(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 809 170**

(51) Int. CI.:

G06F 21/64 (2013.01)
G06F 21/62 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **17.11.2017 PCT/CN2017/111538**

(87) Fecha y número de publicación internacional: **31.05.2018 WO18095275**

(96) Fecha de presentación y número de la solicitud europea: **17.11.2017 E 17873246 (7)**

(97) Fecha y número de publicación de la concesión europea: **22.07.2020 EP 3547198**

(54) Título: **Método, sistema y aparato para el acceso a datos**

(30) Prioridad:

24.11.2016 CN 201611050311

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
03.03.2021

(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:

TONG, JUN

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Método, sistema y aparato para el acceso a datos

CAMPO TÉCNICO

La presente solicitud se refiere al campo de las tecnologías de la información y, en particular, a un método, sistema y aparato para el acceso a datos.

ANTECEDENTES DE LA INVENCIÓN

Con el desarrollo de las tecnologías de la información y la popularidad generalizada de la oficina digital, muchas industrias generan una gran cantidad de datos que necesitan almacenarse cada día. Por lo tanto, la tecnología de almacenamiento de datos se ha convertido en uno de los objetos públicos.

El documento US 2016/292672 da a conocer un sistema informático que se comunica con un sistema informático de cadena de bloques distribuido que incluye múltiples nodos informáticos. El intercambio almacena una cartera de pedidos y una pluralidad de los denominados monederos digitales asociados con diferentes clientes. El sistema informático recibe nuevas demandas de transacciones de datos que se agregan a la cartera de pedidos. Se identifica una coincidencia entre las demandas de transacción de datos y se generan los denominados hashes asociados con los monederos digitales asociados con las demandas de transacción de datos respectivas. Las contrapartes reciben los hashes de la otra parte junto con información sobre la coincidencia y cada parte hace que las transacciones de cadena de bloques se agreguen a la cadena de bloques del sistema informático de cadena de bloques. El sistema informático a continuación supervisa la cadena de bloques para determinar si ambos lados de la coincidencia se han añadido a la cadena de bloques.

El documento US 2016/328713 da a conocer un servicio de gestión de identidad que utiliza una cadena de bloques que proporciona transacciones de identidad entre dispositivos. La lógica en un primer dispositivo remoto da lugar a la captura de datos personales que identifican a un usuario desde una tarjeta de identificación. La lógica genera un valor hash a partir de los datos personales mediante un algoritmo hash y firma el valor hash con una firma digital creada con una clave privada que constituye un par con una clave pública. La lógica transmite, a través de una red, el valor hash firmado y la clave pública del dispositivo remoto a una base de datos pública distribuida para su almacenamiento. La lógica recibe, a través de la red, un número de transacción desde la base de datos pública distribuida. La lógica transmite luego el número de transacción y los datos personales a un segundo dispositivo remoto. La lógica en el segundo dispositivo remoto verifica que el valor hash en el valor hash firmado sea el mismo que el valor hash generado y verifica que el valor hash firmado se haya firmado con la clave privada.

El documento US 2016/306982 da a conocer un sistema y método configurado para proporcionar una plataforma criptográfica para intercambiar información. Una o más transacciones de información, incluyendo la información cifrada, se pueden generar y/o proporcionar a un libro mayor distribuido. La una o más transacciones de información pueden incluir información destinada a una o más partes. Se pueden identificar transacciones de información destinadas a una o más partes. Una transacción de información puede incluir uno o más de un identificador de transacción asociado con una o más partes, una carga útil de información y/o información adicional. La carga útil de información puede incluir información cifrada. La información cifrada puede cifrarse con una o más claves públicas asociadas con una o más partes. Se pueden recuperar una o más transacciones de información del libro mayor distribuido. La información cifrada se puede descifrar con una o más claves privadas que corresponden a las claves públicas. Se puede facilitar la presentación de la información cifrada a una o más partes. Una solución general en la tecnología de almacenamiento de datos existente es poner en práctica el almacenamiento de datos utilizando una tecnología de base de datos. Es decir, uno o más dispositivos que almacenan datos se gestionan mediante el uso de un centro de gestión de bases de datos, y las operaciones de creación, recuperación, actualización y eliminación (CRUD) realizadas en los datos se gestionan mediante el centro de gestión de bases de datos. Con el desarrollo continuo de las tecnologías de almacenamiento de datos existentes, las nuevas tecnologías de almacenamiento de datos, tal como una tecnología de base de datos distribuida, se desarrollan y perfeccionan de manera gradual. En consecuencia, el almacenamiento de datos se mejora de manera significativa no solamente en términos de velocidad de almacenamiento, espacio de ocupación de datos, sino también en términos de conveniencia de gestión de datos, etc., con el fin de satisfacer las demandas de las personas para el almacenamiento de datos.

Sin embargo, en la tecnología existente, las bases de datos utilizadas por diferentes empresas o unidades por lo general se ejecutan de forma independiente, y son gestionadas por separado por los respectivos centros de gestión de bases de datos. Cuando los datos almacenados por separado por una pluralidad de empresas o unidades necesitan obtenerse, los datos correspondientes deben obtenerse por separado de diferentes bases de datos y, en consecuencia, el proceso de adquisición de datos es complejo.

Además, teniendo en cuenta la seguridad de los datos, por lo general, no se puede acceder, de manera pública, a las bases de datos de todas las empresas o unidades. En consecuencia, es difícil obtener datos relacionados, de forma satisfactoria, a través de la red. Además, por lo general, antes de obtener datos, en primer lugar, se debe comprobar

una identidad (o se necesita obtener un certificado digital) en un departamento calificado, con el fin de obtener los datos de la empresa o de la unidad utilizando la información de identidad (o el certificado digital) que ya ha sido probado. En consecuencia, se hace más difícil obtener los datos.

SUMARIO DE LA INVENCIÓN

Las puestas en práctica de la presente invención proporcionan un método, aparato y sistema de almacenamiento y consulta de datos, para atenuar un problema de operaciones complejas de obtención de datos de múltiples bases de datos y baja eficiencia resultante del almacenamiento de datos en diferentes bases de datos que son independientes entre sí en una tecnología de almacenamiento de datos existente.

Las siguientes soluciones técnicas se adoptan en las puestas en práctica de la presente invención.

Se proporciona un método de almacenamiento de datos, que incluye lo siguiente: determinar una instrucción de almacenamiento de datos, donde la instrucción de almacenamiento de datos incluye un identificador y datos que han de guardarse; determinar una cadena de bloques que corresponde al identificador y un par de claves que corresponden al identificador en función del propio identificador y almacenar los datos que han de guardarse en la cadena de bloques en función del par de claves.

Se proporciona un método de consulta de datos, que incluye lo siguiente: determinar una instrucción de consulta de datos, donde la instrucción de consulta de datos incluye un identificador; determinar una cadena de bloques que corresponde al identificador y una clave privada que corresponde al identificador basado en el propio identificador y realizar una consulta después de descifrar datos en la cadena de bloques basada en la clave privada.

Se proporciona un sistema de acceso a datos, que incluye varios dispositivos de almacenamiento, varios dispositivos de consulta y varios nodos de almacenamiento de red de cadena de bloques, donde el nodo de almacenamiento de red de cadena de bloques está configurado para almacenar una cadena de bloques que corresponde a un identificador; el dispositivo de almacenamiento está configurado para determinar una instrucción de almacenamiento de datos, determinar la cadena de bloques que corresponde al identificador y un par de claves que corresponden al identificador basado en el propio identificador incluido en la instrucción de almacenamiento de datos, y almacenar los datos que han de guardarse en la cadena de bloques que corresponde al identificador en el nodo de almacenamiento de red de cadena de bloques en función del par de claves; y el dispositivo de consulta está configurado para determinar una instrucción de consulta de datos, determinar una cadena de bloques que corresponde al identificador y una clave privada que corresponde al identificador basado en un identificador incluido en la instrucción de consulta de datos, descifrar datos en la cadena de bloques utilizando la clave privada y realizar una consulta.

Se proporciona un aparato de almacenamiento de datos, que incluye lo siguiente: un primer módulo de determinación, configurado para determinar una instrucción de almacenamiento de datos, donde la instrucción de almacenamiento de datos incluye un identificador y datos que han de guardarse; un segundo módulo de determinación, configurado para determinar una cadena de bloques que corresponde al identificador y un par de claves que corresponden al identificador basado en el propio identificador; y un módulo de almacenamiento, configurado para almacenar los datos que han de guardarse en la cadena de bloques en función del par de claves.

Se proporciona un aparato de consulta de datos, donde el aparato incluye un motor de vibración y un sensor, y comprende lo siguiente: un primer módulo de determinación, configurado para determinar una instrucción de consulta de datos, donde la instrucción de consulta de datos incluye un identificador; un segundo módulo de determinación, configurado para determinar una cadena de bloques que corresponde al identificador y una clave privada que corresponde al identificador basado en el propio identificador; y un módulo de consulta, configurado para realizar una consulta después de descifrar datos en la cadena de bloques en función de la clave privada.

Al menos una de las soluciones técnicas descritas con anterioridad, utilizadas en las puestas en práctica de la presente invención, puede lograr los siguientes efectos beneficiosos:

Durante un proceso de almacenamiento de datos, en primer lugar, se determina la instrucción de almacenamiento de datos; a continuación, la cadena de bloques y el par de claves que corresponden al identificador se determinan en función del identificador incluido en la instrucción de almacenamiento de datos; por último, los datos que han de guardarse se almacenan en la cadena de bloques en función del par de claves. Durante un proceso de consulta de datos, en primer lugar, se determina la instrucción de consulta de datos; a continuación, la cadena de bloques y la clave privada que corresponde al identificador se determina en función del identificador que corresponde a la instrucción de consulta de datos; por último, se realiza una consulta después de que los datos en la cadena de bloques se descifren en función de la clave privada. Se puede constatar que, de conformidad con el método proporcionado en las puestas en práctica de la presente invención, para acceder a los datos que corresponden al identificador, no es necesario acceder a una pluralidad de bases de datos, sino solamente acceder a la cadena de bloques que corresponde al identificador. Mientras tanto, los datos solamente pueden almacenarse utilizando el par de claves. En consecuencia, se garantiza la seguridad de los datos, se puede reducir la complejidad de la operación y se puede mejorar la eficiencia del acceso a los datos.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Los dibujos adjuntos aquí descritos están destinados a proporcionar una comprensión adicional de la presente invención, y constituyen una parte de la presente invención. Las puestas en práctica ilustrativas de la presente invención y de sus descripciones están destinadas a describir la misma, y no constituyen limitaciones en la presente invención. En los dibujos adjuntos:

la Figura 1 ilustra un proceso de almacenamiento de datos, de conformidad con una puesta en práctica de la presente invención;

la Figura 2 ilustra un proceso de consulta de datos, de conformidad con una puesta en práctica de la presente invención;

la Figura 3 es un diagrama estructural esquemático que ilustra un sistema de acceso a datos, de conformidad con una puesta en práctica de la presente invención;

la Figura 4 es un diagrama estructural esquemático que ilustra otro sistema de acceso a datos, de conformidad con una puesta en práctica de la presente invención;

la Figura 5 es un diagrama estructural esquemático que ilustra un aparato de almacenamiento de datos, de conformidad con una puesta en práctica de la presente invención; y

la Figura 6 es un diagrama estructural esquemático que ilustra otro aparato de consulta de datos, de conformidad con una puesta en práctica de la presente invención.

DESCRIPCIÓN DE LAS PUESTAS EN PRÁCTICA

Para aclarar los objetivos, las soluciones técnicas y las ventajas de la presente invención, a continuación, se da a conocer de manera clara y completa las soluciones técnicas de la presente invención con referencia a puestas en práctica específicas y dibujos adjuntos de la presente invención. Evidentemente, las puestas en práctica descritas son simplemente algunas, pero no todas de las puestas en práctica de la presente invención. La invención se define por las reivindicaciones adjuntas. La presente invención se refiere a una tecnología de cadena de bloques. Antes de describir las puestas en práctica de la presente invención en detalle, en primer lugar, se da a conocer, de manera adecuada, un concepto de cadena de bloques. Un "bloque" de una "cadena de bloques" es una unidad básica que forma una cadena de bloques. El bloque puede incluir dos partes: una cabecera de bloque y un cuerpo de bloque.

La cabecera del bloque puede incluir al menos tres tipos de información, es decir, información de identificación (por ejemplo, un valor hash) del bloque actual, información de identificación de un bloque anterior del bloque actual, una marca de tiempo, etc. Puesto que un solo bloque incluye información de identificación de un bloque anterior, una pluralidad de bloques puede formar una cadena y, además, formar una red de cadena de bloques. La cadena de bloques tiene muchas características excelentes tal como se da a conocer a continuación. Descentralización: debido al uso del libro mayor distribuido y del almacenamiento, no existe una organización centralizada de gestión o de hardware, y los derechos y obligaciones de cualquier nodo son iguales; los bloques de datos en el sistema son mantenidos de manera conjunta por los nodos con funciones de mantenimiento en todo el sistema. Autonomía: la cadena de bloques adopta especificaciones y protocolos basados en el consenso (tal como un conjunto de algoritmos abiertos y transparentes) para permitir que todos los nodos en el sistema completo intercambien datos de forma libre y segura en un entorno no fiable. En consecuencia, la confianza en las "personas" se convierte en confianza en las máquinas, y no hay intervención humana. No manipulación: una vez que la información ha sido verificada y agregada a la cadena de bloques, la información se almacena de forma permanente. A menos que más del 51% de los nodos del sistema puedan controlarse al mismo tiempo, la modificación de la base de datos no es válida. Por lo tanto, la estabilidad de datos y la fiabilidad de la cadena de bloques son muy elevadas. Las soluciones técnicas proporcionadas en las puestas en práctica de la presente invención, se da a conocer en detalle a continuación, haciendo referencia a los dibujos adjuntos.

La Figura 1 ilustra un proceso de almacenamiento de datos, de conformidad con una puesta en práctica de la presente invención. El proceso incluye las siguientes etapas.

S101: Determinar una instrucción de almacenamiento de datos.

Por lo general, en un proceso de almacenamiento de datos, un dispositivo de almacenamiento de datos puede almacenar datos, que han de guardarse, en un dispositivo de almacenamiento especificado en función de una instrucción de almacenamiento de datos. Por ejemplo, al almacenar datos en una base de datos, el dispositivo de almacenamiento de datos puede almacenar los datos en el dispositivo de una base de datos en función de una instrucción de almacenamiento de datos recibida. El dispositivo, en este caso, puede ser un dispositivo separado, o puede ser un sistema que incluye una pluralidad de dispositivos. El dispositivo puede ser un teléfono móvil, un

ordenador personal, una tableta electrónica, un servidor, etc. El dispositivo no está limitado en la presente solicitud. En esta puesta en práctica de la presente invención, se proporcionan, además, un método y aparato de consulta de datos. Para facilitar la descripción (pero no para limitarla), a continuación, los dispositivos que ejecutan un proceso de almacenamiento de datos se referirán como un dispositivo de almacenamiento.

Habida cuenta de que el dispositivo de almacenamiento puede configurarse para ejecutar un proceso de almacenamiento de datos, el dispositivo de almacenamiento puede determinar una instrucción de almacenamiento de datos. La instrucción de almacenamiento de datos puede ser generada por el dispositivo de almacenamiento o puede ser recibida por el dispositivo de almacenamiento. La fuente de la instrucción de almacenamiento de datos no está limitada en la presente solicitud, siempre que el dispositivo de almacenamiento pueda determinar la instrucción de almacenamiento de datos. En esta puesta en práctica de la presente invención, la instrucción de almacenamiento de datos puede incluir un identificador y datos para ser almacenados. Es decir, al determinar la instrucción de almacenamiento de datos, el dispositivo de almacenamiento puede determinar el identificador incluido en la instrucción de almacenamiento de datos y los datos que necesitan almacenarse utilizando la instrucción de almacenamiento de datos. El identificador puede ser un número de tarjeta de identidad de un ciudadano, un identificador de cuenta, un identificador de buzón, etc. El identificador no está limitado en la presente solicitud, siempre que el identificador sea un identificador único global. Por supuesto, para facilitar la descripción posterior, a continuación, se proporciona una descripción utilizando un ejemplo de que un identificador es un número de tarjeta de identidad de un ciudadano.

S102: Determinar una cadena de bloques que corresponde a un identificador y un par de claves que corresponden al identificador basado en el propio identificador.

En esta puesta en práctica de la presente invención, después de que el dispositivo de almacenamiento determina la instrucción de almacenamiento de datos, puesto que el dispositivo de almacenamiento puede determinar, además, el identificador incluido en la instrucción de almacenamiento de datos y los datos que han de guardarse, el dispositivo de almacenamiento puede determinar, además, la cadena de bloques que corresponde al identificador y el par de claves que corresponden al identificador basado en el propio identificador. En un proceso de almacenamiento de datos posterior, los datos que han de guardarse, determinados en la etapa S101, se almacenan en la cadena de bloques.

En esta puesta en práctica de la presente invención, "una cadena de bloques que corresponde a un identificador" indica una relación entre un identificador y una cadena de bloques. En un proceso de aplicación real, el identificador puede clasificarse en al menos dos tipos en función de una característica del identificador: un identificador específico del sujeto y un identificador específico de la transacción, y diferentes tipos de identificadores pueden corresponder a diferentes cadenas de bloques. Para el primero, diferentes sujetos (por ejemplo, persona A y persona B) pueden corresponder a diferentes cadenas de bloques, y para el segundo, diferentes transacciones (por ejemplo, transacciones de registro para compras de libros y transacciones de reuniones) pueden corresponder a diferentes cadenas de bloques. A continuación, se describe por separado, un identificador y una cadena de bloques correspondiente mediante el uso de ejemplos.

Se supone que actualmente se utiliza una tecnología de cadena de bloques para el almacenamiento de archivos personales. El archivo personal suele incluir una pluralidad de tipos de información, y la información procede de registros en diferentes departamentos gubernamentales o instituciones relacionadas. Por ejemplo, para la persona A, la información del archivo puede incluir información de registro del domicilio que se registra por un departamento de policía, información del estado civil que se registra por un departamento de asuntos civiles y formada en base al estado civil de la persona A, información del préstamo registrado por un banco y formado en base a un préstamo personal de dicha persona A, y la información de empleo que es registrada por un empleador y formada en base a una relación de empleo personal de la persona A. La información se forma en diferentes períodos y se puede almacenar en una cadena de bloques utilizando la tecnología de cadena de bloques. Por lo tanto, la cadena de bloques es una cadena de bloques dedicada a (correspondiente a) la persona A. Del mismo modo, para la persona B, puede haber una cadena de bloques que almacene un archivo personal de B. En consecuencia, puede haber cadenas de bloques masivas que se forman debido a diferentes identidades de personas. De esta manera, debido a que una pluralidad de cadena de bloques puede coexistir en una red formada por una pluralidad de nodos de almacenamiento de red de cadena de bloques, para escribir información de archivo personal recién generada por un sujeto en una cadena de bloques existente del sujeto, una cadena de bloques que corresponde al sujeto necesita ser primero determinada (identificada) en función de un identificador del sujeto. Este tipo de identificador es un identificador específico del sujeto.

Se supone que las transacciones de registro para la compra de libros necesitan realizarse en un grupo WECHAT que actualmente utiliza la tecnología de cadena de bloques. La primera persona que inicia una actividad de registro en el libro A envía el número de serie y el nombre (1, nombre 1) al grupo WECHAT; la segunda persona que también desea adquirir el libro A, añade información personal a la información de la primera persona y envía la información (1, nombre 1; 2, nombre 2) al grupo WECHAT; y así sucesivamente. Todo este proceso forma una cadena de bloques (cadena de bloques A) para comprar el libro A. Sin embargo, en el grupo WECHAT, también puede existir una actividad de registro para el libro B (u otras transacciones tales como organizar una cena). La primera persona que inicia una actividad de registro en el libro B puede enviar el número de serie y el nombre al grupo WECHAT, y así sucesivamente, para formar una cadena de bloques (cadena de bloques B) para comprar el libro B. Cuando dos o más cadenas de bloques coexisten en un solo grupo WECHAT, una persona que necesita añadir información a la cadena necesita

identificar una cadena de bloques correspondiente. Por ejemplo, una persona que quiere comprar el libro A necesita identificar la cadena de bloques A, y una persona que desea comprar el libro B necesita identificar la cadena de bloques B. De esta manera, puesto que una pluralidad de cadena de bloques puede coexistir en una red formada por una pluralidad de nodos de almacenamiento de la red de cadena de bloques (similar a un dispositivo de un miembro del grupo en un grupo WECHAT), para escribir la información de actualización de la transacción generada para una transacción en una cadena de bloques existente de la transacción, primero debe determinarse (identificarse) una cadena de bloques que corresponde a la transacción en función de una identidad de la transacción. Este tipo de identificador es un identificador específico de la transacción.

En esta puesta en práctica de la presente invención, la cadena de bloques que corresponde al identificador puede ser una cadena de bloques de consorcio, es decir, no todos los dispositivos de usuario final tienen permiso para realizar una operación de almacenamiento de datos en la cadena de bloques, y solamente un dispositivo de usuario final especificado tiene permiso para realizar una operación de almacenamiento de datos en la cadena de bloques, para garantizar la seguridad y la autenticidad de los datos en la cadena de bloques durante un proceso de almacenamiento de datos. Por supuesto, en otra puesta en práctica de la presente invención, la cadena de bloques también puede ser una cadena de bloques pública, una cadena de bloques privada, etc. Conviene señalar que una forma de determinar el dispositivo de usuario final aquí especificado en un proceso real está relacionada con factores como una característica de una cadena de bloques. La ruta no está limitada en la presente solicitud. Por ejemplo, en la puesta en práctica anterior de la presente invención, la cadena de bloques es una cadena de bloques de consorcio, y el dispositivo de usuario final especificado puede ser determinado por el consorcio. Sobre esta base, en la puesta en práctica anterior de la presente invención, un dispositivo de almacenamiento que realiza las etapas S101, S102 y un proceso de almacenamiento de datos posterior puede ser el dispositivo de usuario final especificado, es decir, un dispositivo de usuario final que tiene permiso para almacenar datos en la cadena de bloques.

En esta puesta en práctica de la presente invención, el dispositivo de almacenamiento puede determinar si existe una cadena de bloques que corresponde al identificador en el nodo de almacenamiento de red de cadena de bloques basándose en el identificador determinado en la etapa S101 y una relación de mapeo de correspondencia pre-almacenada entre el identificador y cada uno del par de clave y cadena de bloques. Si existe una pluralidad de nodos de almacenamiento de red de cadena de bloques, el dispositivo de almacenamiento puede determinar una cadena de bloques que corresponde al identificador buscando al menos un nodo de almacenamiento de red de cadena de bloques. En este caso, una relación de mapeo de correspondencia entre el identificador y la cadena de bloques puede almacenarse en el dispositivo de almacenamiento, o puede almacenarse en cada nodo en una red formada por nodos de almacenamiento de red de cadena de bloques, o incluso puede almacenarse en un dispositivo de terceros. En la práctica, una ubicación de almacenamiento de la relación de mapeo de correspondencia puede considerarse desde la perspectiva de la comodidad de lectura, una velocidad de lectura, seguridad, etc. Por ejemplo, la relación de mapeo de correspondencia entre un identificador y una cadena de bloques se almacena localmente en el dispositivo de almacenamiento, de modo que puede ser más conveniente para las funciones de lectura y escritura. Del mismo modo, una relación de mapeo de correspondencia entre el identificador y el par de claves se puede almacenar en un lugar en función de una situación real. Conviene señalar, además, que el nodo de almacenamiento de red de cadena de bloques y el dispositivo de almacenamiento pueden ser, en este caso, el mismo dispositivo o pueden ser dispositivos diferentes. Las puestas en práctica no están limitadas en la presente solicitud. Para garantizar la seguridad de los datos, por lo general, puede haber una pluralidad de nodos de almacenamiento de red de cadena de bloques en la tecnología de cadena de bloques. En consecuencia, la cadena de bloques se puede almacenar en la pluralidad de nodos de almacenamiento de red de cadena de bloques. Cuando un nodo de almacenamiento de red de cadena de bloques está defectuoso (por ejemplo, se produce una fallo o una pérdida de datos), cualquier otro nodo de almacenamiento de red de cadena de bloques que no esté defectuoso puede sustituir el nodo para que funcione, y el nodo de almacenamiento de red de cadena de bloques defectuoso se puede restaurar en función de datos almacenados en el nodo de almacenamiento de la red de cadena de bloques que no está defectuoso (es decir, datos almacenados en la cadena de bloques).

Después de determinar, si existe una cadena de bloques que corresponde al identificador, el par de claves que corresponden al identificador puede determinarse de manera adicional. Si la cadena de bloques que corresponde al identificador no existe, se genera la cadena de bloques que corresponde al identificador y el par de claves que corresponden al identificador. Los detalles son como se indican a continuación.

Cuando existe la cadena de bloques, en la presente solicitud, debido a que el dispositivo de almacenamiento puede especificarse, el dispositivo de almacenamiento puede almacenar previamente el par de claves que corresponden al identificador, y el dispositivo de almacenamiento puede determinar la cadena de bloques que corresponde al identificador y el par de claves que corresponden al identificador. La cadena de bloques determinada almacena un paquete de datos cifrados que corresponde al identificador, el par de claves se puede utilizar para descifrar y cifrar el paquete de datos cifrados que corresponde al identificador, y el dispositivo de almacenamiento determina la cadena de bloques y el par de claves para proceder con un posterior proceso de almacenamiento de datos. Conviene señalar que, cuando existe la cadena de bloques que corresponde al identificador, durante un proceso de determinación del par de claves, el dispositivo de almacenamiento también puede enviar una demanda para obtener el par de claves que corresponden al identificador a otro dispositivo especificado, donde la demanda puede incluir un identificador del dispositivo de almacenamiento, de modo que el otro dispositivo especificado determine que el dispositivo de

almacenamiento también pertenece al dispositivo especificado y que tiene permiso para obtener el par de claves, y el par de claves se devuelve para que el dispositivo de almacenamiento pueda obtener el par de claves. Conviene señalar que, al determinar el par de claves, el dispositivo de almacenamiento también puede utilizar diferentes métodos basados en las demandas reales en la práctica. Las puestas en práctica no están limitadas en la presente solicitud.

Cuando no existe una cadena de bloques que corresponde al identificador, el dispositivo de almacenamiento puede generar una cadena de bloques que corresponde al identificador y un par de claves que corresponden al identificador. La cadena de bloques generada se utiliza para almacenar datos que corresponden al identificador, y para garantizar la seguridad de los datos, los datos pueden ser un paquete de datos cifrados que se obtenga después de una operación de empaquetado y cifrado, es decir, la cadena de bloques puede almacenar un paquete de datos cifrados que corresponden al identificador. El par de claves se puede utilizar para permitir que un dispositivo especificado almacene datos en la cadena de bloques, es decir, el par de claves se puede utilizar para descifrar y cifrar un paquete de datos cifrados que corresponde al identificador, de modo que el dispositivo especificado pueda almacenar datos en la cadena de bloques.

S103: Almacenar los datos que han de guardarse en la cadena de bloques en función del par de claves. En esta puesta en práctica de la presente invención, después de que el dispositivo de almacenamiento determine la cadena de bloques que corresponde al identificador y el par de claves que corresponden al identificador, el dispositivo de almacenamiento puede almacenar los datos que han de guardarse, incluidos en la instrucción de almacenamiento de datos en la cadena de bloques, para completar el proceso de almacenamiento de datos.

En la etapa S102, un caso en donde el dispositivo de almacenamiento determina la cadena de bloques y un caso en donde el dispositivo de almacenamiento determine que el par de claves son diferentes, según se describe a continuación:

Caso 1: Cuando se determina que existe una cadena de bloques que corresponde al identificador, el dispositivo de almacenamiento puede realizar las siguientes etapas. El dispositivo de almacenamiento puede recuperar primero, desde el nodo de almacenamiento de la red de cadena de bloques, un paquete de datos cifrados que corresponde al identificador en la cadena de bloques. A continuación, el dispositivo de almacenamiento puede descifrar el paquete de datos cifrados utilizando una clave privada en el par de claves para obtener todos los datos que corresponden al identificador en el paquete de datos cifrados. A continuación, el dispositivo de almacenamiento puede actualizar todos los datos basados en los datos que han de guardarse, para obtener datos actualizados que corresponden al identificador. Por último, el dispositivo de almacenamiento puede cifrar los datos actualizados como un paquete de datos cifrados actualizado mediante el uso de una clave pública en el par de claves y, después de agregar una marca de tiempo al paquete de datos cifrados actualizado, almacenar el paquete de datos cifrados actualizado y la marca de tiempo en la cadena de bloques y almacenar, en el nodo de almacenamiento de red de cadena de bloques, la cadena de bloques que almacena el paquete de datos cifrados actualizado y la marca de tiempo. Después de actualizar todos los datos anteriores que corresponden al identificador para obtener los datos actualizados, los datos actualizados se convierten en todos los datos que corresponden al identificador. Conviene señalar que, debido a que la tecnología de cadena de bloques se utiliza en la presente solicitud, cuando la cadena de bloques se almacena en el nodo de almacenamiento de la red de cadena de bloques, el nodo de almacenamiento de la red de cadena de bloques puede transmitir la cadena de bloques a otro nodo de almacenamiento de la red de cadena de bloques, de modo que la actual cadena de bloques almacenada en todos los nodos de almacenamiento de red de cadena de bloques sea la misma.

Caso 2: Cuando el dispositivo de almacenamiento determina que no existe una cadena de bloques que corresponde al identificador, el dispositivo de almacenamiento puede generar una cadena de bloques que corresponde al identificador y un par de claves que corresponden al identificador, y puede realizar las siguientes etapas específicas. El dispositivo de almacenamiento puede generar, en primer lugar, datos iniciales que corresponden al identificador basado en el propio identificador; actualizar los datos iniciales basados en los datos que han de guardarse en datos actualizados; generar el par de claves que corresponden al identificador y cifrar los datos actualizados como un paquete de datos cifrados que corresponde al identificador mediante el uso de una clave pública en el par de claves; generar la cadena de bloques que corresponde al identificador y almacenar el paquete de datos cifrados en la cadena de bloques; y almacenar, en el nodo de almacenamiento de la red de cadena de bloques, la cadena de bloques que almacena el paquete de datos cifrados actualizado. Un tipo específico de datos incluidos en los datos iniciales del identificador no está limitado en la presente solicitud, y puede determinarse en función de las demandas durante un proceso de uso real.

Además, en la presente solicitud, los datos que han de guardarse se almacenan en el bloque de datos generado más recientemente en la cadena de bloques. Además, después de determinar la cadena de bloques, el dispositivo de almacenamiento puede determinar el bloque de datos generado más recientemente en función del tiempo de generación de cada bloque de datos en la cadena de bloques. Además, debido a que un bloque de datos puede almacenar una pluralidad de paquetes de datos cifrados que corresponden al identificador, en la presente solicitud, el dispositivo de almacenamiento puede determinar, además, el paquete de datos cifrados almacenado más recientemente en función de una marca de tiempo incluida en cada paquete de datos cifrados, tal como un paquete de datos cifrados que corresponde al identificador.

Además, debido a que cuando el dispositivo de almacenamiento almacena los datos que han de guardarse, los datos se actualizan después de que se recupera el paquete de datos cifrados que corresponde al identificador, el dispositivo de almacenamiento puede agregar todos los datos, que corresponden al identificador, al paquete de datos cifrados almacenado en la cadena de bloques. Es decir, cada paquete de datos cifrados actualizado incluye todos los datos que corresponden al identificador, de modo que, al recuperar el paquete de datos cifrados en función de una marca de tiempo, un dispositivo que recupera el paquete de datos cifrados puede obtener todos los datos que corresponden al identificador, y no es necesario recuperar otros datos.

Asimismo, cuando se genera el par de claves que corresponden al identificador, el dispositivo de almacenamiento puede enviar, además, el par de claves y el identificador a cada dispositivo predeterminado. El dispositivo de almacenamiento puede enviar el par de claves y el identificador a cada dispositivo en función de una dirección predeterminada de cada dispositivo. Los dispositivos predeterminados pueden ser dispositivos especificados, es decir, dispositivos que tienen permiso para realizar el almacenamiento de datos en una cadena de bloques que corresponde al identificador.

Conviene señalar que, en la presente solicitud, la cadena de bloques se almacena en el nodo de almacenamiento de la red de cadena de bloques, donde cada nodo de almacenamiento de la red de cadena de bloques puede ser un sistema que incluye un dispositivo o una pluralidad de dispositivos, y está configurado para almacenar la cadena de bloques. La cadena de bloques almacena un paquete de datos cifrados que corresponde al identificador, la cadena de bloques se puede almacenar en diferentes nodos de almacenamiento de la red de cadena de bloques, y la cadena de bloques, en los diferentes nodos de almacenamiento de la red de cadena de bloques, es coherente. La cadena de bloques y el nodo de almacenamiento de red de cadena de bloques son conceptos diferentes y deben entenderse de manera diferente.

Según el método de almacenamiento de datos ilustrado en la Figura 1, los datos que han de guardarse se almacenan en una cadena de bloques que corresponde al identificador, de modo que todos los datos que corresponden al identificador se pueden almacenar en la cadena de datos, y cuando los datos que corresponden al identificador se almacenan en diferentes dispositivos de almacenamiento, no es necesario recuperar los datos de forma repetida, lo que mejora la eficiencia del almacenamiento de datos y una consulta de datos. Además, de conformidad con el método de la tecnología de cadena de bloques de consorcio, solamente un dispositivo de almacenamiento especificado tiene permiso para almacenar datos que corresponden al identificador. Además, según una característica de la tecnología de cadena de bloques, cualquier operación realizada en los datos que corresponden al identificador se registra en la cadena de bloques, de modo que se garantiza la seguridad de los datos que corresponden al identificador y también se mejora la posibilidad de rastrear un cambio de los datos que corresponden al identificador.

Además, el dispositivo de almacenamiento puede determinar el par de claves que corresponden al identificador en la etapa S102, de modo que el dispositivo de almacenamiento puede descifrar el paquete de datos cifrados recuperados que corresponde al identificador, y obtener todos los datos que corresponden al identificador. A continuación, el dispositivo de almacenamiento necesita, además, cifrar los datos actualizados en función del par de claves para almacenar el paquete de datos cifrados que corresponde al identificador en la cadena de bloques. En consecuencia, solamente el dispositivo de almacenamiento que tiene el par de claves que corresponden al identificador puede almacenar los datos en la cadena de bloques, y en la presente solicitud, solamente el dispositivo especificado puede obtener el par de claves, y garantizar la seguridad de los datos en la cadena de bloques

Además, en la presente solicitud, para garantizar la seguridad del almacenamiento de datos en la cadena de bloques, al recuperar los datos en la cadena de bloques, el dispositivo de almacenamiento puede recuperar solamente el paquete de datos cifrados en la cadena de bloques y determinar que solamente los datos obtenidos después del cifrado realizado mediante el uso de la clave privada en el par de claves es creíble y seguro.

Asimismo, en la presente solicitud, todos los datos que corresponden al identificador pueden almacenarse en una cadena de bloques que corresponde al identificador. Sin embargo, en la red de cadena de bloques de consorcio, se pueden configurar diferentes dispositivos especificados para almacenar diferentes datos que corresponden al identificador. Por ejemplo, el identificador puede corresponder a datos básicos (por ejemplo, un atributo de usuario o un tipo de usuario), o puede corresponder a datos contables (por ejemplo, un saldo de cuenta o un tipo de cuenta), o puede corresponder a información de hábito operativo (por ejemplo, datos de comportamiento histórico). Se puede constatar que los datos básicos pueden ser mantenidos por un dispositivo responsable de la información básica que corresponde al identificador (por ejemplo, un centro de usuarios), y los datos contables pueden ser mantenidos por un dispositivo responsable de mantener las cuentas, y los datos de hábitos operativos se pueden mantener mediante un dispositivo de publicidad. Es decir, en la presente solicitud, diferentes dispositivos pueden mantener datos de diferentes tipos que corresponden al identificador.

Se pueden asignar diferentes pares de claves a diferentes dispositivos especificados en la red de cadena de bloques de consorcio, donde diferentes pares de claves incluyen la misma clave privada, utilizada para descifrar paquetes de datos cifrados que corresponden al identificador. Sin embargo, diferentes pares de claves incluyen diferentes claves públicas, y se pueden utilizar diferentes claves públicas para cifrar solamente datos de un tipo especificado, de modo que los dispositivos que tienen diferentes pares de claves pueden almacenar solamente datos de un tipo especificado.

La configuración del par de claves puede ser determinada por el personal. Se omite un método de configuración específico por simplicidad en la presente solicitud, siempre que el par de claves permita que diferentes dispositivos tengan permiso para realizar el cifrado de datos en datos de diferentes tipos.

Por ejemplo, el dispositivo A, el dispositivo B y el dispositivo C, respectivamente, tienen diferentes pares de claves X, Y y Z, y los pares de claves X, Y y Z se pueden utilizar para cifrar los datos de tipo x, tipo y, y tipo z en todos los datos que corresponden al identificador a, tal como se muestra en la Tabla 1.

Tabla 1

Dispositivo	Par de claves	Tipo de datos
Dispositivo A	Par de claves X	Datos de tipo x
Dispositivo B	Par de claves Y	Datos de tipo y
Dispositivo C	Par de claves Z	Datos de tipo z

Los datos de tipo x, tipo y, y tipo z incluyen todos los datos que corresponden al identificador a. Por lo tanto, los dispositivos A, B y C pueden almacenar solamente una parte de los datos que corresponde al identificador a mediante el uso de diferentes pares de claves. Mejora la seguridad durante un proceso de almacenamiento de datos y reduce la probabilidad de realizar una operación incorrecta en los datos que corresponden al identificador.

Conviene señalar que todas las etapas del método proporcionado en las puestas en práctica de la presente invención pueden ser realizadas por el mismo dispositivo, o el método puede ser realizado por diferentes dispositivos. Por ejemplo, la etapa S101 y la etapa S102 pueden realizarse por el dispositivo 1, y la etapa S103 puede realizarse por el dispositivo 2. En otro ejemplo, la etapa S101 puede realizarse por el dispositivo 1, y la etapa S102 y la etapa S103 pueden realizarse por el dispositivo 2.

En base al proceso de almacenamiento de datos ilustrado en la Figura 1, de manera correspondiente, una puesta en práctica de la presente invención proporciona, además, un método de consulta de datos, tal como se muestra en la Figura 2.

La Figura 2 ilustra un proceso de consulta de datos, de conformidad con una puesta en práctica de la presente invención. El proceso incluye las siguientes etapas: S201: Determinar una instrucción de consulta de datos.

En esta puesta en práctica de la presente invención, un dispositivo de usuario final puede determinar una instrucción de consulta de datos y proseguir con un proceso de consulta de datos posterior. El dispositivo de usuario final puede ser un teléfono móvil, una tableta electrónica, un ordenador personal, un servidor, etc. y el dispositivo de usuario final puede ser un dispositivo separado o puede ser un sistema que incluya una pluralidad de dispositivos. Las puestas en práctica no están limitadas en la presente solicitud.

La instrucción de consulta de datos puede incluir un identificador, y se utiliza para determinar posteriormente una cadena de bloques para consultar datos. La instrucción de consulta de datos puede ser generada y determinada por el dispositivo del usuario final. Por supuesto, en esta puesta en práctica de la presente invención, el dispositivo del usuario final también puede recibir la instrucción de consulta de datos y determinar la instrucción de consulta de datos. No hay limitación en la forma de generar la instrucción de consulta de datos en la presente solicitud, siempre que el dispositivo del usuario final pueda determinar la instrucción de consulta de datos.

Conviene señalar que, en la presente solicitud, un dispositivo de ejecución (es decir, el dispositivo del usuario final) en el proceso de consulta de datos que se muestra en la Figura 2, puede ser diferente de un dispositivo de ejecución en el proceso de almacenamiento de datos ilustrado en la Figura 1. Para fines de distinción, en la descripción siguiente, un dispositivo de consulta representa a un dispositivo de usuario final que ejecuta el proceso de consulta de datos, y un dispositivo de almacenamiento representa un dispositivo de usuario final que ejecuta el proceso de almacenamiento de datos.

S202: Determinar una cadena de bloques que corresponde a un identificador y una clave privada que corresponde al identificador basado en el propio identificador.

En esta puesta en práctica de la presente invención, debido a que el dispositivo de consulta solamente necesita consultar los datos que corresponden al identificador, el dispositivo de consulta puede determinar la cadena de bloques que corresponde al identificador y la clave privada que corresponde al identificador basándose en propio identificador.

En esta puesta en práctica de la presente invención, el dispositivo de consulta puede determinar la clave privada basándose en la relación de mapeo de correspondencia pre-almacenada entre el identificador y la clave privada en el par de claves. De manera alternativa, cuando la clave privada que corresponde al identificador no se almacena previamente en el dispositivo de consulta, el dispositivo de consulta puede enviar, además, una demanda de

adquisición de clave privada al dispositivo de usuario final especificado (es decir, el dispositivo de almacenamiento) en la Figura 1, y recibir la clave privada devuelta. La demanda de adquisición de clave privada puede incluir el identificador de dispositivo del dispositivo de consulta y el identificador, de modo que el dispositivo de almacenamiento pueda determinar la clave privada en el par de claves en función del identificador, y determinar devolver la clave privada al dispositivo de consulta utilizando el identificador del dispositivo.

Además, los datos que corresponden al identificador se almacenan en una cadena de bloques que corresponde al identificador. Por lo tanto, en la presente solicitud, el dispositivo de consulta puede determinar, además, la cadena de bloques que corresponde al identificador en el nodo de almacenamiento de red de cadena de bloques en función del identificador, para proseguir con una operación de consulta de datos posterior.

El dispositivo de consulta puede buscar en el nodo de almacenamiento de la red de cadena de bloques basándose en el identificador de la cadena de bloques que corresponde al identificador, y determinar la cadena de bloques. Por supuesto, si una cadena de bloques que corresponde al identificador no se identifica en el nodo de almacenamiento de red de cadena de bloques, el dispositivo de consulta puede indicar un error y mostrar información de error de consulta.

S203: Realizar una consulta después de descifrar datos en la cadena de bloques basada en la clave privada.

En esta puesta en práctica de la presente invención, después de determinar la clave privada, el dispositivo de consulta puede consultar los datos en función de la cadena de bloques determinada y de la clave privada que corresponde al identificador.

El dispositivo de consulta puede determinar primero, a partir de un nodo de almacenamiento de red de cadena de bloques, cada paquete de datos cifrados que corresponde al identificador en la cadena de bloques, determinar el paquete de datos cifrados recientemente almacenado como el paquete de datos cifrados que corresponde al identificador basado en un secuencia de tiempo de almacenamiento de cada paquete de datos cifrados (es decir, basado en una secuencia de marcas de tiempo incluidas en paquetes de datos cifrados), descifrar el paquete de datos cifrados en función de la clave privada después de recuperar el paquete de datos cifrados que corresponde al identificador, para obtener todos los datos que corresponden al identificador y por último, consultar todos los datos basados en la instrucción de consulta de datos.

Puesto que el dispositivo de consulta solamente tiene una clave privada que corresponde al identificador, el dispositivo de consulta solamente puede descifrar un paquete de datos cifrados que corresponde al identificador, pero no puede cifrar el paquete de datos cifrados. En consecuencia, el dispositivo de consulta no puede almacenar los datos en la cadena de bloques después de actualizar los datos que corresponden al identificador, garantizando así la seguridad de almacenar los datos en la cadena de bloques.

Además, cuando se determina cada paquete de datos cifrados que corresponde al identificador a partir del nodo de almacenamiento de la red de cadena de bloques, el dispositivo del usuario final puede determinar en primer lugar un tiempo de generación de cada bloque de datos en la cadena de bloques, y determinar cada paquete de datos cifrados a partir del bloque de datos generado más reciente, es decir, determinar que cada paquete de datos cifrados se almacena en el bloque de datos generado más reciente en la cadena de bloques y proceder con una operación posterior.

Conviene señalar que todas las etapas del método proporcionado en las puestas en práctica de la presente invención pueden ser realizadas por el mismo dispositivo, o el método puede ser realizado por diferentes dispositivos. Por ejemplo, la etapa S201 y la etapa S202 pueden realizarse por el dispositivo 1, y la etapa S203 puede realizarse por el dispositivo 2. Por otro ejemplo, la etapa S201 puede realizarse por el dispositivo 1, y la etapa S202 y la etapa S203 pueden realizarse por el dispositivo 2.

En base al proceso de almacenamiento de datos ilustrado en la Figura 1 y el proceso de consulta de datos ilustrado en la Figura 2, de forma correspondiente, se proporciona, además, un sistema de acceso a datos en esta puesta en práctica de la presente invención, tal como se muestra en la Figura 3.

La Figura 3 es un diagrama estructural esquemático que ilustra un sistema de acceso a datos, de conformidad con una puesta en práctica de la presente invención. El sistema de acceso a datos incluye varios dispositivos de almacenamiento, varios dispositivos de consulta y varios nodos de almacenamiento de red de cadena de bloques.

El nodo de almacenamiento de red de cadena de bloques está configurado para almacenar una cadena de bloques que corresponde a un identificador.

El dispositivo de almacenamiento (es decir, el dispositivo de almacenamiento que se muestra en la Figura 1, en esta puesta en práctica de la presente invención) está configurado para determinar una instrucción de almacenamiento de datos, determinar la cadena de bloques que corresponde al identificador y un par de claves que corresponden al identificador basado en el propio identificador incluido en la instrucción de almacenamiento de datos, y almacenar los

datos que han de guardarse en la cadena de bloques que corresponde al identificador en el nodo de almacenamiento de red de cadena de bloques en función del par de claves.

El dispositivo de consulta (es decir, el dispositivo de consulta que se muestra en la Figura 2, en esta puesta en práctica de la presente invención) está configurado para determinar una instrucción de consulta de datos, determinar una cadena de bloques que corresponde al identificador y una clave privada que corresponde al identificador basado en un identificador incluido en la instrucción de consulta de datos, descifrar datos en la cadena de bloques utilizando la clave privada y realizar una consulta.

Cuando cualquier dispositivo de almacenamiento en el sistema de acceso a datos genera una cadena de bloques que corresponde al identificador, el dispositivo de almacenamiento que genera el identificador puede enviar el identificador y el par de claves que corresponden al identificador a otro dispositivo de almacenamiento especificado. Además, el dispositivo de almacenamiento que genera el identificador puede generar la cadena de bloques solamente en un nodo de almacenamiento de la red de cadena de bloques, y el nodo de almacenamiento de la red de cadena de bloques puede transmitir la red de cadena de bloques a otro nodo de almacenamiento de la red de cadena de bloques en el sistema de acceso a datos, de modo que los datos en todos los nodos de almacenamiento de la red de cadena de bloques en el sistema de acceso a datos son consistentes.

Además, al determinar la clave privada que corresponde al identificador, el dispositivo de consulta de datos puede enviar una demanda de adquisición de clave privada a cualquier dispositivo de almacenamiento, para obtener la clave privada y realizar una operación de consulta de datos posterior.

Además, en diferentes dispositivos de almacenamiento en el sistema de acceso a datos, los pares de claves previamente almacenados que corresponden al identificador pueden ser diferentes entre sí, y se pueden utilizar diferentes pares de claves para cifrar datos de diferentes tipos.

Asimismo, en el sistema de acceso a datos, cualquier dispositivo puede obtener un paquete de datos cifrados que corresponde al identificador, y realizar el descifrado para obtener datos que corresponden al identificador. Por lo tanto, para garantizar la seguridad y la credibilidad de los datos en la cadena de bloques, solamente el dispositivo de almacenamiento (es decir, el dispositivo especificado por la red de cadena de bloques de consorcio) puede cifrar los datos que corresponden al identificador. Por lo tanto, en el sistema de acceso a datos, solamente los datos cifrados almacenados en el nodo de almacenamiento de la red de cadena de bloques son datos creíbles. En consecuencia, al obtener los datos que corresponden al identificador utilizando el nodo de almacenamiento de la red de cadena de bloques, el dispositivo de consulta de datos y el dispositivo de almacenamiento solamente pueden obtener el paquete de datos cifrados en el nodo de almacenamiento de la red de cadena de bloques.

Además, puesto que existe una pluralidad de nodos de almacenamiento de red de cadena de bloques en el sistema de acceso a datos, para facilitar la coherencia de los datos almacenados, cada dispositivo de almacenamiento y cada dispositivo de consulta de datos pueden acceder a uno de los nodos de almacenamiento de red de cadena de bloques. Otro nodo de almacenamiento de red de cadena de bloques puede ser un nodo secundario. Cuando el nodo de almacenamiento de red de cadena de bloques no puede funcionar con normalidad, cualquier nodo de almacenamiento de red de cadena de bloques secundario se selecciona para continuar funcionando, y el nodo de almacenamiento de red de cadena de bloques, que no puede funcionar con normalidad, se restaura utilizando cualquier nodo de almacenamiento de red de cadena de bloques secundario. Por supuesto, el personal puede establecer cómo habilitar normalmente el nodo de almacenamiento de red de cadena de bloques secundario y cómo determinar que el nodo de almacenamiento de red de cadena de bloques en funcionamiento no puede funcionar con normalidad en función de una situación en la práctica. Las puestas en práctica no están limitadas en la presente solicitud. Además, para evitar un caso en donde un servicio no puede ejecutarse con normalidad cuando el dispositivo primario deja de funcionar, una solución técnica para utilizar el dispositivo secundario para sustituir el dispositivo primario se suele utilizar no normalidad. Por lo tanto, los detalles se omiten por simplicidad en la presente solicitud.

Además, en el sistema de acceso a datos, el nodo de almacenamiento de red de cadena de bloques y el dispositivo de almacenamiento pueden el mismo. Es decir, cada nodo de almacenamiento de red de cadena de bloques también es un dispositivo de almacenamiento. De manera alternativa, cuando una cantidad de nodos de almacenamiento de red de cadena de bloques en el sistema de acceso a datos es incompatible con una cantidad de dispositivos de almacenamiento, algunos de los nodos de almacenamiento de red de cadena de bloques también son dispositivos de almacenamiento, y los nodos de almacenamiento de red de cadena de bloques restantes son simplemente nodos de almacenamiento de red de cadena de bloques, o algunos de los dispositivos de almacenamiento también son nodos de almacenamiento de red de cadena de bloques, y los dispositivos de almacenamiento restantes son simplemente dispositivos de almacenamiento.

Según el sistema de acceso a datos descrito en la Figura 3, en esta puesta en práctica de la presente invención, se puede constatar que diferentes dispositivos de almacenamiento pueden almacenar datos de diferentes tipos que corresponden al identificador, y datos que corresponden al identificador se almacenan en una cadena de bloques que corresponde al identificador. Además, cualquier dispositivo de consulta de datos puede acceder y recuperar datos del nodo de almacenamiento de la red de cadena de bloques para que el sistema de acceso a datos, en la presente

solicitud, pueda atenuar de manera efectiva un problema de baja eficiencia y operaciones complejas resultantes del almacenamiento de datos en múltiples dispositivos.

Asimismo, en otra puesta en práctica de la presente invención, el identificador puede ser un número de tarjeta de identidad de un ciudadano, el dispositivo de almacenamiento puede ser un dispositivo de almacenamiento de datos de una unidad creíble tal como un departamento gubernamental o una unidad gubernamental, y el dispositivo de consulta de datos puede ser cualquier dispositivo en la sociedad que necesite realizar una consulta de datos, tal como se muestra en la Figura 4. En la presente solicitud, el acceso a datos puede ser según se ilustra en la Figura 4. El nodo de almacenamiento de red de cadena de bloques puede ser un nodo de almacenamiento de datos proporcionado por el gobierno, y todos los datos que corresponden al número del documento de identidad del ciudadano pueden ser datos de archivo, datos de crédito, datos de cuentas bancarias, etc. de dicho ciudadano. Por supuesto, cualquier dato relacionado con el ciudadano puede ser objeto de escritura en una cadena de bloques que corresponde al número del documento de identidad del ciudadano.

Además, los dispositivos de almacenamiento de datos de unidades creíbles tales como diferentes departamentos gubernamentales o unidades gubernamentales pueden utilizarse para almacenar datos de diferentes tipos en una cadena de bloques que corresponde al número del documento de identidad del ciudadano. Por ejemplo, un departamento de policía puede realizar una operación de almacenamiento de datos en el registro de delitos, información del domicilio, etc. del ciudadano, un departamento de asuntos civiles puede realizar una operación de almacenamiento de datos sobre el estado civil del ciudadano, y un banco puede realizar una operación de almacenamiento de datos en los datos contables y los datos de crédito del ciudadano. Se puede poner en práctica un proceso específico utilizando diferentes pares de claves en la etapa S102 y en la Figura 1.

Asimismo, el dispositivo de consulta de datos puede ser un dispositivo en poder del ciudadano, o puede ser un dispositivo de consulta de datos de otro departamento gubernamental o de una sociedad. Por ejemplo, un departamento de aprobación de visados puede enviar una demanda de recuperación de clave privada al departamento gubernamental anterior o a la unidad gubernamental anterior, para obtener la clave privada que corresponde al documento de identidad del ciudadano y consultar la información sobre dicho ciudadano. De manera alternativa, una unidad de empleo puede enviar una demanda de recuperación de clave privada al departamento gubernamental anterior o a la unidad gubernamental anterior, para obtener la clave privada que corresponde al documento de identidad del ciudadano y consultar la información sobre dicho ciudadano.

Además, en otra puesta en práctica de la presente invención, el dispositivo de almacenamiento pueden ser dispositivos de almacenamiento que corresponden, por separado, a una pluralidad de empresas o unidades que tienen una relación de consorcio, por ejemplo, un dispositivo de almacenamiento que corresponde a una empresa de alquiler de automóviles, un banco o una autoridad de gestión de transporte. El dispositivo de consulta puede ser un dispositivo de usuario final en poder de un conductor o un dispositivo de usuario final en poder de un policía de tráfico. En consecuencia, puesto que todos los datos que corresponden al ciudadano pueden almacenarse en la cadena de bloques, no hay necesidad de crear un sistema de consulta especial, y de conformidad con el sistema de acceso a datos descrito en la Figura 4, puede ser conveniente revisar un vehículo y a un conductor en la carretera.

En base al proceso de almacenamiento de datos ilustrado en la Figura 1, de manera correspondiente, una puesta en práctica de la presente invención proporciona, además, un aparato de almacenamiento de datos, tal como se muestra en la Figura 5.

La Figura 5 es un diagrama estructural esquemático que ilustra un aparato de almacenamiento de datos, de conformidad con una puesta en práctica de la presente invención. El aparato incluye lo siguiente: un primer módulo de determinación 301, configurado para determinar una instrucción de almacenamiento de datos, donde la instrucción de almacenamiento de datos incluye un identificador y datos que han de guardarse; un segundo módulo de determinación 302, configurado para determinar una cadena de bloques que corresponde al identificador y un par de claves que corresponden al identificador basado en el propio identificador; y un módulo de almacenamiento 303, configurado para almacenar los datos que han de guardarse en la cadena de bloques en función del par de claves.

El módulo de almacenamiento 303 almacena los datos que han de guardarse en el bloque de datos generado más recientemente en la cadena de bloques.

El segundo módulo de determinación 302 determina si existe una cadena de bloques que corresponde al identificador en un nodo de almacenamiento de red de cadena de bloques en base a una relación de mapeo de correspondencia pre-almacenada entre el identificador y cada uno de los pares de claves y la cadena de bloques; en respuesta a la determinación de que la cadena de bloques, que corresponde al identificador, existe en el nodo de almacenamiento de la red de cadena de bloques, determina una cadena de bloques que corresponde al identificador y un par de claves que corresponden al identificador en el nodo de almacenamiento de la red de cadena de bloques; y en respuesta a la determinación de que la cadena de bloques que corresponde al identificador no existe en el nodo de almacenamiento de red de cadena de bloques, genera una cadena de bloques que corresponde al identificador y un par de claves que corresponden al identificador.

Cuando el segundo módulo de determinación 302 determina que existe una cadena de bloques que corresponde al identificador, el módulo de almacenamiento 303 recupera, desde el nodo de almacenamiento de la red de cadena de bloques, un paquete de datos cifrados que corresponde al identificador en la cadena de bloques; descifra el paquete de datos cifrados utilizando una clave privada en el par de claves para obtener todos los datos que corresponden al identificador en el paquete de datos cifrados; actualiza todos los datos que corresponden al identificador en el paquete de datos cifrados en función de los datos que han de guardarse, para obtener datos actualizados; cifra los datos actualizados como un paquete de datos cifrados actualizado mediante el uso de una clave pública en el par de claves; agrega una marca de tiempo al paquete de datos cifrados actualizado y almacena el paquete de datos cifrados actualizado y la marca de tiempo en la cadena de bloques; y almacena, en el nodo de almacenamiento de red de cadena de bloques, la cadena de bloques que almacena el paquete de datos cifrados actualizado y la marca de tiempo.

Cuando el segundo módulo de determinación 302 determina que no existe una cadena de bloques que corresponde al identificador, el módulo de almacenamiento 303 genera datos iniciales que corresponden al identificador basado en el propio identificador; actualiza los datos iniciales basados en los datos que han de guardarse en para datos actualizados; genera el par de claves que corresponden al identificador y cifra los datos actualizados como un paquete de datos cifrados que corresponde al identificador mediante el uso de una clave pública en el par de claves; genera la cadena de bloques que corresponde al identificador y almacena el paquete de datos cifrados en la cadena de bloques; y almacena, en el nodo de almacenamiento de red de cadena de bloques, la cadena de bloques que almacena el paquete de datos cifrados actualizado.

El segundo módulo de determinación 302 envía el par de claves generado que corresponde al identificador y el identificador a cada dispositivo predeterminado.

El aparato de almacenamiento de datos anterior, ilustrado en la Figura 5, puede ubicarse en un dispositivo de usuario final. El dispositivo del usuario final puede ser un teléfono móvil, una tableta electrónica, etc., o el aparato de almacenamiento de datos puede estar ubicado en un servidor. El servidor puede ser un dispositivo separado o un sistema que incluya una pluralidad de dispositivos, es decir, un servidor distribuido.

En base al proceso de consulta de datos ilustrado en la Figura 2, de forma correspondiente, una puesta en práctica de la presente invención proporciona, además, un aparato de consulta de datos, tal como se muestra en la Figura 6.

La Figura 6 es un diagrama estructural esquemático que ilustra otro aparato de consulta de datos, de conformidad con una puesta en práctica de la presente invención. El aparato incluye lo siguiente: un primer módulo de determinación 401, configurado para determinar una instrucción de consulta de datos, donde la instrucción de consulta de datos incluye un identificador; un segundo módulo de determinación 402, configurado para determinar una cadena de bloques que corresponde al identificador y una clave privada que corresponde al identificador basado en el propio identificador; y un módulo de consulta 403, configurado para realizar una consulta después de descifrar datos en la cadena de bloques en función de la clave privada.

El segundo módulo de determinación 402 determina la clave privada basada en una relación de mapeo de correspondencia pre-almacenada entre el identificador y una clave privada en un par de claves, o envía una demanda de adquisición de clave privada a un dispositivo especificado basado en el identificador, y recibe la clave privada devuelta.

El módulo de consulta 403 determina, a partir de un nodo de almacenamiento de red de cadena de bloques, cada paquete de datos cifrados que corresponde al identificador en la cadena de bloques; determina un paquete de datos cifrados almacenado más recientemente basado en una secuencia de tiempo de almacenamiento de los paquetes de datos cifrados, como un paquete de datos cifrados que corresponde al identificador; y realiza una consulta después de descifrar el paquete de datos cifrados en función de la clave privada.

El aparato de consulta de datos anterior, ilustrado en la Figura 6, puede ubicarse en un dispositivo de usuario final. El dispositivo del usuario final puede ser un teléfono móvil, una tableta electrónica, etc., o el aparato de almacenamiento de datos puede estar ubicado en un servidor. El servidor puede ser un dispositivo separado o un sistema que incluya una pluralidad de dispositivos, es decir, un servidor distribuido.

Un experto en esta técnica debería comprender que una puesta en práctica de la presente invención se puede proporcionar como un método, un sistema o un producto de programa informático. Por lo tanto, la presente invención puede utilizar una forma de puestas en práctica solamente de hardware, puestas en práctica solamente de software o puestas en práctica con una combinación de software y hardware. Además, la presente invención puede utilizar una forma de un producto de programa informático que se pone en práctica en uno o más medios de almacenamiento utilizables por ordenador (que incluyen, entre otros, una memoria de disco, un CD-ROM, una memoria óptica, etc.) que incluyen código de programa utilizable por ordenador.

La presente invención se da a conocer con referencia a los diagramas de flujo y/o diagramas de bloques del método, el dispositivo (sistema) y el producto de programa informático basado en las puestas en práctica de la presente invención. Conviene señalar que las instrucciones del programa informático se pueden utilizar para poner en práctica

cada proceso y/o cada bloque en los diagramas de flujo y/o los diagramas de bloque y una combinación de un proceso y/o un bloque en los diagramas de flujo y/o los diagramas de bloque. Estas instrucciones de programa informático se pueden proporcionar para un ordenador de uso general, un ordenador dedicado, un procesador incorporado o un procesador de otro dispositivo de procesamiento de datos programable para generar una máquina, de modo que las instrucciones ejecutadas por el ordenador o el procesador del otro dispositivo de procesamiento de datos programable genere un dispositivo para poner en práctica una función específica en uno o más procesos en los diagramas de flujo y/o en uno o más bloques en los diagramas de bloques.

Estas instrucciones del programa informático pueden almacenarse en una memoria legible por ordenador que puede indicar al ordenador u a otro dispositivo de procesamiento de datos programable que funcione de una manera específica, de modo que las instrucciones almacenadas en la memoria legible por ordenador generen un dispositivo que incluya un aparato de instrucción. El aparato de instrucción pone en práctica una función específica en uno o más procesos en los diagramas de flujo y/o en uno o más bloques en los diagramas de bloques.

Estas instrucciones del programa informático pueden cargarse en el ordenador u en otro dispositivo de procesamiento de datos programable, de modo que se realicen una serie de operaciones y etapas en el ordenador u en el otro dispositivo programable, generando así el procesamiento puesto en práctica por ordenador. Por lo tanto, las instrucciones ejecutadas en el ordenador u en otro dispositivo programable proporcionan etapas para poner en práctica una función específica 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, un dispositivo informático incluye uno o más procesadores (CPU), una o más interfaces de entrada/salida, una o más interfaces de red y una o más memorias.

La memoria puede incluir una memoria no persistente, una memoria de acceso aleatorio (RAM), una memoria no volátil y/u otra forma que esté en un medio legible por ordenador, por ejemplo, una memoria de solamente lectura (ROM) o una memoria instantánea (memoria instantánea RAM). La memoria es un ejemplo del medio legible por ordenador.

El medio legible por ordenador incluye medios persistentes, no persistentes, móviles e inmóviles que pueden almacenar información utilizando cualquier método o tecnología. La información puede ser una instrucción legible por ordenador, una estructura de datos, un módulo de programa u otros datos. Los ejemplos de un medio de almacenamiento de ordenador incluyen, entre otros, una memoria de acceso aleatorio de cambio de fase (PRAM), una memoria estática de acceso aleatorio (SRAM), una memoria dinámica de acceso aleatorio (DRAM), otro tipo de memoria de acceso aleatorio (RAM), una memoria de solamente lectura (ROM), una memoria de solamente lectura programable y borrable eléctricamente (EEPROM), una memoria instantánea u otra tecnología de memoria, una memoria de solamente lectura de disco compacto (CD-ROM), un disco versátil digital (DVD) u otro almacenamiento óptico, una cinta magnética de casete, una cinta magnética/almacenamiento de disco magnético u otro dispositivo de almacenamiento magnético. El medio de almacenamiento informático se puede utilizar para almacenar información accesible por el dispositivo de cálculo. Según la definición en la presente especificación, el medio legible por ordenador no incluye medios transitorios legibles por ordenador (medios transitorios) tales como una señal de datos modulada y un portador.

Conviene señalar que los términos "incluir", "contener", o sus otras variantes están destinados a cubrir una inclusión no exclusiva, por lo que un proceso, un método, un producto o un dispositivo que incluye una lista de elementos no solamente incluye esos elementos, sino que también incluye otros elementos que no están expresamente enumerados, o incluye elementos inherentes a dicho procesos, métodos, productos o dispositivos. Sin más restricciones, un elemento precedido por "incluye un ..." no excluye la existencia de elementos idénticos adicionales en el proceso, método, producto o dispositivo que incluye el elemento.

Un experto en esta técnica debería comprender que una puesta en práctica de la presente invención puede proporcionarse como un método, un sistema o un producto de programa informático. Por lo tanto, la presente solicitud puede utilizar una forma de puesta en práctica solamente de hardware, puesta en práctica solamente de software o puesta en práctica con una combinación de software y hardware. Además, la presente solicitud puede utilizar una forma de un producto de programa informático que se pone en práctica en uno o más medios de almacenamiento utilizables por ordenador (que incluyen, entre otros, una memoria de disco, un CD-ROM, una memoria óptica, etc.) que comprende un código de programa utilizable por ordenador.

Las puestas en práctica anteriores son puestas en práctica de la presente invención, y no están destinadas a limitar la presente solicitud. Un experto en esta técnica puede realizar diversas modificaciones y cambios en la presente invención.

REIVINDICACIONES

1. Un método puesto en práctica por ordenador que comprende:

determinar (S101), mediante un dispositivo de almacenamiento, una instrucción de almacenamiento de datos, en donde la instrucción de almacenamiento de datos incluye un identificador y datos que han de guardarse;

determinar (S102), mediante el dispositivo de almacenamiento y en base al identificador, una cadena de bloques que corresponde al identificador y un par de claves que corresponden al identificador;

almacenar (S103), por el dispositivo de almacenamiento, los datos que han de guardarse en la cadena de bloques en función del par de claves; y

acceder, mediante un dispositivo de consulta, a los datos que corresponden al identificador accediendo a la cadena de bloques que corresponde al identificador, en donde

determinar (S102) una cadena de bloques que corresponde al identificador y un par de claves que corresponden al identificador comprende:

determinar si existe una cadena de bloques que corresponde al identificador en un nodo de almacenamiento de red de cadena de bloques en función de una relación de mapeo de correspondencia pre-almacenada entre el identificador y cada uno de los pares de claves y la cadena de bloques;

en respuesta a la determinación de que la cadena de bloques que corresponde al identificador existe en el nodo de almacenamiento de la red de cadena de bloques, determinar una cadena de bloques que corresponde al identificador y un par de claves que corresponden al identificador en el nodo de almacenamiento de la red de cadena de bloques; y

en respuesta a la determinación de que la cadena de bloques que corresponde al identificador no existe en el nodo de almacenamiento de red de cadena de bloques, generar una cadena de bloques que corresponde al identificador y un par de claves que corresponden al identificador.

2. El método según la reivindicación 1, en donde almacenar los datos a guardar en la cadena de bloques comprende almacenar los datos a guardar en un bloque de datos generado más recientemente en la cadena de bloques.

3. El método según una cualquiera de las reivindicaciones 1 o 2, en donde cuando se determina que existe una cadena de bloques que corresponde al identificador, almacenar los datos que han de guardarse en la cadena de bloques en función del par de claves comprende:

recuperar, desde el nodo de almacenamiento de la red de cadena de bloques, un paquete de datos cifrados que corresponde al identificador en la cadena de bloques;

descifrar el paquete de datos cifrados utilizando una clave privada en el par de claves para obtener todos los datos que corresponden al identificador en el paquete de datos cifrados;

actualizar todos los datos que corresponden al identificador en el paquete de datos cifrados en función de los datos que han de guardarse para obtener datos actualizados;

cifrar los datos actualizados como un paquete de datos cifrados actualizados utilizando una clave pública en el par de claves;

agregar una marca de tiempo al paquete de datos cifrados actualizado y almacenar el paquete de datos cifrados actualizado y la marca de tiempo en la cadena de bloques; y

almacenar, en el nodo de almacenamiento de red de cadena de bloques, la cadena de bloques que almacena el paquete de datos cifrados actualizado y la marca de tiempo.

4. El método según una cualquiera de las reivindicaciones 1 a 3, en donde cuando se determina que no existe una cadena de bloques que corresponde al identificador, almacenar los datos que han de guardarse en la cadena de bloques en función del par de claves comprende:

generar datos iniciales que corresponden al identificador basado en el propio identificador;

actualizar los datos iniciales basados en los datos que han de guardarse en datos actualizados;

generar el par de claves que corresponden al identificador y cifrar los datos actualizados como un paquete de datos cifrados que corresponde al identificador mediante el uso de una clave pública en el par de claves;

generar la cadena de bloques que corresponde al identificador y almacenar el paquete de datos cifrados en la cadena de bloques; y almacenar, en el nodo de almacenamiento de red de cadena de bloques, la cadena de bloques que almacena el paquete de datos cifrados actualizado.

5. El método según la reivindicación 4, en donde generar el par de claves que corresponden al identificador comprende enviar el par de claves generado que corresponde al identificador y el identificador a cada dispositivo predeterminado.

6. El método según una cualquiera de las reivindicaciones 1 a 5, en donde el acceso, mediante un dispositivo de consulta, a los datos que corresponden al identificador comprende:

determinar una instrucción de consulta de datos, en donde la instrucción de consulta de datos incluye el identificador;

determinar, en función del identificador, la cadena de bloques que corresponde al identificador y una clave privada que corresponde al identificador; y

realizar una consulta después de descifrar datos en la cadena de bloques en función de la clave privada.

7. El método según la reivindicación 6, en donde determinar una clave privada que corresponde al identificador comprende:

determinar la clave privada basada en una relación de mapeo de correspondencia pre-almacenada entre el identificador y una clave privada en un par de claves; o

enviar una demanda de adquisición de clave privada a un dispositivo especificado basado en el identificador, y recibir la clave privada devuelta.

8. Método según la reivindicación 6, en donde realizar una consulta después de descifrar datos en la cadena de bloques basada en la clave privada comprende:

determinar, a partir de un nodo de almacenamiento de red de cadena de bloques, cada paquete de datos cifrados que corresponde al identificador en la cadena de bloques;

determinar un paquete de datos cifrados almacenado más recientemente basado en una secuencia de tiempo de almacenamiento de los paquetes de datos cifrados, como un paquete de datos cifrados que corresponde al identificador; y

realizar una consulta después de descifrar el paquete de datos cifrados en función de la clave privada.

9. Un sistema de acceso a datos, en donde el sistema comprende varios dispositivos de almacenamiento, varios dispositivos de consulta y varios nodos de almacenamiento de red de cadena de bloques, en donde

cada nodo de almacenamiento de red de cadena de bloques está configurado para almacenar una cadena de bloques que corresponde a un identificador;

cada dispositivo de almacenamiento está configurado para determinar (S101) una instrucción de almacenamiento de datos, determinar (S102) la cadena de bloques que corresponde al identificador y un par de claves que corresponden al identificador en función del identificador incluido en la instrucción de almacenamiento de datos, y almacenar (S103) datos que han de guardarse en la cadena de bloques que corresponden al identificador en el nodo de almacenamiento de red de cadena de bloques en función del par de claves; y

cada dispositivo de consulta está configurado para determinar una instrucción de consulta de datos, determinar una cadena de bloques que corresponde al identificador y una clave privada que corresponde al identificador en función de un identificador incluido en la instrucción de consulta de datos, descifrar datos en la cadena de bloques utilizando la clave privada y realizar una consulta en donde

cada dispositivo de almacenamiento está configurado, además, para:

determinar si existe una cadena de bloques que corresponde al identificador en un nodo de almacenamiento de red de cadena de bloques en función de una relación de mapeo de correspondencia pre-almacenada entre el identificador y cada uno del par de claves y la cadena de bloques;

en respuesta a la determinación de que la cadena de bloques que corresponde al identificador existe en el nodo de almacenamiento de la red de cadena de bloques, determinar una cadena de bloques que corresponde al identificador y un par de claves que corresponden al identificador en el nodo de almacenamiento de la red de cadena de bloques; y

en respuesta a la determinación de que la cadena de bloques que corresponde al identificador no existe en el nodo de almacenamiento de red de cadena de bloques, generar una cadena de bloques que corresponde al identificador y un par de claves que corresponden al identificador.

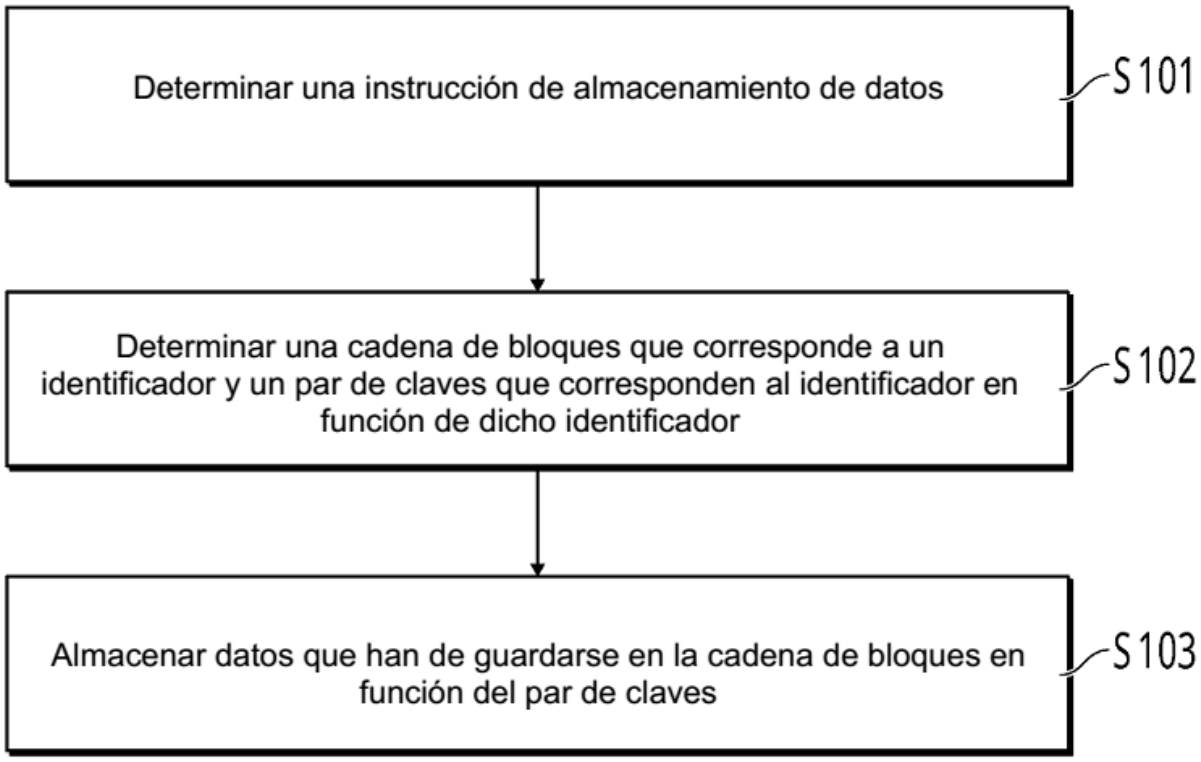
Determinar una instrucción de almacenamiento de datos
S101
Determinar una cadena de bloques que corresponde a un identificador y un par de claves que corresponden al identificador en función de dicho identificador
S102
Almacenar datos que han de guardarse en la cadena de bloques en función del par de claves
S103

FIG. 1

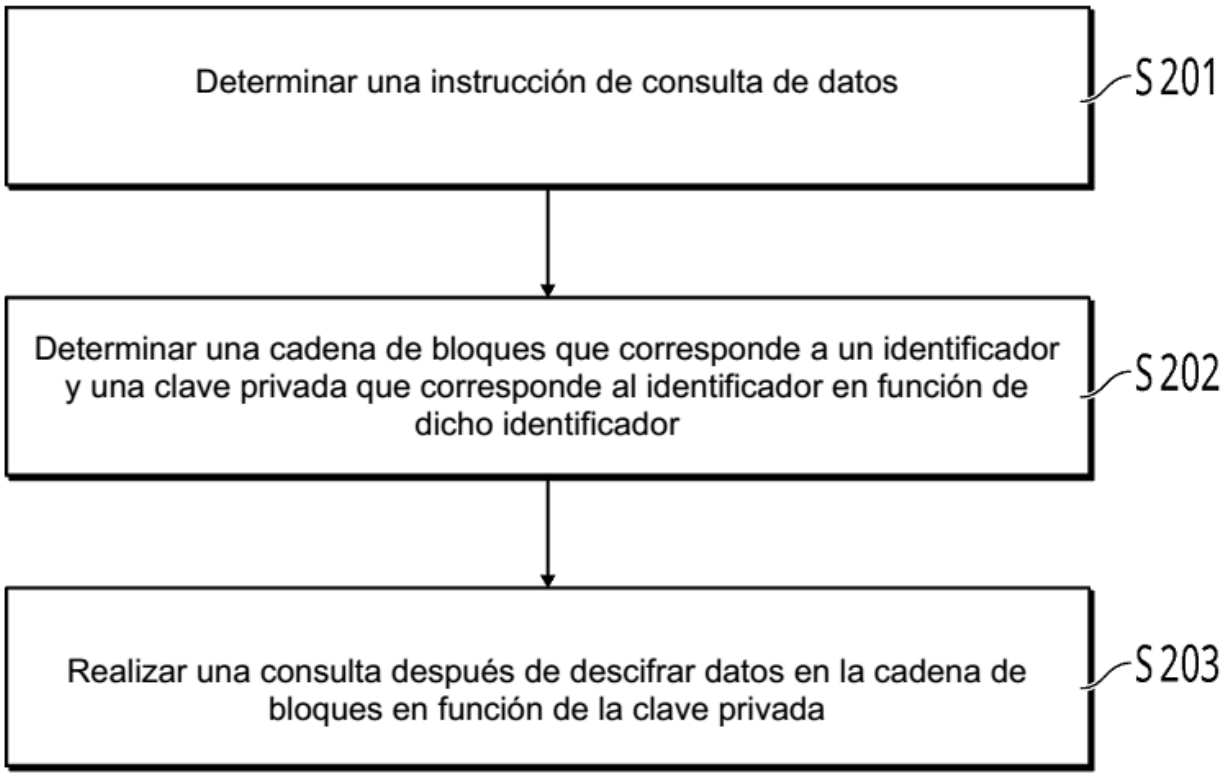
Determinar una instrucción de consulta de datos
S201
Determinar una cadena de bloques que corresponde a un identificador y una clave privada que corresponde al identificador en función de dicho identificador
S202
Realizar una consulta después de descifrar datos en la cadena de bloques en función de la clave privada
S203

FIG. 2

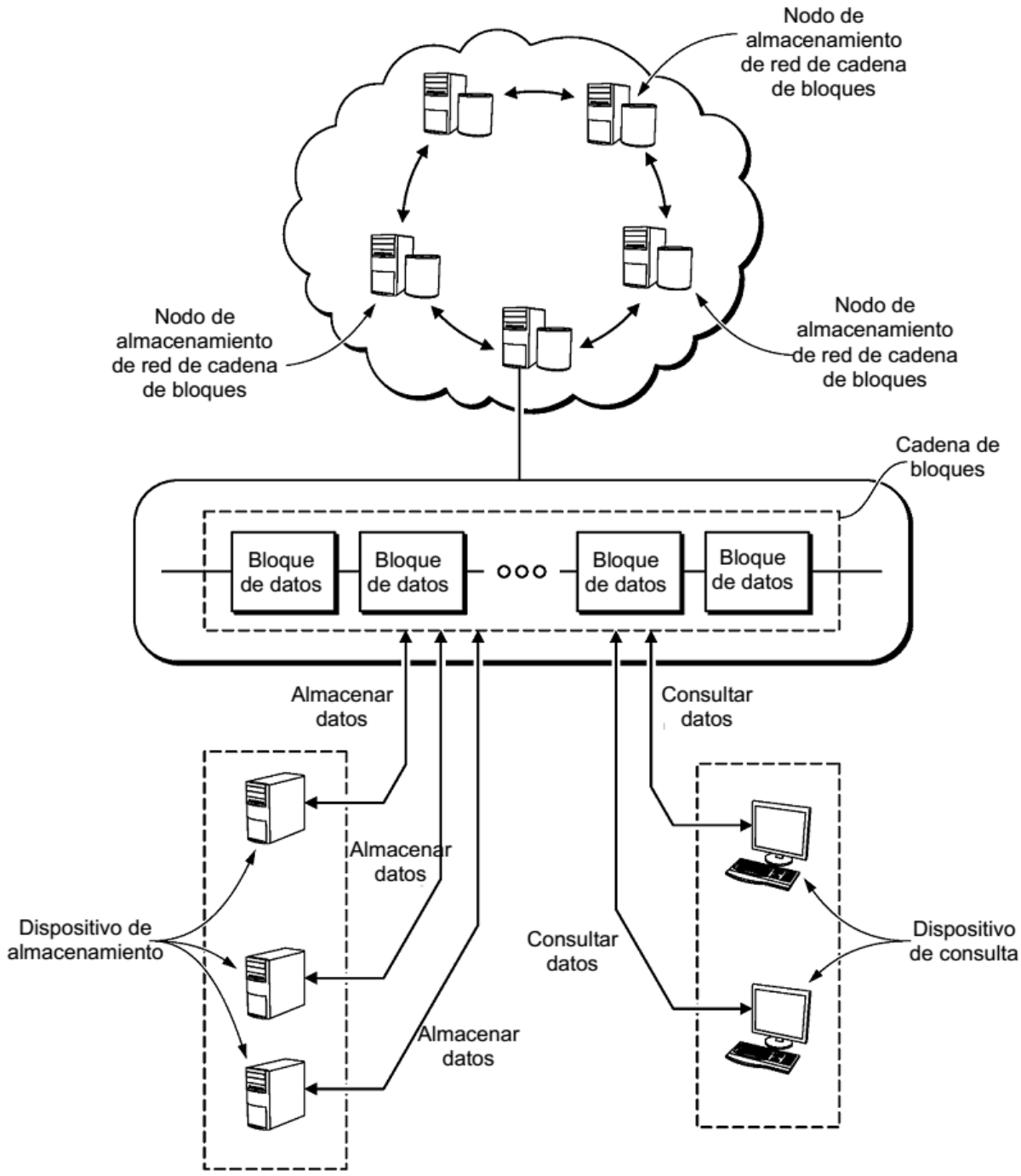
Nodo de almacenamiento de red de cadena de bloques
Nodo de almacenamiento de red de cadena de bloques
Nodo de almacenamiento de red de cadena de bloques
Cadena de bloques
Bloque de datos
Bloque de datos
Bloque de datos
Bloque de datos
Almacenar datos
Consultar datos
Almacenar datos
Dispositivo de almacenamiento
Consultar datos
Dispositivo de consulta
Almacenar datos

FIG. 3

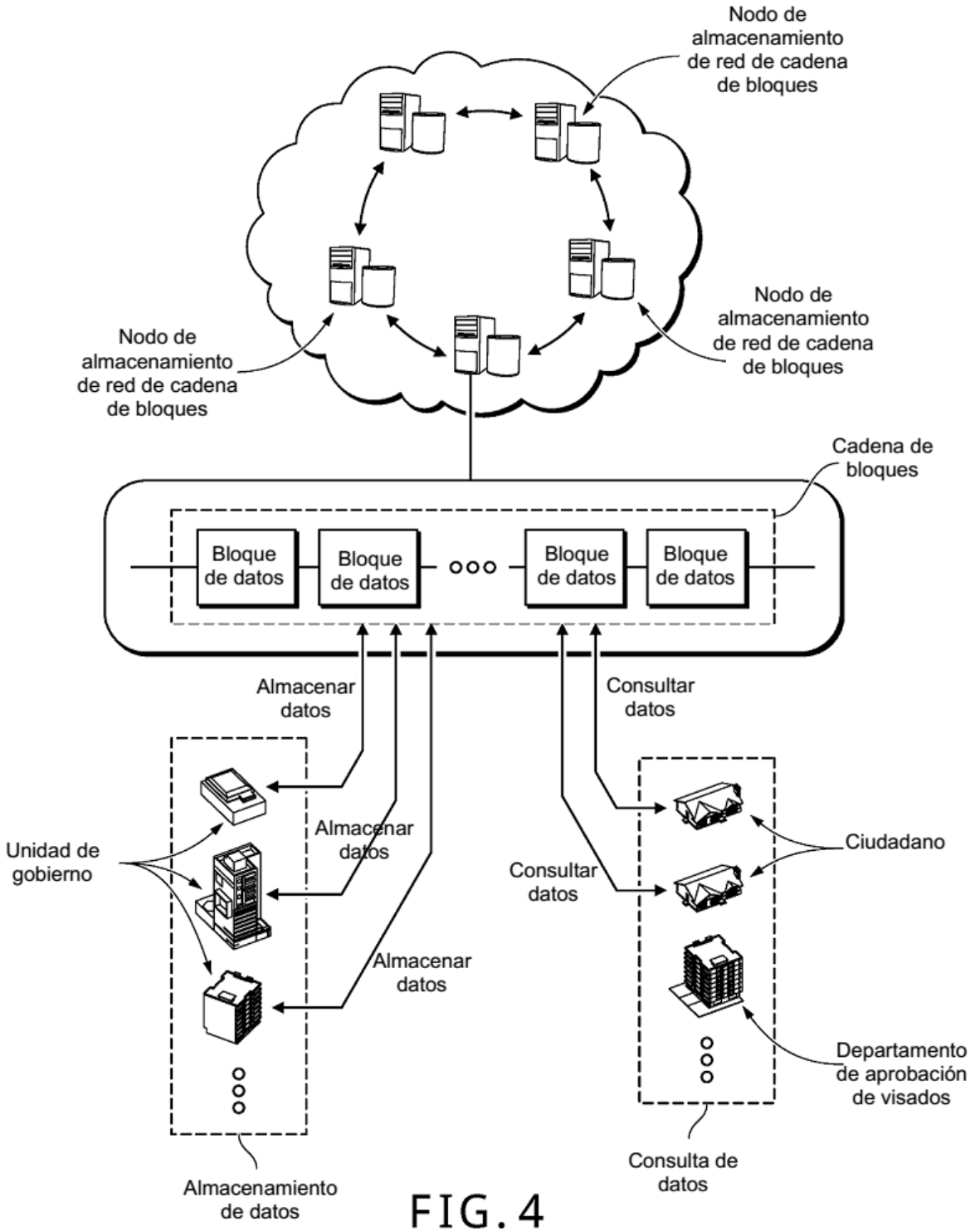
Nodo de almacenamiento de red de cadena de bloques
Nodo de almacenamiento de red de cadena de bloques
Nodo de almacenamiento de red de cadena de bloques
Cadena de bloques
Bloque de datos
Bloque de datos
Bloque de datos
Bloque de datos
Almacenar datos
Consultar datos
Unidad de gobierno
Almacenar datos
Almacenar datos
Consultar datos
Ciudadano
Departamento de aprobación de visados
Almacenamiento de datos
Consulta de datos

FIG. 4

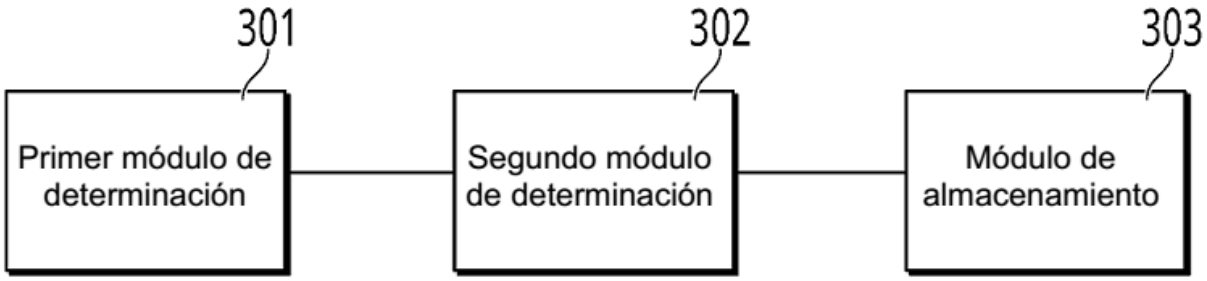
301
302
303
Primer módulo de determinación
Segundo módulo de determinación
Módulo de almacenamiento

FIG. 5

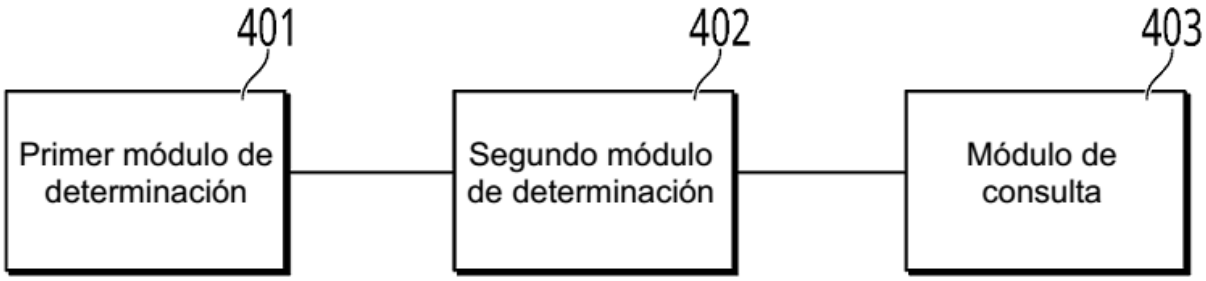
401
402
403
Primer módulo de determinación
Segundo módulo de determinación
Módulo de consulta

FIG. 6