros nodos de cadena de bloques asociados a la cadena de bloques para hacer que cada uno de los otros nodos de cadena de bloques almacene los datos cifrados en la cadena de bloques después de realizar la verificación del consenso sobre los datos cifrados con éxito;
- 15 determinar (S300), mediante un segundo nodo de cadena de bloques asociado a la cadena de bloques, los datos que se van a consultar en los datos cifrados almacenados en la cadena de bloques;
determinar (S302), a través de un contrato inteligente, si el segundo nodo de cadena de bloques tiene permiso para descifrar los datos que se van a consultar;
- 20 si el segundo nodo de cadena de bloques tiene permiso, enviar (S304), a través del segundo nodo de cadena de bloques, los datos que se van a consultar a un dispositivo de cifrado a través del contrato inteligente para hacer que el dispositivo de cifrado descifre los datos que se van a consultar y devolver los datos obtenidos del descifrado al segundo nodo de cadena de bloques, y si el segundo nodo de cadena de bloques no tiene el permiso, rechazar (S306) el envío de los datos que se van a consultar al dispositivo de cifrado;
- 25 enviar, a través del segundo nodo de cadena de bloques, una solicitud de recarga a un dispositivo de recarga para hacer que el dispositivo de recarga determine un certificado de recarga de acuerdo con la solicitud de recarga y devuelva el certificado de recarga al segundo nodo de cadena de bloques; comprendiendo el certificado de recarga un primer valor que se usa para representar un valor añadido en una cuenta del segundo nodo de cadena de bloques; y
enviar el identificador de nodo del segundo nodo de cadena de bloques y el certificado de recarga a otros nodos de cadena de bloques asociados a la cadena de bloques para hacer que cada uno de los otros nodos de cadena de bloques almacene el identificador de nodo y el primer valor en la cadena de bloques después de realizar con éxito la verificación del consenso en el identificador de nodo y el certificado de recarga.

2. El método de acuerdo con la reivindicación 1, que además comprende:

- 35 determinar, a través del primer nodo de cadena de bloques, un segundo valor correspondiente a los datos a través de un contrato inteligente, utilizándose el segundo valor para representar un valor añadido en una cuenta del primer nodo de cadena de bloques para compartir los datos; y
enviar el propio identificador de nodo del primer nodo de cadena de bloques y el segundo valor a los otros nodos de cadena de bloques para hacer que el propio identificador de nodo y el segundo valor se almacenen en la
- 40 cadena de bloques después de que se ha superado una verificación del consenso sobre el propio identificador de nodo y el segundo valor por los nodos de cadena de bloques.

3. El método de acuerdo con la reivindicación 1, en el que se hace que el dispositivo de cifrado cifre una parte de los datos.

45 4. El procedimiento de acuerdo con la reivindicación 1, en el que:

- 50 cada dato cifrado almacenado en la cadena de bloques comprende una parte no cifrada; y
la determinación, a través del segundo nodo de cadena de bloques asociado a la cadena de bloques, los datos que se van a consultar en los datos cifrados almacenados en la cadena de bloques, comprende:

- determinar, a través del segundo nodo de cadena de bloques, una condición de consulta de datos;
- determinar, a través del contrato inteligente y de acuerdo con la condición de consulta de datos, si la parte no cifrada comprendida en cada dato cifrado almacenado en la cadena de bloques satisface la condición de
- 55 consulta de datos;
- si se satisface la condición de consulta de datos, usar los datos cifrados que contienen la parte no cifrada que satisface la condición de consulta de datos como datos a consultar; y
- si no se cumple la condición de consulta de datos, no utilizar ningún dato cifrado como datos que se van a consultar.

60 5. El método de acuerdo con la reivindicación 1, en el que, cuando el segundo nodo de cadena de bloques tiene permiso para descifrar los datos que se van a consultar, el método comprende además:

- 65 determinar, mediante segundo nodo de cadena de bloques, a través del contrato inteligente, un tercer valor correspondiente a los datos devueltos por el dispositivo de cifrado, utilizándose el tercer valor para representar un valor deducido de una cuenta del segundo nodo de cadena de bloques; y

enviar, mediante el segundo nodo de cadena de bloques, a través del contrato inteligente, el identificador de nodo del segundo nodo de cadena de bloques y el tercer valor a otros nodos de cadena de bloques asociados a la cadena de bloques para hacer que cada uno de los otros nodos de cadena de bloques almacene el identificador de nodo y el tercer valor en la cadena de bloques después de realizar con éxito la verificación del consenso en el identificador de nodo y el tercer valor.

6. El método de acuerdo con la reivindicación 1, en el que, cuando el segundo nodo de cadena de bloques tiene permiso para descifrar los datos que se van a consultar, el método comprende además:

determinar, mediante el segundo nodo de cadena de bloques, a través del contrato inteligente, un cuarto valor correspondiente a los datos y los identificadores de nodo de otros nodos de cadena de bloques que comparten los datos, utilizándose el cuarto valor para representar un valor añadido en las cuentas de los otros nodos de cadena de bloques que comparten los datos; y
enviar, mediante el segundo nodo de cadena de bloques, a través del contrato inteligente, los identificadores de nodo de determinados y el cuarto valor a los otros nodos de cadena de bloques para hacer que cada uno de los otros nodos de cadena de bloques almacene los identificadores de nodos determinados y el cuarto valor en la cadena de bloques después de realizar con éxito la verificación del consenso en los identificadores de nodo determinados y el cuarto valor.

7. Un sistema que comprende un primer nodo de cadena de bloques y un segundo nodo de cadena de bloques asociados a una cadena de bloques, comprendiendo cada uno del primer nodo de cadena de bloques y el segundo nodo de cadena de bloques un procesador y un medio de almacenamiento no transitorio legible por ordenado que almacena instrucciones que, cuando son ejecutadas por los procesadores, hacen que los procesadores realicen un método de almacenamiento de datos, estando adaptado el sistema para:

enviar (S 100), a través del primer nodo de cadena de bloques, datos a un dispositivo de cifrado para hacer que el dispositivo de cifrado cifre los datos y devuelva los datos cifrados al nodo de cadena de bloques;
recibir (S102), por el primer nodo de cadena de bloques, los datos cifrados devueltos por el dispositivo de cifrado;
y
enviar (S104), a través del primer nodo de cadena de bloques, los datos cifrados a otros nodos de cadena de bloques asociados a la cadena de bloques para hacer que cada uno de los otros nodos de cadena de bloques almacene los datos cifrados en la cadena de bloques después de realizar con éxito la verificación del consenso sobre los datos cifrados;
determinar (S300), a través del segundo nodo de cadena de bloques, los datos que se van a consultar en los datos cifrados almacenados en la cadena de bloques;
determinar (S302), mediante el segundo nodo de cadena de bloques, a través de un contrato inteligente, si el segundo nodo de cadena de bloques tiene permiso para descifrar los datos que se van a consultar;
si el segundo nodo de cadena de bloques tiene el permiso, enviar (S304) a través del segundo nodo de cadena de bloques, los datos que se van a consultar a un dispositivo de cifrado a través del contrato inteligente para hacer que el dispositivo de cifrado descifre los datos que se van a consultar y devuelva los datos obtenidos del descifrado al segundo nodo de cadena de bloques y si el segundo nodo de cadena de bloques no tiene el permiso, rechazar (S306) el envío de los datos que se van a consultar al dispositivo de cifrado;
enviar, a través del segundo nodo de cadena de bloques, una solicitud de recarga a un dispositivo de recarga para hacer que el dispositivo de recarga determine un certificado de recarga de acuerdo con la solicitud de recarga y devuelva el certificado de recarga al segundo nodo de cadena de bloques; comprendiendo el certificado de recarga un primer valor y utilizándose el primer valor para representar un valor añadido en una cuenta del segundo nodo de cadena de bloques; y
enviar el identificador de nodo del segundo nodo de cadena de bloques y el certificado de recarga a otros nodos de cadena de bloques asociados a la cadena de bloques para hacer que cada uno de los otros nodos de cadena de bloques almacene el identificador de nodo y el primer valor en la cadena de bloques después de realizar con éxito la verificación del consenso en el identificador de nodo y el certificado de recarga.

8. El sistema de acuerdo con la reivindicación 7, en el que el sistema está adaptado además para
determinar, a través del primer nodo de cadena de bloques, un segundo valor correspondiente a los datos a través de un contrato inteligente, utilizándose el segundo valor para representar un valor añadido en una cuenta del primer nodo de cadena de bloques para compartir los datos; y
enviar, a través del primer nodo de cadena de bloques, el propio identificador de nodo del primer nodo de cadena de bloques y el segundo valor a los otros nodos de cadena de bloques para hacer que el propio identificador de nodo y el segundo valor se almacenen en la cadena de bloques después de que han superado una verificación del consenso sobre el propio identificador de nodo del primer nodo de cadena de bloques y el segundo valor por los nodos de cadena de bloques.

9. El sistema de acuerdo con la reivindicación 7, en el que se hace que el dispositivo de cifrado cifre una parte de los datos.

10. El sistema de acuerdo con la reivindicación 7, en el que:

cada dato cifrado almacenado en la cadena de bloques comprende una parte no cifrada; y la determinación, a través del segundo nodo de cadena de bloques, los datos que se van a consultar en los datos cifrados almacenados en la cadena de bloques, comprende:

5 determinar, a través del segundo nodo de cadena de bloques, una condición de consulta de datos; determinar, a través del contrato inteligente y de acuerdo con la condición de consulta de datos, si la parte no cifrada comprendida en cada dato cifrado almacenado en la cadena de bloques satisface la condición de consulta de datos; 10 si se satisface la condición de consulta de datos, usar los datos cifrados que contienen la parte no cifrada que satisface la condición de consulta de datos como datos a consultar; y si no se cumple la condición de consulta de datos, no utilizar ningún dato cifrado como datos que se van a consultar.

15 11. El sistema de acuerdo con la reivindicación 7, en el que, cuando el segundo nodo de cadena de bloques tiene permiso para descifrar los datos que se van a consultar, el sistema está adaptado además para determinar, a través del segundo nodo de cadena de bloques, a través del contrato inteligente, un tercer valor correspondiente a los datos devueltos por el dispositivo de cifrado, utilizándose el tercer valor para representar un valor deducido de una cuenta del segundo nodo de cadena de bloques; y 20 enviar, mediante el segundo nodo de cadena de bloques, a través del contrato inteligente, el identificador de nodo del segundo nodo de cadena de bloques y el tercer valor a otros nodos de cadena de bloques para hacer que cada uno de los otros nodos de cadena de bloques almacene el identificador de nodo y el tercer valor en la cadena de bloques después de realizar con éxito la verificación del consenso en el identificador de nodo y el tercer valor.

25 12. El sistema de acuerdo con la reivindicación 7, en el que, cuando el segundo nodo de cadena de bloques tiene permiso para descifrar los datos que se van a consultar, el sistema está adaptado además para determinar, a través del contrato inteligente, un cuarto valor correspondiente a los datos y los identificadores de nodo de otros nodos de cadena de bloques que comparten los datos, utilizándose el cuarto valor para representar un valor añadido en las cuentas de los otros nodos de cadena de bloques que comparten los datos; y 30 enviar, a través del contrato inteligente, los identificadores de nodo determinados y el cuarto valor a los otros nodos de cadena de bloques para hacer que cada uno de los otros nodos de cadena de bloques almacene los identificadores de nodos determinados y el cuarto valor en la cadena de bloques después de realizar con éxito la verificación de consenso en los identificadores de nodos determinados y el cuarto valor.

35 13. Un método de consulta de datos, que comprende:

 determinar (S300), a través de un nodo de cadena de bloques asociado a una cadena de bloques, datos a consultar en datos cifrados almacenados en la cadena de bloques; 40 determinar (S302), a través de un contrato inteligente, si el nodo de cadena de bloques tiene permiso para descifrar los datos que se van a consultar; si el nodo de cadena de bloques tiene el permiso, enviar (S304), a través del nodo de cadena de bloques, los datos que se van a consultar a un dispositivo de cifrado a través del contrato inteligente para hacer que el dispositivo de cifrado descifre los datos que se van a consultar y devolver los datos obtenidos del descifrado al nodo de cadena de bloques; y si el nodo de cadena de bloques no tiene el permiso, rechazar (S306) el envío de 45 los datos que se van a consultar al dispositivo de cifrado; enviar, a través del nodo de cadena de bloques, una solicitud de recarga a un dispositivo de recarga para hacer que el dispositivo de recarga determine un certificado de recarga de acuerdo con la solicitud de recarga y devuelva el certificado de recarga al segundo nodo de cadena de bloques; comprendiendo el certificado de recarga un primer valor y utilizándose el primer valor para representar un valor añadido en una cuenta del nodo 50 de cadena de bloques; y enviar, a través del nodo de cadena de bloques, el identificador del nodo del nodo de cadena de bloques y el certificado de recarga a otros nodos de cadena de bloques para hacer que cada uno de los otros nodos de cadena de bloques almacene el identificador del nodo y el primer valor en la cadena de bloques después de realizar con éxito la verificación del consenso en el identificador de nodo y el certificado de recarga.

55 14. El procedimiento de acuerdo con la reivindicación 13, en el que:

 cada dato cifrado almacenado en la cadena de bloques comprende una parte no cifrada; y la determinación, a través del nodo de cadena de bloques en la cadena de bloques, los datos que se van a 60 consultar en los datos cifrados almacenados en la cadena de bloques comprende:

 determinar, a través del nodo de cadena de bloques, una condición de consulta de datos; determinar, a través del contrato inteligente y de acuerdo con la condición de consulta de datos, si la parte no cifrada comprendida en cada dato cifrado almacenado en la cadena de bloques satisface la condición de 65 consulta de datos; si se satisface la condición de consulta de datos, usar los datos cifrados que contienen la parte no cifrada que

satisface la condición de consulta de datos como datos a consultar; y
si no se cumple la condición de consulta de datos, no utilizar ningún dato cifrado como datos que se van a consultar.

- 5 15. El método de acuerdo con la reivindicación 13, en el que, cuando el nodo de cadena de bloques tiene permiso para descifrar los datos que se van a consultar, el método comprende además:

10 determinar, a través del contrato inteligente, un segundo valor correspondiente a los datos devueltos por el dispositivo de cifrado, utilizándose el segundo valor para representar un valor deducido de una cuenta del nodo de cadena de bloques; y

15 enviar, a través del contrato inteligente, el identificador de nodo del nodo de cadena de bloques y el segundo valor a otros nodos de cadena de bloques en la cadena de bloques para hacer que cada uno de los otros nodos de cadena de bloques almacene el identificador de nodo y el segundo valor en la cadena de bloques después de realizar con éxito la verificación del consenso en el identificador de nodo y el segundo valor, y/o
comprendiendo el método además:

20 determinar, a través del contrato inteligente, un tercer valor correspondiente a los datos y los identificadores de nodo de los otros nodos de cadena de bloques que comparten los datos, utilizándose el tercer valor para representar un valor añadido en las cuentas de los otros nodos de cadena de bloques que comparten los datos; y

25 enviar, a través del contrato inteligente, los identificadores de nodo determinados y el tercer valor a los otros nodos de cadena de bloques para hacer que cada uno de los otros nodos de cadena de bloques almacenen los identificadores de nodos determinados y el tercer valor en la cadena de bloques después de realizar con éxito la verificación del consenso en los identificadores de nodos determinados y el tercer valor.

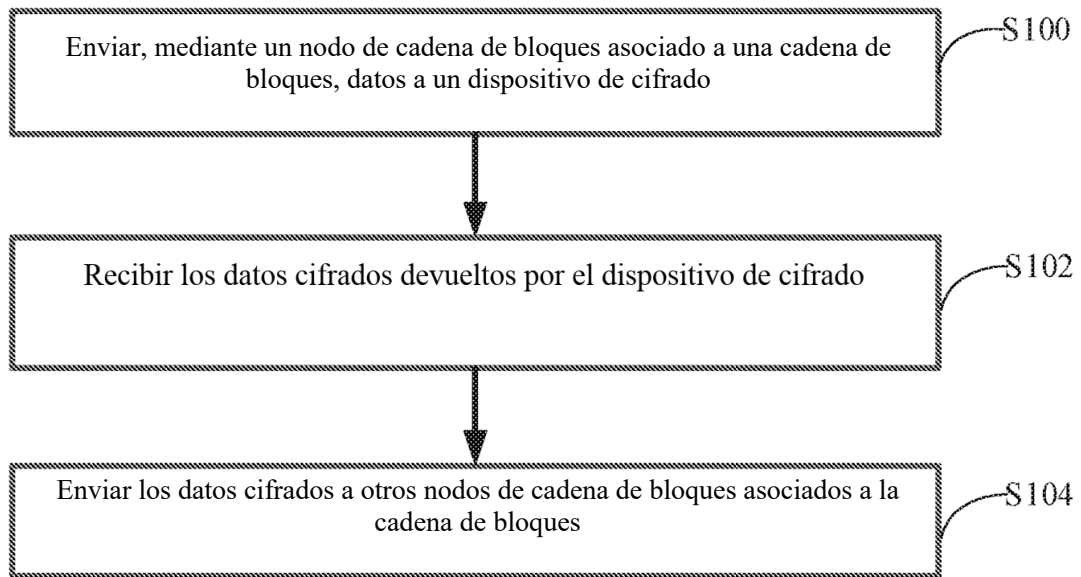


FIG. 1

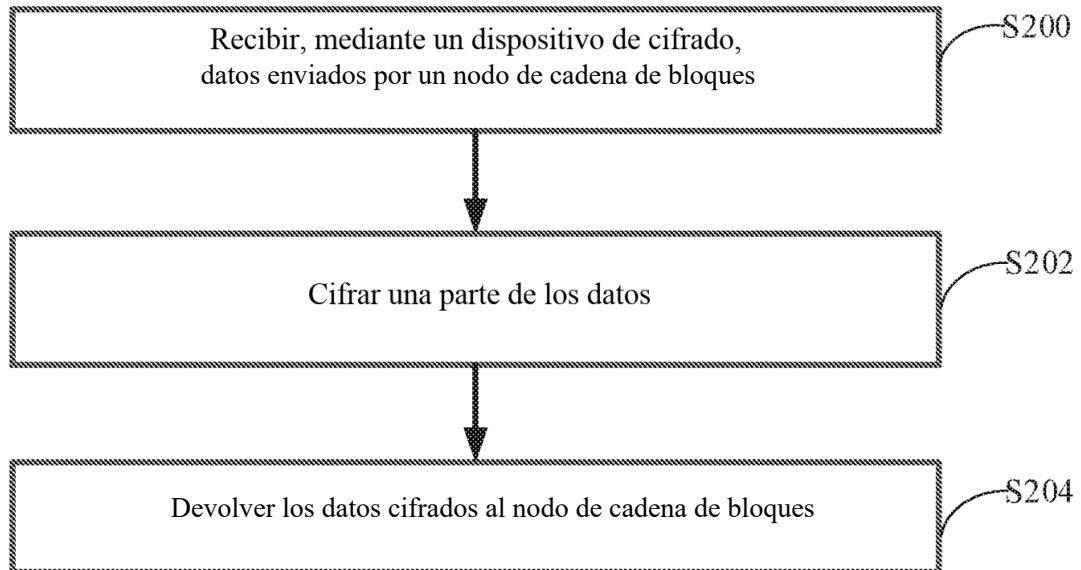


FIG. 2

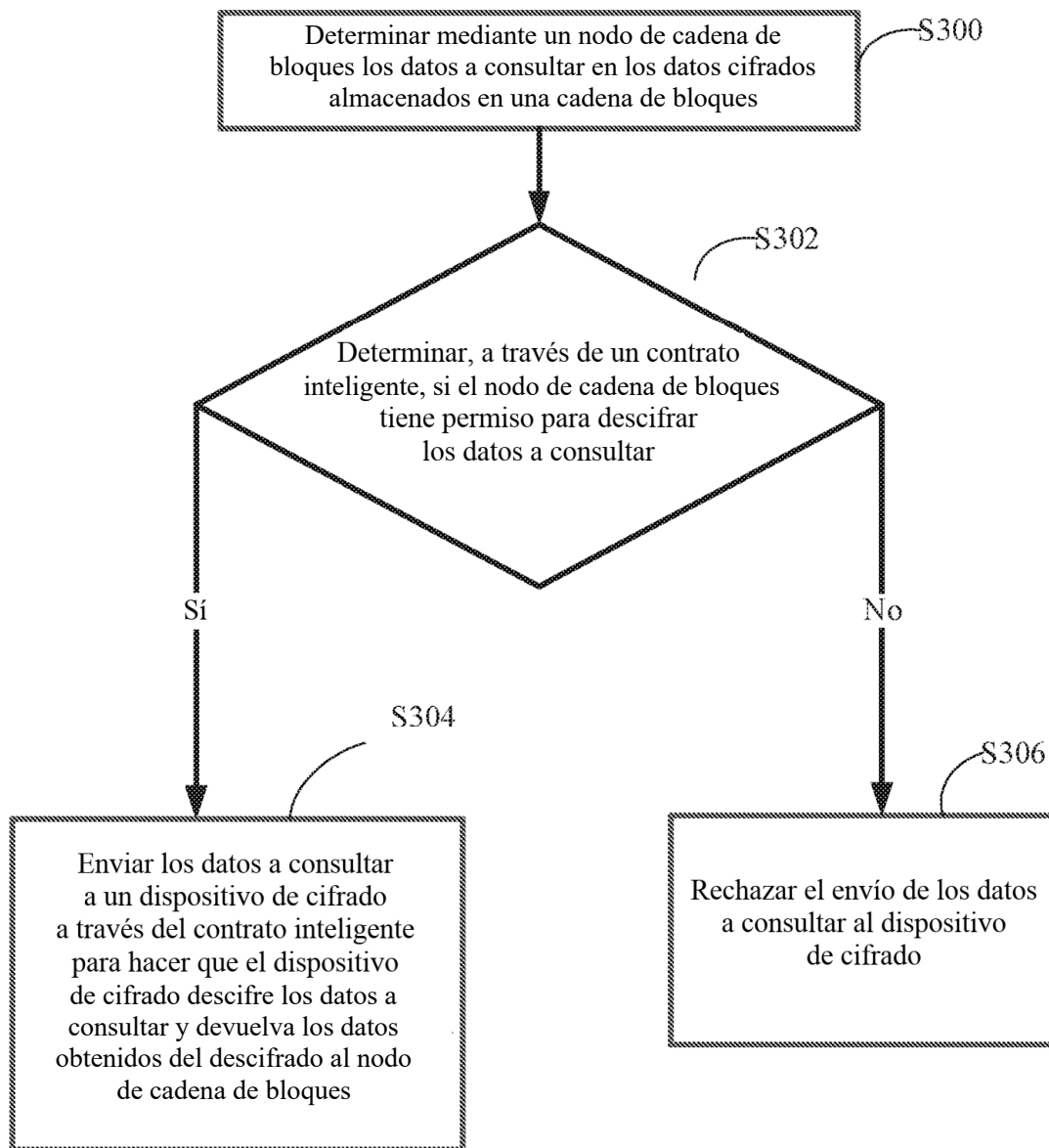


FIG. 3

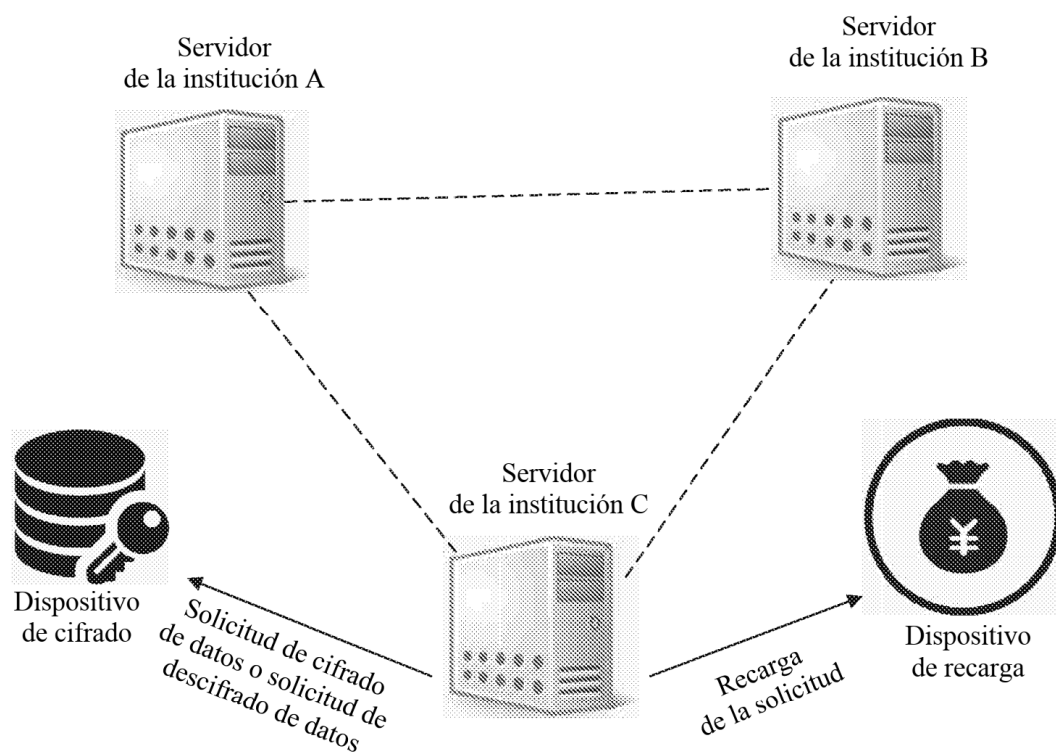


FIG. 4

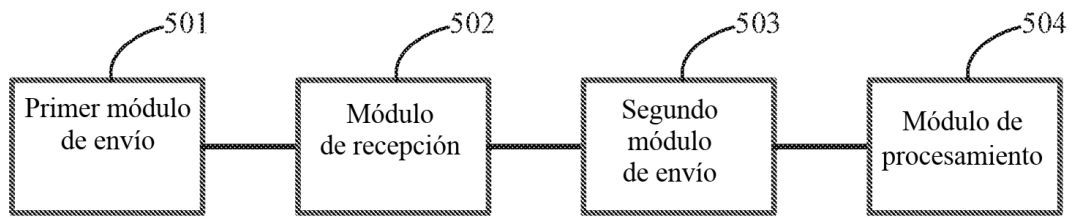


FIG. 5

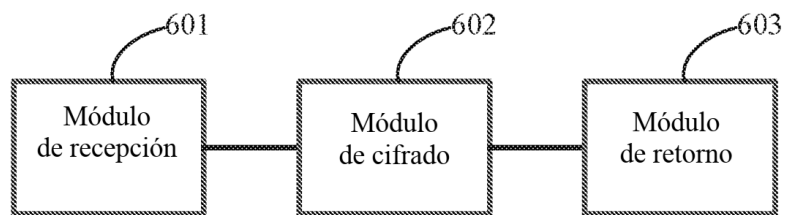
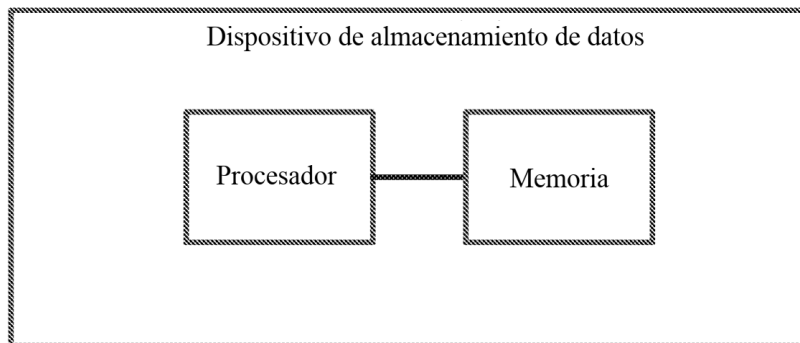
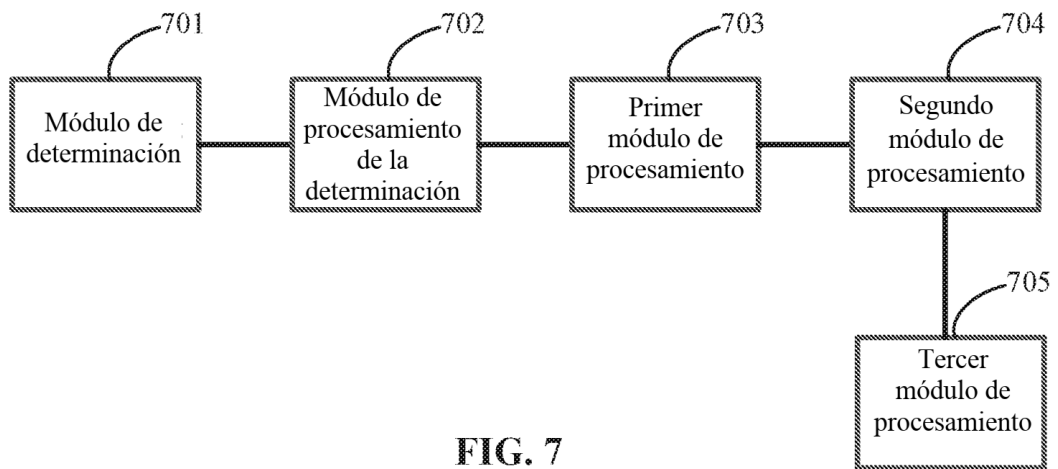


FIG. 6



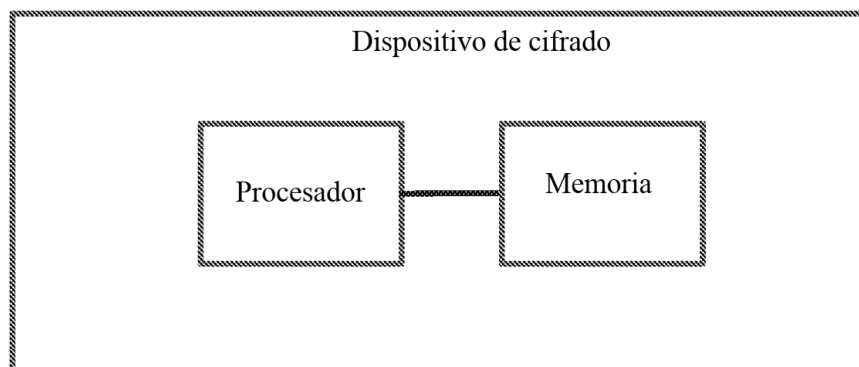


FIG. 9

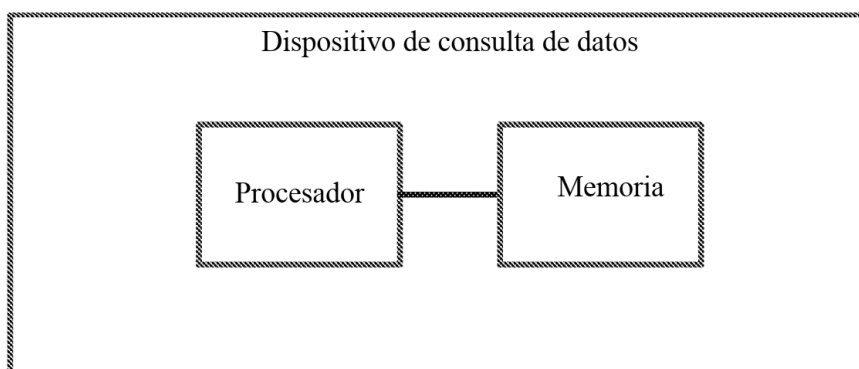


FIG. 10