(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 866 161**

(51) Int. CI.:

H04W 12/06 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **26.07.2018 PCT/US2018/043914**

(87) Fecha y número de publicación internacional: **31.01.2019 WO19023466**

(96) Fecha de presentación y número de la solicitud europea: **26.07.2018 E 18756326 (7)**

(97) Fecha y número de publicación de la concesión europea: **17.02.2021 EP 3602959**

(54) Título: **Método y aparato para la comunicación entre nodos de la cadena de bloques**

(30) Prioridad:

26.07.2017 CN 201710616370

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
19.10.2021

(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:

QIU, HONGLIN

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Método y aparato para la comunicación entre nodos de la cadena de bloques

REFERENCIA CRUZADA A SOLICITUDES RELACIONADAS

CAMPO TÉCNICO

La presente patente se refiere al campo de las tecnologías de la información y, en particular, a un método y un aparato de comunicación entre nodos de la cadena de bloques.

ANTECEDENTES

Como rama de la tecnología de cadenas de bloques, la tecnología de cadenas de bloques de consorcio se aplica cada vez más ampliamente. Los nodos de la cadena de bloques en una red de cadenas de bloques de consorcio incluyen pero no limitan nodos de servicio y nodos de consenso. El nodo de servicio participa en un servicio, y el nodo de consenso es responsable de recibir los datos de servicio enviados por el nodo de servicio y de realizar la verificación de consenso de los datos de servicio.

El nodo de servicio anterior es en realidad un servidor de servicios de cada institución que se une a la red de cadenas de bloques de consorcio, y el software utilizado para comunicarse con otro nodo de la red de cadenas de bloques de consorcio se instala en el servidor (el software se denomina como un programa de comunicación en la presente patente). Si dos nodos tienen una relación de servicio fija, los dos nodos pueden almacenar localmente por separado la relación de servicio (la relación de servicio se denomina como relación de mapeo en la presente patente).

La FIG 1 es un diagrama arquitectónico que ilustra una red de cadenas de bloques de consorcio. Según se muestra en la FIG 1, los círculos sólidos son nodos de consenso, y los círculos huecos son nodos de servicio. Diferentes nodos de servicio proporcionan servicios para diferentes aplicaciones (APP). El nodo de servicio envía los datos de servicio generados por la APP al nodo de consenso para la verificación de consenso. Suponiendo que un nodo de servicio es un servidor correspondiente a una aplicación de restauración, y otro nodo de servicio es un servidor correspondiente a una aplicación de pago. Un usuario puede pagar a través de la aplicación de pago después de hacer un pedido a través de una APP correspondiente a la aplicación de restauración; los dos nodos de servicio participan en un mismo servicio y pueden registrar una relación de servicio mostrada en la FIG 1 con la red de cadenas de bloques de consorcio.

Hardjono, Pentland: "Verifiable Anonymous Identities and Access Control in Permissioned Blockchains") aborda la cuestión del control de la identidad y el acceso en las cadenas de bloques compartidas autorizadas. Los autores proponen un sistema que proporciona identidades anónimas pero verificables para las entidades de la cadena de bloques. El sistema también proporciona un control de acceso a las entidades que desean enviar transacciones a la cadena de bloques para leer/verificar las transacciones en la cadena de bloques autorizada. Los nodos de consenso imponen el control de acceso a la cadena de bloques compartida y autorizada mediante una consulta de una lista (de sólo lectura) de claves públicas de los elementos anónimos. El sistema también proporciona la capacidad de desvinculación de las transacciones que pertenecen a una entidad en la cadena de bloques. Esto permite a una entidad describir opcionalmente su identidad cuando se cuestiona una transacción (por ejemplo, por requisitos normativos o de conformidad), pero sin que ello afecte al anonimato y la capacidad de desvinculación de sus transacciones restantes.

En la red de cadenas de bloques de consorcio, cada nodo de servicio almacena los datos de su servicio participante, y los datos del servicio suelen incluir los datos privados del usuario. En función de la tecnología existente, se necesita un método de comunicación más seguro.

El artículo "Verifiable Anonymous Identities and Access Control in Permissioned Blockchains" aborda la cuestión del control de la identidad y el acceso en cadenas de bloques compartidas autorizadas.

RESUMEN

Las implementaciones de la presente patente proporcionan un método y un aparato para la comunicación entre nodos de la cadena de bloques de forma que se resuelva el problema de que los datos privados de un usuario en los datos de servicio almacenados en un nodo de servicio sean propensos a las fugas.

Para resolver el problema técnico anterior, las implementaciones de la presente patente se describen en las reivindicaciones independientes adjuntas.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Para describir las soluciones técnicas en las implementaciones de la presente patente o en la tecnología existente con mayor claridad, a continuación, se describen brevemente los dibujos adjuntos necesarios para describir las

implementaciones o la tecnología existente. Aparentemente, los dibujos adjuntos en la siguiente descripción simplemente muestran algunas implementaciones de la presente patente, y un experto en la técnica puede deducir otros dibujos de estos dibujos adjuntos sin esfuerzos creativos.

La FIG 1 es un diagrama arquitectónico que ilustra una red de cadenas de bloques de consorcio.

La FIG. 2 es un diagrama de flujo que ilustra un método de comunicación entre nodos de la cadena de bloques, de acuerdo con una implementación de la presente patente.

La FIG. 3 es un diagrama arquitectónico esquemático que ilustra otra red de cadenas de bloques de consorcio.

La FIG. 4 es un diagrama esquemático que ilustra un aparato para la comunicación entre nodos de la cadena de bloques, de acuerdo con una implementación de la presente patente.

La FIG. 5 es un diagrama esquemático que ilustra un dispositivo para la comunicación entre nodos de la cadena de bloques, de acuerdo con una implementación de la presente patente.

La FIG. 6 es un diagrama de flujo que ilustra un ejemplo de un método de comunicación implementado por ordenador entre nodos de la cadena de bloques, de acuerdo con una implementación de la presente descripción.

DESCRIPCIÓN DE LAS IMPLEMENTACIONES

En una red de cadenas de bloques de consorcio, los datos de servicio generados por un nodo de servicio que participa en un servicio incluyen pero no limitan los datos privados del usuario. Por consiguiente, para impedir que los datos privados del usuario se filtren a un nodo de servicio que no participe en el servicio, cada nodo de servicio almacena solo los datos de servicio de su servicio participante en la red de cadenas de bloques de consorcio.

Sin embargo, una aplicación real de un servicio, por ejemplo, un nodo de servicio A que no participa en el servicio, puede establecer una conexión de comunicación con un nodo de servicio B que participa en el servicio a través de un programa de comunicación, y puede utilizar un medio técnico (tal como el craqueo de la base de datos) para robar los datos de servicio almacenados en el nodo de servicio B. Es decir, cada nodo de servicio que establece una conexión de comunicación a través de un programa de comunicación puede utilizar un medio técnico para obtener los datos de servicio almacenados en otro nodo de servicio que establece una conexión de comunicación con el nodo de servicio. Dado que los datos de servicio pueden incluir los datos privados del usuario, la presente patente proporciona una solución tecnológica de comunicación más segura.

Para que un experto en la técnica comprenda mejor las soluciones técnicas de la presente patente, a continuación, se describen de forma clara y completa las soluciones técnicas de las implementaciones de la presente patente con referencia a los dibujos adjuntos a las implementaciones de la presente patente. Aparentemente, las implementaciones descritas son sólo algunas y no todas las implementaciones de la presente patente. La invención se define en las reivindicaciones adjuntas.

Las soluciones técnicas proporcionadas en las implementaciones de la presente patente se describen en detalle a continuación con referencia a los dibujos adjuntos.

La FIG. 2 es un diagrama de flujo que ilustra un método de comunicación entre nodos de la cadena de bloques, de acuerdo con una implementación de la presente patente. El método incluye las siguientes etapas.

S200. Un primer nodo de la cadena de bloques recibe una solicitud de comunicación enviada por un segundo nodo de la cadena de bloques.

Un escenario de aplicación de una o más implementaciones de la presente patente es una red de cadenas de bloques, y los nodos de la cadena de bloques incluyen pero no limitan nodos de servicio. Un nodo de servicio puede ser un servidor de una institución que participa en un servicio, y los nodos de servicio intercambian datos a través de un programa de comunicación instalado para ejecutar un servicio. Los nodos de servicio que participan en un mismo servicio tienen una relación de servicio que se muestra en la FIG 1. En la presente patente, la relación de servicio entre los nodos de servicio es una relación de mapeo entre los nodos de la cadena de bloques. Por consiguiente, una relación de mapeo entre los nodos de servicio es en realidad una relación de servicio entre los nodos de servicio.

En esta implementación de la presente patente, el primer nodo de la cadena de bloques es un nodo de la cadena de bloques al que se le solicita establecer una conexión de comunicación, y el segundo nodo de la cadena de bloques es un nodo de la cadena de bloques que solicita establecer una conexión de comunicación.

S202. Determinar si el segundo nodo de la cadena de bloques tiene una relación de mapeo con el primer nodo de la cadena de bloques; y en caso afirmativo, realizar la etapa S204; o en caso contrario, realizar la etapa S206.

S204. Establecer una conexión de comunicación con el segundo nodo de la cadena de bloques.

S206. Rechazar el establecimiento de una conexión de comunicación con el segundo nodo de la cadena de bloques.

Cuando tanto el primer nodo de la cadena de bloques como el segundo nodo de la cadena de bloques son nodos de servicio, el primer nodo de la cadena de bloques que recibe la solicitud de comunicación verifica el segundo nodo de la cadena de bloques que envía la solicitud de comunicación. Si el primer nodo de la cadena de bloques tiene una relación de mapeo con el segundo nodo de la cadena de bloques, indica que el primer nodo de la cadena de bloques y el segundo nodo de la cadena de bloques participan en un mismo servicio, y el primer nodo de la cadena de bloques puede establecer una conexión de comunicación con el segundo nodo de la cadena de bloques. Sin embargo, si el primer nodo de la cadena de bloques no tiene una relación de mapeo con el segundo nodo de la cadena de bloques, indica que el primer nodo de la cadena de bloques y el segundo nodo de la cadena de bloques participan en diferentes servicios, y el primer nodo de la cadena de bloques se puede negar a establecer una conexión de comunicación con el segundo nodo de la cadena de bloques. Cabe señalar que la lógica de ejecución anterior se puede preconfigurar en un programa de comunicación instalado en cada nodo de la cadena de bloques.

Además, los nodos de la cadena de bloques pueden incluir nodos de consenso, y un nodo de consenso es responsable de realizar la verificación de consenso de los datos de servicio generados por un nodo de servicio que participa en un servicio. Para cada nodo de servicio, un nodo de consenso que realiza la verificación de consenso de los datos de servicio generados por el nodo de servicio puede tener una relación de mapeo con el nodo de servicio. Además, para cada nodo de servicio, diferentes nodos de consenso que realizan la verificación de consenso de los datos de servicio generados por el nodo de servicio también pueden tener una relación de mapeo.

Por consiguiente, cuando tanto el primer nodo de la cadena de bloques como el segundo nodo de la cadena de bloques son nodos de consenso, o cuando el primer nodo de la cadena de bloques es un nodo de servicio y el segundo nodo de la cadena de bloques es un nodo de consenso (o cuando el primer nodo de la cadena de bloques es un nodo de consenso y el segundo nodo de la cadena de bloques es un nodo de servicio), el primer nodo de la cadena de bloques puede verificar si el segundo nodo de la cadena de bloques tiene una relación de mapeo con el primer nodo de la cadena de bloques, de forma que se determine si el primer nodo de la cadena de bloques debe establecer una conexión de comunicación con el segundo nodo de la cadena de bloques.

Obviamente, los datos de servicio almacenados en los nodos de servicio que participan en un mismo servicio son datos de servicio del mismo servicio, y no hay riesgo de fuga de datos privados entre los dos nodos de servicio. Del mismo modo, los nodos de consenso que realizan la verificación de consenso sobre un mismo servicio no necesitan robar los datos de servicio entre sí, y un nodo de consenso que realiza la verificación de consenso de los datos de servicio generados por un nodo de servicio tampoco necesita robar los datos de servicio almacenados en el nodo de servicio. Por consiguiente, se puede establecer una conexión de comunicación entre los nodos de la cadena de bloques (independientemente de los nodos de servicio o los nodos de consenso) que tengan una relación de mapeo, y no hay riesgo de fuga de datos privados.

Cabe señalar que cada nodo de la cadena de bloques (independientemente de un nodo de servicio o un nodo de consenso) puede configurar una lista de nodos de la cadena de bloques que tienen una relación de mapeo con el nodo de la cadena de bloques, es decir, los nodos de la cadena de bloques en los que el nodo de la cadena de bloques confía pueden establecer una conexión de comunicación con el nodo de la cadena de bloques.

Además, cuando el primer nodo de la cadena de bloques determina que el segundo nodo de la cadena de bloques tiene una relación de mapeo con el primer nodo de la cadena de bloques, el primer nodo de la cadena de bloques puede enviar una solicitud de verificación al segundo nodo de la cadena de bloques, de modo que el segundo nodo de la cadena de bloques determine si el primer nodo de la cadena de bloques tiene una relación de mapeo con el segundo nodo de la cadena de bloques en función de la solicitud de verificación. En caso afirmativo, el segundo nodo de la cadena de bloques establece una conexión de comunicación con el primer nodo de la cadena de bloques; en caso contrario, el segundo nodo de la cadena de bloques se rechaza a establecer una conexión de comunicación con el primer nodo de la cadena de bloques.

De este modo, se puede implementar una verificación bidireccional entre los dos nodos de la cadena de bloques que necesitan establecer una conexión de comunicación, de modo que el primer nodo de la cadena de bloques determine que el segundo nodo de la cadena de bloques es de confianza. El segundo nodo de la cadena de bloques determina que el primer nodo de la cadena de bloques es de confianza, y la seguridad de la comunicación se mejora adicionalmente.

Ciertamente, el primer nodo de la cadena de bloques puede enviar la solicitud de verificación al segundo nodo de la cadena de bloques después de recibir la solicitud de comunicación enviada por el segundo nodo de la cadena de bloques. El segundo nodo de la cadena de bloques puede utilizar el mismo método para determinar si debe establecer una conexión con el primer nodo de la cadena de bloques.

En el método mostrado en la FIG 2, antes de establecer una conexión de comunicación entre dos nodos de servicio, un nodo de servicio que solicita realizar una comunicación verifica una identidad del nodo de servicio que solicita realizar una comunicación. Una conexión de comunicación se puede establecer entre los dos nodos de servicio sólo cuando el nodo de servicio solicita realizar la comunicación y cuando el nodo de servicio que solicita realizar la comunicación participa en un mismo servicio. Por consiguiente, no se establece una conexión de comunicación entre nodos de servicio que no participan en un mismo servicio, y un nodo de servicio que no participa en un servicio no puede robar datos de servicio almacenados en un nodo de servicio que participa en el servicio a través de un programa de comunicación, garantizando de este modo la seguridad de los datos privados en los datos de servicio.

Además, en una red de cadena de bloques existente, especialmente en una red de cadenas de bloques de consorcio existente, la comunicación entre los nodos de la cadena de bloques se suele basar en el protocolo de seguridad de la capa de transporte (TLS). Por lo general, cada nodo de la cadena de bloques posee un certificado emitido por una autoridad de certificación (AC) de confianza, y el certificado incluye una firma de la AC además de información de atributos del nodo de la cadena de bloques (un servidor) (por ejemplo, los nombres del país, la provincia, la ciudad y la institución a la que pertenece el servidor, y un nombre de dominio del servidor). Basándose en el protocolo TLS, dos nodos de la cadena de bloques que necesitan establecer una conexión de comunicación necesitan intercambiar sus certificados para verificar que sus identidades son autenticadas por la AC (los certificados incluyen pero no limitan firmas de la AC); y los dos nodos de la cadena de bloques pueden establecer una conexión de comunicación si sus identidades son válidas. Obviamente, el protocolo TLS existente no puede impedir el establecimiento de una conexión de comunicación entre nodos de la cadena de bloques que tienen identidades válidas, pero que no tienen una relación de mapeo.

Una o más implementaciones de la presente patente se pueden implementar basándose en el protocolo TLS. Sin embargo, para cada nodo de la cadena de bloques, cuando el nodo de la cadena de bloques solicita a la AC un certificado, el nodo de la cadena de bloques debe proporcionar un identificador del nodo de la cadena de bloques a la AC de modo que la AC pueda añadir el identificador del nodo de la cadena de bloques al certificado del nodo de la cadena de bloques. El identificador del nodo de la cadena de bloques es un identificador único del nodo de la cadena de bloques y puede ser un número del nodo de la cadena de bloques.

Por consiguiente, cada nodo de la cadena de bloques puede almacenar un identificador de nodo de la cadena de bloques que tiene una relación de mapeo con el nodo de la cadena de bloques. En la etapa S200 mostrado en la FIG 1, el primer nodo de la cadena de bloques puede recibir una solicitud de comunicación enviada por el segundo nodo de la cadena de bloques que incluye un certificado del segundo nodo de la cadena de bloques. En la etapa S202, el primer nodo de la cadena de bloques puede obtener un identificador de nodo del certificado del segundo nodo de la cadena de bloques y determinar si el identificador de nodo obtenido tiene una relación de mapeo con un identificador de nodo del primer nodo de la cadena de bloques.

La FIG. 3 es un diagrama arquitectónico esquemático que ilustra otra red de cadenas de bloques de consorcio. Según se muestra en la FIG 3, varios servicios y grupos de verificación de consenso pueden existir en la red de cadenas de bloques de consorcio, y los grupos de verificación de consenso son responsables de verificar diferentes servicios. En esta arquitectura, un certificado emitido por la AC para un nodo de servicio puede incluir además un identificador de servicio de un servicio en el que participa el nodo de servicio, y un certificado emitido por la AC para un nodo de consenso puede incluir además un identificador de un grupo de verificación de consenso al que pertenece el nodo de consenso.

Cada nodo de servicio puede almacenar además un identificador de servicio de su servicio participante, y cada nodo de consenso puede almacenar además un identificador de grupo de un grupo de verificación de consenso que incluye el nodo de consenso. Por consiguiente, el nodo de servicio puede determinar si el nodo de la cadena de bloques tiene una relación de mapeo con el nodo de servicio basándose en un certificado de un nodo de la cadena de bloques que solicita comunicarse con el nodo de servicio; y el nodo de consenso puede determinar si el nodo de la cadena de bloques tiene una relación de mapeo con el nodo de consenso basándose en un certificado de un nodo de la cadena de bloques que solicita comunicarse con el nodo de consenso. En este caso, cabe señalar que cada vez que un primer nodo de la cadena de bloques realiza la verificación, el primer nodo de la cadena de bloques recorre los identificadores de servicio y los identificadores de grupo almacenados en el primer nodo de la cadena de bloques para determinar si existe un identificador de servicio o un identificador de grupo en un certificado de un segundo nodo de la cadena de bloques.

Además, cuando la AC emite un certificado para más de un nodo de la cadena de bloques en una red de cadenas de bloques, la AC puede añadir un identificador de red de la red de cadenas de bloques que incluye el nodo de la cadena de bloques al certificado del nodo de la cadena de bloques. Por consiguiente, cuando se determina que un identificador de red en el certificado del segundo nodo de la cadena de bloques es diferente de un identificador de red de una red de cadenas de bloques que incluye el primer nodo de la cadena de bloques, el primer nodo de la cadena de bloques se puede negar a establecer una conexión de comunicación con el segundo nodo de la cadena de bloques sin realizar una verificación adicional.

Se puede observar que, en esta implementación de la presente patente, un certificado de un nodo de la cadena de bloques puede incluir más campos (tales como el identificador del nodo anterior, el identificador de servicio, el identificador de grupo y el identificador de red) para indicar una identidad del nodo de la cadena de bloques en una red de cadenas de bloques.

Por último, cabe señalar que una o más implementaciones de la presente patente pueden no estar basadas en el protocolo TLS, sino que se especifica un protocolo de comunicaciones y se construye en un programa de comunicación correspondiente a la red de cadenas de bloques. El protocolo de comunicaciones no se limita en la presente patente, siempre que el protocolo de comunicaciones pueda implementar las etapas mostradas en la FIG. 2.

Basándose en el método de comunicación entre nodos de la cadena de bloques mostrado en la FIG. 2, una implementación de la presente patente proporciona además un aparato para la comunicación entre nodos de la cadena de bloques, según se muestra en la FIG. 4. Los nodos de la cadena de bloques en una red de cadenas de bloques incluyen pero no limitan nodos de servicio, y los nodos de servicio que participan en un mismo servicio tienen una relación de mapeo. El aparato incluye lo siguiente: un módulo receptor 401, configurado para recibir una solicitud de comunicación enviada por un segundo nodo de la cadena de bloques; y un módulo de determinación y procesamiento 402, configurado para determinar si el segundo nodo de la cadena de bloques tiene una relación de mapeo con el aparato; y en caso afirmativo, establecer una conexión de comunicación con el segundo nodo de la cadena de bloques; o en caso contrario, negarse a establecer una conexión de comunicación con el segundo nodo de la cadena de bloques.

El nodo de la cadena de bloques incluye además un nodo de consenso. Para cada nodo de servicio, un nodo de consenso que realiza la verificación de consenso de los datos de servicio generados por el nodo de servicio tiene una relación de mapeo con el nodo de servicio; y/o para cada nodo de servicio, los nodos de consenso que realizan la verificación de consenso de los datos de servicio generados por el nodo de servicio tienen una relación de mapeo.

El módulo receptor 401 recibe una solicitud de comunicación enviada por el segundo nodo de la cadena de bloques que incluye un certificado del segundo nodo de la cadena de bloques.

El certificado del segundo nodo de la cadena de bloques incluye un identificador de nodo del segundo nodo de la cadena de bloques.

El módulo de determinación y procesamiento 402 obtiene el identificador de nodo del certificado del segundo nodo de la cadena de bloques, y determina, basándose en el identificador de nodo obtenido, si el identificador de nodo obtenido tiene una relación de mapeo con un identificador de nodo del aparato.

El módulo de determinación y procesamiento 402 envía una solicitud de verificación al segundo nodo de la cadena de bloques, de modo que el segundo nodo de la cadena de bloques determina si el aparato tiene una relación de mapeo con el segundo nodo de la cadena de bloques basándose en la solicitud de verificación; y en caso afirmativo, el segundo nodo de la cadena de bloques establece una conexión de comunicación con el aparato; o en caso contrario, el segundo nodo de la cadena de bloques se rechaza a establecer una conexión de comunicación con el aparato.

Basándose en el método de formación de módulos mostrado en la FIG 2, una implementación de la presente patente proporciona además un dispositivo para la comunicación entre nodos de la cadena de bloques. El dispositivo incluye uno o más procesadores y una memoria, la memoria almacena un programa, y el programa es ejecutado por el uno o más procesadores para realizar las siguientes etapas: recibir una solicitud de comunicación enviada por un segundo nodo de la cadena de bloques; determinar si el segundo nodo de la cadena de bloques tiene una relación de mapeo con el dispositivo; y en caso afirmativo, establecer una conexión de comunicación con el segundo nodo de la cadena de bloques; o en caso contrario, negarse a establecer una conexión de comunicación con el segundo nodo de la cadena de bloques.

Los nodos de la cadena de bloques en una red de cadenas de bloques incluyen pero no limitan los nodos de servicio, y los nodos de servicio que participan en un mismo servicio tienen una relación de mapeo.

Todas las implementaciones de la presente patente se describen de forma progresiva. Se puede hacer referencia mutua a estas implementaciones para partes iguales o similares en las implementaciones. Cada implementación se centra en una diferencia entre otras implementaciones. En particular, el dispositivo para la comunicación entre nodos de la cadena de bloques mostrado en la FIG. 5 es básicamente similar a la implementación del método y, por consiguiente, se describe brevemente. es básicamente similar a la implementación del método y, por consiguiente, se describe brevemente.

En los años 90, la mejora de una tecnología se puede distinguir claramente entre la mejora del hardware (por ejemplo, la mejora de estructuras de circuitos tales como un diodo, un transistor y un interruptor) y la mejora del software (la mejora de un procedimiento de método). Sin embargo, con el desarrollo de las tecnologías, la mejora de muchos procedimientos de métodos se pueden considerar una mejora directa de una estructura de circuito de hardware. Los diseñadores casi siempre programan un procedimiento de método mejorado en un circuito de hardware para obtener una estructura de circuito de hardware correspondiente. Por consiguiente, no se puede decir que una mejora de un

procedimiento de método no se pueda implementar utilizando un módulo de entidad de hardware. Por ejemplo, un dispositivo lógico programable (PLD) (por ejemplo, una matriz de puertas programables en campo (FPGA)) es un tipo de circuito integrado. La función lógica del PLD se determina mediante la programación de componentes ejecutada por un usuario. Los diseñadores realizan la programación para "integrar" un sistema digital en un único PLD sin necesidad de que un fabricante de chips diseñe y produzca un chip de circuito integrado dedicado. Además, en lugar de producir manualmente un chip de circuito integrado, la programación se lleva a cabo en su mayor parte mediante un software "compilador lógico", que es similar a un compilador de software utilizado durante el desarrollo de programas. El código original antes de la compilación también se escribe en un lenguaje de programación específico, que se denomina lenguaje de descripción de hardware (HDL). Puede haber varios HDL, tales como un lenguaje de expresión booleana avanzada (ABEL), un lenguaje de descripción de hardware de altera (AHDL), confluence, un lenguaje de programación de la universidad de Cornell (CUPL), un HDCal, un lenguaje de descripción de hardware de Java (JHDL), un Lava, un Lola, un MyHDL, un PALASM y un lenguaje de descripción de hardware de Rubí (RHDL). Actualmente, los lenguajes de descripción de hardware de circuitos integrados de muy alta velocidad (VHDL) y Verilog son los más utilizados. Un experto en la técnica debe entender también que un procedimiento de método sólo se necesita programar de forma lógica, y programar el circuito integrado mediante el uso de los lenguajes de descripción de hardware anteriores, de modo que se puede obtener fácilmente un circuito de hardware que implemente el procedimiento de método lógico.

El controlador se puede implementar de cualquier manera adecuada. Por ejemplo, el controlador puede ser un microprocesador, un procesador, un medio legible por ordenador que almacene un código de programa legible por ordenador (por ejemplo, software o firmware) que se pueda ejecutar por un (micro) procesador, una puerta lógica, un interruptor, un circuito integrado de aplicación específica (ASIC), un controlador lógico programable o un microcontrolador integrado. Los ejemplos del controlador incluyen, entre otros a los siguientes microcontroladores: ARC 625D, Atmel AT91SAM, Microchip PIC18F26K20 y Silicone Labs C8051F320. El controlador de memoria también se puede implementar como una parte de la lógica de control de la memoria. Un experto en la técnica sabe también que un controlador se puede implementar únicamente en forma de código de programa legible por ordenador, y las etapas en el método se pueden programar de forma lógica para permitir que el controlador implemente además las mismas funciones en forma de una puerta lógica, un interruptor, un circuito integrado de aplicación específica, un controlador lógico programable, un microcontrolador integrado, etc. Por consiguiente, el controlador se puede considerar como un componente de hardware, y un aparato incluido en el controlador y configurado para implementar diversas funciones también se puede considerar como una estructura en el componente de hardware. Como alternativa, un aparato configurado para implementar diversas funciones se puede considerar tanto un módulo de software para implementar el método como una estructura en un componente de hardware.

El sistema, el aparato, el módulo o la unidad descritos en las implementaciones anteriores se pueden implementar mediante un chip de ordenador o una entidad, o se pueden implementar mediante un producto con una función específica. Un dispositivo de implementación típico es un ordenador. El 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, una consola de juegos, un ordenador tipo tableta, un dispositivo para llevar puesto o una combinación de cualquiera de estos dispositivos.

Para facilitar la descripción, el aparato anterior se describe dividiendo las funciones en diversas unidades. Ciertamente, cuando se implementa la presente patente, las funciones de cada unidad se pueden implementar en una o más piezas de software y/o hardware.

Un experto en la técnica debe entender que una o más implementaciones de la presente patente se pueden proporcionar como un método, un sistema o un producto de programa informático. Por consiguiente, la una o más implementaciones de la presente patente pueden utilizar una forma de implementaciones sólo de hardware, implementaciones sólo de software, o implementaciones con una combinación de software y hardware. Además, la una o más implementaciones de la presente patente pueden utilizar una forma de producto de programa informático que se implemente en uno o más medios de almacenamiento utilizables en ordenador (incluyendo, pero sin limitarse a, una memoria de disco, un CD-ROM, una memoria óptica, etc.) que incluyan un código de programa utilizable por ordenador.

La presente patente se describe 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 una o más implementaciones de la presente patente. Se debe entender que las instrucciones de programa informático se pueden utilizar para implementar cada proceso y/o cada bloque en los diagramas de flujo y/o los diagramas de bloques y una combinación de un proceso y/o un bloque en los diagramas de flujo y/o los diagramas de bloques. Estas instrucciones de programa informático se pueden proporcionar para un ordenador de propósito general, un ordenador dedicado, un procesador integrado o un procesador de cualquier otro dispositivo de procesamiento de datos programable para generar una máquina, de modo que las instrucciones ejecutadas por un ordenador o un procesador de cualquier otro dispositivo de procesamiento de datos programable generen un aparato para implementar una función específica en uno o más procedimientos en los diagramas de flujo y/o en uno o más bloques en los diagramas de bloques.

Estas instrucciones de programa informático se pueden almacenar en una memoria legible por ordenador que puede dar instrucciones al ordenador o a cualesquiera otros dispositivos de procesamiento de datos programables para que funcionen de una manera específica, de modo que las instrucciones almacenadas en la memoria legible por ordenador puedan generar un artefacto que incluya un aparato de instrucción. El aparato de instrucción implementa una función específica en uno o más procedimientos en los diagramas de flujo y/o en uno o más bloques en los diagramas de bloques.

Estas instrucciones de programa informático se pueden cargar en un ordenador o en otro dispositivo de procesamiento de datos programable, de modo que se ejecuten una serie de operaciones y etapas en el ordenador o en el otro dispositivo programable, generando de este modo un procesamiento implementado por ordenador. Por consiguiente, las instrucciones ejecutadas en el ordenador u otro dispositivo programable proporcionan etapas para implementar una función específica en uno o más procedimientos 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 una o más unidades centrales de procesamiento (CPU), una interfaz de entrada/salida, una interfaz de red y una memoria.

La memoria puede incluir una memoria no persistente, una memoria de acceso aleatorio (RAM), una memoria no volátil, y/o otra forma que se encuentre en un medio legible por ordenador, por ejemplo, una memoria de sólo lectura (ROM) o una memoria flash (flash RAM). La memoria es un ejemplo de medio legible por ordenador.

El medio legible por ordenador incluye medios persistentes, no persistentes, móviles e inamovibles 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 del medio de almacenamiento informático incluyen, entre otros, una memoria de acceso aleatorio paramétrico (PRAM), una memoria de acceso aleatorio estática (SRAM), una memoria de acceso aleatorio dinámica (DRAM), otro tipo de memoria de acceso aleatorio (RAM), una memoria de sólo lectura (ROM), una memoria de sólo lectura programable eléctricamente borrable (EEPROM) una memoria flash u otra tecnología de memoria, una memoria de sólo lectura en disco compacto (CD-ROM), un disco versátil digital (DVD) u otro tipo de almacenamiento óptico, una cinta magnética de casete, un almacenamiento en cinta y disco u otro dispositivo de almacenamiento magnético, o cualquier otro medio que no sea de transmisión y que se pueda configurar para almacenar información a la que pueda acceder un dispositivo informático. Según se describe en la presente patente, el medio legible por ordenador no incluye los medios transitorios legibles por ordenador (medios transitorios), tales como una señal de datos modulada y una portadora.

Cabe señalar además que, los términos "incluye", "comprende", o cualquier variante de los mismos, pretenden abarcar una inclusión no exclusiva, de modo que un proceso, un método, un producto básico o un dispositivo que incluya una lista de elementos no sólo incluya dichos elementos, sino que también incluya otros elementos que no estén expresamente enumerados, o incluya además elementos inherentes a dicho proceso, método, producto básico o dispositivo. Sin más limitaciones, un elemento descrito por la frase "incluye un ..." incluye además otro elemento idéntico en el proceso, método, producto básico o dispositivo que incluye el elemento.

Un experto en la técnica debe entender que una o más implementaciones de la presente patente se pueden proporcionar como un método, un sistema o un producto de programa informático. Por consiguiente, la presente patente puede utilizar una forma de implementaciones de sólo hardware, implementaciones de sólo software, o implementaciones con una combinación de software y hardware. Además, la presente patente puede utilizar una forma de producto de programa informático que se implementa en uno o más medios de almacenamiento utilizables por ordenador (incluyendo, pero sin limitarse a, una memoria de disco, un CD-ROM, una memoria óptica, etc.) que incluyen pero no limitan, un código de programa utilizable por ordenador.

La presente patente se puede describir en el contexto general de las instrucciones ejecutables por un ordenador, por ejemplo, un módulo de programa. Por lo general, el módulo de programa incluye una rutina, un programa, un objeto, un componente, una estructura de datos, etc. para ejecutar una tarea particular o implementar un tipo de datos abstracto particular. La presente patente también se puede poner en práctica en entornos informáticos distribuidos en los que las tareas son realizadas por dispositivos de procesamiento remotos que están conectados mediante el uso de una red de comunicaciones. En los entornos informáticos distribuidos, los módulos de programa pueden estar ubicados en medios de almacenamiento informático tanto locales como remotos, incluyendo dispositivos de almacenamiento.

Las implementaciones anteriores son simplemente implementaciones de la presente patente, y no pretenden limitar la presente patente. Un experto en la técnica puede realizar diversas modificaciones y variaciones de la presente patente.

La FIG. 6 es un diagrama de flujo que ilustra un ejemplo de un método 600 implementado por ordenador para la comunicación entre nodos de la cadena de bloques, de acuerdo con una implementación de la presente descripción. Por claridad de presentación, la descripción que sigue describe generalmente el método 600 en el contexto de las otras figuras de esta descripción. Sin embargo, se entenderá que el método 600 se puede realizar, por ejemplo, por cualquier sistema, entorno, software y hardware, o una combinación de sistemas, entornos, software y hardware,

según corresponda. En algunas implementaciones, diversas etapas del método 600 se pueden ejecutar en paralelo, en combinación, en bucles, o en cualquier orden.

En general, antes de que se establezca una conexión de comunicación entre dos nodos en una cadena de bloques, uno o ambos nodos a los que se les solicita realizar una comunicación pueden verificar la identidad del otro nodo antes de establecer la conexión de comunicación y permitir que se produzca la comunicación. En particular, al menos algunos de los nodos de la cadena de bloques se pueden considerar nodos de servicio, donde los nodos de servicio pueden ser un servidor de una institución que participa en un servicio, y donde los nodos de servicio intercambian datos a través de un programa de comunicación instalado para ejecutar un servicio. Se puede considerar que los nodos de servicio que participan en un mismo servicio tienen una relación de servicio, en donde la relación de servicio corresponde a una relación de mapeo entre los dos nodos de servicio. Cuando dos nodos de la cadena de bloques participan en un mismo servicio, se considera que los dos nodos tienen una relación de mapeo, y pueden permitir que se establezca una conexión de comunicación. Si los dos nodos no participan en el mismo servicio, entonces la conexión de comunicación puede ser rechazada, evitando potencialmente el intercambio de datos no autorizados entre nodos que no participan en el mismo servicio.

En algunos casos, los nodos de la cadena de bloques pueden incluir nodos de consenso, en los donde los nodos de consenso son responsables de realizar la verificación de consenso de los datos de servicio generados por un nodo de servicio que participa en un servicio. Para cada nodo de servicio, se puede considerar que un nodo de consenso que realiza la verificación de consenso de los datos de servicio generados por ese nodo de servicio tiene una relación de mapeo con el nodo de servicio. Además, para cada nodo de servicio, los diferentes nodos de consenso que realizan la verificación de consenso de los datos de servicio generados por el nodo de servicio también pueden tener una relación de mapeo.

Volviendo a la ilustración del método 600, en 602, un primer nodo de una red de cadenas de bloques recibe una solicitud de comunicación de un segundo nodo de la red de cadenas de bloques. A partir de 602, el método 600 pasa a 604.

En 604, se determina si el segundo nodo tiene una relación de mapeo con el primer nodo. Si se determina que el segundo nodo tiene una relación de mapeo con el primer nodo, entonces el método 600 pasa a 606. En caso contrario, si se determina que el segundo nodo no tiene una relación de mapeo con el segundo nodo, entonces el método 600 pasa a 608.

La determinación de si el segundo nodo tiene una relación de mapeo con el primer nodo se puede realizar de diversas maneras. En un caso, se puede determinar de forma general si el primer nodo y el segundo participan en los mismos o diferentes servicios. Si los dos nodos participan en el mismo servicio, entonces existe una relación de servicio, que es un tipo de relación de mapeo, entre los nodos, y se determina que existe la relación de mapeo. Si los dos nodos no participan en el mismo servicio, sino en servicios diferentes y no superpuestos, entonces se determina que no existe ninguna relación de mapeo entre los nodos.

Como se ha señalado anteriormente, cuando tanto el primer nodo como el segundo son nodos de consenso asociados a un nodo de servicio común, cuando el primer nodo es un nodo de servicio y el segundo nodo es un nodo de consenso del primer nodo, o cuando el primer nodo es un nodo de consenso del segundo nodo, entonces se determina que existe una relación de mapeo entre los nodos.

En algunos casos, un nodo particular de la cadena de bloques, que incluye tanto los nodos de servicio como los nodos de consenso, puede configurar, generar, mantener o tener acceso de otro modo a una lista de nodos que tienen una relación de mapeo con ese nodo. En otras palabras, el nodo particular de la cadena de bloques puede almacenar o utilizar información que identifique otros nodos de la cadena de bloques con los que exista una relación de confianza basada en una relación de mapeo. En un ejemplo, un nodo particular puede almacenar un identificador de nodo de cada nodo que tenga una relación de mapeo con el nodo particular. El identificador de nodo para cada nodo se puede incluir o asociar de otro modo con un certificado digital que se emita para esos nodos. Por ejemplo, cuando un nodo de la cadena de bloques solicita a una autoridad de certificación (AC) un certificado digital, el nodo de la cadena de bloques puede proporcionar un identificador de nodo a la AC de modo que la AC pueda añadir el identificador de nodo del nodo de la cadena de bloques al certificado digital del nodo de la cadena de bloques. El identificador del nodo de la cadena de bloques puede ser un identificador único del nodo de la cadena de bloques, y puede ser, en algunos casos, un número del nodo de la cadena de bloques. El nodo particular, por consiguiente, puede almacenar los identificadores de nodo únicos de al menos algunos de los otros nodos con los que el nodo particular tenga una relación de mapeo. En estos casos, la determinación de si existe una relación de mapeo incluye la obtención de un identificador de nodo del nodo solicitante (tal como, a partir de un certificado digital del nodo solicitante incluido en la solicitud) y la determinación de si el identificador de nodo obtenido está asociado a un nodo que tiene una relación de mapeo con el nodo particular.

En todavía otros casos, la AC puede emitir certificados digitales para los nodos de servicio, donde el certificado digital incluya un identificador de servicio en el que participe el nodo de servicio. La AC también pueden emitir certificados digitales para nodos de consenso que pueden incluir un identificador de grupo de un grupo de verificación de consenso

al que pertenece el nodo de consenso. Cada nodo de servicio puede almacenar o estar asociado de otro modo a un identificador de servicio de su servicio participante, y cada nodo de consenso puede almacenar un identificador de grupo de un grupo de verificación de consenso que incluya el nodo de consenso. Utilizando esa información, un nodo de servicio puede determinar si el nodo de la cadena de bloques que solicita la conexión de comunicación tiene una relación de mapeo con el nodo de servicio, y el nodo de consenso puede determinar si el nodo de la cadena de bloques tiene una relación de mapeo con el nodo de consenso basándose en un certificado de un nodo de la cadena de bloques que solicita comunicarse con el nodo de consenso. En este caso, cabe señalar que cada vez que un primer nodo de la cadena de bloques realiza la verificación, el primer nodo de la cadena de bloques recorre los identificadores de servicio y los identificadores de grupo almacenados en el primer nodo de la cadena de bloques para determinar si existe un identificador de servicio o un identificador de grupo en un certificado de un segundo nodo de la cadena de bloques.

Además, cuando la AC emite un certificado para más de un nodo de la cadena de bloques en una red de cadenas de bloques, la AC puede añadir un identificador de red de la red de cadenas de bloques que incluya el nodo de la cadena de bloques al certificado del nodo de la cadena de bloques. Por consiguiente, cuando se determina que un identificador de red en el certificado del segundo nodo de la cadena de bloques es diferente de un identificador de red de una red de cadenas de bloques que incluye el primer nodo de la cadena de bloques, el primer nodo de la cadena de bloques se puede negar a establecer una conexión de comunicación con el segundo nodo de la cadena de bloques sin realizar una verificación adicional.

En una implementación, un certificado de un nodo de la cadena de bloques puede incluir más campos (tal como el identificador de nodo, el identificador de servicio, el identificador de grupo y el identificador de red) para indicar una identidad del nodo de la cadena de bloques en una red de cadenas de bloques.

En 608, después de determinar que no existe relación de mapeo entre el primer nodo y el segundo nodo, el primer nodo se puede negar a establecer una comunicación con el segundo nodo basándose en la determinación. Después de 608, el método 600 se puede detener.

Como se ha señalado, cuando se determina que existe una relación de mapeo entre el primer nodo y el segundo nodo, el método 600 continúa en 606. En 606, se determina si un protocolo de comunicación de la cadena de bloques requiere verificación bidireccional. En caso negativo, el método 600 continúa en 610, donde el primer nodo puede establecer la conexión de comunicación desde el primer nodo al segundo nodo basándose en la relación de mapeo determinada. Después de 610, el método 600 se puede detener. Sin embargo, si se requiere una verificación bidireccional, el método 600 pasa a 612.

En 612, el primer nodo puede enviar una solicitud de verificación del primer nodo al segundo nodo. En respuesta a la solicitud, el segundo nodo realiza una determinación en 614 sobre si el primer nodo tiene una relación de mapeo con el segundo nodo. En caso afirmativo, el segundo nodo puede establecer una conexión de comunicación con el primer nodo en 616, mientras que, en caso negativo, el segundo nodo puede rechazar el intento de conexión de comunicación con el primer nodo en 618. Al requerir la verificación bidireccional, la seguridad de la comunicación dentro de la cadena de bloques se puede mejorar y aumentar, asegurando que las comunicaciones estén permitidas en ambas direcciones antes de establecer la conexión de comunicación. Después de 616 o 618, el método 600 se puede detener.

En una red de cadenas de bloques existente, tal como una red de cadenas de bloques de consorcio, la comunicación entre los nodos de la cadena de bloques se puede basar en el protocolo de seguridad de la capa de transporte (TLS). Por lo general, cada nodo de la cadena de bloques posee un certificado digital emitido por una AC de confianza, y el certificado digital incluye una firma de la AC además de información de atributos del nodo de la cadena de bloques (un servidor) (por ejemplo, los nombres del país, la provincia, la ciudad y la institución a la que pertenece el servidor, y un nombre de dominio del servidor). Basándose en el protocolo TLS, dos nodos de la cadena de bloques que necesitan establecer una conexión de comunicación necesitan intercambiar sus certificados digitales para verificar que sus identidades estén autenticadas por la AC (los certificados incluyen pero no limitan firmas de la AC). Los dos nodos de la cadena de bloques pueden establecer una conexión de comunicación si sus identidades son válidas.

Las implementaciones de la solución descrita proporcionan importantes ventajas técnicas. Como los datos de servicio almacenados en los nodos de servicio que participan en un mismo servicio son datos de servicio del mismo servicio, no hay riesgo de fuga de datos privados entre dos nodos de servicio cuando dichos nodos de servicio participan en el mismo servicio. Del mismo modo, los nodos de consenso que realizan la verificación de consenso de un mismo servicio no necesitan robar los datos de servicio uno del otro, y un nodo de consenso que realiza la verificación de consenso de los datos de servicio generados por un nodo de servicio tampoco necesita robar los datos de servicio almacenados en el nodo de servicio. Por consiguiente, se puede establecer una conexión de comunicación entre los nodos de la cadena de bloques (independientemente de los nodos de servicio o los nodos de consenso) que tengan una relación de mapeo, sin riesgo de fuga de datos privados.

Las soluciones descritas pueden garantizar que existen relaciones satisfactorias entre los nodos de una cadena de bloques antes de establecer conexiones de comunicación entre los nodos. Al hacerlo, la seguridad de la comunicación dentro de la cadena de bloques se incrementa al limitar las conexiones internodales permitidas a aquellos nodos con

una relación de mapeo existente. La relación de mapeo existente se puede basar en la participación de los nodos en un servicio común, donde los datos de servicio asociados a ese servicio ya están disponibles para cada nodo. Como las conexiones de comunicación no se establecen, y de hecho se rechazan, entre nodos de servicio que no participan en un mismo servicio, los nodos de servicio que no participan en un servicio particular no se pueden utilizar para robar o interceptar datos de servicio almacenados en un nodo de servicio que participa en ese servicio particular, garantizando de este modo la seguridad de los datos privados de los datos de servicio del servicio.

Las formas de realización y las operaciones descritas en esta memoria descriptiva se pueden implementar con circuitos electrónicos digitales, o con software, firmware o hardware informático, incluyendo las estructuras descritas en esta memoria descriptiva o en combinaciones de una o más de ellas. Las operaciones se pueden implementar como operaciones realizadas por un aparato de procesamiento de datos sobre datos almacenados en uno o más dispositivos de almacenamiento legibles por ordenador o recibidos de otras fuentes. Un aparato de procesamiento de datos, ordenador o dispositivo informático puede abarcar aparatos, dispositivos y máquinas para el procesamiento de datos, incluyendo a modo de ejemplo un procesador programable, un ordenador, un sistema en un chip, o múltiples o combinaciones de los anteriores. El aparato puede incluir circuitos lógicos de propósito especial, por ejemplo, una unidad central de procesamiento (CPU), una matriz de puertas programables en campo (FPGA) o un circuito integrado de aplicación específica (ASIC). El aparato también puede incluir código que crea un entorno de ejecución para el programa informático en cuestión, por ejemplo, código que constituye el firmware del procesador, una pila de protocolos, un sistema de gestión de bases de datos, un sistema operativo (por ejemplo, un sistema operativo o una combinación de sistemas operativos), un entorno de ejecución multiplataforma, una máquina virtual, o una combinación de uno o más de ellos. El aparato y el entorno de ejecución pueden realizar diversas infraestructuras de modelos de computación diferentes, tales como servicios web, computación distribuida e infraestructuras de computación en red.

Un programa informático (también conocido, por ejemplo, como programa, software, aplicación de software, módulo de software, unidad de software, script o código) se puede escribir en cualquier forma de lenguaje de programación, incluyendo lenguajes compilados o interpretados, lenguajes declarativos o procedimentales, y se puede implementar en cualquier forma, incluyendo como un programa independiente o como un módulo, componente, subrutina, objeto u otra unidad adecuada para su utilización en un entorno informático. Un programa se puede almacenar en una parte de un archivo que contiene otros programas o datos (por ejemplo, uno o más scripts almacenados en un documento de lenguaje de marcas), en un único archivo dedicado al programa en cuestión, o en múltiples archivos coordinados (por ejemplo, archivos que almacenan uno o más módulos, subprogramas o partes de código). Un programa informático se puede ejecutar en un ordenador o en varios ordenadores situados en un mismo sitio o distribuidos en varios sitios e interconectados por una red de comunicación.

Los procesadores para la ejecución de un programa informático incluyen, a modo de ejemplo, tanto los microprocesadores de propósito general como los de propósito especial, y uno o varios procesadores de cualquier clase de ordenador digital. Por lo general, un procesador recibirá instrucciones y datos de una memoria de sólo lectura, de una memoria de acceso aleatorio o de ambas. Los elementos esenciales de un ordenador son un procesador para realizar acciones de acuerdo con las instrucciones y uno o más dispositivos de memoria para almacenar instrucciones y datos. Por lo general, un ordenador también incluirá, o se acoplará de forma operativa para recibir datos desde o transferir datos a, o ambos, uno o más dispositivos de almacenamiento masivo para almacenar datos. Un ordenador se puede integrar en otro dispositivo, por ejemplo, un dispositivo móvil, un asistente digital personal (PDA), una consola de juegos, un receptor del sistema de posicionamiento global (GPS) o un dispositivo de almacenamiento portátil. Los dispositivos adecuados para almacenar las instrucciones y los datos del programa informático incluyen pero no limitan memorias no volátiles, medios y dispositivos de memoria, incluyendo, a modo de ejemplo, dispositivos de memoria de semiconductores, discos magnéticos y discos magneto-ópticos. El procesador y la memoria se pueden complementar por, o incorporar en, circuitos lógicos de propósito especial.

Los dispositivos móviles pueden incluir teléfonos, equipos de usuario (UE), teléfonos móviles (por ejemplo, teléfonos inteligentes), tabletas, dispositivos para llevar puestos (por ejemplo, relojes inteligentes y gafas inteligentes), dispositivos implantados dentro del cuerpo humano (por ejemplo, biosensores, implantes cocleares), u otros tipos de dispositivos móviles. Los dispositivos móviles se pueden comunicar de forma inalámbrica (por ejemplo, utilizando señales de radiofrecuencia (RF)) con diversas redes de comunicación (descritas a continuación). Los dispositivos móviles pueden incluir sensores para determinar las características del entorno actual del dispositivo móvil. Los sensores pueden incluir cámaras, micrófonos, sensores de proximidad, sensores GPS, sensores de movimiento, acelerómetros, sensores de luz ambiental, sensores de humedad, giroscopios, brújulas, barómetros, sensores de huellas dactilares, sistemas de reconocimiento facial, sensores de RF (por ejemplo, radios Wi-Fi y celulares), sensores térmicos u otros tipos de sensores. Por ejemplo, las cámaras pueden incluir una cámara orientada hacia delante o hacia atrás con lentes móviles o fijas, un flash, un sensor de imagen y un procesador de imágenes. La cámara puede ser una cámara de megapíxeles que puede capturar detalles para el reconocimiento facial y/o del iris. La cámara, junto con un procesador de datos y la información de autentificación almacenada en la memoria o a la que se accede de forma remota, puede formar un sistema de reconocimiento facial. El sistema de reconocimiento facial o uno o más sensores, por ejemplo, micrófonos, sensores de movimiento, acelerómetros, sensores GPS o sensores RF, se pueden utilizar para la autentificación del usuario.

Para posibilitar la interacción con un usuario, las formas de realización se pueden implementar en un ordenador que tenga un dispositivo de visualización y un dispositivo de entrada, por ejemplo, una pantalla de cristal líquido (LCD) o un diodo orgánico de emisión de luz (OLED)/realidad virtual (VR)/realidad aumentada (AR) para mostrar información al usuario y una pantalla táctil, un teclado y un dispositivo señalador mediante el cual el usuario pueda proporcionar información al ordenador. También se pueden utilizar otras clases de dispositivos para posibilitar la interacción con el usuario; por ejemplo, la retroalimentación que se proporciona al usuario puede ser cualquier forma de retroalimentación sensorial, por ejemplo, retroalimentación visual, auditiva o táctil; y la entrada del usuario se puede recibir de cualquier forma, incluyendo entrada acústica, verbal o táctil. Además, un ordenador puede interactuar con un usuario enviando documentos a y recibiendo documentos de un dispositivo utilizado por el usuario; por ejemplo, enviando páginas web a un navegador web en un dispositivo cliente del usuario en respuesta a las solicitudes recibidas del navegador web.

Las formas de realización se pueden implementar utilizando dispositivos informáticos interconectados por cualquier forma o medio de comunicación de datos digital cableado o inalámbrico (o una combinación de los mismos), por ejemplo, una red de comunicación. Ejemplos de dispositivos interconectados son un cliente y un servidor generalmente remotos entre sí que suelen interactuar a través de una red de comunicación. Un cliente, por ejemplo, un dispositivo móvil, puede realizar transacciones por sí mismo, con un servidor, o a través de un servidor, por ejemplo, realizando transacciones de compra, venta, pago, regalo, envío o préstamo, o autorizando las mismas. Dichas transacciones se pueden realizar en tiempo real, de tal manera que una acción y una respuesta sean temporalmente próximas; por ejemplo, un individuo percibe que la acción y la respuesta se producen, en esencia, de forma simultánea, la diferencia de tiempo para una respuesta que sigue a la acción del individuo es inferior a 1 milisegundo (ms) o inferior a 1 segundo (s), o la respuesta es sin retraso intencionado teniendo en cuenta las limitaciones de procesamiento del sistema.

Los ejemplos de redes de comunicación incluyen pero no limitan una red de área local (LAN), una red de acceso de radio (RAN), una red de área metropolitana (MAN) y una red de área amplia (WAN). La red de comunicación puede incluir la totalidad o una parte de Internet, otra red de comunicación o una combinación de redes de comunicación. La información se puede transmitir en la red de comunicación de acuerdo con diversos protocolos y estándares, incluyendo la evolución a largo plazo (LTE), 5G, IEEE 802, protocolo de Internet (IP), u otros protocolos o combinaciones de protocolos. La red de comunicación puede transmitir voz, vídeo, datos biométricos o de autentificación, u otra información entre los dispositivos informáticos conectados.

Las características descritas como implementaciones separadas se pueden implementar, en combinación, en una única implementación, mientras que las características descritas como una única implementación se pueden implementar en múltiples implementaciones, por separado, o en cualquier subcombinación adecuada. Las operaciones descritas y reivindicadas en un orden particular no se deben entender como que se requiere ese orden particular, ni que se deban realizar todas las operaciones ilustradas (algunas operaciones pueden ser opcionales). Según el caso, se puede realizar la multitarea o el procesamiento en paralelo (o una combinación de multitarea y procesamiento en paralelo).

REIVINDICACIONES

1. Un método de comunicación entre nodos de la cadena de bloques, comprendiendo el método:

recibir (S200, 602), por un primer nodo de la cadena de bloques de una red de cadenas de bloques, una solicitud de comunicación enviada por un segundo nodo de la cadena de bloques de la red de cadenas de bloques, comprendiendo la solicitud de comunicación un certificado del segundo nodo de la cadena de bloques, comprendiendo el certificado del segundo nodo de la cadena de bloques varios identificadores, que incluyen:

un identificador de nodo del segundo nodo de la cadena de bloques,

un identificador de red,

un identificador del nodo anterior, y

un identificador de servicio o un identificador de grupo;

obtener los varios identificadores a partir del certificado del segundo nodo de la cadena de bloques;

determinar (S202, 604), basándose en los varios identificadores obtenidos, si el segundo nodo de la cadena de bloques tiene una relación de mapeo con el primer nodo de la cadena de bloques; y

establecer (S204, 610), mediante el primer nodo de la cadena de bloques, una conexión de comunicación desde el primer nodo de la cadena de bloques al segundo nodo de la cadena de bloques, si se determina que el segundo nodo de la cadena de bloques tiene una relación de mapeo con el primer nodo de la cadena de bloques; o

rechazar (S206, 608), mediante el primer nodo de la cadena de bloques, establecer una conexión de comunicación desde el primer nodo de la cadena de bloques al segundo nodo de la cadena de bloques, si se determina que el segundo nodo de la cadena de bloques no tiene una relación de mapeo con el primer nodo de la cadena de bloques.

2. El método de acuerdo con la reivindicación 1, en donde la red de cadenas de bloques comprende nodos de servicio y dos o más nodos de servicio que participan en un mismo servicio tienen una relación de mapeo.

3. El método de acuerdo con una cualquiera de las reivindicaciones 1 a 2, en donde la red de cadenas de bloques comprende además nodos de consenso.

4. El método de acuerdo con la reivindicación 3, en donde para cada nodo de servicio, uno de los nodos de consenso que realiza una verificación de consenso de los datos de servicio generados por el nodo de servicio tiene una relación de mapeo con el nodo de servicio.

5. El método de acuerdo con una cualquiera de las reivindicaciones 3 a 4, en donde para cada nodo de servicio, diferentes nodos de consenso que realizan la verificación de consenso de los datos de servicio generados por el nodo de servicio tienen una relación de mapeo.

6. El método de acuerdo con una cualquiera de las reivindicaciones 1 a 5 que comprende, además:

determinar si el identificador de red en el certificado del segundo nodo de la cadena de bloques es diferente de un identificador de red de una red de cadenas de bloques que incluye el primer nodo de la cadena de bloques;

rechazar, mediante el primer nodo de la cadena de bloques, establecer una conexión de comunicación entre el primer nodo de la cadena de bloques y el segundo nodo de la cadena de bloques sin realizar más verificaciones, si se determina que el identificador de red del certificado del segundo nodo de la cadena de bloques es diferente del identificador de red de la red de cadenas de bloques que incluye el primer nodo de la cadena de bloques.

7. El método de acuerdo con una cualquiera de las reivindicaciones 1 a 6, en donde establecer una conexión de comunicación con el segundo nodo de la cadena de bloques comprende en concreto:

enviar una solicitud de verificación al segundo nodo de la cadena de bloques, de modo que el segundo nodo de la cadena de bloques determine, basándose en la solicitud de verificación, si el primer nodo de la cadena de bloques tiene una relación de mapeo con el segundo nodo de la cadena de bloques; y en caso afirmativo, el segundo nodo de la cadena de bloques establece una conexión de comunicación con el primer nodo de la cadena de bloques; o en caso

contrario, el segundo nodo de la cadena de bloques se rechaza a establecer una conexión de comunicación con el primer nodo de la cadena de bloques.

8. El método de acuerdo con una cualquiera de las reivindicaciones 1 a 7, en donde determinar si el segundo nodo de la cadena de bloques tiene una relación de mapeo con el primer nodo de la cadena de bloques comprende una verificación bidireccional entre el primer nodo de la cadena de bloques y el segundo nodo de la cadena de bloques.

9. Un aparato de comunicación entre nodos de la cadena de bloques, comprendiendo el aparato varios módulos configurados para llevar a cabo el método de acuerdo con una cualquiera de las reivindicaciones 1 a 8.

10. Un dispositivo de comunicación entre nodos de la cadena de bloques, en donde el dispositivo comprende uno o más procesadores y una memoria, la memoria almacena un programa, y el programa es ejecutado por uno o más procesadores para realizar el método de acuerdo con una cualquiera de las reivindicaciones 1 a 8.

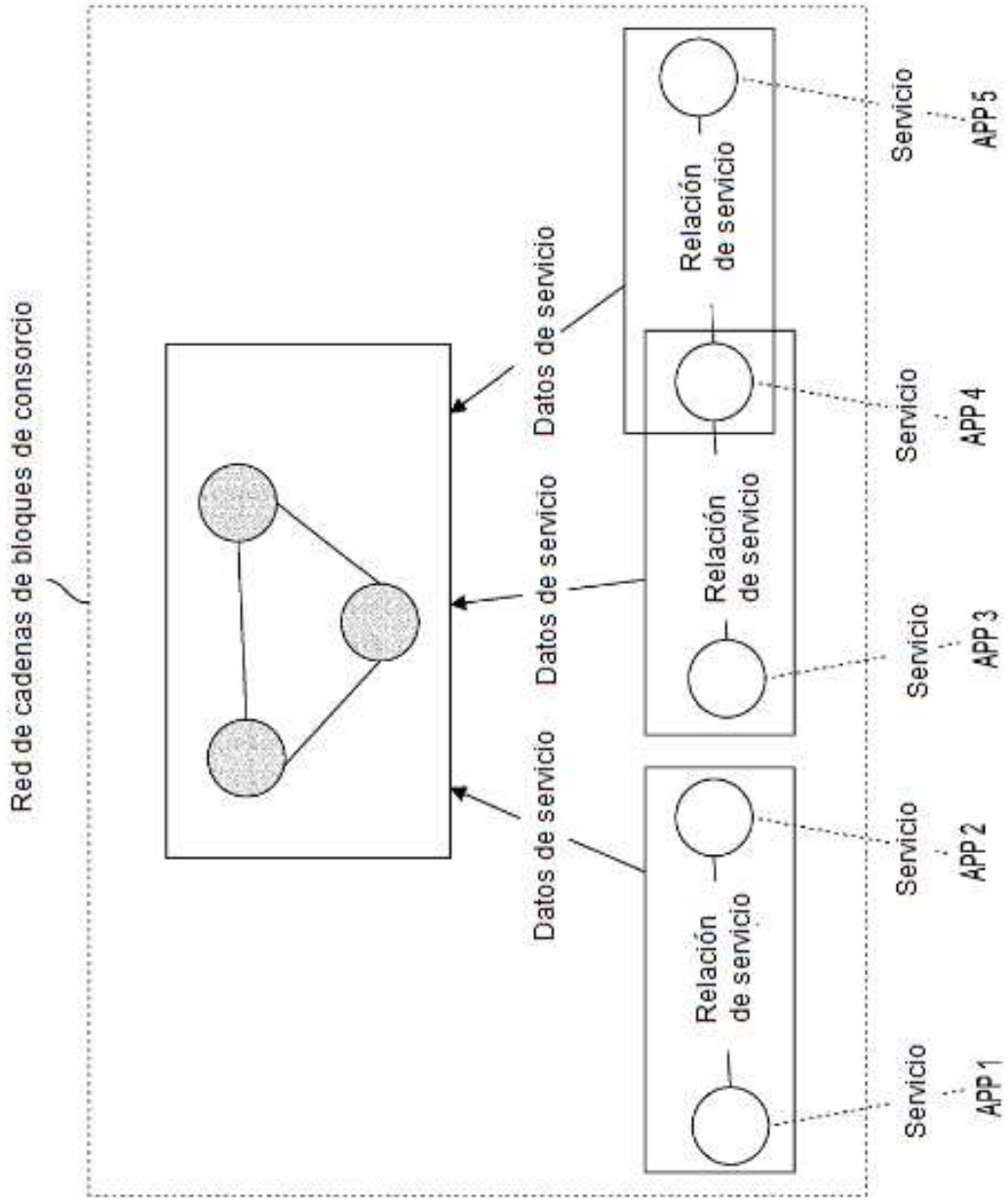
Red de cadenas de bloques de consorcio
Datos de servicio
Datos de servicio
Datos de servicio
Relación de servicio
Relación de servicio
Relación de servicio
Servicio
APP 1
Servicio
APP 2
Servicio
APP 3
Servicio
APP 4
Servicio
APP 5

FIG. 1

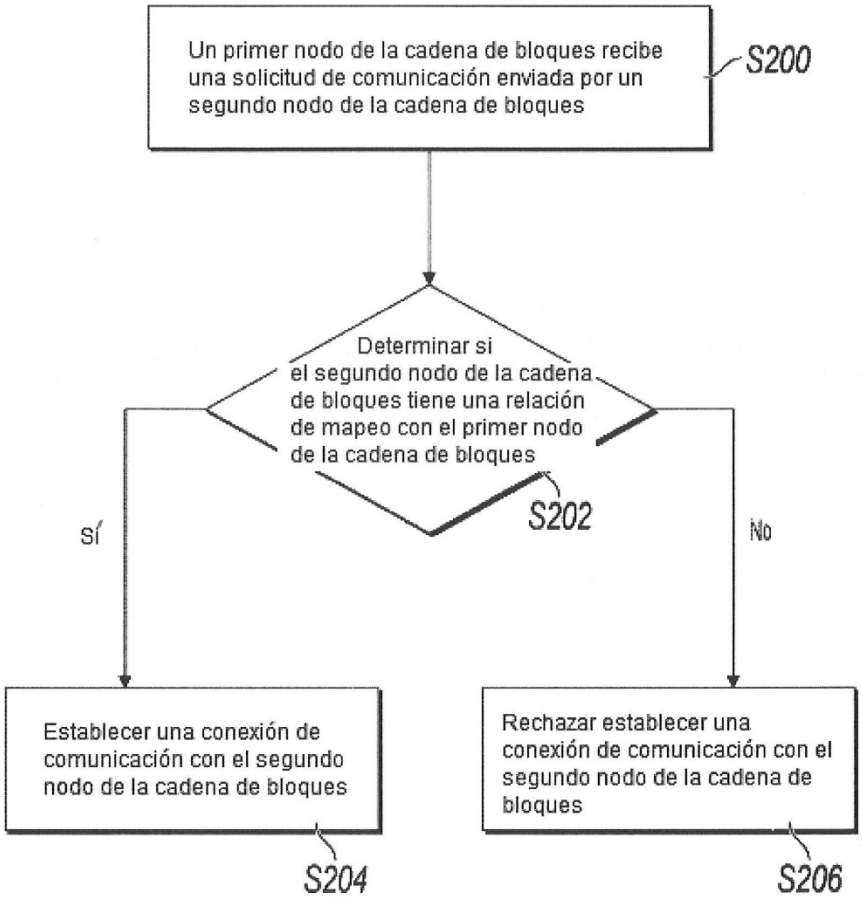
Un primer nodo de la cadena de bloques recibe una solicitud de comunicación enviada por un segundo nodo de la cadena de bloques
S200
Determinar si el segundo nodo de la cadena de bloques tiene una relación de mapeo con el primer nodo de la cadena de bloques
S202
Sí
No
Establecer una conexión de comunicación con el segundo nodo de la cadena de bloques
S204
Rechazar establecer una conexión de comunicación con el segundo nodo de la cadena de bloques
S206

FIG. 2

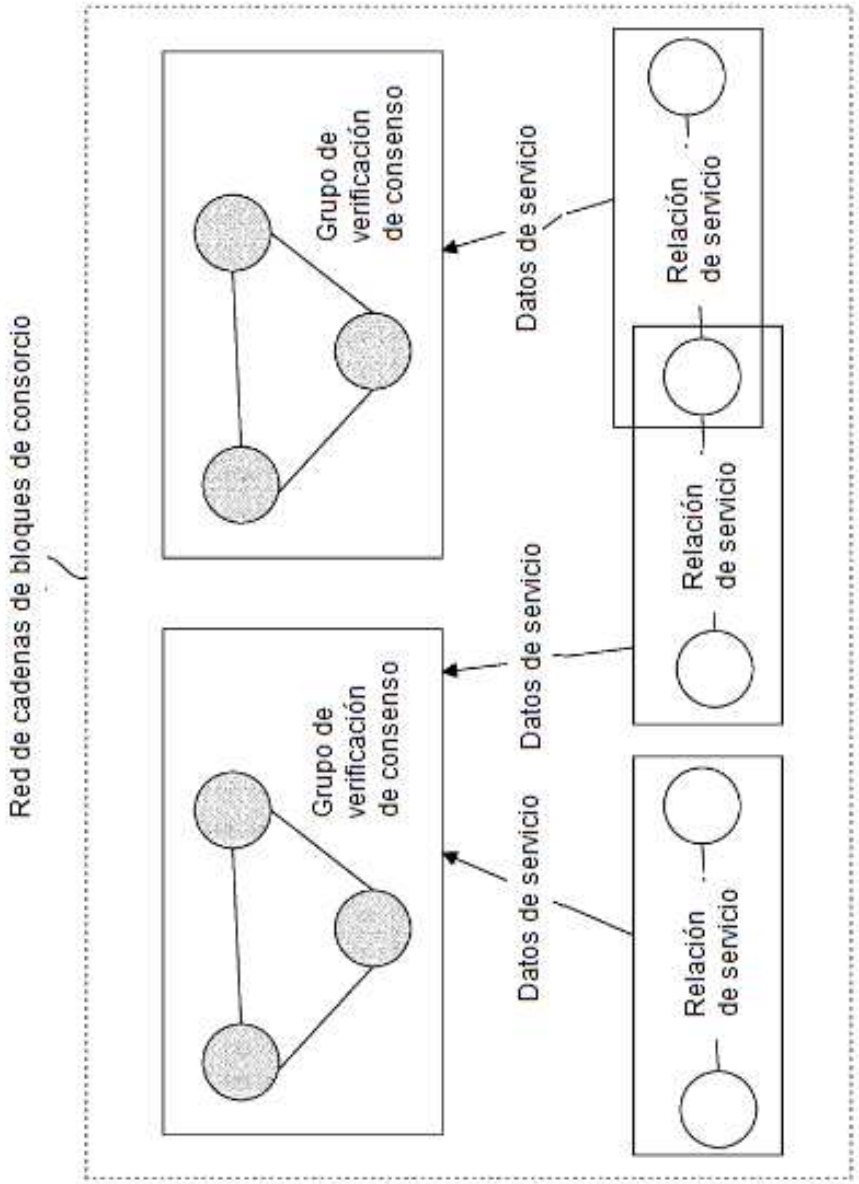
Red de cadenas de bloques de consorcio
Grupo de verificación de consenso
Grupo de verificación de consenso
Datos de servicio
Datos de servicio
Datos de servicio
Relación de servicio
Relación de servicio
Relación de servicio

FIG. 3

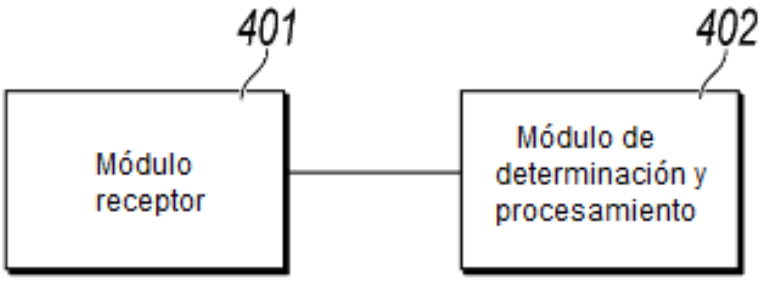
401
402
Módulo receptor
Módulo de determinación y procesamiento

FIG. 4

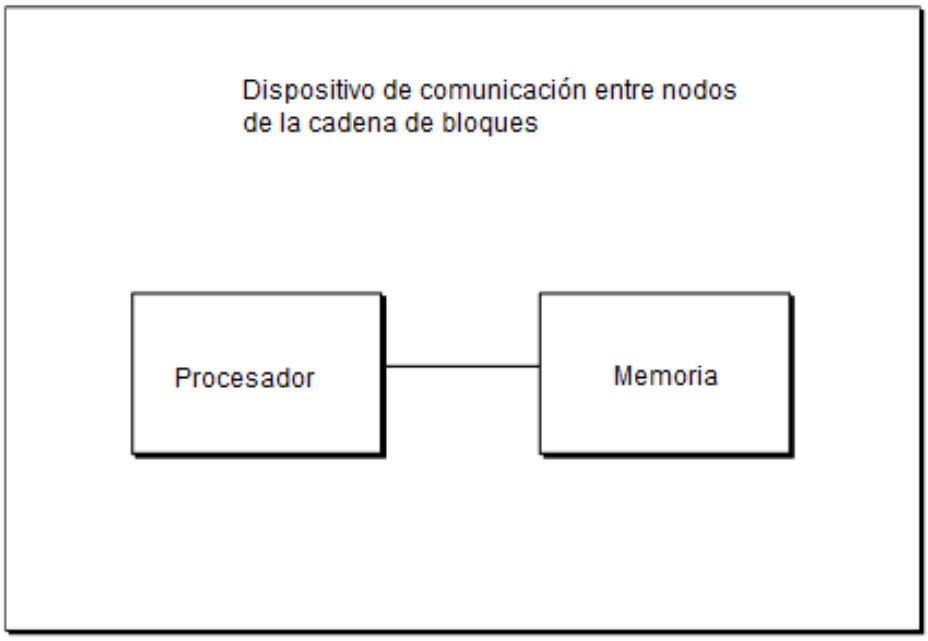
Dispositivo de comunicación entre nodos
de la cadena de bloques
Procesador
Memoria

FIG. 5

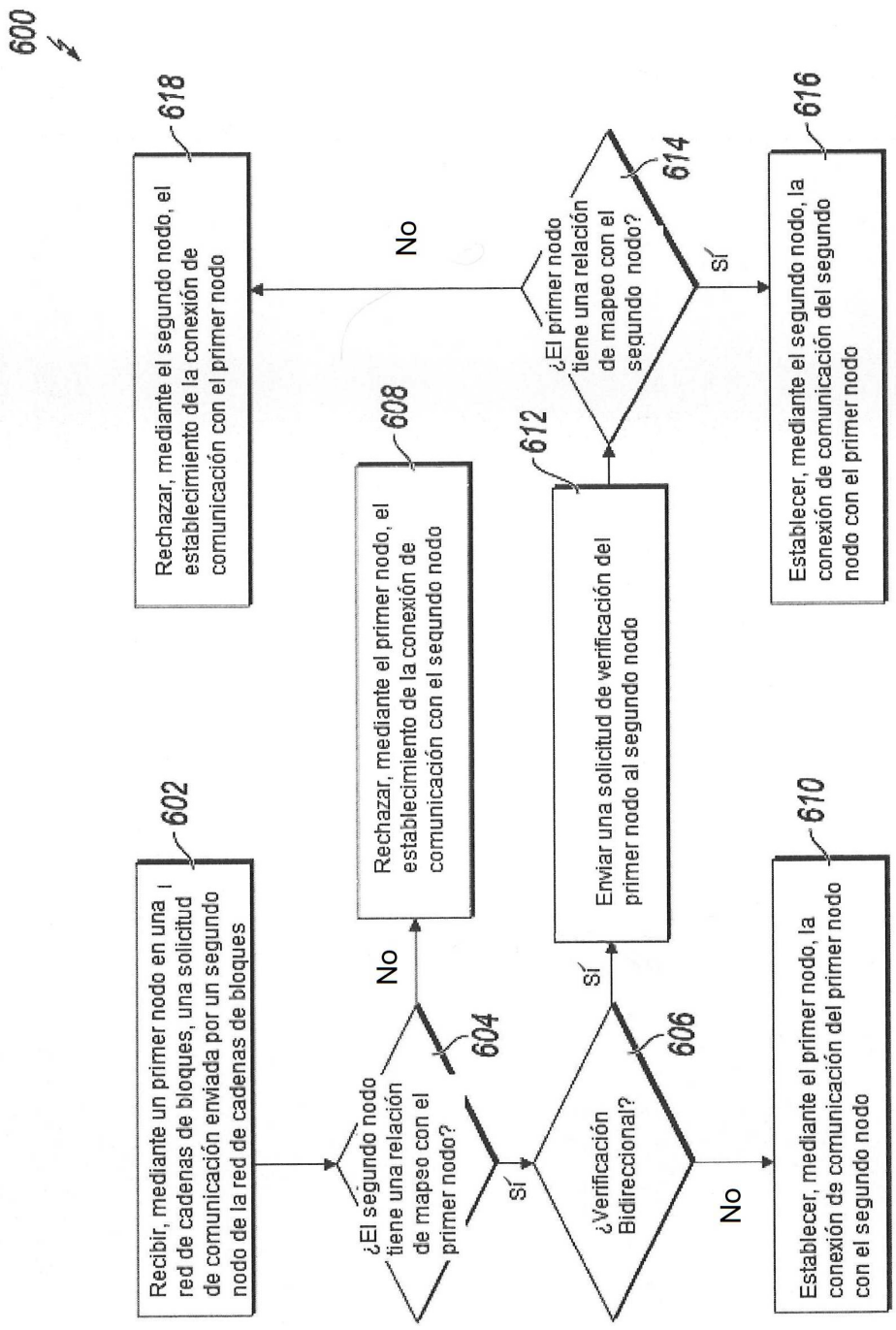
600
Recibir, mediante un primer nodo en una red de cadenas de bloques, una solicitud de comunicación enviada por un segundo nodo de la red de cadenas de bloques
602
¿El segundo nodo tiene una relación de mapeo con el primer nodo?
604
No
Rechazar, mediante el primer nodo, el establecimiento de la conexión de comunicación con el segundo nodo
608
Sí
¿Verificación Bidireccional?
606
Sí
Enviar una solicitud de verificación del primer nodo al segundo nodo
612
No
Establecer, mediante el primer nodo, la conexión de comunicación del primer nodo con el segundo nodo
610
¿El primer nodo tiene una relación de mapeo con el segundo nodo?
614
No
Rechazar, mediante el segundo nodo, el establecimiento de la conexión de comunicación con el primer nodo
618
Sí
Establecer, mediante el segundo nodo, la conexión de comunicación del segundo nodo con el primer nodo
616

FIG. 6