(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 732 497**

(51) Int. CI.:

H04L 9/32 (2006.01)
H04L 9/08 (2006.01)
G06Q 20/04 (2012.01)
G06Q 20/06 (2012.01)
G06Q 20/10 (2012.01)
G06Q 20/36 (2012.01)
G06Q 20/38 (2012.01)
G06Q 20/40 (2012.01)
G06Q 30/02 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **30.01.2017 E 17153843 (2)**

(97) Fecha y número de publicación de la concesión europea: **27.03.2019 EP 3247070**

(54) Título: **Verificación de la participación en eventos basados en criptodivisas**

(30) Prioridad:

20.05.2016 US 201615161001

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
22.11.2019

(73) Titular/es:

FUJITSU LIMITED (100.0%)
1-1, Kamikodanaka 4-chome, Nakahara-ku
Kawasaki-shi Kanagawa 211-8588, JP

(72) Inventor/es:

MANDAL, AVRADIP;
ROY, ARNAB y
MONTGOMERY, HART

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Verificación de la participación en eventos basados en criptodivisas

Campo

Los modos de realización expuestos en el presente documento están relacionados con la verificación de la participación en eventos basados en criptodivisas.

Antecedentes

Una criptodivisa es un medio de intercambio digital que utiliza la criptografía para asegurar y realizar transacciones entre entidades. Algunos ejemplos de criptodivisas incluyen BITCOIN® y MONEDAS COLOREADAS. En algunos sistemas de criptodivisa, se usa un sistema descentralizado de autenticación de transacciones. Por ejemplo, en Bitcoin, se utiliza una cadena de bloques, que es un tipo de libro mayor de solo escritura, para publicar públicamente una transacción para que los mineros se autentiquen. La cadena de bloques registra cada transacción en secuencia, lo que permite a los mineros autenticar cada transacción que involucre a Bitcoin.

La materia reivindicada en el presente documento no se limita a modos de realización que resuelven desventajas o que funcionan solo en entornos como los descritos anteriormente. Más bien, estos antecedentes se proporcionan solo para ilustrar un área de tecnología de ejemplo donde se pueden llevar a la práctica algunos modos de realización descritos en el presente documento.

El documento US2015235255 (A1) divulga un sistema de recompensa basado en la frecuencia, un método y un medio legible por ordenador (en conjunto, el "Sistema"). El Sistema puede comprender un programa de recompensa que tiene una primera porción y una segunda porción. La primera porción puede configurarse para determinar una primera recompensa para una primera transacción basada en el importe de la transacción. El Sistema también puede configurarse para supervisar una serie de transacciones asociadas con una cuenta de transacción. La segunda porción puede configurarse para determinar una segunda recompensa en respuesta al número de transacciones asociadas con una cuenta de transacción que exceda un umbral. La segunda recompensa puede ser una función de la recompensa total ganada por todas las transacciones asociadas con una cuenta de transacción para un período de tiempo.

El documento US2015371224 (A1) divulga métodos y sistemas para gestionar una red de pago de criptodivisa que comprende uno o más nodos emisores y uno o más nodos de distribución. A los nodos emisores se les pueden otorgar derechos diferentes a los nodos de distribución con respecto a la emisión y distribución de divisa digital dentro de la red de pago de criptodivisa. Un ordenador servidor del sistema de administración puede generar pares de claves de verificación de nodo únicos para cada nodo en la red de pago de criptodivisa, donde los pares de claves de verificación de nodo se pueden usar para identificar y autenticar los nodos emisores y los nodos distribuidores.

Resumen

La presente invención está definida por las reivindicaciones independientes adjuntas, a las que ahora se ha de hacer referencia. Modos de realización específicos están definidos en las reivindicaciones dependientes.

Las ventajas de los modos de realización se realizarán y se lograrán al menos por los elementos, características y combinaciones señaladas de manera concreta en las reivindicaciones.

Ha de entenderse que tanto la descripción general anterior como la siguiente descripción detallada son de ejemplo y explicativas y no son restrictivas de la invención, como se reivindica.

Breve descripción de los dibujos

Se describirán y explicarán modos de realización de ejemplo con especificidad y detalle adicionales mediante el uso de los dibujos adjuntos, en los que:

La figura 1 es un diagrama de bloques de un entorno operativo de ejemplo en el que se pueden implementar algunos modos de realización descritos en el presente documento;

La figura 2A es un diagrama de bloques de una primera porción de un proceso de verificación de participación de ejemplo que puede implementarse en el entorno operativo de la figura 1;

La figura 2B es un diagrama de bloques de una segunda porción del proceso de verificación de participación de la figura 2A;

La figura 2C es un diagrama de bloques de una tercera porción del proceso de verificación de participación de la figura 2A;

La figura 3 es un diagrama de bloques de un sistema informático configurado para la verificación de la participación; y

Las figuras 4A-4C son un diagrama de flujo de un método de ejemplo de verificación de participación en un evento,

todo de acuerdo con al menos un modo de realización descrito en esta divulgación.

Descripción de algunos modos de realización de ejemplo

Una autoridad central tal como una entidad comercial o una entidad gubernamental puede querer recompensar a los usuarios por participar en un conjunto o serie de eventos. Por ejemplo, una entidad comercial puede recompensar a los usuarios por visitar un conjunto de ubicaciones diferentes o por la recolección de un conjunto de cupones. La autoridad central puede querer permitir que los usuarios prueben de forma segura que han participado en los eventos, a la vez que dificulta que los usuarios afirmen haber participado cuando en realidad no lo han hecho.

Por consiguiente, los modos de realización descritos en esta divulgación usan criptodivisa y una aplicación de verificación para permitir a los usuarios probar de forma segura que han participado en los eventos. En algunos modos de realización, la autoridad central genera o recibe criptodivisa en cantidades que están relacionadas con el número de usuarios y el número de eventos. Por ejemplo, la autoridad central puede generar conjuntos de monedas de criptodivisa (conjuntos de monedas). El número de conjuntos de monedas puede ser igual al número de eventos y cada uno de los conjuntos de monedas puede correlacionarse con uno de los eventos. El número de monedas en cada uno de los conjuntos de monedas puede ser igual a un número de usuarios.

Durante una interacción inicial entre la autoridad central y el usuario, el usuario puede descargar la aplicación de verificación. Además, la autoridad central puede asignar una clave pública al usuario, que puede ser comunicada al usuario. A medida que el usuario participa en los eventos, el usuario comunica las solicitudes de moneda a la autoridad central. Las solicitudes de moneda pueden especificar el evento en el que el usuario participa a través de la identificación del conjunto de monedas correlacionado con el evento. La solicitud de moneda también puede incluir un conjunto de datos que confirme o pruebe que el usuario realmente participó en el evento.

La autoridad central verifica que el usuario realmente participó en el evento basándose en el conjunto de datos. Utilizando una transacción de criptodivisa, la autoridad central transfiere una de las monedas de criptodivisa del conjunto de monedas identificado al usuario. Se produce un proceso similar para cada solicitud de moneda en base a cada evento en el que el usuario participa. Las transacciones de criptodivisa pueden ejecutarse utilizando un libro mayor de solo escritura y una validación pública.

Después de que el usuario haya recopilado una moneda de criptodivisa de cada uno de los conjuntos de monedas, la autoridad central puede verificarlo a través de la revisión del libro mayor de solo escritura. La autoridad central puede recompensar al usuario por su participación en los eventos.

Debido a que la autoridad central es propietaria de cada uno de los conjuntos de monedas y el usuario no tiene acceso a las claves secretas, las transacciones de criptodivisa que involucran los conjuntos de monedas están limitadas. Por ejemplo, la autoridad central solo puede transferir las monedas de criptodivisa a los usuarios y no al revés. Además, el uso del libro mayor de solo escritura permite la revisión pública y un historial de transacciones. En algunos modos de realización, la autoridad central puede usar la porción de MONEDA COLOREADA del sistema BITCOIN® o un sistema de criptodivisa similar. Estos y otros modos de realización se describen haciendo referencia a las figuras adjuntas en las que números de elemento similares indican una estructura similar a menos que se especifique lo contrario.

La figura 1 es un diagrama de bloques de un entorno 100 operativo de ejemplo en el que se puede realizar una verificación segura de la participación en el evento (de aquí en adelante, "verificación de participación"). La verificación de participación puede permitir que un servidor 106 de autoridad central (servidor CA) verifique que uno o más usuarios 112A y 112B (generalmente, el usuario 112 o los usuarios 112) hayan participado en un conjunto de eventos. La verificación de participación puede basarse en el servidor 106 CA o en un servidor 128 de entidad delegada (servidor DE) que transfiera una o más monedas de criptodivisa a los usuarios 112 a cambio de que los usuarios 112 confirmen su participación en uno o más eventos del conjunto de eventos. El servidor 106 CA puede entonces verificar que el usuario 112 ha participado en cada evento en un conjunto de eventos mediante la verificación de un conjunto de transacciones de criptodivisa. A cambio de que los usuarios 112 participen en el conjunto de eventos, los usuarios 112 pueden recibir una recompensa de una entidad 150 de autoridad central (entidad CA) asociada con el servidor 106 CA y/o una entidad 152 delegada asociada con el servidor 128 de entidad delegada.

En algunos modos de realización, el entorno 100 operativo puede implementar monedas de criptodivisa o una o más criptodivisas similares. Las monedas de criptodivisa pueden tener poco o ningún valor monetario aparte del uso en la verificación de participación. Por ejemplo, las MONEDAS COLOREADAS, que se implementan en infraestructuras BITCOIN® o una criptodivisa similar, pueden usarse en el entorno 100 operativo. Las transacciones de criptodivisa que involucran MONEDAS COLOREADAS pueden ser autenticadas por un dispositivo 144 minero utilizando un libro 140 mayor de solo escritura, el cual puede ser denominado como una cadena de bloques. Algunos detalles

adicionales de las MONEDAS COLOREADAS y la cadena de bloques se describen en http://en.bitcoin.it/wiki/Help:Introduction y http://en.bitcoin.it/wiki/Colored_Coins.

El uso de criptodivisa puede permitir la verificación de la participación en el entorno 100 operativo que es seguro y fiable. Por ejemplo, la verificación de la participación puede configurarse de manera que los usuarios 112 puedan probar la participación del usuario 112 y/o los dispositivos 115A y 115B de usuario (generalmente, el dispositivo 115 de usuario o los dispositivos 115 de usuario) asociados con el usuario 112 mientras previenen o previenen considerablemente trampas (por ejemplo, intentar confirmar la participación sin participación en el evento) por parte de los usuarios 112. Además, la verificación de la participación puede configurarse para garantizar que solo uno o más usuarios 112 que participaron realmente en el conjunto de eventos son capaces de probar al servidor 106 CA y/o al servidor 128 de entidad delegada.

El entorno 100 operativo de la figura 1 puede incluir el servidor 106 CA, los dispositivos 115 de usuario, los usuarios 112, el servidor 128 de entidad delegada, la entidad 152 delegada, el dispositivo 144 minero y un servidor 124 público. El servidor 106 CA, los dispositivos 115 de usuario, los usuarios 112, el servidor 128 de entidad delegada, la entidad 152 delegada, el dispositivo 144 minero y el servidor 124 público se denominan de manera conjunta "componentes de entorno". Los componentes de entorno pueden configurarse para comunicar datos e información a través de una red 122. Cada uno de los componentes de entorno y la red 122 se describen a continuación.

La red 122 puede incluir configuraciones por cable o inalámbricas, y puede tener configuraciones que incluyan una configuración en estrella, una configuración en anillo con paso de testigo u otras configuraciones. Además, la red 122 puede incluir una red de área local (LAN), una red de área amplia (WAN) (por ejemplo, Internet), y/u otras rutas de datos interconectadas a través de las cuales pueden comunicarse múltiples dispositivos. En algunos modos de realización, la red 122 puede incluir una red entre pares. La red 122 también puede estar acoplada o incluir porciones de una red de telecomunicaciones que puede permitir la comunicación de datos en una variedad de diferentes protocolos de comunicación.

En algunos modos de realización, la red 122 incluye redes de comunicación BLUETOOTH® y/o redes de comunicación móvil para enviar y recibir datos, incluso a través del servicio de mensajes cortos (SMS), servicio de mensajes multimedia (MMS), protocolo de transferencia de hipertexto (HTTP), conexión directa de datos, protocolo de aplicación inalámbrica (WAP), correo electrónico, etc. La red 122 puede permitir la comunicación a través de un protocolo basado en estándares como el perfil de energía inteligente (SEP), Echonet Lite, OpenADR u otro protocolo adecuado (por ejemplo, Wi-Fi, ZigBee, etc.).

El dispositivo 144 minero puede incluir cualquier sistema informático que incluya un procesador, una memoria y capacidades informáticas. En los modos de realización ilustrados, el dispositivo 144 minero puede estar conectado a la red 122 para enviar y recibir información con uno o más de los componentes de entorno a través de la red 122. Por ejemplo, el dispositivo 144 minero puede estar configurado para recibir información relacionada con los usuarios 112, el servidor 106 CA, el servidor 128 de entidad delegada o algunas combinaciones de los mismos que se utilizan en las transacciones de criptodivisa.

En algunos modos de realización, los datos e información recibidos por el dispositivo 144 minero pueden incluir claves públicas asignadas a los usuarios 112 y/o los dispositivos 115 de usuario. Además, los datos e información recibidos por el dispositivo 144 minero pueden incluir claves secretas que pueden correlacionarse con una moneda de criptodivisa en concreto. Además, los datos e información recibidos por el dispositivo 144 minero pueden incluir un número y/o un tipo de monedas de criptodivisa incluidas en una transacción de criptodivisa.

El dispositivo 144 minero puede incluir un módulo 142 de transacción. El módulo 142 de transacción puede configurarse para validar la transacción de criptodivisa. En concreto, la transacción de criptodivisa puede incluir la validación pública de la transferencia de una moneda de criptodivisa desde el primer conjunto de monedas identificado al dispositivo 115 de usuario a través de un libro mayor de solo escritura.

Por ejemplo, las transacciones de criptodivisa pueden validarse utilizando la red BITCOIN®. Algunos detalles adicionales de la red BITCOIN® se proporcionan en https://en.wikipedia.org/wiki/Bitcoin_network#Bitcoin_mining. Si bien el entorno 100 operativo incluye un único dispositivo 144 minero, en algunos modos de realización, se pueden incluir múltiples dispositivos 144 mineros para realizar la validación de transacciones de criptodivisa.

El servidor 124 público puede incluir un servidor de hardware que incluya un procesador, memoria y capacidades de comunicación. En los modos de realización ilustrados, el servidor 124 público puede estar acoplado a la red 122 para enviar y recibir datos e información hacia y desde uno o más de los componentes de entorno a través de la red 122. El servidor 124 público puede tener almacenado en el mismo el libro 140 mayor de solo escritura. Algunos detalles de un ejemplo del libro 140 mayor de solo escritura se describen en https://en.bitcoin.it/wiki/Help:Introduction.

En algunos modos de realización, el libro 140 mayor de solo escritura puede ser parte del dominio público. Por consiguiente, el libro 140 mayor de solo escritura puede ser almacenado, accedido y actualizado por uno o más de los componentes de entorno en el entorno 100 operativo. Por ejemplo, el dispositivo 144 minero puede añadir un bloque de transacción al libro 140 mayor de solo escritura. De manera adicional o como alternativa, el servidor 106

CA y/o el servidor 128 de entidad delegada pueden acceder al libro 140 mayor de solo escritura para verificar si uno o más de los usuarios 112 han participado en un conjunto de eventos, que pueden reflejarse como transferencias de criptodivisa (por ejemplo, monedas de criptodivisa) desde el servidor 106 CA y/o el servidor 128 de entidad delegada hasta los usuarios 112 o los dispositivos 115 de usuario.

Los usuarios 112 pueden incluir cualquier entidad, conjunto de entidades, uno o más dispositivos, o alguna combinación de los mismos. Por ejemplo, en el modo de realización representado, los usuarios 112 pueden incluir individuos. Los individuos pueden participar en uno o más de los eventos y participar en transacciones de criptodivisa con el servidor 106 CA y/o el servidor 128 de entidad delegada usando uno de los dispositivos 115 de usuario. En otros modos de realización, los usuarios 112 pueden incluir múltiples individuos, que pueden estar relacionados. Por ejemplo, el usuario 112 puede incluir un grupo de individuos que trabajan todos en el mismo lugar y que pueden tener acceso a uno de los dispositivos 115 de usuario. Los individuos, individualmente o como un grupo, pueden participar en los eventos. De manera adicional o como alternativa, el usuario 112 puede incluir uno o más dispositivos (por ejemplo, vehículos, piezas de equipo, etc.) que pueden estar asociados con uno o más individuos. Por ejemplo, el usuario 112 puede incluir una pieza de equipo que use cada uno de un conjunto de individuos en la participación de uno o más de los eventos.

Los usuarios 112 pueden estar asociados con los dispositivos 115 de usuario. Como se utiliza en esta divulgación, el término asociado puede indicar que el usuario 112 posee o hace funcionar regularmente el dispositivo 115 de usuario.

Los dispositivos 115 de usuario pueden incluir cualquier sistema informático que incluya un procesador, memoria y capacidades informáticas. En los modos de realización ilustrados, los dispositivos 115 de usuario pueden estar conectados a la red 122 para enviar y recibir información hacia y desde uno o más componentes de entorno a través de la red 122. Algunos ejemplos de los dispositivos 115 de usuario pueden incluir un teléfono inteligente, un ordenador de escritorio, y similares.

Los dispositivos 115 de usuario pueden incluir módulos 110 de dispositivo. Los módulos 110 de dispositivo o alguna porción de los mismos pueden descargarse desde el servidor 106 CA y/o el servidor 128 de entidad delegada a través de la red 122. Por ejemplo, en algunos modos de realización, los dispositivos 115 de usuario pueden comunicar una solicitud de inclusión en un servicio de verificación desde el servidor 106 CA y/o el servidor 128 de entidad delegada. En respuesta, el servidor 106 CA y/o el servidor 128 de entidad delegada pueden permitir que los dispositivos 115 de usuario descarguen una aplicación de verificación. Además, en respuesta a la solicitud, el servidor 106 CA y/o el servidor 128 de entidad delegada pueden comunicar una o más claves públicas a los dispositivos 115 de usuario. Las claves públicas pueden asignarse a los usuarios 112 y/o a los dispositivos 115 de usuario.

La aplicación de verificación puede incluir una aplicación móvil. La aplicación de verificación puede configurarse para comunicarse con el servidor 106 CA y/o el servidor 128 de entidad delegada. Por ejemplo, la aplicación de verificación puede estar configurada para comunicar solicitudes de moneda al servidor 106 CA y/o al servidor 128 de entidad delegada. Las solicitudes de moneda pueden incluir la clave pública asignada al usuario 112, un conjunto de monedas concreto y un conjunto de datos que se pueden usar para confirmar la participación del usuario 112 en uno o más de los eventos.

Además, la aplicación de verificación puede configurarse para comunicar una solicitud de finalización al servidor 106 CA y/o al servidor 128 de entidad delegada. La solicitud de finalización se puede configurar para certificar que se le ha transferido al usuario 112 una moneda de criptodivisa de cada uno de múltiples conjuntos de monedas de criptodivisa (conjuntos de monedas), que pueden representar la participación en el conjunto de eventos. La aplicación de verificación también puede recibir notificaciones. Las notificaciones pueden incluir una notificación de que se está llevando a cabo una transacción de criptodivisa entre el servidor 106 CA y/o el servidor 128 de entidad delegada y los dispositivos 115 de usuario.

El módulo 110 de dispositivo puede implementarse utilizando hardware que incluya un procesador, un microprocesador (por ejemplo, para realizar o controlar la realización de una o más operaciones), una matriz de puerta programable por campo (FPGA) o un circuito integrado para aplicaciones específicas (ASIC). En algunos otros ejemplos, el módulo 110 de dispositivo puede implementarse utilizando una combinación de hardware y software. La implementación en software puede incluir la activación y desactivación rápidas de uno o más transistores o elementos de transistor, como los que se pueden incluir en el hardware de un sistema informático (por ejemplo, el dispositivo 115 de usuario). De manera adicional, las instrucciones definidas por el software pueden funcionar con información dentro de los elementos de transistor. La implementación de las instrucciones del software puede al menos reconfigurar temporalmente las rutas electrónicas y transformar el hardware informático.

La entidad 150 CA puede asociarse con el servidor 106 CA. La entidad 152 delegada puede asociarse con el servidor 128 de entidad delegada. La entidad 150 CA y la entidad 152 delegada pueden incluir cualquier entidad, como una entidad comercial, una entidad gubernamental, y similares. Un ejemplo de la entidad 150 CA puede incluir una entidad comercial interesada en dirigir a los usuarios 112 a múltiples puestos en una conferencia. Un ejemplo de

la entidad 152 delegada puede incluir un organismo gubernamental que esté interesado en dirigir a los usuarios 112 a múltiples ubicaciones geográficas.

El servidor 106 CA puede incluir un módulo 108 de verificación del servidor. El módulo 108 de verificación del servidor puede configurarse para establecer la criptodivisa, para verificar la participación de los usuarios 112, para entrar en transacciones de criptodivisa y para verificar la finalización de un conjunto de las transacciones de criptodivisa. En algunos modos de realización, el módulo 108 de verificación del servidor puede comunicar o permitir el acceso a una recompensa a cambio de la participación en el conjunto de eventos.

Por ejemplo, el módulo 108 de verificación del servidor puede generar una clave secreta maestra y una clave pública maestra. Una serie de claves secretas maestras y claves públicas maestras pueden estar relacionadas con un número de conjuntos de monedas. Por ejemplo, el módulo 108 de verificación del servidor puede generar la clave secreta maestra y la clave pública maestra para cada uno de los conjuntos de monedas.

El módulo 108 de verificación del servidor puede generar un primer número de conjuntos de monedas. Uno o más de los conjuntos de monedas pueden tener un segundo número de monedas de criptodivisa. Uno o más de los conjuntos de monedas pueden correlacionarse con un evento en el conjunto de eventos para los cuales se verificará la participación. La clave secreta maestra y/o la clave pública maestra se pueden usar en la creación de monedas.

El módulo 108 de verificación del servidor puede generar un par de claves de usuario. Una o más de las claves de usuario pueden incluir una clave pública única y una clave secreta de usuario. Por ejemplo, las claves de usuario pueden incluir una clave pública única para cada uno de los usuarios 112. El segundo número, que puede ser el número de monedas en los conjuntos de monedas, puede ser igual al número de usuarios 112. Por ejemplo, pueden ser cinco conjuntos de monedas de criptodivisa, que pueden correlacionarse con cinco eventos para los cuales se realizará la verificación. El entorno 100 operativo puede incluir dos usuarios 112. Por consiguiente, cada uno de los conjuntos de monedas puede incluir dos monedas de criptodivisa.

En los modos de realización en los que está involucrada la entidad 152 delegada, uno o más conjuntos de monedas, la clave secreta maestra, la clave pública maestra, el par de claves de usuario o alguna combinación de las mismas pueden comunicarse al servidor 128 de entidad delegada desde el servidor 106 CA. Por ejemplo, uno de los conjuntos de monedas, una clave pública maestra asociada, una clave secreta maestra asociada y alguna porción del conjunto de claves públicas únicas pueden comunicarse al módulo 130 de verificación DE del servidor 128 de entidad delegada.

Después de que el módulo 130 de verificación DE recibe una combinación de los conjuntos de monedas, las claves públicas maestras, las claves secretas maestras o el par de claves de usuario, el módulo 130 de verificación DE puede configurarse para realizar al menos alguna porción de la verificación de participación como se describe en esta divulgación. Por ejemplo, el módulo 130 de verificación DE puede realizar la verificación segura de participación en eventos con respecto a un subconjunto de eventos, con respecto a un subconjunto de usuarios 112, etc.

Por consiguiente, en modos de realización en los que está involucrada la entidad 152 delegada, el módulo 130 de verificación DE puede realizar alguna porción de la verificación de participación y el módulo 108 de verificación del servidor puede realizar una porción restante de la verificación de participación. En modos de realización en los que la entidad 152 delegada no está involucrada, el módulo 108 de verificación del servidor puede realizar la verificación de la participación.

La verificación de la participación realizada por el módulo 130 de verificación DE y el módulo 108 de verificación del servidor puede ser similar o la misma. Por ejemplo, como se mencionó anteriormente, el usuario 112 puede comunicar una solicitud al servidor 106 CA y/o al servidor 128 de entidad delegada solicitando la inclusión en un servicio de verificación. En respuesta a la solicitud, el módulo 108 de verificación del servidor o el módulo 130 de verificación DE pueden asignar las claves públicas únicas al usuario 112 y/o al dispositivo 115 de usuario que está asociado con el usuario 112 que comunicó la solicitud. El módulo 108 de verificación del servidor o el módulo 130 de verificación DE pueden comunicar la clave pública única asignada al dispositivo 115 de usuario.

El módulo 108 de verificación del servidor o el módulo 130 de verificación DE pueden prevenir el acceso a las claves secretas del usuario junto con la clave pública única asignada. Prevenir el acceso a las claves secretas del usuario limita o impide que los usuarios 112 ingresen en transacciones de criptodivisa que no incluyan el servidor 106 CA o el servidor 128 DE. Además, en respuesta a la solicitud, el módulo 108 de verificación del servidor o el módulo 130 de verificación DE pueden permitir la descarga de la aplicación de verificación al dispositivo 115 de usuario.

El módulo 108 de verificación del servidor o el módulo 130 de verificación DE también pueden recibir la solicitud de moneda del dispositivo 115 de usuario. En respuesta a la solicitud de moneda, el módulo 108 de verificación del servidor o el módulo 130 de verificación DE pueden verificar que el usuario 112 participó en uno de los eventos basándose en el conjunto de datos incluido en la solicitud de moneda.

En algunos modos de realización, en respuesta a la solicitud de moneda, el módulo 108 de verificación del servidor o el módulo 130 de verificación DE también pueden verificar que el usuario 112 no ha recibido aún una de las monedas de criptodivisa del conjunto de monedas identificado usando el libro mayor 140 de solo escritura. De

manera adicional o como alternativa, en respuesta a la solicitud de moneda, el módulo 108 de verificación del servidor o el módulo 130 de verificación DE pueden autenticar que un usuario concreto de los usuarios 112 tiene el control del dispositivo 115 de usuario que envió la solicitud de moneda. Por ejemplo, puede comunicarse un reto al dispositivo 115 de usuario. El reto puede configurarse para verificar que el usuario 112 tiene el control del dispositivo 115 de usuario. Por ejemplo, el reto puede requerir que el usuario 112 ingrese una contraseña o clave. De manera adicional o como alternativa, el reto puede solicitar una entrada de autenticación biométrica para verificar que el usuario 112 tiene el control del dispositivo 115 de usuario. Ejemplos de la entrada de autenticación biométrica pueden incluir una huella digital, una exploración de la retina y similares.

En respuesta a la verificación de la participación en el evento por parte del usuario 112, el módulo 108 de verificación del servidor o el módulo 130 de verificación DE pueden ejecutar una transacción de criptodivisa con el dispositivo 115 de usuario. Como se describió anteriormente, la transacción de criptodivisa puede incluir una validación pública de la transferencia de una moneda de criptodivisa desde el conjunto de monedas identificado en la solicitud de moneda al dispositivo 115 de usuario a través del libro 140 mayor de solo escritura. La transacción de criptodivisa con el dispositivo 115 de usuario se puede registrar en el libro 140 mayor de solo escritura.

El módulo 108 de verificación del servidor o el módulo 130 de verificación DE pueden recibir del dispositivo 115 de usuario la solicitud de finalización. La solicitud de finalización puede configurarse para certificar que se le ha transferido al usuario 112 una moneda de criptodivisa de cada uno de los conjuntos de monedas. En respuesta a las solicitudes de finalización, el módulo 108 de verificación del servidor o el módulo 130 de verificación DE pueden verificar que al usuario 112 se le haya transferido una de las monedas de criptodivisa de cada uno de los conjuntos de monedas utilizando el libro 140 mayor de solo escritura. De manera adicional, en algunos modos de realización, en respuesta a la verificación de que se le ha transferido al usuario una de las monedas de criptodivisa de cada uno de los conjuntos de monedas, el módulo 108 de verificación del servidor o el módulo 130 de verificación DE pueden comunicar o permitir el acceso a una recompensa al dispositivo 115 de usuario del usuario 112.

El módulo 108 de verificación del servidor o el módulo 130 de verificación DE pueden implementarse utilizando hardware que incluya un procesador, un microprocesador (por ejemplo, para realizar o controlar la realización de una o más operaciones), una FPGA o un ASIC. En algunos otros ejemplos, el módulo 108 de verificación del servidor o el módulo 130 de verificación DE pueden implementarse utilizando una combinación de hardware y software. La implementación en el software puede incluir la activación y desactivación rápidas de uno o más transistores o elementos de transistor, como los que se pueden incluir en el hardware de un sistema informático (por ejemplo, el servidor 106 CA o el servidor 128 DE). De manera adicional, las instrucciones definidas por el software pueden funcionar con información dentro de los elementos de transistor. La implementación de las instrucciones del software puede al menos reconfigurar temporalmente las rutas electrónicas y transformar el hardware informático.

Se pueden realizar modificaciones, adiciones u omisiones en el entorno 100 operativo sin apartarse del alcance de la presente divulgación. La presente divulgación puede aplicarse a entornos operativos que pueden incluir una o más entidades 150 CA, una o más entidades 152 delegadas, uno o más servidores 106 CA, uno o más dispositivos 115 de usuario, uno o más usuarios 112, uno o más servidores 128 de entidad delegada, uno o más dispositivos 144 mineros, uno o más servidores 124 públicos, una o más redes 122, o cualquier combinación de los mismos. Por ejemplo, el entorno 100 operativo puede incluir dispositivos 144 mineros que validen las transacciones.

Además, la separación de varios componentes en los modos de realización descritos en el presente documento no pretende indicar que la separación se produce en todos los modos de realización. Puede entenderse con el beneficio de esta divulgación que los componentes descritos pueden integrarse juntos en un solo componente o separarse en múltiples componentes. Por ejemplo, el dispositivo 144 minero y el servidor 124 público pueden ser un solo sistema informático.

Las figuras 2A-2C representan un ejemplo de proceso 200 de verificación de participación que puede implementarse en el entorno 100 operativo. El proceso 200 de verificación de participación puede implementarse para verificar que los usuarios 112 han visitado varias ubicaciones 226A-226C (generalmente, ubicación 226 o ubicaciones 226). En el ejemplo de las figuras 2A-2C, visitar las ubicaciones 226 son el conjunto de eventos descritos haciendo referencia a la figura 1. En el ejemplo de las figuras 2A-2C, cada una de las ubicaciones 226 puede ser una ubicación geográfica diferente. Por ejemplo, el servidor 106 CA puede estar interesado en que los usuarios 112 visiten cada una de las ubicaciones 226. En otros modos de realización, el proceso 200 de verificación de participación puede implementarse para verificar la participación en otro conjunto de eventos. De hecho, el proceso 200 de verificación de participación puede implementarse en cualquier escenario que implique probar que se ha completado o conseguido algún conjunto de eventos. Por ejemplo, el conjunto de eventos puede incluir una prueba de que los usuarios 112 han visto un documento o una prueba de que un mensajero ha entregado un conjunto de artículos correctamente, etc.

En las figuras 2A-2C, el servidor 106 CA está realizando el proceso 200 de verificación de participación. Como se describió anteriormente, el servidor 128 DE de la figura 1 puede realizar una o más porciones del proceso 200 de verificación de participación.

La figura 2A representa una primera porción del proceso 200 de verificación de participación. En la primera porción, un módulo 211 de generación del módulo 108 de verificación del servidor puede generar conjuntos 204 de monedas, un par de claves 205 de usuario y claves 208 maestras.

Las claves 208 maestras pueden incluir una clave secreta maestra y una clave pública maestra para cada uno de los conjuntos 204 de monedas. Por ejemplo, en las claves 208 maestras de la figura 2A hay una clave pública maestra (por ejemplo, MPK_1, MPK_2 y MPK_3) y una clave secreta maestra (por ejemplo, MSK_1, MSK_2 y MSK_3) para cada uno de los conjuntos 204 de monedas. Las claves 208 maestras se pueden generar de manera simultánea o en gran parte de manera simultánea con los conjuntos 204 de monedas.

El módulo 211 de generación puede generar un número concreto de conjuntos 204 de monedas. La generación de conjuntos 204 de monedas puede basarse en las claves 208 maestras. El número concreto de conjuntos 204 de monedas puede corresponder y/o puede ser equivalente a un número de las ubicaciones 226. Por ejemplo, en la figura 2A, los conjuntos 204 de monedas incluyen "C_1, C_2 y C_3" que corresponden a una primera ubicación 226A, una segunda ubicación 226B y una tercera ubicación 226C. Los conjuntos 204 de monedas pueden incluir cada uno otro número concreto de monedas. El otro número concreto de monedas puede corresponder y/o puede ser equivalente a un número de usuarios 112. El servidor 106 CA puede otorgarse a sí mismo la propiedad de todas las monedas en todos los conjuntos 204 de monedas.

El par de claves 205 de usuario puede incluir claves 206 públicas y claves 207 secretas de usuario. El par de claves 205 de usuario puede generarse usando cualquier proceso de generación de claves que pueda dar como resultados pares de claves que incluyan las claves 206 públicas y las claves 207 secretas de usuario. Las claves 206 públicas pueden incluir una clave pública única para cada uno de los usuarios 112. Por ejemplo, en la figura 2A, las claves 206 públicas pueden incluir PK_{U1} que puede ser una clave pública única para el usuario 112.

El módulo 108 de verificación del servidor puede recibir una solicitud 210 de inclusión del dispositivo 115 de usuario. En respuesta a la solicitud 210 de inclusión, el módulo 108 de verificación del servidor puede comunicar la primera clave 206A pública única al dispositivo 115 de usuario. El módulo 108 de verificación del servidor también puede permitir la descarga de una aplicación 211 de verificación.

En algunos modos de realización, las claves 206 públicas pueden generarse y asignarse al usuario 112 en respuesta a una solicitud 210 de inclusión. Por consiguiente, la generación y asignación de las claves 206 públicas puede ser "en tiempo real", lo que puede reducir la posible pérdida de confidencialidad directa que puede ocurrir con la generación previa de las claves 206 públicas.

La figura 2B representa una segunda porción del proceso 200 de verificación de participación. En la segunda porción, el usuario 112 puede visitar la primera ubicación 226A y puede tener el control del dispositivo 115 de usuario. Cuando lo solicite el usuario 112 o automáticamente, la aplicación 211 de verificación puede comunicar una solicitud 214 de moneda al servidor 106 CA. La solicitud 214 de moneda puede incluir un conjunto 204A de monedas identificado, la primera clave 206A pública del usuario 112, y un conjunto 212 de datos. En la figura 2B, el conjunto 204A de monedas identificado se representa como el primer conjunto C_1 de monedas que puede indicar que la solicitud 214 de moneda incluye una identificación de un primer conjunto 204A de monedas que puede correlacionarse con la primera ubicación 226A. La primera clave 206A pública puede ser la clave pública única asignada al usuario 112 y/o al dispositivo 115 de usuario. El conjunto 212 de datos puede incluir información y datos configurados para probar que el usuario 112 y/o el dispositivo 115 de usuario están visitando la primera ubicación 226A. Por ejemplo, el primer conjunto 212 de datos puede incluir una o más de una combinación de una señal de GPS (sistema de posicionamiento global), un código de respuesta rápida (QR) y datos de ubicación inalámbricos locales.

En modos de realización en los que el conjunto de eventos incluye otro conjunto o serie de eventos, el conjunto 212 de datos puede incluir información diferente. Por ejemplo, en modos de realización en los que el conjunto de eventos incluye una prueba de que los usuarios 112 vieron un documento, el conjunto 212 de datos puede incluir una firma digital en el documento y/o metadatos modificados asociados con el documento. En modos de realización en los que el conjunto de eventos incluye una prueba de que el usuario entregó artículos, el conjunto 212 de datos puede incluir firmas de los destinatarios de los artículos.

Un módulo 213 de verificación puede recibir la solicitud 214 de moneda y verificar que el usuario 112 participó en el primer evento (por ejemplo, visitó la primera ubicación 226A) basándose en el conjunto 212 de datos. Por ejemplo, el módulo 213 de verificación puede correlacionar el conjunto 212 de datos a una lista de coordenadas de las ubicaciones 226. En algunos modos de realización, el módulo 213 de verificación puede verificar que el usuario 112 aún no ha recibido una de las monedas de criptodivisa del conjunto 204A de monedas identificado utilizando el libro 140 mayor de solo escritura. Por ejemplo, el módulo 213 de verificación puede acceder al libro 140 mayor de solo escritura. El módulo 213 de verificación puede entonces revisar el libro 140 mayor de solo escritura para determinar si el servidor 106 CA ya ha transferido una moneda de criptodivisa del conjunto 204A de monedas identificado al usuario 112 o al dispositivo 115 de usuario.

Además, el módulo 213 de verificación puede autenticar que el usuario 112 tiene el control del dispositivo 115 de usuario en el momento en que la solicitud 214 de moneda se comunica al servidor 106 CA. Por ejemplo, el módulo 213 de verificación puede comunicar al dispositivo 115 de usuario un reto 217 configurado para verificar que el usuario 112 tiene el control del dispositivo 115 de usuario. Por ejemplo, el reto 217 puede solicitar una entrada de autenticación biométrica para verificar que el usuario 112 tiene el control del dispositivo 115 de usuario o puede solicitar que el usuario 112 ingrese una contraseña en el dispositivo 115 de usuario.

De manera adicional, en respuesta a la verificación de la participación en el primer evento (por ejemplo, que el usuario 112 visitó realmente la primera ubicación 226A) por parte del usuario 112 (por ejemplo, la visita de la primera ubicación 226A por el usuario 112), un módulo 215 de transacción del servidor del módulo 108 de verificación del servidor puede ejecutar una transacción de criptodivisa con el dispositivo 115 de usuario. La ejecución de la transacción de criptodivisa puede incluir la comunicación de información 216 de transacción de criptodivisa. La información 216 de transacción de criptodivisa se puede agregar al libro 140 mayor de solo escritura. El dispositivo 144 minero puede validar públicamente la transacción de criptodivisa. La transacción de criptodivisa puede incluir la validación pública de la transferencia de una moneda de criptodivisa desde el conjunto 204A de monedas identificado al dispositivo 115 de usuario a través de un libro 140 mayor de solo escritura utilizando la información 216 de transacción de criptodivisa.

La información 216 de transacción de criptodivisa puede incluir una función resumen de un número de monedas del conjunto 204A de monedas identificado para transferir al usuario 112 y la primera clave 206A pública del usuario 112. La función resumen puede firmarse usando la clave secreta maestra MSK_1 del conjunto 204A de monedas identificado. Basándose en la información 216 de transacción de criptodivisa, el dispositivo 144 minero puede usar el libro 140 mayor de solo escritura para validar públicamente la transacción de criptodivisa entre el servidor 106 CA y el dispositivo 115 de usuario. Se proporcionan algunos detalles adicionales de la validación pública del libro 140 mayor de solo escritura en https://en.bitcoin.it/wiki/How_bitcoin_works.

Después de ser validada por el dispositivo 144 minero, la transacción de criptodivisa se puede registrar en el libro 140 mayor de solo escritura. El servidor 106 CA puede entonces comunicar una notificación 219 al dispositivo 115 de usuario. El dispositivo 115 de usuario puede entonces registrar que la moneda del conjunto 204A de monedas se ha transferido desde el servidor 106 CA al dispositivo 115 de usuario en una lista 223 de monedas.

Cuando el usuario 112 visita la segunda ubicación 226B y la tercera ubicación 226C, el dispositivo 115 de usuario puede comunicar solicitudes 214 de monedas adicionales al servidor 106 CA. Las solicitudes 214 de monedas adicionales pueden incluir la primera clave 206A pública, pueden identificar un conjunto 204 de monedas que se correlaciona con la segunda ubicación 226B y la tercera ubicación 226C. Además, las solicitudes 214 de monedas adicionales pueden incluir conjuntos 212 de datos adicionales que estén configurados para confirmar que el usuario 112 realmente visitó la segunda ubicación 226B y la tercera ubicación 226C. El módulo 108 de verificación del servidor puede entonces proceder como se describió anteriormente.

En algunos modos de realización, se puede implementar una técnica de anonimización de modo que el servidor 106 CA no tenga acceso a la información de identificación del usuario 112. En algunos modos de realización, la técnica de anonimización se puede implementar en toda la técnica de criptodivisa. Por ejemplo, puede implementarse zcash o una criptodivisa similar con criptografía y/o puede implementarse un mecanismo de lavado. De manera adicional o como alternativa, el proceso 200 de verificación de participación puede implementar software que permita el acceso a recursos en línea de forma anónima, como Tor, que está disponible en TorProject.org.

La figura 2C representa una tercera porción del proceso 200 de verificación de participación. En la tercera porción, la aplicación 211 de verificación puede determinar a partir de la lista 223 de monedas que el usuario 112 ha visitado cada una de las ubicaciones 226. Por ejemplo, después de que la aplicación 211 de verificación comunica una solicitud de moneda (por ejemplo, 214 de la figura 2B) para la tercera ubicación 226C y recibe una notificación (por ejemplo, 219 de la figura 2B) que indica la ejecución de una transacción de criptodivisa para una moneda del tercer conjunto de monedas, la aplicación 211 de verificación puede determinar que el usuario 112 ha visitado cada una de las ubicaciones 226.

La aplicación 211 de verificación puede comunicar una solicitud 235 de finalización al servidor 106 CA. La solicitud 235 de finalización puede configurarse para certificar que se le ha transferido al usuario 112 una moneda de criptodivisa de cada uno de los conjuntos de monedas (por ejemplo, 204 de la figura 2A). En respuesta a la solicitud 235 de finalización, un módulo 239 de recompensa del módulo 108 de verificación del servidor puede verificar que se le ha transferido al usuario 112 una de las monedas de criptodivisa de cada uno de los conjuntos de monedas (por ejemplo, 204 de la figura 2A) usando el libro 140 mayor de solo escritura. Por ejemplo, el módulo 239 de recompensa puede revisar el libro 140 mayor de solo escritura para las transferencias desde el servidor 106 CA al dispositivo 115 de usuario. El libro 140 mayor de solo escritura puede incluir cada una de las transferencias, por lo tanto, la revisión del libro 140 mayor de solo escritura da como resultado la confirmación de que se le ha transferido al usuario 112 una moneda de criptodivisa de cada uno de los conjuntos de monedas.

En respuesta a la verificación de que se le ha transferido al usuario 112 una de las monedas de criptodivisa de cada uno de los conjuntos de monedas, el módulo 239 de recompensa puede comunicar una recompensa 237 al dispositivo 115 de usuario del usuario 112.

Haciendo referencia conjunta a las figuras 2A-2C, durante el proceso 200 de verificación de participación, el usuario 112 no puede transferir monedas de criptodivisa porque el usuario 112 y el dispositivo 115 de usuario carecen de las claves 207 secretas de usuario correspondientes a sus claves 206 públicas únicas. Además, el usuario 112 no puede crear u obtener artificialmente monedas de criptodivisa porque el servidor 106 CA toma posesión de las monedas de criptodivisa. Además, el usuario 112 no puede recibir indebidamente la recompensa 237 porque el servidor 106 de CA o cualquier otra entidad puede verificar la propiedad a través del libro 140 mayor de solo escritura.

La figura 3 ilustra un sistema 300 informático de ejemplo configurado para la verificación de la participación. El sistema 300 informático puede implementarse, por ejemplo, en el entorno 100 operativo de la figura 1. Ejemplos del sistema 300 informático pueden incluir el servidor 124 público, los dispositivos 115 de usuario, el servidor 128 DE, el dispositivo 144 minero y el servidor 106 CA. El sistema 300 informático puede incluir uno o más procesadores 304, una memoria 308, una unidad 302 de comunicación, el dispositivo 314 de interfaz de usuario y un almacenamiento 301 de datos que incluye el módulo 108 de verificación del servidor, el módulo 142 de transacción, el módulo 130 de verificación DE y el módulo 110 del dispositivo (en conjunto, los módulos 108, 142, 130, y 110).

El procesador 304 puede incluir cualquier ordenador, entidad informática o dispositivo de procesamiento de propósito especial o de propósito general adecuado que incluya diversos módulos de software o hardware informático y pueda configurarse para ejecutar instrucciones almacenadas en cualquier medio de almacenamiento legible por ordenador aplicable. Por ejemplo, el procesador 304 puede incluir un microprocesador, un microcontrolador, un procesador de señal digital (DSP), un ASIC, una FPGA o cualquier otro circuito digital o analógico configurado para interpretar y/o ejecutar instrucciones de programa y/o para procesar datos.

Aunque se ilustra como un único procesador en la figura 3, el procesador 304 puede incluir de manera más general cualquier número de procesadores configurados para realizar individual o colectivamente cualquier número de operaciones descritas en la presente divulgación. Además, uno o más de los procesadores 304 pueden estar presentes en uno o más dispositivos electrónicos o sistemas informáticos diferentes. En algunos modos de realización, el procesador 304 puede interpretar y/o ejecutar instrucciones de programa y/o procesar datos almacenados en la memoria 308, el almacenamiento 301 de datos, o la memoria 308 y el almacenamiento 301 de datos. En algunos modos de realización, el procesador 304 puede obtener instrucciones de programa del almacenamiento 301 de datos y cargar las instrucciones de programa en la memoria 308. Después de que las instrucciones de programa se carguen en la memoria 308, el procesador 304 puede ejecutar las instrucciones de programa.

La memoria 308 y el almacenamiento 301 de datos pueden incluir medios de almacenamiento legibles por ordenador para transportar o tener instrucciones o estructuras de datos ejecutables por ordenador almacenadas en ellos. Dichos medios de almacenamiento legibles por ordenador pueden incluir cualquier medio disponible al que se pueda acceder mediante un ordenador de propósito general o de propósito especial, como el procesador 304. A modo de ejemplo, y no de limitación, dichos medios de almacenamiento legibles por ordenador pueden incluir medios de almacenamiento legibles por ordenador no transitorios o tangibles, incluyendo RAM, ROM, EEPROM, CD-ROM u otro almacenamiento en disco óptico, almacenamiento en disco magnético u otros dispositivos de almacenamiento magnético, dispositivos de memoria flash (por ejemplo, dispositivos de memoria de estado sólido) o cualquier otro medio de almacenamiento que pueda usarse para transportar o almacenar el código de programa deseado en forma de instrucciones o estructuras de datos ejecutables por ordenador y al que se pueda acceder mediante un ordenador de propósito general o de propósito especial. Combinaciones de lo anterior también pueden incluirse dentro del alcance de los medios de almacenamiento legibles por ordenador. Las instrucciones ejecutables por ordenador pueden incluir, por ejemplo, instrucciones y datos configurados para hacer que el procesador 304 realice una determinada operación o grupo de operaciones.

La unidad 302 de comunicación puede incluir una o más piezas de hardware configuradas para recibir y enviar comunicaciones. En algunos modos de realización, la unidad 302 de comunicación puede incluir uno o más de una antena, un puerto con cable y hardware de modulación/demodulación, entre otros dispositivos de hardware de comunicación. En concreto, la unidad 302 de comunicación puede estar configurada para recibir una comunicación desde fuera del sistema 300 informático y para presentar la comunicación al procesador 304 o para enviar una comunicación desde el procesador 304 a otro dispositivo o red (por ejemplo, 122 de la figura 1).

El dispositivo 314 de interfaz de usuario puede incluir una o más piezas de hardware configuradas para recibir entradas y/o proporcionar salidas a un usuario. En algunos modos de realización, el dispositivo 304 de interfaz de usuario puede incluir uno o más de un altavoz, un micrófono, una pantalla de visualización, un teclado, una pantalla táctil o una proyección holográfica, entre otros dispositivos de hardware.

Los módulos 108, 142, 130 y 110 pueden incluir instrucciones de programa almacenadas en el almacenamiento 301 de datos. El procesador 304 puede estar configurado para cargar los módulos 108, 142, 130 y 110 en la memoria

308 y ejecutar los módulos 108, 142, 130 y 110. Como alternativa, el procesador 304 puede ejecutar los módulos 108, 142, 130 y 110 línea por línea desde el almacenamiento 301 de datos sin cargarlos en la memoria 308. Al ejecutar los módulos 108, 142, 130 y 110, el procesador 304 puede configurarse para realizar un proceso de verificación de participación como se describió en otra parte de esta divulgación.

Se pueden hacer modificaciones, adiciones u omisiones al sistema 300 informático sin apartarse del alcance de la presente divulgación. Por ejemplo, en algunos modos de realización, el sistema 300 informático puede no incluir el dispositivo 314 de interfaz de usuario. En algunos modos de realización, los diferentes componentes del sistema 300 informático pueden estar físicamente separados y pueden estar conectados comunicativamente a través de cualquier mecanismo adecuado. Por ejemplo, el almacenamiento 301 de datos puede ser parte de un dispositivo de almacenamiento que esté separado de un servidor, que incluye el procesador 304, la memoria 308 y la unidad 302 de comunicación, que está acoplada comunicativamente al dispositivo de almacenamiento.

Las figuras 4A-4C son un diagrama de flujo de un método 400 de ejemplo de verificación de participación. El método 400 se puede realizar en un sistema operativo como el entorno 100 operativo de la figura 1. En algunos modos de realización el método 400 puede ser realizado de manera programable por el servidor 106 CA y/o el servidor 128 DE descritos haciendo referencia a la figura 1. En algunos modos de realización, el servidor 106 CA y/o el servidor 128 DE u otro sistema informático pueden incluir o pueden estar acoplados comunicativamente a un medio legible por ordenador no transitorio (por ejemplo, la memoria 308 de la figura 3) que tenga almacenado en él mismo código de programación o instrucciones que sean ejecutables por uno o más procesadores (como el procesador 304 de la figura 3) para hacer que un sistema informático y/o el servidor 106 CA y/o el servidor 128 DE realicen o controlen la realización del método 400. De manera adicional o como alternativa, el servidor 106 CA y/o el servidor 128 DE pueden incluir el procesador 304 descrito anteriormente que está configurado para ejecutar instrucciones informáticas para hacer que el servidor 106 CA y/o el servidor 128 DE u otro sistema informático realicen o controlen la realización del método 400. Aunque ilustrados como bloques distintos, varios bloques en la figura 4 pueden dividirse en bloques adicionales, combinarse en menos bloques, o eliminarse, dependiendo de la implementación deseada.

Haciendo referencia a la figura 4A, el método 400 puede comenzar en el bloque 402, en el que pueden generarse una clave secreta maestra y una clave pública maestra. La clave secreta maestra y la clave pública maestra pueden generarse para cada conjunto de monedas, que están descritos en otra parte de esta divulgación. En algunos modos de realización, la clave secreta maestra y la clave pública maestra pueden ser generadas por un servidor como el servidor 106 CA descrito haciendo referencia a la figura 1.

En el bloque 404, se genera un primer número de conjuntos de monedas. Uno o más de los conjuntos de monedas pueden incluir un segundo número de monedas de criptodivisa. Además, uno o más de los conjuntos de monedas pueden estar correlacionados con un evento en un conjunto de eventos para los cuales se verificará la participación. Las monedas de criptodivisa pueden no tener valor monetario. En algunos modos de realización, el conjunto de eventos puede incluir visitar un conjunto o serie de ubicaciones. Por ejemplo, el conjunto o la serie de ubicaciones pueden ser puestos en una conferencia y/o diversas ubicaciones geográficas. La clave secreta maestra y una clave pública maestra pueden usarse en la generación de los conjuntos de monedas. En algunos modos de realización, el primer número de conjuntos de monedas puede ser generado por un servidor como el servidor 106 CA descrito haciendo referencia a la figura 1.

En el bloque 405, se puede recibir una solicitud de inclusión. La solicitud de inclusión puede recibirse desde un dispositivo de usuario como el primer dispositivo 115A de usuario de la figura 1. La solicitud de inclusión puede solicitar que se incluya información y datos en un servicio de verificación de participación.

En el bloque 406, se puede generar un par de claves de usuario. El par de claves de usuario puede incluir una clave pública única y una clave secreta de usuario. El par de claves de usuario puede incluir la clave pública única para el usuario asociado con el dispositivo de usuario desde el cual se envía la solicitud de inclusión. En algunos modos de realización, el par de claves de usuario puede ser generado por un servidor como el servidor 106 CA descrito haciendo referencia a la figura 1.

En el bloque 408, las claves públicas únicas pueden asignarse a un usuario y a un dispositivo de usuario que esté asociado con el usuario. En algunos modos de realización, el conjunto de claves de usuario se puede generar y asignar al usuario (por ejemplo, se pueden realizar los bloques 406 y 408) en respuesta a la solicitud de inclusión. La generación y la asignación pueden ser "en tiempo real" para reducir la posible pérdida de la confidencialidad directa que puede ocurrir con la generación previa de las claves de usuario. En algunos modos de realización, las claves públicas únicas pueden ser asignadas por un servidor como el servidor 106 CA descrito haciendo referencia a la figura 1.

En el bloque 410, la clave pública única asignada puede comunicarse al dispositivo de usuario. Por ejemplo, en algunos modos de realización, un servidor como el servidor 106 CA de la figura 1 puede comunicar la clave pública única asignada a un dispositivo de usuario como el primer dispositivo 115A de usuario a través de la red 122.

En el bloque 412, se puede prevenir el acceso a la clave secreta de usuario emparejada con la clave pública única asignada. La prevención del acceso puede incluir el almacenamiento de la clave secreta de usuario o la eliminación de la clave secreta de usuario por un servidor como el servidor 106 CA de la figura 1. Al prevenir el acceso, se pueden prevenir las transacciones entre dispositivos de usuario de las monedas de criptodivisa. En el bloque 414, puede estar habilitada la descarga de una aplicación de verificación al dispositivo de usuario. Por ejemplo, en algunos modos de realización, puede ser habilitada la descarga de la aplicación de verificación al dispositivo de usuario, como el primer dispositivo 115A de usuario, por un servidor como el servidor 106 CA de la figura 1. En algunos modos de realización, los bloques 408, 410, 412, 414, o alguna combinación de los mismos se puede realizar en respuesta al usuario del conjunto de usuarios que solicitan la inclusión en un servicio de verificación.

Haciendo referencia a la figura 4B, en el bloque 416, se puede recibir una primera solicitud de moneda. La primera solicitud de moneda puede recibirse desde la aplicación de verificación del dispositivo de usuario. La primera solicitud de moneda puede incluir una identificación de un primer conjunto de monedas de los conjuntos de monedas, la clave pública única que se asigna al usuario, un primer conjunto de datos que está configurado para probar la participación del usuario en un primer evento que se correlaciona con el primer conjunto de monedas, alguna otra información, o alguna combinación de los mismos. Por ejemplo, en algunos modos de realización, un dispositivo de usuario como el primer dispositivo 115A de usuario puede comunicar la primera solicitud de moneda a un servidor como el servidor 106 CA. El servidor 106 CA puede recibir la primera solicitud de moneda.

En el bloque 418, el método puede incluir autenticar si el usuario tiene el control del dispositivo de usuario en el momento en que se transmite la primera solicitud de moneda. La autenticación se puede realizar en respuesta a la recepción de la primera solicitud de moneda. En algunos modos de realización, la autenticación puede incluir comunicar al dispositivo de usuario un reto configurado para verificar que el usuario tiene el control del dispositivo de usuario en respuesta a la recepción de la primera solicitud de moneda. De manera adicional o como alternativa, la autenticación puede incluir solicitar una entrada de autenticación biométrica para verificar que el usuario tiene el control del dispositivo de usuario.

En el bloque 420, se puede verificar la participación del usuario en el primer evento. La participación del usuario puede ser verificada basándose en el primer conjunto de datos. En algunos modos de realización, el primer conjunto de datos incluye una señal de GPS (sistema de posicionamiento global), un código de respuesta rápida (QR), datos de ubicación inalámbricos locales o alguna combinación de los mismos. Por ejemplo, el conjunto de eventos puede incluir que el usuario visite una o más de un conjunto de ubicaciones. El primer conjunto de datos puede ser coordenadas de GPS u otro de los primeros ejemplos de conjuntos de datos generados por el dispositivo de usuario cuando el usuario se encuentra en una o más del conjunto de ubicaciones. En el bloque 422, se puede verificar que el usuario no ha recibido aún una de las monedas de criptodivisa del primer conjunto de monedas identificado utilizando un libro mayor de solo escritura.

En el bloque 424, se puede ejecutar una transacción de criptodivisa con el dispositivo de usuario. La transacción de criptodivisa puede ejecutarse en respuesta a la verificación de la participación en el primer evento por parte del usuario. La transacción de criptodivisa puede incluir la validación pública de la transferencia de una moneda de criptodivisa desde el primer conjunto de monedas identificado al dispositivo de usuario a través del libro mayor de solo escritura. La ejecución de la transacción de criptodivisa puede involucrar la clave secreta maestra para el primer conjunto de monedas identificado y la clave pública única asignada.

En el bloque 426, se puede recibir una segunda solicitud de moneda desde la aplicación de verificación del dispositivo de usuario. La segunda solicitud de moneda puede incluir una identificación de un segundo conjunto de monedas de los conjuntos de monedas, la clave pública única que se asigna al usuario, y un segundo conjunto de datos configurado para probar la participación del usuario en un segundo evento que se correlaciona con el segundo conjunto de monedas. En el bloque 428, se puede verificar que el usuario participó en el segundo evento basándose en el segundo conjunto de datos.

Haciendo referencia a la figura 4C, en el bloque 430, se puede ejecutar una segunda transacción de criptodivisa con el dispositivo de usuario. La segunda transacción de criptodivisa puede ejecutarse en respuesta a la verificación de la participación en el segundo evento por parte del usuario. La segunda transacción de criptodivisa puede incluir la validación pública de la transferencia de una moneda de criptodivisa desde el segundo conjunto de monedas identificado al dispositivo de usuario a través del libro mayor de solo escritura.

En el bloque 432, la transacción de criptodivisa con el dispositivo de usuario puede registrarse en el libro mayor de solo escritura. En algunos modos de realización, el registro de la transacción de criptodivisa incluye el registro de la clave secreta maestra para el primer conjunto de monedas identificado y la clave pública única asignada al usuario como una cadena de firmas en el libro mayor de solo escritura. En el bloque 434, el dispositivo de usuario puede ser notificado de la transacción de criptodivisa. En el bloque 436, se puede recibir una solicitud de finalización desde el dispositivo de usuario. La solicitud de finalización puede configurarse para certificar que se le ha transferido al usuario una moneda de criptodivisa de cada uno de los conjuntos de monedas.

En el bloque 438, se puede verificar que se le ha transferido al usuario una de las monedas de criptodivisa de cada uno de los conjuntos de monedas utilizando el libro mayor de solo escritura en respuesta a las solicitudes de

finalización. En el bloque 440, se puede comunicar una recompensa al dispositivo de usuario del usuario en respuesta a la verificación de que se le ha transferido al usuario una de las monedas de criptodivisa de cada uno de los conjuntos de monedas.

En el bloque 442, al menos un conjunto de monedas de los conjuntos de monedas y la clave secreta maestra y las claves públicas maestras de al menos un conjunto de monedas pueden comunicarse a una entidad delegada. La entidad delegada puede recibir de la aplicación de verificación del dispositivo de usuario cualquier solicitud de moneda de criptodivisa para monedas de criptodivisa de al menos un conjunto de monedas y ejecuta transacciones de criptodivisa que impliquen la transferencia de monedas de criptodivisa de al menos un conjunto de monedas. La entidad delegada puede realizar uno o más de los bloques 408, 410, 412, 414, 416, 418, 420, 422, 424, 426, 428, 430, 432, 434, 436, 438, 440, o alguna combinación de los mismos.

Un experto en la técnica apreciará que, para este y otros procedimientos y métodos divulgados en el presente documento, las funciones realizadas en los procesos y métodos pueden implementarse en un orden diferente. Además, las etapas y operaciones descritas solo se proporcionan como ejemplos, y algunas de las etapas y operaciones pueden ser opcionales, combinadas en menos etapas y operaciones, o ampliadas en etapas y operaciones adicionales sin restar importancia a los modos de realización divulgados.

Los modos de realización descritos en el presente documento pueden incluir el uso de un ordenador de propósito especial o de propósito general que incluya varios módulos de software o hardware informático, como se expone con mayor detalle a continuación.

Los modos de realización descritos en el presente documento pueden implementarse usando medios legibles por ordenador para transportar o tener instrucciones o estructuras de datos ejecutables por ordenador almacenadas en los mismos. Dichos medios legibles por ordenador puede ser cualquier medio disponible al que se pueda acceder mediante un ordenador de propósito general o de propósito especial. A modo de ejemplo, y no de limitación, dichos medios legibles por ordenador pueden incluir medios de almacenamiento legibles por ordenador no transitorios o tangibles que incluyen RAM, ROM, EEPROM, CD-ROM u otro almacenamiento en disco óptico, almacenamiento en disco magnético u otros dispositivos de almacenamiento magnético, o cualquier otro medio de almacenamiento no transitorio que pueda usarse para transportar o almacenar el código de programa deseado en forma de instrucciones o estructuras de datos ejecutables por ordenador y al que se puede acceder mediante un ordenador de propósito general o de propósito especial. También pueden incluirse combinaciones de los anteriores dentro del alcance de los medios legibles por ordenador.

Las instrucciones ejecutables por ordenador comprenden, por ejemplo, instrucciones y datos que hacen que un ordenador de propósito general, ordenador de propósito especial o dispositivo de procesamiento de propósito especial realice una determinada función o grupo de funciones. Aunque la materia se ha descrito en un lenguaje específico para características estructurales y/o actos metodológicos, ha de entenderse que la materia definida en las reivindicaciones adjuntas no está necesariamente limitada a las características o actos específicos descritos anteriormente. Más bien, las características y los actos específicos descritos anteriormente se divulgan como formas de ejemplo de implementación de las reivindicaciones.

Como se utilizan en el presente documento, los términos "módulo", "componente" y/o "motor" pueden referirse a objetos o rutinas de software que se ejecutan en el sistema informático. Los diferentes componentes, módulos, motores y servicios descritos en el presente documento pueden implementarse como objetos o procesos que se ejecutan en el sistema informático (por ejemplo, como subprocesos separados). Si bien el sistema y los métodos descritos en el presente documento se implementan preferiblemente en software, también son posibles y contempladas implementaciones en hardware o una combinación de software y hardware. En esta descripción, una "entidad informática" puede ser cualquier sistema informático como se definió anteriormente en el presente documento, o cualquier módulo o combinación de módulos que se ejecuten en un sistema informático.

Todos los ejemplos y el lenguaje condicional citados en el presente documento están destinados para que los objetos pedagógicos ayuden al lector a comprender la invención y los conceptos aportados por el inventor para promover la técnica, y ha de interpretarse que no están limitados a dichos ejemplos y condiciones específicamente citados.

En cualquiera de los aspectos anteriores, las diversas características pueden implementarse en hardware, o como módulos de software que se ejecutan en uno o más procesadores. Las características de un aspecto pueden aplicarse a cualquiera de los otros aspectos.

La invención también proporciona un programa informático o un producto de programa informático para llevar a cabo cualquiera de los métodos descritos en el presente documento, y un medio legible por ordenador que tiene almacenado en el mismo un programa para llevar a cabo cualquiera de los métodos descritos en el presente documento. Un programa de ordenador que realice la invención puede almacenarse en un medio legible por ordenador, o podría, por ejemplo, estar en la forma de una señal como una señal de datos descargable provista desde un sitio web de Internet, o podría estar en cualquier otra forma.

REIVINDICACIONES

1. Un método de verificación segura de participación en un evento, el método que comprende:

generar, por un servidor de autoridad central, un primer número de conjuntos de monedas de criptodivisa (conjuntos de monedas), teniendo cada uno de los conjuntos de monedas un segundo número de monedas de criptodivisa y estando cada uno de los conjuntos de monedas correlacionado con un evento en un conjunto de eventos;

generar, mediante el servidor de autoridad central, una clave secreta maestra y una clave pública maestra para cada uno de los conjuntos de monedas;

en respuesta a un usuario de un conjunto de usuarios que incluye un segundo número de usuarios que solicitan su inclusión en un servicio de verificación:

generar, por el servidor de autoridad central, un par de claves de usuario que incluyan una clave pública única para el usuario y una clave secreta de usuario;

asignar, por el servidor de autoridad central, la clave pública única al usuario y a un dispositivo de usuario que está asociado al usuario;

comunicar, por el servidor de autoridad central, la clave pública única asignada al dispositivo de usuario;

prevenir, por el servidor de autoridad central, el acceso a la clave secreta de usuario emparejada con la clave pública única asignada; y

permitir, por el servidor de autoridad central, la descarga de una aplicación de verificación al dispositivo de usuario;

recibir, por el servidor de autoridad central y la aplicación de verificación del dispositivo de usuario, una primera solicitud de moneda, la primera solicitud de moneda que incluye una identificación de un primer conjunto de monedas de los conjuntos de monedas, la clave pública única que se asigna al usuario, y un primer conjunto de datos que está configurado para probar la participación del usuario en un primer evento que se correlaciona con el primer conjunto de monedas;

verificar, por el servidor de autoridad central, que el usuario participó en el primer evento basándose en el primer conjunto de datos;

en respuesta a la verificación de la participación en el primer evento por parte del usuario, ejecutar, por el servidor de autoridad central, una transacción de criptodivisa con el dispositivo de usuario, la ejecución de la transacción de criptodivisa que incluye una transferencia, por el servidor de autoridad central, de una moneda de criptodivisa desde el primer conjunto de monedas identificado al dispositivo de usuario y la validación pública de la transferencia de la moneda de criptodivisa del primer conjunto de monedas identificado al dispositivo de usuario a través de un libro mayor de solo escritura utilizando una función resumen de un número de monedas del primer conjunto de monedas identificado para transferir al usuario y la clave pública única de usuario, estando la función resumen firmada usando la clave secreta maestra del primer conjunto de monedas identificado; y

registrar la transacción de criptodivisa con el dispositivo de usuario en el libro mayor de solo escritura, en donde el registro de la transacción de criptodivisa incluye registrar la clave secreta maestra del primer conjunto de monedas identificado y la clave pública única asignada al usuario como una cadena de firmas en el libro mayor de solo escritura.

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

recibir de la aplicación de verificación del dispositivo de usuario, una segunda solicitud de moneda, incluyendo la segunda solicitud de moneda una identificación de un segundo conjunto de monedas de los conjuntos de monedas, la clave pública única que se asigna al usuario, y un segundo conjunto de datos configurado para probar la participación del usuario en un segundo evento que se correlaciona con el segundo conjunto de monedas;

verificar que el usuario participó en el segundo evento basándose en el segundo conjunto de datos; y

en respuesta a la verificación de la participación en el segundo evento por parte del usuario, ejecutar una segunda transacción de criptodivisa con el dispositivo de usuario, la segunda transacción de criptodivisa que incluye la validación pública de la transferencia de una moneda de criptodivisa del segundo conjunto de monedas identificado al dispositivo de usuario a través del libro mayor de solo escritura.

3. El método de la reivindicación 1 o 2, que comprende además:

recibir desde el dispositivo de usuario una solicitud de finalización, la solicitud de finalización configurada para certificar que se le ha transferido al usuario una moneda de criptodivisa de cada uno de los conjuntos de monedas;

en respuesta a la solicitud de finalización verificar que se le ha transferido al usuario una de las monedas de criptodivisa de cada uno de los conjuntos de monedas utilizando el libro mayor de solo escritura; y

en respuesta a la verificación de que se le ha transferido al usuario una de las monedas de criptodivisa de cada uno de los conjuntos de monedas, comunicar una recompensa al dispositivo de usuario del usuario.

4. El método de acuerdo con cualquiera de las reivindicaciones anteriores, que comprende además verificar que el usuario no ha recibido aún una de las monedas de criptodivisa del primer conjunto de monedas identificado utilizando el libro mayor de solo escritura.

5. El método de acuerdo con cualquiera de las reivindicaciones anteriores, que además comprende notificar al dispositivo de usuario de la transacción de criptodivisa.

6. El método de acuerdo con cualquiera de las reivindicaciones anteriores, que comprende además:

en respuesta a la recepción de la primera solicitud de moneda:

comunicar al dispositivo de usuario un reto configurado para verificar que el usuario tiene el control del dispositivo de usuario; o

solicitar una entrada de autenticación biométrica para verificar que el usuario tiene el control del dispositivo de usuario.

7. El método de acuerdo con cualquiera de las reivindicaciones anteriores, en donde las monedas de criptodivisa no tienen valor monetario.

8. El método de acuerdo con cualquiera de las reivindicaciones anteriores, en donde:

el conjunto de eventos incluye visitar un conjunto o serie de ubicaciones, y

el primer conjunto de datos incluye uno o más o una combinación de una señal de GPS (sistema de posicionamiento global), un código de respuesta rápida (QR) y datos de ubicación inalámbricos locales.

9. El método de acuerdo con cualquiera de las reivindicaciones anteriores, que además comprende comunicar a una entidad delegada al menos un conjunto de monedas de los conjuntos de monedas y una clave secreta maestra y una clave pública maestra de al menos un conjunto de monedas, en donde la entidad delegada recibe de la aplicación de verificación del dispositivo de usuario cualquier solicitud de monedas de criptodivisa para monedas de criptodivisa de al menos un conjunto de monedas y ejecuta transacciones de criptodivisa que involucran la transferencia de monedas de criptodivisa de al menos un conjunto de monedas.

10. Un medio legible por ordenador no transitorio que tiene codificado el código de programación ejecutable por uno o más procesadores para realizar o controlar la realización de las operaciones que comprenden el método de acuerdo con cualquiera de las reivindicaciones 1 a 9.

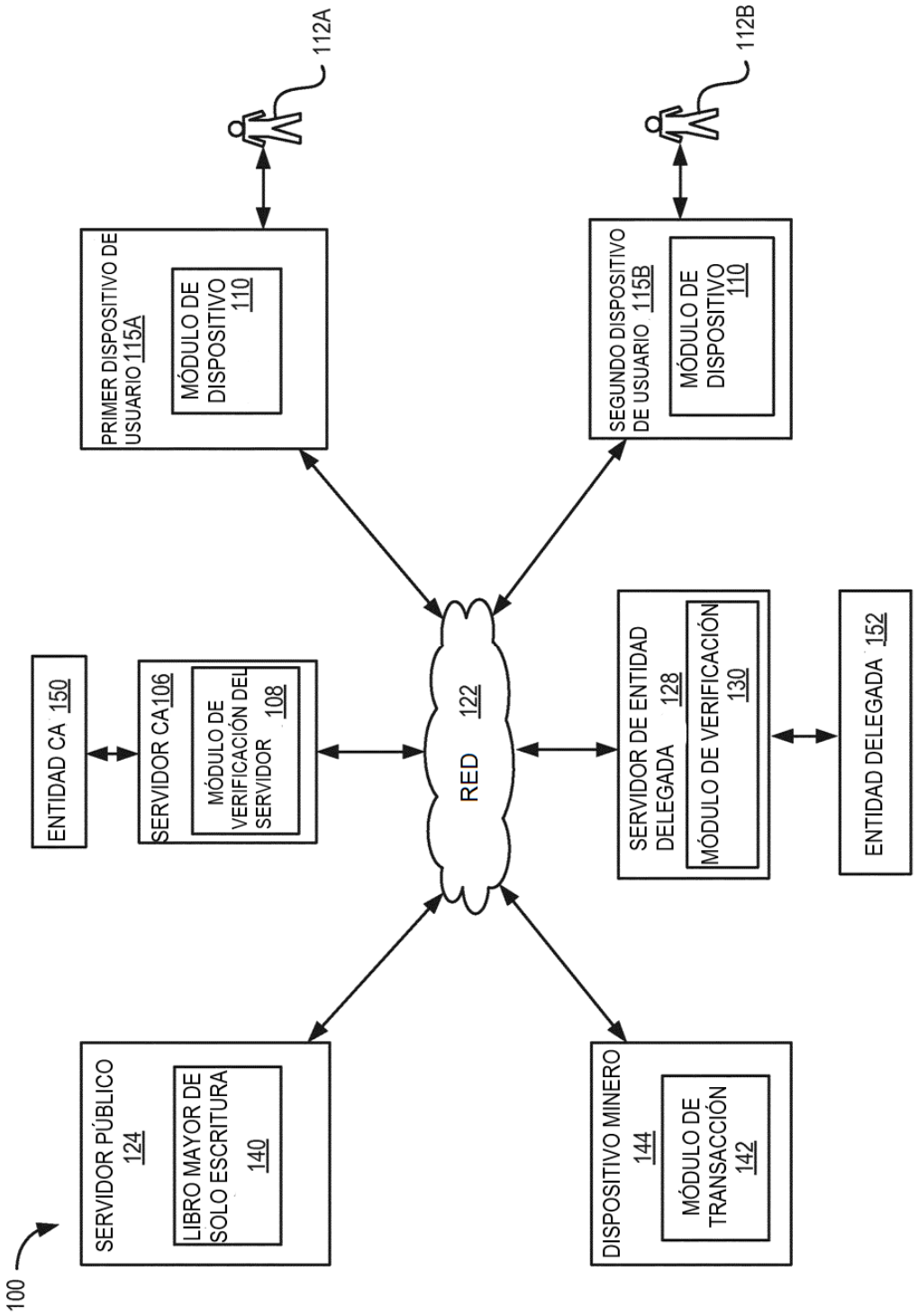
100
SERVIDOR PÚBLICO 124
LIBRO MAYOR DE SOLO ESCRITURA 140
PRIMER DISPOSITIVO DE USUARIO 115A
MÓDULO DE DISPOSITIVO 110
112A
SEGUNDO DISPOSITIVO DE USUARIO 115B
MÓDULO DE DISPOSITIVO 110
112B
ENTIDAD CA 150
SERVIDOR CA 106
MÓDULO DE VERIFICACIÓN DEL SERVIDOR 108
RED 122
SERVIDOR DE ENTIDAD DELEGADA 128
MÓDULO DE VERIFICACIÓN 130
ENTIDAD DELEGADA 152
DISPOSITIVO MINERO 144
MÓDULO DE TRANSACCIÓN 142

FIG. 1

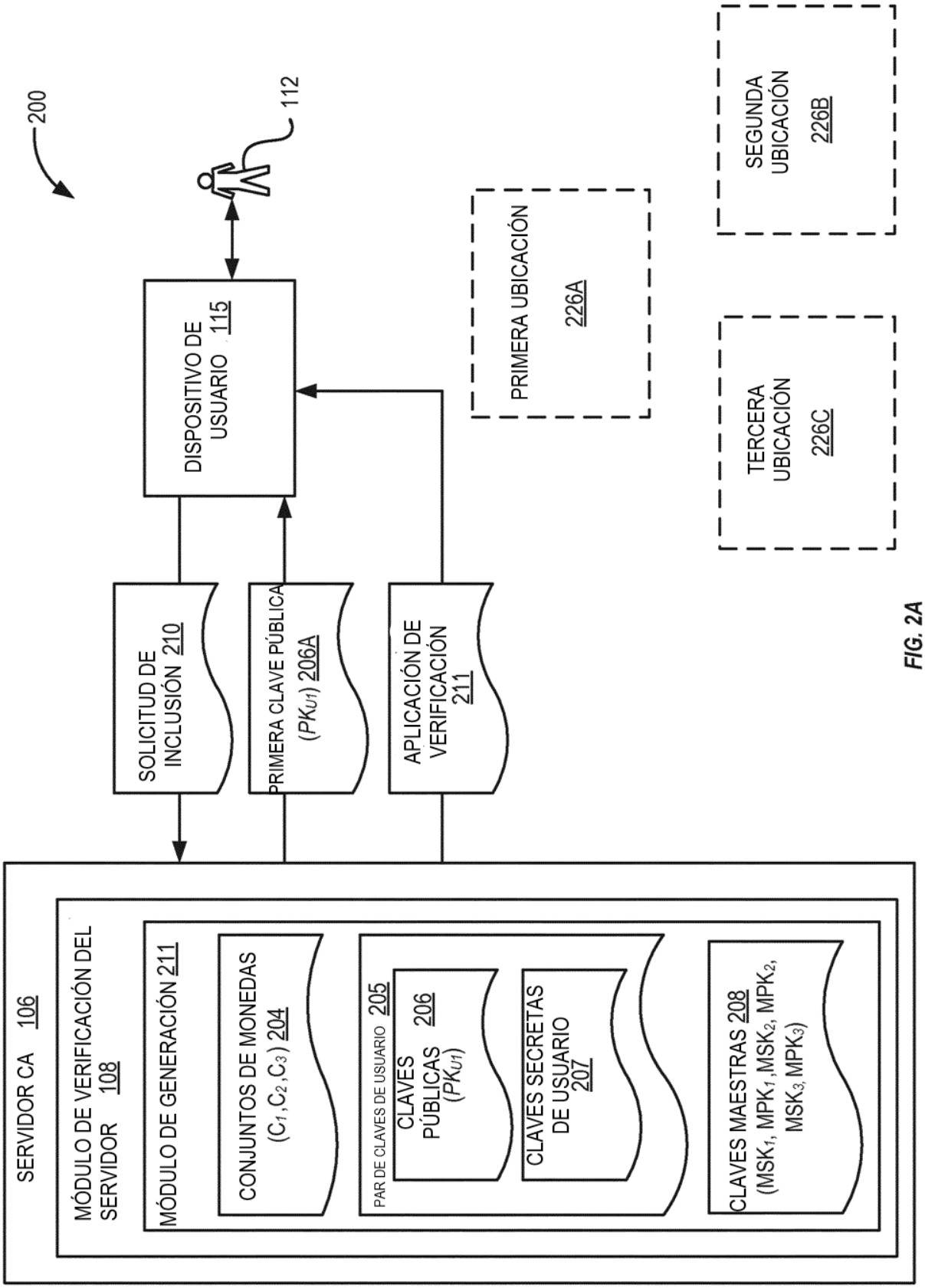
200
112
DISPOSITIVO DE USUARIO 115
SOLICITUD DE INCLUSIÓN 210
PRIMERA CLAVE PÚBLICA (PK_{U1}) 206A
APLICACIÓN DE VERIFICACIÓN 211
PRIMERA UBICACIÓN 226A
SEGUNDA UBICACIÓN 226B
TERCERA UBICACIÓN 226C
SERVIDOR CA 106
MÓDULO DE VERIFICACIÓN DEL SERVIDOR 108
MÓDULO DE GENERACIÓN 211
CONJUNTOS DE MONEDAS (C_1, C_2, C_3) 204
PAR DE CLAVES DE USUARIO 205
CLAVES PÚBLICAS 206 (PK_{U1})
CLAVES SECRETAS DE USUARIO 207
CLAVES MAESTRAS 208 (MSK_1, MPK_1, MSK_2, MPK_2, MSK_3, MPK_3)

FIG. 2A

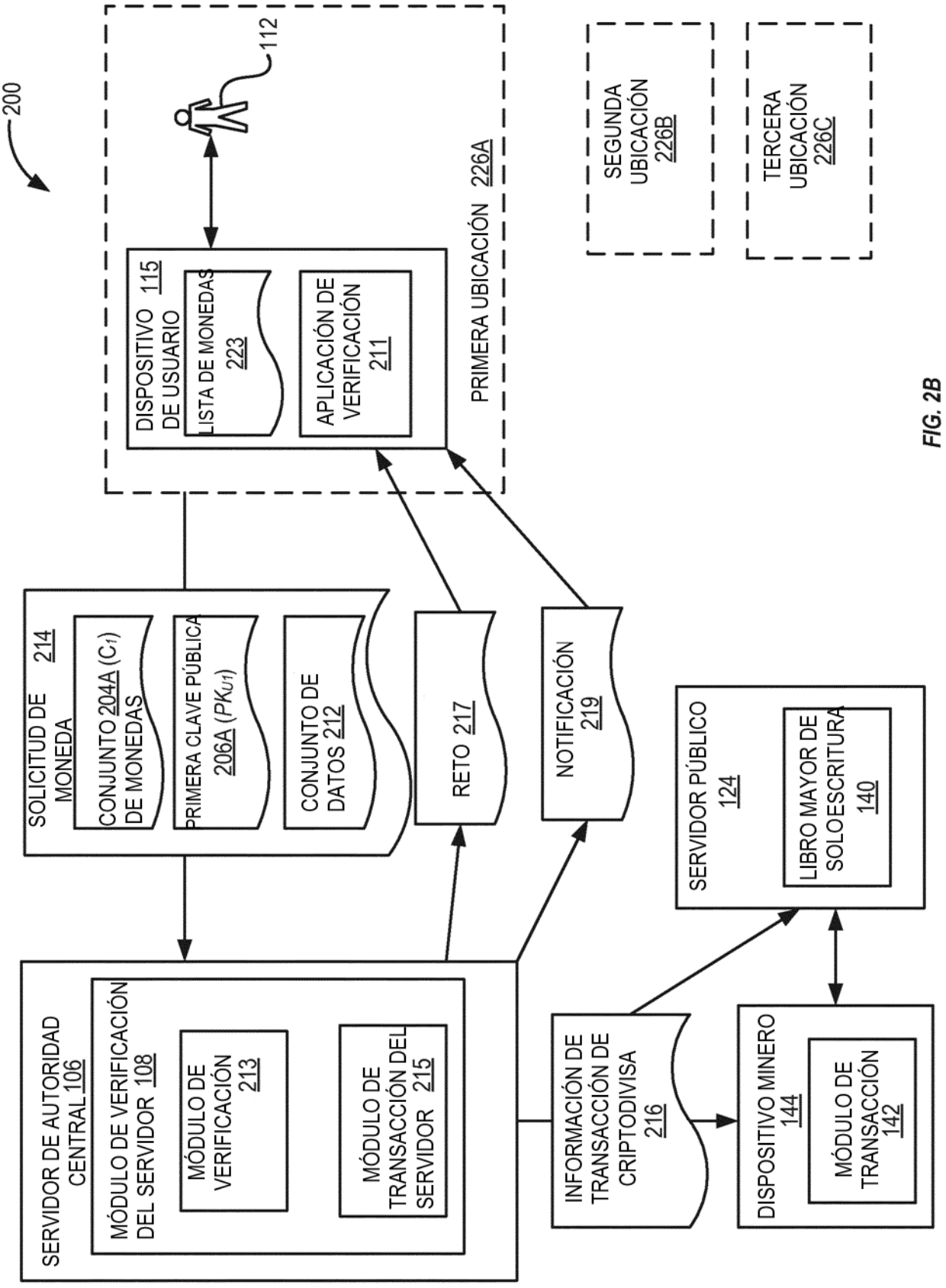
200
112
PRIMERA UBICACIÓN 226A
DISPOSITIVO DE USUARIO 115
LISTA DE MONEDAS 223
APLICACIÓN DE VERIFICACIÓN 211
SEGUNDA UBICACIÓN 226B
TERCERA UBICACIÓN 226C
SOLICITUD DE MONEDA 214
CONJUNTO DE MONEDAS 204A (C_1)
PRIMERA CLAVE PÚBLICA 206A (PK_{U1})
CONJUNTO DE DATOS 212
RETO 217
NOTIFICACIÓN 219
SERVIDOR PÚBLICO 124
LIBRO MAYOR DE SOLOESCRITURA 140
SERVIDOR DE AUTORIDAD CENTRAL 106
MÓDULO DE VERIFICACIÓN DEL SERVIDOR 108
MÓDULO DE VERIFICACIÓN 213
MÓDULO DE TRANSACCIÓN DEL SERVIDOR 215
INFORMACIÓN DE TRANSACCIÓN DE CRIPTODIVISA 216
DISPOSITIVO MINERO 144
MÓDULO DE TRANSACCIÓN 142

FIG. 2B

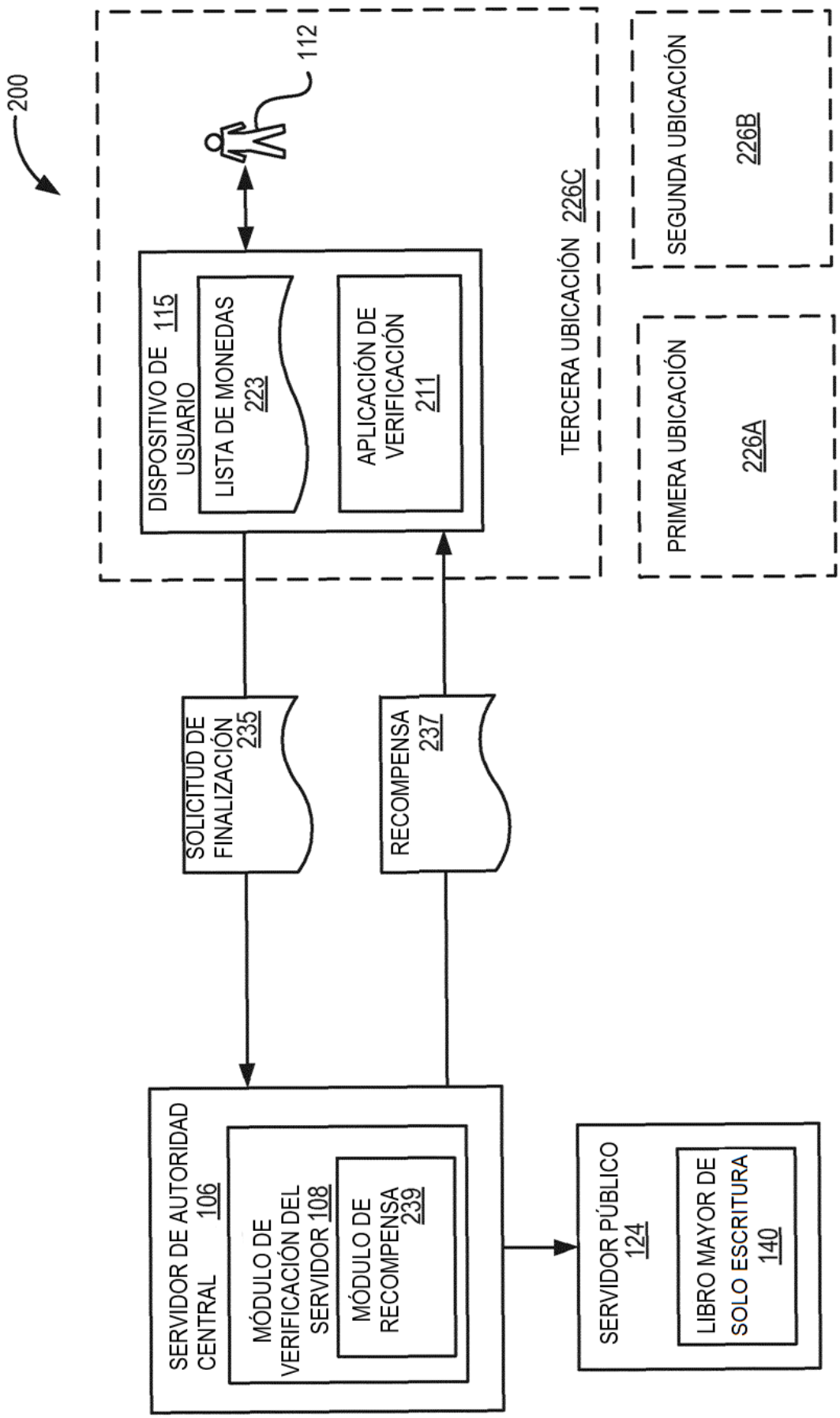
200
112
DISPOSITIVO DE USUARIO 115
LISTA DE MONEDAS 223
APLICACIÓN DE VERIFICACIÓN 211
TERCERA UBICACIÓN 226C
SEGUNDA UBICACIÓN 226B
PRIMERA UBICACIÓN 226A
SOLICITUD DE FINALIZACIÓN 235
RECOMPENSA 237
SERVIDOR DE AUTORIDAD CENTRAL 106
MÓDULO DE VERIFICACIÓN DEL SERVIDOR 108
MÓDULO DE RECOMPENSA 239
SERVIDOR PÚBLICO 124
LIBRO MAYOR DE SOLO ESCRITURA 140

FIG. 2C

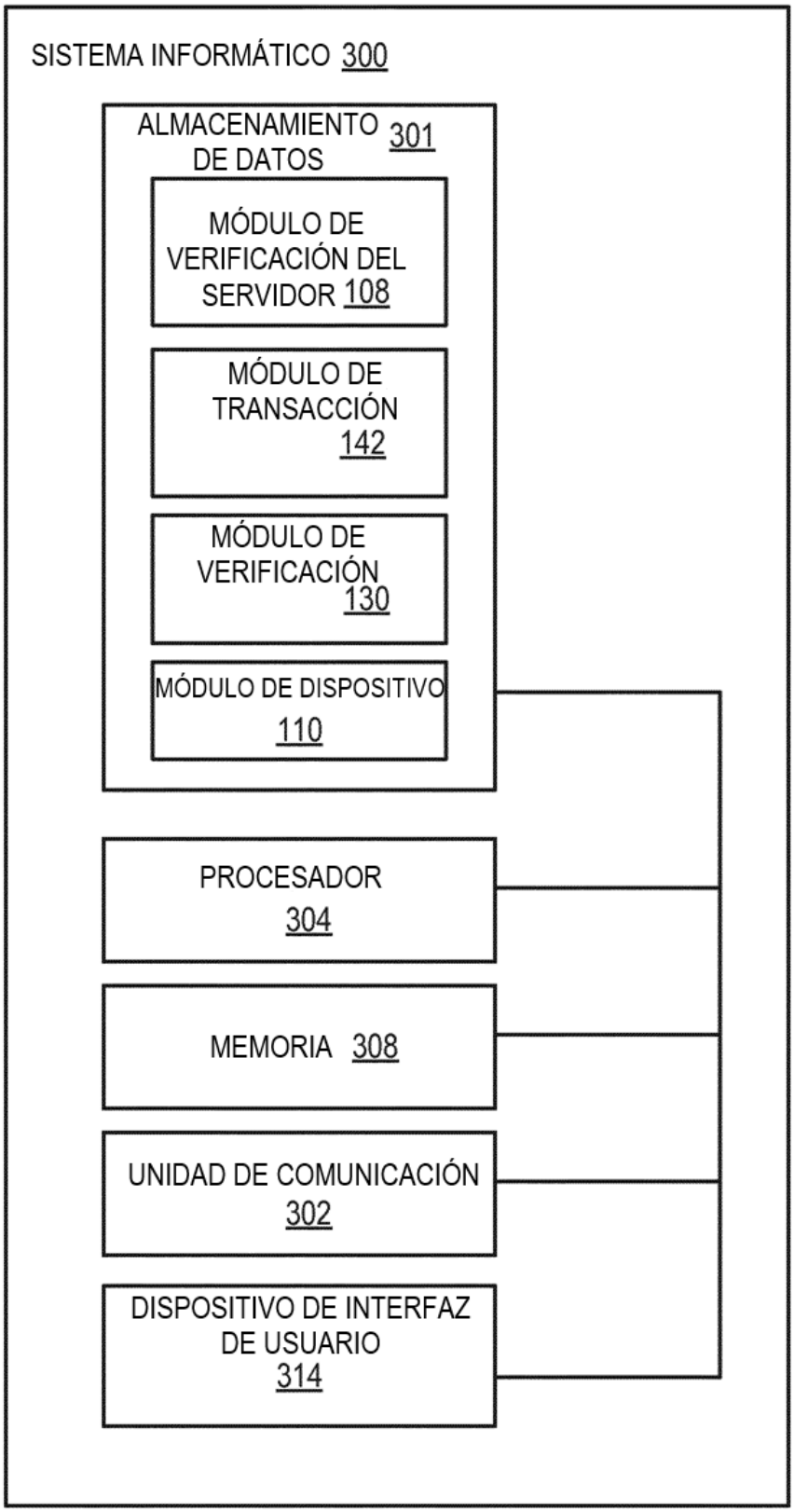
SISTEMA INFORMÁTICO 300
ALMACENAMIENTO DE DATOS 301
MÓDULO DE VERIFICACIÓN DEL SERVIDOR 108
MÓDULO DE TRANSACCIÓN 142
MÓDULO DE VERIFICACIÓN 130
MÓDULO DE DISPOSITIVO 110
PROCESADOR 304
MEMORIA 308
UNIDAD DE COMUNICACIÓN 302
DISPOSITIVO DE INTERFAZ DE USUARIO 314

FIG. 3

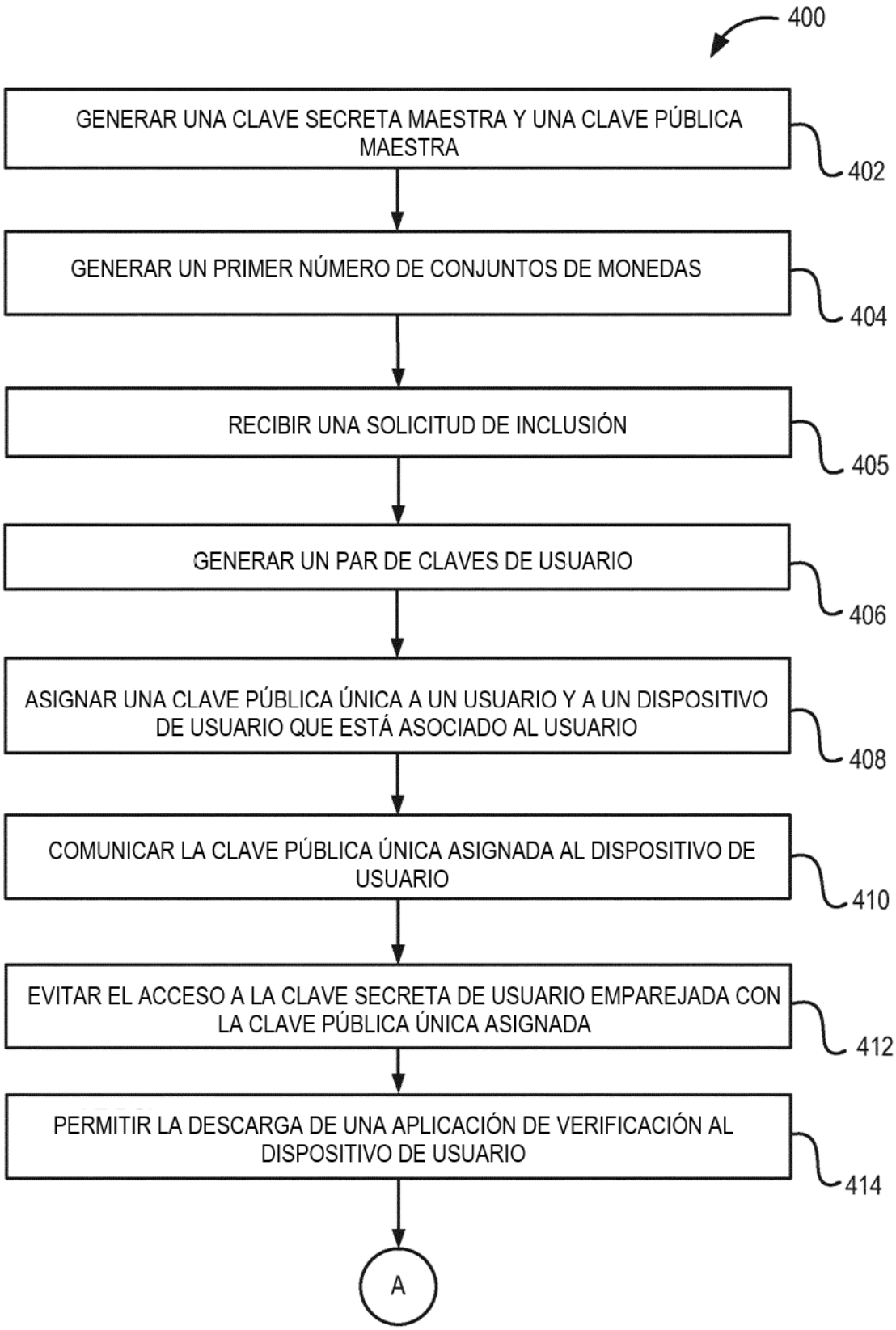
400
GENERAR UNA CLAVE SECRETA MAESTRA Y UNA CLAVE PÚBLICA MAESTRA
402
GENERAR UN PRIMER NÚMERO DE CONJUNTOS DE MONEDAS
404
RECIBIR UNA SOLICITUD DE INCLUSIÓN
405
GENERAR UN PAR DE CLAVES DE USUARIO
406
ASIGNAR UNA CLAVE PÚBLICA ÚNICA A UN USUARIO Y A UN DISPOSITIVO DE USUARIO QUE ESTÁ ASOCIADO AL USUARIO
408
COMUNICAR LA CLAVE PÚBLICA ÚNICA ASIGNADA AL DISPOSITIVO DE USUARIO
410
EVITAR EL ACCESO A LA CLAVE SECRETA DE USUARIO EMPAREJADA CON LA CLAVE PÚBLICA ÚNICA ASIGNADA
412
PERMITIR LA DESCARGA DE UNA APLICACIÓN DE VERIFICACIÓN AL DISPOSITIVO DE USUARIO
414
A

FIG. 4A

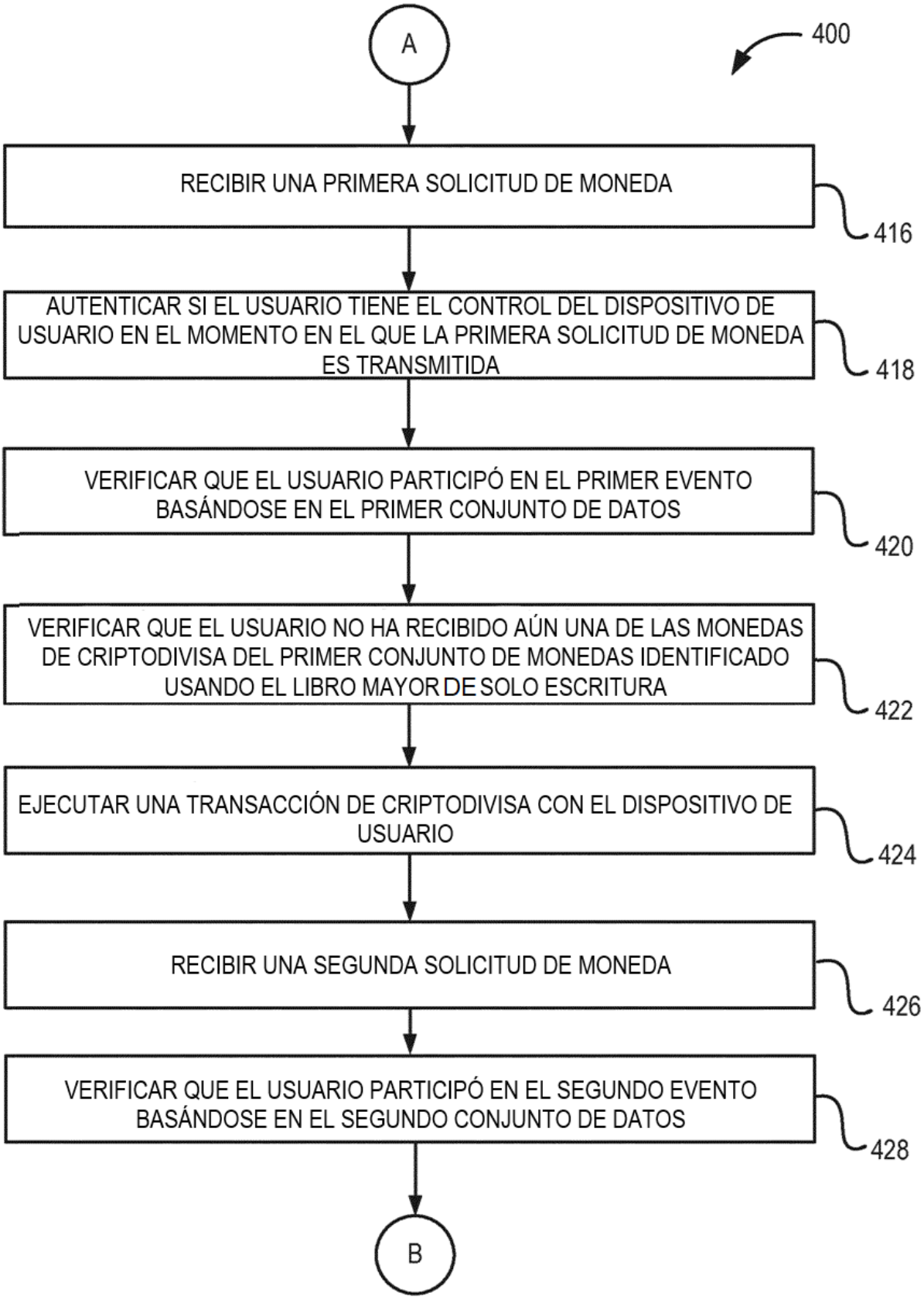
A
400
RECIBIR UNA PRIMERA SOLICITUD DE MONEDA
416
AUTENTICAR SI EL USUARIO TIENE EL CONTROL DEL DISPOSITIVO DE USUARIO EN EL MOMENTO EN EL QUE LA PRIMERA SOLICITUD DE MONEDA ES TRANSMITIDA
418
VERIFICAR QUE EL USUARIO PARTICIPÓ EN EL PRIMER EVENTO BASÁNDOSE EN EL PRIMER CONJUNTO DE DATOS
420
VERIFICAR QUE EL USUARIO NO HA RECIBIDO AÚN UNA DE LAS MONEDAS DE CRIPTODIVISA DEL PRIMER CONJUNTO DE MONEDAS IDENTIFICADO USANDO EL LIBRO MAYOR DE SOLO ESCRITURA
422
EJECUTAR UNA TRANSACCIÓN DE CRIPTODIVISA CON EL DISPOSITIVO DE USUARIO
424
RECIBIR UNA SEGUNDA SOLICITUD DE MONEDA
426
VERIFICAR QUE EL USUARIO PARTICIPÓ EN EL SEGUNDO EVENTO BASÁNDOSE EN EL SEGUNDO CONJUNTO DE DATOS
428
B

FIG. 4B

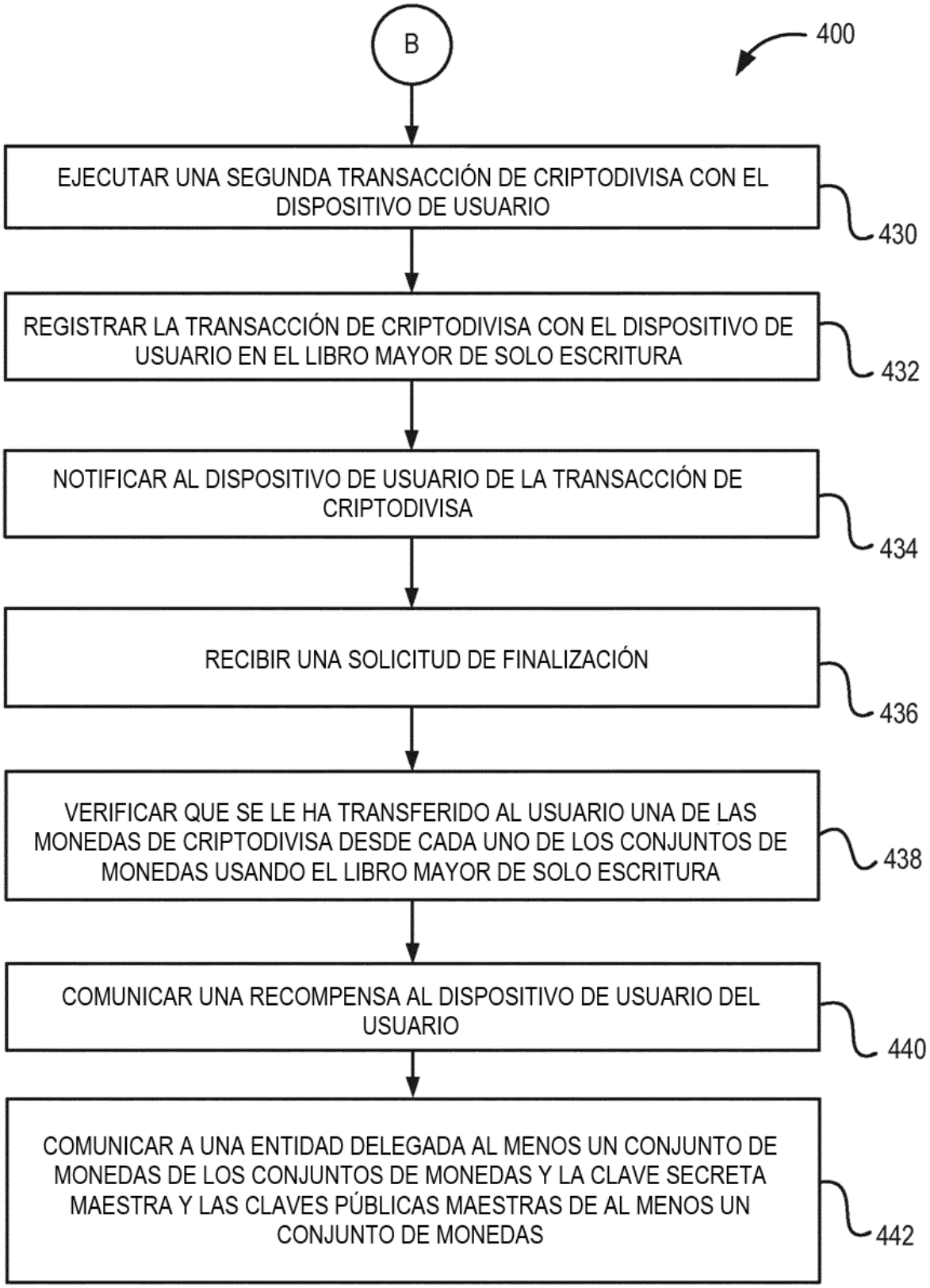
B
400
EJECUTAR UNA SEGUNDA TRANSACCIÓN DE CRIPTODIVISA CON EL DISPOSITIVO DE USUARIO
430
REGISTRAR LA TRANSACCIÓN DE CRIPTODIVISA CON EL DISPOSITIVO DE USUARIO EN EL LIBRO MAYOR DE SOLO ESCRITURA
432
NOTIFICAR AL DISPOSITIVO DE USUARIO DE LA TRANSACCIÓN DE CRIPTODIVISA
434
RECIBIR UNA SOLICITUD DE FINALIZACIÓN
436
VERIFICAR QUE SE LE HA TRANSFERIDO AL USUARIO UNA DE LAS MONEDAS DE CRIPTODIVISA DESDE CADA UNO DE LOS CONJUNTOS DE MONEDAS USANDO EL LIBRO MAYOR DE SOLO ESCRITURA
438
COMUNICAR UNA RECOMPENSA AL DISPOSITIVO DE USUARIO DEL USUARIO
440
COMUNICAR A UNA ENTIDAD DELEGADA AL MENOS UN CONJUNTO DE MONEDAS DE LOS CONJUNTOS DE MONEDAS Y LA CLAVE SECRETA MAESTRA Y LAS CLAVES PÚBLICAS MAESTRAS DE AL MENOS UN CONJUNTO DE MONEDAS
442

FIG. 4C