(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 890 236**

(51) Int. CI.:

G06Q 20/40 (2012.01)
H04L 29/06 (2006.01)
H04L 9/32 (2006.01)
G06Q 20/06 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **13.04.2017 PCT/AU2017/000090**

(87) Fecha y número de publicación internacional: **19.10.2017 WO17177260**

(96) Fecha de presentación y número de la solicitud europea: **13.04.2017 E 17781627 (9)**

(97) Fecha y número de publicación de la concesión europea: **16.06.2021 EP 3443519**

(54) Título: **Sistema de seguridad que usa protocolo de cadena de bloques**

(30) Prioridad:

13.04.2016 AU 2016901453

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
18.01.2022

(73) Titular/es:

HAVENTEC PTY LTD (100.0%)
Level 27, 1 Market Street
Sydney NSW 2000, AU

(72) Inventor/es:

RICHARDSON, RIC B

(74) Agente/Representante:

PONS ARIÑO, Ángel

DESCRIPCIÓN

Sistema de seguridad que usa protocolo de cadena de bloques

Campo técnico

La presente invención se refiere a una metodología y componentes de sistema para atribuir confianza en dispositivos de red que operan en un entorno de cadena de bloques. En un aspecto, se refiere al campo de estructuras de registros de datos y, más particularmente, aunque no exclusivamente, a aquellas estructuras cuando se usan como parte de un sistema para transmisión de información que usa un protocolo de cadena de bloques que encapsula datos especificados relacionados con la identidad única de al menos una entidad o dispositivo emisor.

Antecedentes

BitCoin y el protocolo de cadena de bloques son bien conocidos en la técnica. Principalmente, el protocolo se ha usado para aplicaciones en una moneda de estado independiente. Debido a su naturaleza altamente segura y a su integridad matemática inherente, el protocolo también es una oportunidad ideal para aplicaciones de seguridad, aunque hasta la fecha no se ha usado como tal.

En su uso tradicional, la cadena de bloques es un historial documentado de transacciones que muestra tanto el vendedor como el comprador de testigos de valor a lo largo del tiempo con una capacidad incorporada para minimizar la oportunidad de actividad fraudulenta, tal como el gasto doble de los testigos.

Se analizan las estructuras de cadena de bloques en el contexto del uso inicial para el almacenamiento de Bitcoin y las transacciones en la publicación: MultiChain Private Blockchain - White Paper por Dr. Gideon Greenspan, fundador y director ejecutivo, Coin Sciences Ltd-disponible en el archivo de retorno <http://web.archive.org/web/20160403063334/http://www.multichain.com/download/MultiChain-White-Paper.pdf >recuperado de Internet publicado el 3 de abril de 2016 como un motor de retorno e incluye la siguiente porción que se cita específicamente: "Bitcoin se reconoce ahora como un método barato, rápido y fiable para mover valor económico a través de Internet en una manera entre pares.

CADENAS DE BLOQUES Y CONVERSIÓN A TESTIGOS

En el corazón de bitcoin radica la cadena de bloques, un libro mayor descentralizado global que almacena el historial completo de todas las transacciones de bitcoin. La cadena de bloques se verifica y almacena por cada nodo en la red de bitcoin, de los cuales hay aproximadamente 6.000 en junio de 2015. El protocolo de bitcoin garantiza que, prohibiendo discrepancias temporales, cada nodo en la red tiene la misma versión de la cadena de bloques, sin requerir que se determine este consenso por una autoridad central. Otra característica principal de bitcoin (y de la estructura de cadena de bloques) es que los nodos pueden unirse o dejar la red en cualquier momento, sin interrumpir el funcionamiento de otros nodos o el procesamiento de transacciones en curso. Pueden crearse nuevas transacciones por cualquier nodo y se propagan a través de la red en una forma entre pares. Cualquier nodo puede tomar un conjunto de estas transacciones pendientes y crear ("minar") un nuevo bloque que las contiene junto con un enlace al bloque anterior. El nuevo bloque "confirma" las transacciones y también se propaga a través de la red. Para evitar el control minoritario a través de la minería, bitcoin usa la "prueba de trabajo" para hacer computacionalmente difícil y caro crear un nuevo bloque.

Si tiene lugar una "bifurcación", en la que dos bloques competidores se minan casi simultáneamente, la prueba de trabajo también actúa como un mecanismo de resolución de disputa. Puesto que los bloques son difíciles de crear, es poco probable que ambas bifurcaciones crecerán a una velocidad idéntica. El protocolo especifica que la bifurcación con la mayor cantidad de trabajo es la correcta, por lo que la red recupera rápidamente un consenso global unificado.

Junto con las transacciones de bitcoin, la cadena de bloques puede usarse para almacenar cualquier dato digital. Aunque algunos ven tales usos como "inflar la cadena de bloques", la naturaleza descentralizada de bitcoin significa que no puede detenerse de manera efectiva. Esto conduce a que los desarrolladores de Bitcoin Core, el cliente de bitcoin oficial, introduzcan un mecanismo oficial para añadir metadatos arbitrarios a transacciones a principios de 20143. Este mecanismo se usa por servicios tales como la prueba de existencia y la firma de bloque para notarizar la existencia de un documento integrando una firma digital de ese documento dentro de una transacción. Otras herramientas tales como phpOP_RETURN posibilitan que se almacenen y recuperen piezas de datos más grandes de la cadena de bloques, volviéndola un almacén de datos descentralizado permanente de propósito general".

Una característica del diseño de la red BitCoin es la seguridad innata de una cartera que se asegura mediante encriptación de clave pública donde la clave privada del par de claves públicas se mantiene secreta. La cartera y, por lo tanto, el propietario de la cartera, se identifica por su clave pública. Esto es conocido en la técnica. El asunto es que, aunque la estructura de cadena de bloques proporciona seguridad de los datos contenidos dentro de la cartera, puede existir una vulnerabilidad al compromiso en el dispositivo de red o dispositivo que aloja la cartera y que de otra manera forma parte de o participa en la cadena de bloques.

Por ejemplo, el dispositivo de red completo puede sustituirse sin que otros miembros participantes de la cadena de bloques tengan conocimiento de que esto ha ocurrido. Esto puede conducir a vulnerabilidades de suplantación de identidad o equivalentes.

Es un objeto de la presente invención buscar mejorar la integridad de dispositivos de red o dispositivos que forman nodos en una cadena de bloques y mejorar de esta manera la integridad de la cadena de bloques y los datos almacenados y transmitidos dentro de ella.

Se observa que hay otros identificadores de un usuario o, más específicamente, su dispositivo que participa en la cadena de bloques. Los identificadores disponibles para la verificación de la identidad pueden incluir, por ejemplo, un número de IP del dispositivo en una red pública o privada. Hasta ahora, estos no se han utilizado para ayudar a mejorar la integridad de dispositivos de red o dispositivos dentro de la cadena de bloques.

Incluyendo esta información en un registro de transacciones, tal como la cadena de bloques, puede permitir que se realicen aplicaciones adicionales del protocolo de cadena de bloques, los documentos US2015/310424 y US2015/363777 desvelan un mecanismo para validación de integridad de la cadena de bloques.

NOTAS

La expresión "que comprende" (y variaciones gramaticales de la misma) se usa en esta memoria descriptiva en el sentido inclusivo de "que tiene" o "que incluye", y no en el sentido exclusivo de "que consiste únicamente en".

El análisis anterior de la técnica anterior en los antecedentes de la invención, no es una admisión de que cualquier información analizada en la misma es la técnica anterior citable o parte del conocimiento general común de los expertos en la materia en cualquier país.

Breve descripción de la invención

La presente invención se refiere a la materia objeto como se desvela por las reivindicaciones adjuntas.

Dibujos

Las realizaciones de la presente invención se describirán ahora con referencia a los dibujos adjuntos en donde:

La Figura 1 ilustra los componentes principales de una realización de ejemplo

La Figura 2 ilustra una transacción de la realización de ejemplo

La Figura 3 ilustra el detalle de una transacción de la realización de ejemplo

La Figura 4 ilustra el proceso de verificación de identificador único de la realización de ejemplo

La Figura 5 ilustra una capacidad de reenvío automático de testigo de la realización de ejemplo.

La Figura 6 es un diagrama de bloques de un sistema que opera de acuerdo con una realización adicional.

La Figura 7 es un diagrama de estructura de datos usable de acuerdo con el protocolo de cadena de bloques.

La Figura 8 es un diagrama de red de dispositivos que participan en una cadena de bloques.

Descripción y operación

La Figura 1 desvela los componentes principales de la realización de ejemplo. Cada red de cadena de bloques comprende múltiples dispositivos 10 11 12, cada uno de los cuales tiene y típicamente debe tener una dirección IP única 13 14 15. Para que cada dispositivo 10 11 12 sea parte de una red de cadena de bloques, cada dispositivo 10 11 12 tendría típicamente una cartera 16 que se acompaña por una clave pública 17 que se comparte con el resto de la red para propósitos de identificación, encriptación y desencriptación, así como una clave privada que se usa para propósitos de autenticación, encriptación y desencriptación.

La cartera 16 se acompañaría también por un registro de transacciones de cadena de bloques 19. Típicamente no incluiría 19 de manera tradicional el número de IP de cada emisor y receptor de los testigos de red 21, sin embargo, en el caso de la realización de ejemplo, está incluido el número de IP de tanto el emisor 22 como el receptor 23 en una transacción. Todos los dispositivos en la red 10 11 12 cada uno tiene una cartera.

La Figura 2 desvela una transacción de ejemplo de la realización de ejemplo. Una cartera 30 recibe 31 un testigo de

otra cartera en la red. La cartera 30 incluye una clave pública 33 que se usa para encriptación y desencriptación, así como identificación. La cartera 30 también tiene una clave privada 34 que se usa para encriptación, desencriptación y autenticación. La cartera 30 también tiene una dirección IP de dispositivo asociado 35. La cartera 30 también tiene acceso a un libro mayor de transacciones 36 que usa protocolos de cadena de bloques para permanecer en sincronización con otros libros mayores 27 en la red.

Cuando se recibe un testigo 32 por una cartera 30, el testigo 36 a continuación se vuelve a encaminar a otra cartera 39 que también tiene su propia clave pública 40, clave privada 41 y libro mayor asociado 37. Esta cartera también está asociada con un número de IP de dispositivo 42.

Cuando se envía 38 un testigo 36 de una cartera a otra, se registra información acerca de la transacción en los libros mayores 36 37 que incluye, pero sin limitación, la identidad del testigo 36, la identidad de tanto la cartera emisora 33 como la receptora 40 y la hora de la transacción.

En el caso de la realización de ejemplo, también se registran los números de IP de tanto el dispositivo emisor 35 como el receptor 42 en el libro mayor de transacciones 36 37. El beneficio de esto es que se establece un historial de propiedad e integridad de asociación entre el número de IP y una cartera segura. Este historial de confianza puede usarse para detectar intentos de suplantar un dispositivo en una red.

Si un intruso roba un número de IP, pero no tiene una cartera segura legítima la suplantación puede detectarse fácilmente.

Los libros mayores 36 37 usan un sistema de firma digital que es conocido en la técnica como un medio a prueba de manipulación de la información registrada y de verificación de que el emisor y el receptor son quien dicen ser.

La Figura 3 desvela detalles de una transacción de la realización de ejemplo. Un registro de transacciones 50 típicamente contiene información acerca del testigo que se intercambia 51, información acerca de la parte emisora 52 y la parte receptora 53. Sin embargo, en el caso de la realización de ejemplo, el número de IP del dispositivo emisor 54 y la dirección IP del dispositivo receptor 55 también están incluidos en el registro de transacciones 50. Esta información a continuación se convierte a función de troceo 56 usando un proceso conocido en la técnica y se firma digitalmente usando un proceso que es conocido en la técnica.

Este proceso de conversión a función de troceo y firma del registro de transacciones, significa que el registro no puede manipularse o cambiarse para manipular los datos en el registro, que incluye, pero sin limitación, la dirección IP de los dispositivos emisores o receptores.

La Figura 4 muestra el proceso de verificación de IP de la realización de ejemplo. Un dispositivo 60 al que se hace referencia en un fichero de transacción 62 típicamente tiene una dirección IP única 61, que puede registrarse como parte 63 de un fichero de transacción 62 que a continuación se convierte a función de troceo y se firma para mantener su integridad.

El hecho de que la dirección IP registrada e IP del dispositivo que envía o recibe testigos puede verificarse independientemente 64 significa que la veracidad de una dirección IP del dispositivo puede comprobarse y verificarse y realizarse una decisión en cuanto a si otras partes pueden confiar en ese dispositivo y en su identidad.

La Figura 5 desvela el reenvío automático de la capacidad del testigo de la realización de ejemplo. Cuando una cartera 72 recibe 70 un testigo 71 de otra cartera, se establece un temporizador 73 y mecanismo de temporización para reenviar automáticamente 74 el testigo 71 en otro dispositivo en la red 75. Esto se hace para garantizar que todos los dispositivos en la red reciben una entrega regular de testigos y ayuda a garantizar que el libro mayor de transacciones permanece actual y activo.

La cartera 72 también tiene integrada reglas 80 que se usan para definir si la cartera recibirá o rechazará los testigos 71 que se le envían. Por ejemplo, si el número de IP del dispositivo que envía el testigo 70 no existe en el libro mayor de transacciones 76 entonces rechaza la transacción. Si la identidad del testigo no es conocida y no se encuentra en el libro mayor entonces rechaza el testigo. Otro ejemplo es cuando la IP registrada en el registro de transacciones del dispositivo emisor no coincide con la IP del dispositivo que envía el testigo, entonces el testigo se rechaza.

Cuando el mecanismo de temporización envía un testigo en otro dispositivo en la red, típicamente querrá enviar el testigo al dispositivo de red que no ha recibido un testigo durante más tiempo, lo que garantiza que todos los dispositivos en la red obtienen un buen promedio de transacciones a lo largo del tiempo.

Esto puede conseguirse buscando en el libro mayor de transacciones 76 y hallando el número de IP del dispositivo 79 al que no se le ha enviado un testigo durante más tiempo. Este método garantiza que no se permite que se ignore o excluya ningún dispositivo individual en una red de transacciones regulares y también puede usarse para activar una investigación en cuanto a por qué el dispositivo ya no está disponible más en la red.

REALIZACIÓN ADICIONAL

Con referencia a la figura 6, se ilustra un sistema 200 de acuerdo con una realización adicional de la presente invención que proporciona seguridad adicional a un sistema de cadena de bloques.

En este caso, el sistema incluye al menos un primer nodo 201. En este caso, el nodo 201 comprende un dispositivo de red en forma de un servidor que tiene al menos una memoria 202, un procesador 203 y un dispositivo de entrada/salida 204 operables para comunicase a través de una red 205 con al menos un segundo nodo 206. En este caso, el segundo nodo 206 también comprende un dispositivo de red en forma del servidor que comprende al menos la memoria 207 en comunicación con el procesador 208 que, a su vez, está en comunicación con el dispositivo de entrada salida 209. En formas alternativas, el dispositivo de red puede comprender un encaminador. En formas alternativas, puede comprender cualquier dispositivo inteligente que está conectado en red y tiene suficiente potencia de procesamiento para realizar las funciones señaladas para esta realización.

El sistema 200 opera en un entorno de cadena de bloques de acuerdo con protocolos de cadena de bloques e incluye la transmisión y retención de datos y metadatos relacionados en una estructura de libro mayor 210. Se proporcionan adicionalmente a continuación los detalles adicionales de al menos formas generalizadas de protocolos de cadena de bloques y la utilización de la estructura de libro mayor con referencia a las Figuras 7 y 8.

En uso, el sistema 200 incluye información almacenada en una cartera 211 dentro de la memoria 202. Los campos en la cartera, en este caso, incluyen un campo de testigo 212, un campo de clave pública 213, un campo de clave privada 214 y un campo de identificador de dispositivo 215. Los campos correspondientes están estructurados en la cartera 216 del segundo nodo 206 y, de hecho, en cualquier otro dispositivo que opera dentro de la cadena de bloques del sistema 200.

En uso, en una forma, la cartera 211 contiene un identificador único para el dispositivo 201 en su campo de identificador 215. En una forma preferida, el identificador único es la dirección IP del dispositivo 201. En formas alternativas, puede ser la dirección de MAC del dispositivo 201. En otras formas más, puede estar relacionada con el hardware que comprende el dispositivo 201.

Como parte de la transmisión de un testigo A a través de la red 205 de la primera cartera 211 a la segunda cartera 216, se almacenan diversos elementos de información en forma de datos en el libro mayor, como se ilustra en general en la Figura 6. Estos incluyen la identidad de la primera cartera, en una forma preferida que es la clave pública de la primera cartera 211 almacenada en el registro 213. También se almacenarán en el libro mayor 210 el identificador único del dispositivo 201 que aloja la cartera 211, en este caso específico, la dirección IP del dispositivo 201. El libro mayor 210 se ve sometido a las etapas para ayudar en su verificación de acuerdo con los protocolos de cadena de bloques. En una forma, esto puede incluir aplicar un algoritmo de función de troceo a los datos en el libro mayor. En una forma adicional, esto puede incluir adicionalmente firmar digitalmente la función de troceo resultante de los datos. Esta etapa permite que se realice la comparación contra los datos en el libro mayor en momentos posteriores, preferentemente en los momentos cuando se transmite un testigo a o desde la cartera mediante lo cual si el identificador único del dispositivo 201 que aloja la cartera 211 cambia, esto se detectará, por ejemplo, detectando que el valor de función de troceo ha cambiado.

En formas preferidas, el testigo A se transmite desde dispositivo a dispositivo en la red en una base de rotación para garantizar que cada dispositivo recibe o envía el testigo A a través de un periodo de tiempo predeterminado para probar de esta manera la integridad/identidad de cada dispositivo en la red que está participando en la cadena de bloques.

Se hará notar, que esta prueba de integridad/identidad del dispositivo 201 tendrá lugar en efecto automáticamente como parte del seguimiento normal del protocolo de cadena de bloques mediante la inclusión del identificador de dispositivo dentro del libro mayor 210.

En una forma preferida, el testigo A puede comprender simplemente una secuencia alfanumérica cuyo propósito primario es que se envíe de dispositivo a dispositivo para activar de esta manera pruebas de identidad de dispositivo por medio de verificación de libro mayor que tiene lugar como parte del protocolo de cadena de bloques. En otras formas, el testigo A puede tener un valor representativo, por ejemplo, puede representar un elemento de valor de bit coin, por ejemplo, 1 Satoshi en valor de Bitcoin.

En otras formas más, el testigo A puede ser un elemento de datos que se desea que se transmita desde una cartera a otra por razones asociadas con la naturaleza intrínseca de los datos como una unidad de moneda o como una unidad de información.

Un subproducto de esta comprobación de rutina de identidad es que a medida que aumenta el número de transacciones en un dispositivo de red particular, hay una inferencia de fiabilidad de ese dispositivo de red y su identidad. A la inversa, cuando un dispositivo de red ha cambiado su identificador único, entonces puede realizarse una decisión de no enviar datos a la cartera en esa máquina durante al menos un periodo de tiempo predeterminado.

Ampliamente, la idea es proporcionar un cierto nivel de confianza de que una máquina o dispositivo de red en la red de cadena de bloques es la maquina o dispositivo de red que piensas que es. La rotación de testigo mantiene testigos actuales. Si se rota el testigo lo suficientemente a menudo, entonces es fácil observar si un dispositivo ha cambiado su identificador único o lo ha descartado de la red.

En un aspecto, combinamos tanto un ID de usuario (preferentemente la clave pública) con una huella digital de máquina dentro del libro mayor que opera en un entorno de cadena de bloques de modo que se detectará inmediatamente si la huella digital de máquina cambia la siguiente vez que tiene lugar una sesión de transferencia de testigo con esa máquina.

En otro aspecto, la metodología anteriormente descrita proporciona un método de introducción de un nuevo dispositivo de red o máquina en una red.

Esta metodología puede aplicarse designando una cartera madre o iniciando una cartera que asigna/envía nuevos testigos a un nuevo dispositivo de red.

El nuevo dispositivo de red tiene que crear una cartera, entonces la cartera madre le envía un primer testigo para iniciar de esta manera la máquina/dispositivo de red en la red de cadena de bloques de la que se vuelve una parte confiable.

ESTRUCTURAS DE CADENA DE BLOQUES

Las estructuras de cadena de bloques como se describen en cualquier otra parte en esta memoria descriptiva y a continuación se usan con cualquiera de las realizaciones anteriormente descritas.

La Figura 7 es un diagrama de una estructura de datos de cadena de bloques de ejemplo.

La Figura 8 ilustra el uso esquemático de la estructura de datos de cadena de bloques de la figura 7.

Con referencia a las Figuras 7 y 8, la cadena de bloques es una estructura de datos y sistema de registro distribuido que busca proporcionar una estructura de datos y sistema en el que formas preferidas mantienen un registro completo de todas las transacciones y minimiza el riesgo de alteraciones retrospectivas o transacciones dobles o idénticas.

La estructura de datos consiste en una serie de transacciones agrupadas en bloques, que necesitan verificarse antes de que se añadan a la cadena. Las reglas pueden establecerse para que nunca se eliminen datos, y la cadena más larga se toma como la más reciente, y, así, la cadena registra todas las transacciones de su iniciación en orden cronológico.

Una copia de la cadena puede mantenerse por todos los usuarios y, así, es un sistema de registros distribuidos. Antes de que se añada cualquier transacción, la mayoría de los usuarios necesitan acordar que la transacción sea aceptable y, a continuación, se agrupa con otras transacciones aceptables en un bloque, que se añade a la cadena. Cada bloque tiene un encabezado que puede crearse únicamente conociendo todas las transacciones anteriores. Como resultado, si se realiza una alteración retrospectiva, el encabezado será incorrecto y cualquier nuevo bloque propuesto por ese usuario se rechazará. La seguridad del sistema se mejora adicionalmente teniendo problemas matemáticos que puede resolverse únicamente por ensayo y error, que usan el encabezado y deben resolverse y a continuación verificarse por la mayoría de otros usuarios antes de que se acepte un bloque en la cadena por todos los usuarios. Siempre que haya más usuarios genuinos que atacantes coordinados que intenten alterar la cadena, la cadena será segura. Pueden utilizarse otros métodos para determinar la veracidad de un bloque de datos, esto puede incluir procesos de votación o consentimiento donde a las partes con una participación en la transacción o transacciones relacionadas en la misma cadena se les conceden derechos de 'votación'. Otro proceso puede implicar un sistema de votación o aprobación aleatorio o sistematizado donde se aprueba la validez del bloque de datos de acuerdo con un conjunto de protocolos acordado por aquellos con una participación en la veracidad de la cadena de datos.

En una forma más particular, cada bloque incluye transacciones verificadas y la cadena de bloques mantiene un libro mayor de todas las transacciones anteriores. La cadena de bloques se duplica por todos los ordenadores en una red.

El primer bloque en la cadena es conocido como el bloque de génesis y pueden añadirse nuevos bloques en orden lineal y cronológico. Desde cualquier bloque dado en la cadena, puede recuperarse la información de este bloque de génesis y todos los bloques que conducen de vuelta a este. Una cadena de bloques es esencialmente bloques numerosos conectados a través de encadenación de función de troceo donde cada bloque está comprendido de lo siguiente

- □ Indicación de tiempo: proporciona la prueba de que los datos en un bloque existieron en un tiempo particular
- □ Función de troceo anterior: esencialmente un puntero al bloque anterior
- □ Función de troceo de Merkle: sumario de todas las transacciones ejecutadas

□ Número aleatorio usado solo una vez: identidad de bloques individuales y es un número arbitrario que puede usarse únicamente una vez

La cadena de bloques se gestiona por una red de nodos distribuidos donde cada nodo contiene una copia de la cadena de bloques entera. Cada nodo en la red puede añadir bloques a la cadena, donde cada nodo está añadiendo bloques en el mismo punto en la cadena al mismo tiempo. Cuantos más nodos comprenda la red, más difícil será interrumpir el almacenamiento de la cadena de bloques. A diferencia de sistemas centralizados que se basan en una única autoridad, no hay un único punto de fallo en esta red de nodos distribuidos. Si cambias el contenido de un bloque cambias su función de troceo.

REALIZACIONES ALTERNATIVAS

Las reglas mencionadas con referencia a la figura 5 son ejemplos. Una realización alternativa puede usar cualquier conjunto de reglas para regir la aceptación, rechazo de testigos y el control de la cartera.

La realización de ejemplo usa un dispositivo de IP como un identificador del dispositivo que envía o recibe testigos. Una realización alternativa puede usar cualquier información externamente verificable que puede identificar de manera inequívoca un dispositivo y verificarse por una segunda parte. Ejemplos incluyen una dirección de MAC de un dispositivo o números de serie de partes de componente del dispositivo. Preferentemente, el identificador no puede modificarse fácilmente o en absoluto por una segunda parte sin autorización de seguridad. Adicionalmente, el identificador único externo se incluiría en el registro de transacciones y también se incluye en el cálculo de la función de troceo y la firma digital por la parte o partes emisoras o receptoras.

La realización de ejemplo muestra únicamente unos pocos dispositivos en la red por simplicidad. Una realización alternativa puede tener cualquier número de dispositivos en la red.

La realización de ejemplo usa las metodologías de función de troceo y firma digital convencionales comúnmente usadas en redes de cadenas de bloques. Una realización alternativa puede usar cualquier método de los métodos de integridad, autenticación e identificación disponibles.

La realización de ejemplo usa una regla de temporización como un medio de activación cuando un testigo que se recibe se reenvía a otro dispositivo en la red. Una realización alternativa podría usar cualquier cálculo de activación o método para garantizar que los testigos se circulan en un intervalo normal entre los dispositivos en la red compartida. Los parámetros tales como la congestión de red y el nivel ideal de seguridad a través de verificación de identidad habitual pueden ser factores que pueden incluirse en el cálculo de la frecuencia con la que cada cartera comparte testigos entre los otros ordenadores en la red.

REIVINDICACIONES

1. Una estructura de registro de datos (211) adaptada para transmisión a través de una red (205) de dispositivos de participación de red (201, 206); la estructura de registro de datos (210) generada en un dispositivo de red (201) que participa en una cadena de bloques como un dispositivo de iniciación que tiene un identificador único de dispositivo de iniciación; operando la cadena de bloques de acuerdo con un protocolo de cadena de bloques; conteniendo la estructura de registro de datos al menos un primer registro (212) y un primer registro de identificador único; conteniendo el primer registro (212) datos para transmisión a través de la red (205) a un dispositivo de participación de red (206) en forma de un dispositivo de recepción que tiene un identificador único de dispositivo de recepción; conteniendo el primer registro de identificador único el identificador único de dispositivo de iniciación; y en donde el primer registro (212) contiene datos de identificación de testigo que identifican de manera inequívoca un testigo (212); posibilitando la estructura de registro de datos la comparación del identificador único de dispositivo de iniciación contenido en el registro de datos con el identificador único del dispositivo de red que participa en una cadena de bloques (200) como un dispositivo de iniciación al menos cada vez que se recibe el testigo (212) mediante uno de los dispositivos de participación de red (201, 206); la comparación realizada por medio de la verificación de libro mayor que tiene lugar como parte del protocolo de cadena de bloques; y en donde el testigo se transmite de dispositivo a dispositivo en la red en una base de rotación para garantizar que cada dispositivo recibe o envía el testigo a través de un periodo de tiempo predeterminado para probar de esta manera la integridad/identidad de cada dispositivo en la red que está participando en la cadena de bloques.

2. La estructura de registro de datos de la reivindicación 1, en donde los datos de o que pertenecen al primer registro están contenidos en un libro mayor.

3. La estructura de registro de datos de la reivindicación 1, en donde la estructura de registro de datos está contenida dentro de una cartera.

4. La estructura de registro de datos de la reivindicación 1 o la reivindicación 2, en donde la estructura de registro de datos incluye adicionalmente un segundo registro de dirección IP.

5. La estructura de registro de datos de la reivindicación 4, en donde el segundo registro de dirección IP contiene la dirección IP de dispositivo de recepción.

6. La estructura de una cualquiera de las reivindicaciones 1 a 5, en donde la estructura de registro de datos incluye adicionalmente un segundo registro.

7. La estructura de una cualquiera de las reivindicaciones 1 a 6, en donde la estructura de registro de datos incluye adicionalmente un tercer registro.

8. La estructura de cualquier reivindicación anterior en donde el testigo comprende una secuencia alfanumérica cuyo propósito primario es que se envíe de dispositivo a dispositivo para activar de esta manera pruebas de identidad de dispositivo por medio de verificación de libro mayor que tiene lugar como parte del protocolo de cadena de bloques.

9. La estructura de la reivindicación 8, en donde el testigo se está intercambiando entre el dispositivo de iniciación y el dispositivo de recepción.

10. La estructura de cualquier reivindicación anterior en donde el segundo registro contiene datos que identifican de manera inequívoca una parte emisora.

11. La estructura de cualquier reivindicación anterior en donde el tercer registro contiene datos que identifican de manera inequívoca una parte receptora.

12. La estructura de cualquier reivindicación anterior en donde la estructura de registro de datos incluye adicionalmente un intervalo de función de troceo.

13. Un sistema de transmisión para transmisión de la estructura de registro de datos de una cualquiera de las reivindicaciones 1 a 12.

14. Un método de verificación de identidad de dispositivos que participan en una cadena de bloques (200); operando la cadena de bloques (200) de acuerdo con un protocolo de cadena de bloques; comprendiendo dicha cadena de bloques (200) una pluralidad de libros mayores (210) mantenidos en una pluralidad de dispositivos de red (201, 206); comunicando dichos dispositivos de red (201, 206) contenidos de los libros mayores (210) entre ellos a través de una red (205); verificando dichos dispositivos (201, 206) los contenidos de los libros mayores (210) como parte de la etapa de comunicación de los contenidos de los libros mayores (210); comprendiendo dicho método incorporar un registro de identificador único que representa el identificador único del dispositivo de red dentro del libro mayor (210) mantenido por el dispositivo de red (201, 206); comprendiendo adicionalmente el método comparar los contenidos del registro de identificador único con el identificador único del dispositivo de red (201, 206) en la recepción de un testigo (212); la

etapa de comparar hecha por medio de la verificación del libro mayor que tiene lugar como parte del protocolo de cadena de bloques; y en donde el testigo se transmite de dispositivo a dispositivo en la red en una base de rotación para garantizar que cada dispositivo recibe o envía el testigo a través de un periodo de tiempo predeterminado para probar de esta manera la integridad/identidad de cada dispositivo en la red que está participando en la cadena de bloques.

15. El método de la reivindicación 14, en donde el dispositivo de red almacena una estructura de registro de datos adaptada para transmisión a través de una red; participando el registro de datos generado en el dispositivo de red en una cadena de bloques como un dispositivo de iniciación que tiene un identificador único de dispositivo de iniciación; conteniendo la estructura de registro de datos al menos un primer registro y un primer registro de identificador único; conteniendo el primer registro datos para transmisión a través de la red a un dispositivo que tiene un identificador único de dispositivo de recepción; conteniendo el primer registro de identificador único el identificador único de dispositivo de iniciación.

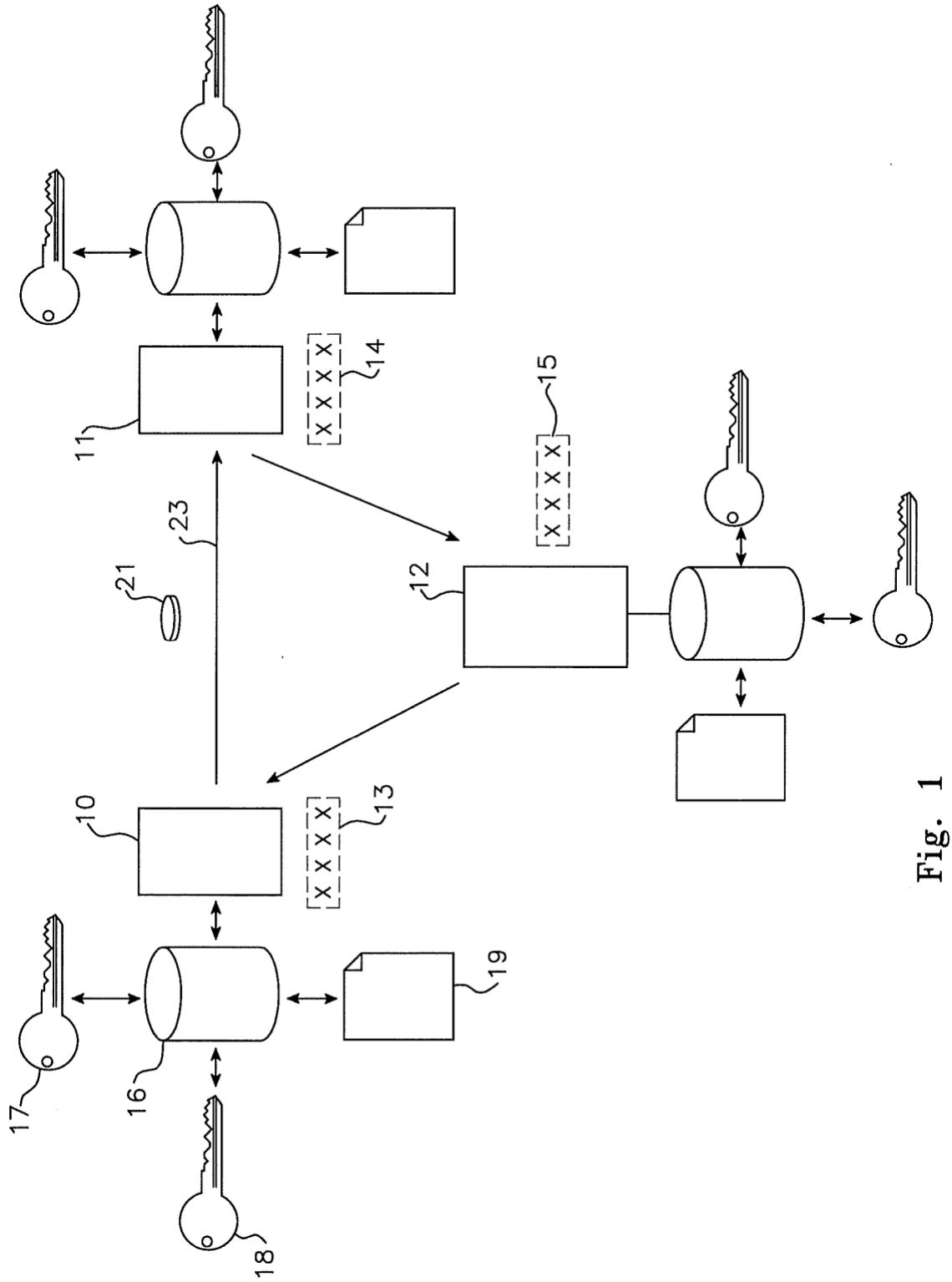

Fig. 1

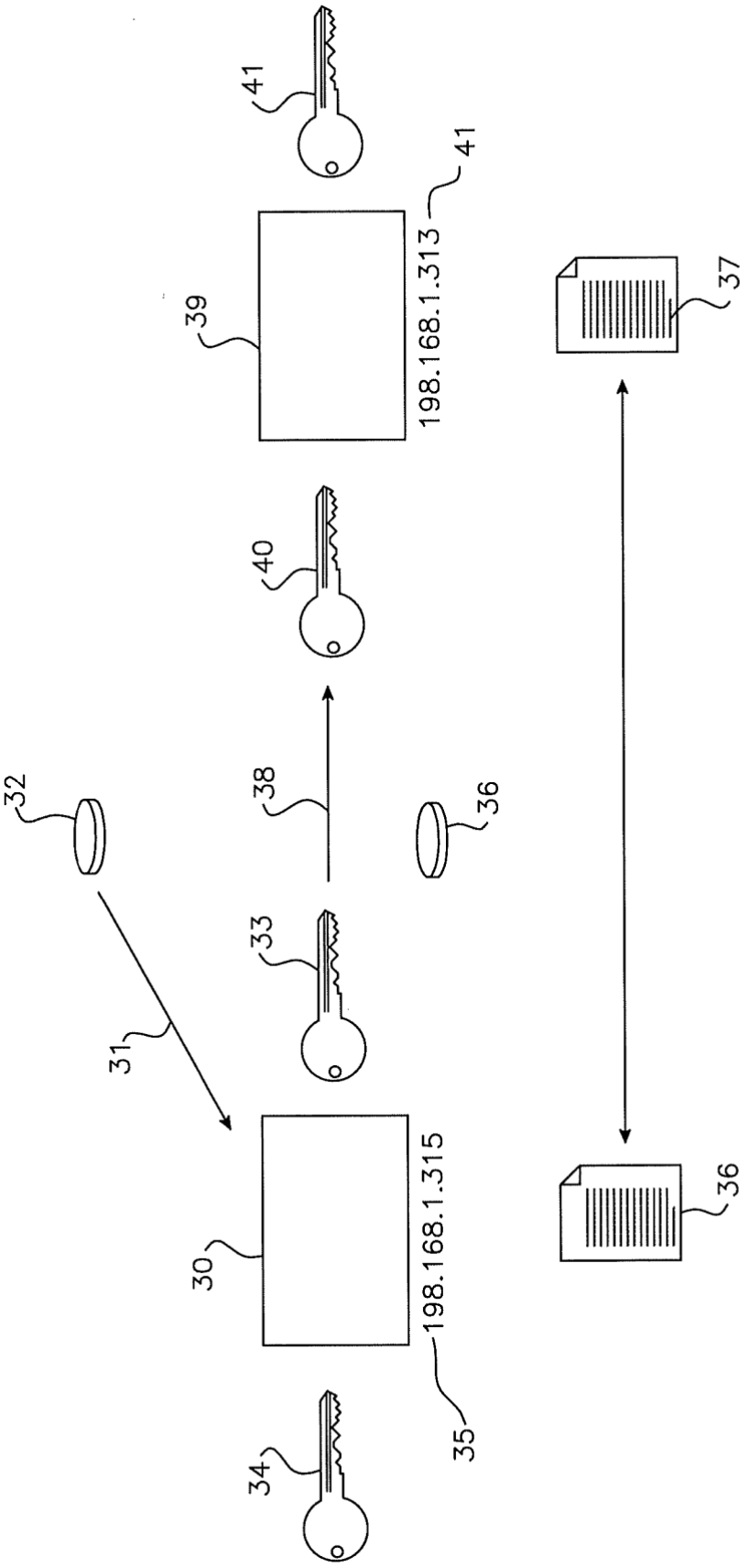

Fig. 2

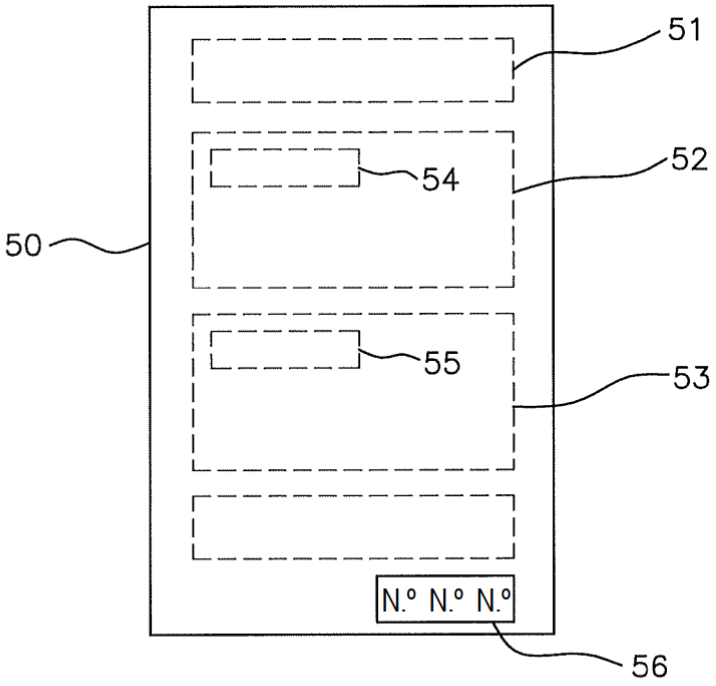

Fig. 3

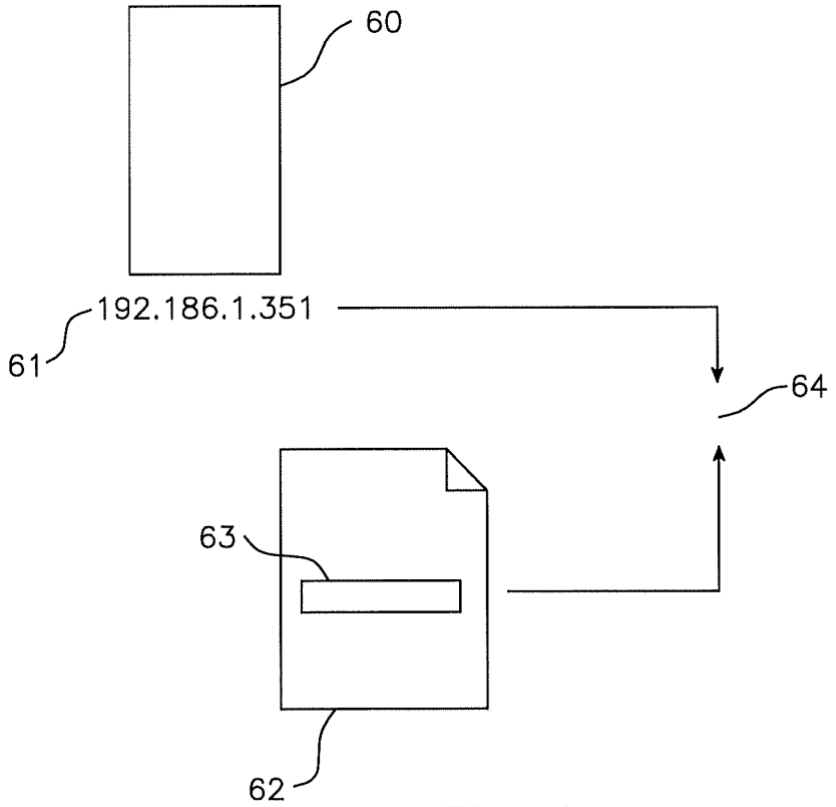

Fig. 4

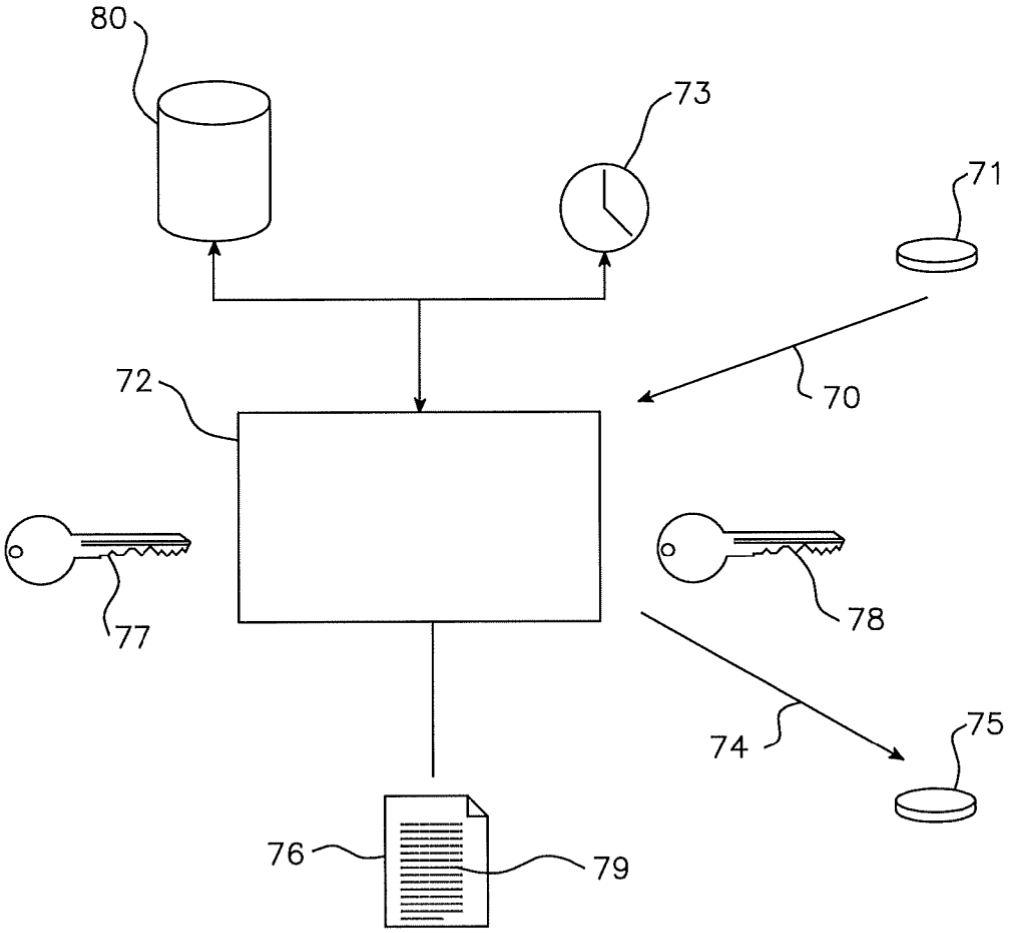

Fig. 5

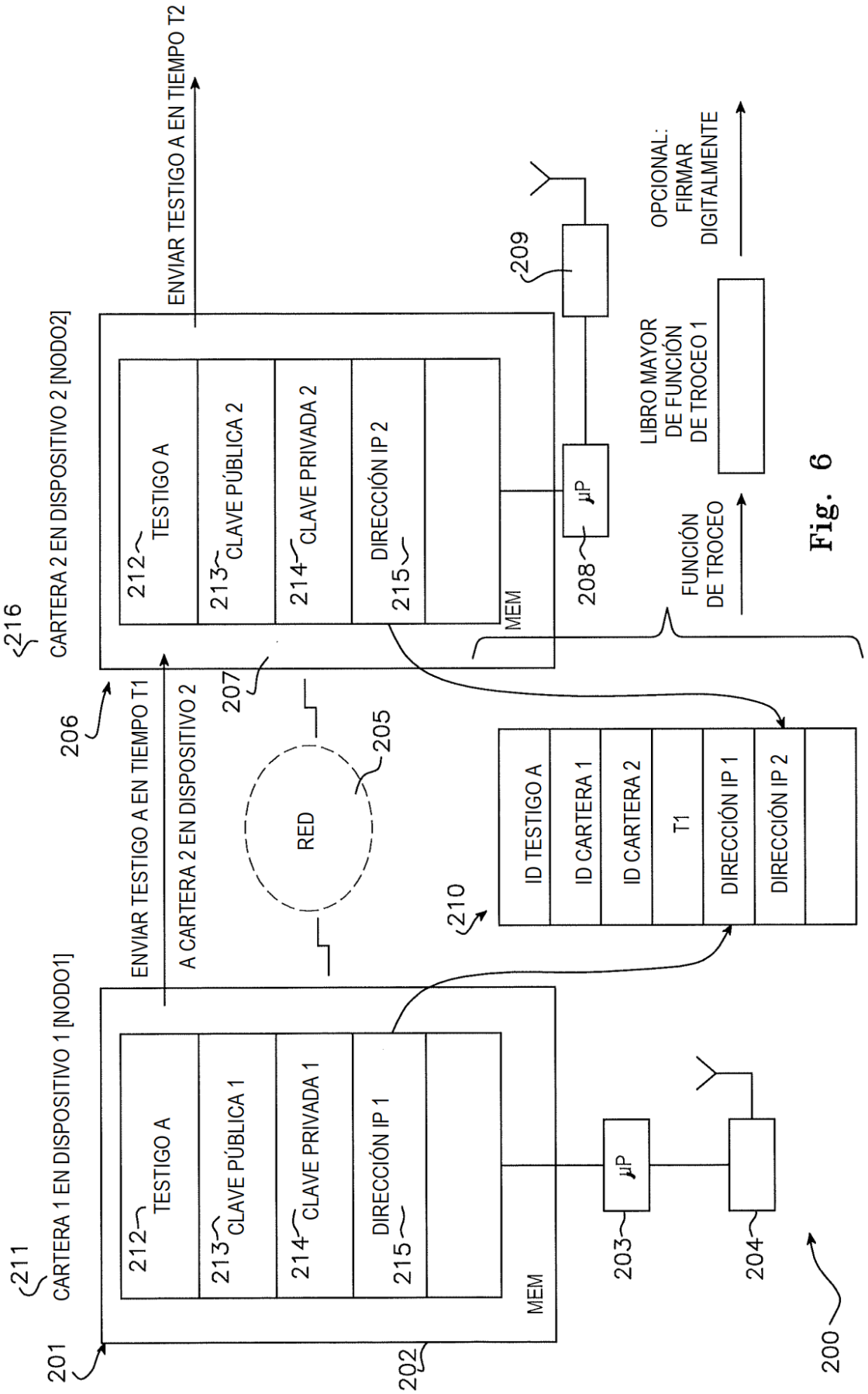
200
201
CARTERA 1 EN DISPOSITIVO 1 [NODO1]
211
202
MEM
212 TESTIGO A
213 CLAVE PÚBLICA 1
214 CLAVE PRIVADA 1
215 DIRECCIÓN IP 1
203
μP
204
ENVIAR TESTIGO A EN TIEMPO T1
A CARTERA 2 EN DISPOSITIVO 2
206
CARTERA 2 EN DISPOSITIVO 2 [NODO2]
216
207
MEM
212 TESTIGO A
213 CLAVE PÚBLICA 2
214 CLAVE PRIVADA 2
215 DIRECCIÓN IP 2
208
μP
209
ENVIAR TESTIGO A EN TIEMPO T2
RED
205
210
ID TESTIGO A
ID CARTERA 1
ID CARTERA 2
T1
DIRECCIÓN IP 1
DIRECCIÓN IP 2
FUNCIÓN DE TROCEO
LIBRO MAYOR DE FUNCIÓN DE TROCEO 1
OPCIONAL: FIRMAR DIGITALMENTE

Fig. 6

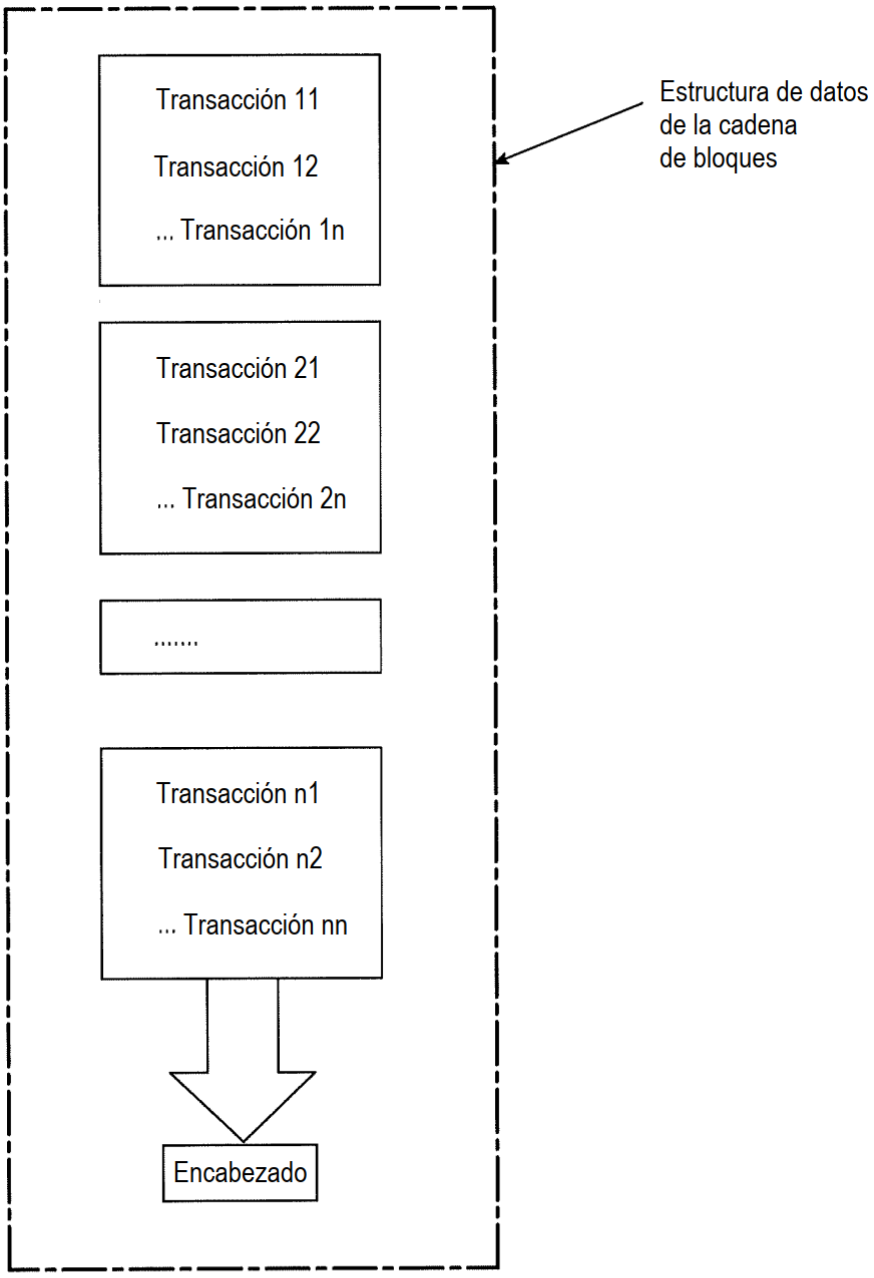
Transacción 11
Transacción 12
... Transacción 1n
Transacción 21
Transacción 22
... Transacción 2n
.....
Transacción n1
Transacción n2
... Transacción nn
Encabezado
Estructura de datos
de la cadena
de bloques

Fig. 7

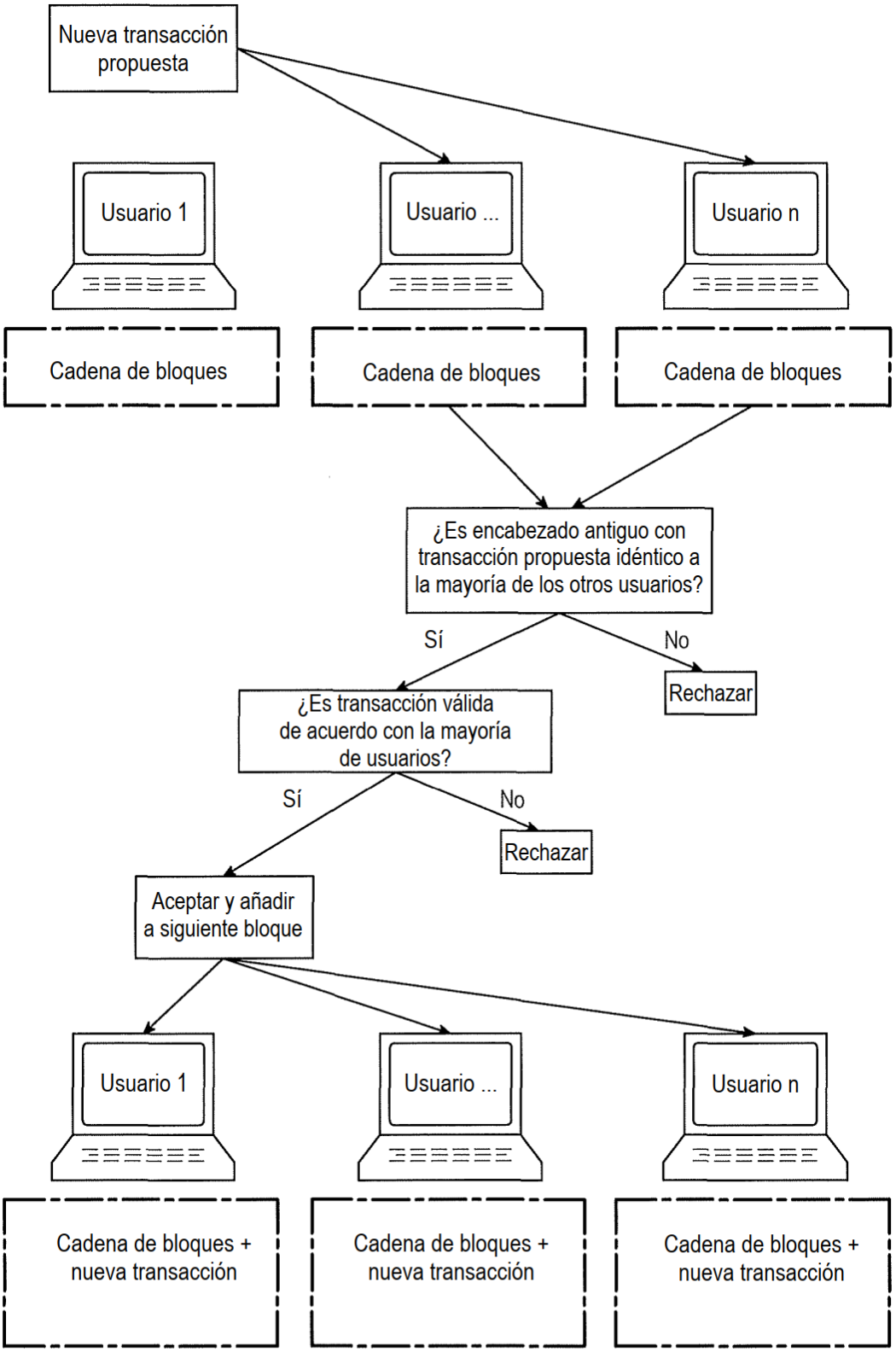
Nueva transacción propuesta
Usuario 1
Usuario ...
Usuario n
Cadena de bloques
Cadena de bloques
Cadena de bloques
¿Es encabezado antiguo con transacción propuesta idéntico a la mayoría de los otros usuarios?
Sí
No
Rechazar
¿Es transacción válida de acuerdo con la mayoría de usuarios?
Sí
No
Rechazar
Aceptar y añadir a siguiente bloque
Usuario 1
Usuario ...
Usuario n
Cadena de bloques + nueva transacción
Cadena de bloques + nueva transacción
Cadena de bloques + nueva transacción

Fig. 8