(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 774 397**

(21) Número de solicitud: 201930030

(51) Int. CI.:

H04L 9/32 (2006.01)
G06F 16/00 (2009.01)

(12) SOLICITUD DE PATENTE A1

(22) Fecha de presentación:

18.01.2019

(43) Fecha de publicación de la solicitud:

20.07.2020

(71) Solicitantes:

TELEFONICA DIGITAL ESPAÑA, S.L.U. (100.0%)
Gran Vía, 28
28013 Madrid ES

(72) Inventor/es:

DE LA ROCHA GÓMEZ-AREVALILLO, Alfonso y
NUÑEZ DÍAZ, José Luis

(74) Agente/Representante:

ARIZTI ACHA, Monica

(54) Título: **MÉTODO Y SISTEMA PARA RECUPERACIÓN DE CLAVES CRIPTOGRÁFICAS DE UNA RED DE CADENA DE BLOQUES**

(57) Resumen:

Método y sistema para recuperación de claves criptográficas de una red de cadena de bloques. Un dispositivo de computación o un elemento asociado al mismo tiene almacenadas un par de claves criptográficas representativas de la identidad del usuario en una red de cadena de bloques incluyendo una clave pública y una clave privada. Un gestor de identidades mantiene un registro del usuario en un directorio distribuido. Al recibir una solicitud del usuario debido a la pérdida/robo de su clave privada, se elimina del registro la información de la clave pública del usuario y se revoca al usuario como propietario de un contrato inteligente; se genera un nuevo par de claves, almacenándose en el dispositivo o en dicho elemento: y se identifica y autentifica al usuario. Una vez autenticado correctamente, el gestor recibe la nueva clave pública del usuario, actualiza el registro y actualiza la propiedad del contrato inteligente.

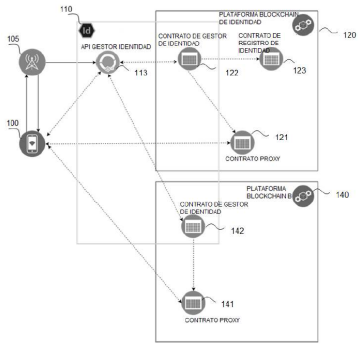

Fig. 1

ES 2 774 397 A1

DESCRIPCIÓN

MÉTODO Y SISTEMA PARA RECUPERACIÓN DE CLAVES CRIPTOGRÁFICAS DE UNA RED DE CADENA DE BLOQUES

Campo de la técnica

La presente invención concierne en general a tecnologías de contratos inteligentes (*Smart Contracts*) y seguridad. En particular, la invención concierne a un método y un sistema para recuperación de claves criptográficas de una red de cadena de bloques (*Blockchain*). La invención implementa un mecanismo de recuperación de las claves criptográficas que representan la identidad de un usuario en la red de cadena de bloques a través de la infraestructura de red, una serie de contratos inteligentes y un dispositivo de computación operado por el usuario sin comprometer la seguridad relacionada con el posible robo o uso indebido de las mismas por terceros.

Antecedentes de la invención

Uno de los principales problemas en la gestión de identidades en las plataformas de cadena de bloques actuales es que, si un usuario pierde el control sobre las claves criptográficas, perderá el control sobre su identidad y todos los activos asociados a la misma (criptomonedas y tokens criptográficos), sin que exista una manera confiable de recuperarlas sin delegar el control de sus claves a terceros de confianza.

Otro problema que presentan las identidades en las redes de cadena de bloques es que no existe una correspondencia entre la identidad del usuario en la red y su identidad física, esto favorece a la privacidad de los usuarios en la red ya que a partir de su identidad (clave pública) no se puede inferir su identidad real, pero complica la implementación de mecanismos simples de gestión y recuperación de claves, porque estas son intransferibles y solo conocidas por el usuario en cuestión.

Para poder acceder a una plataforma de cadena de bloques, un usuario debe disponer de un par de claves criptográficas asimétricas que representen su identidad de acceso a la red. La clave pública representa unívocamente al usuario en la plataforma, y todas las acciones y transacciones que el usuario realice sobre la red estarán firmadas utilizando su clave privada, de manera que cualquier participante de la red pueda identificar el origen de la

acción. Estas claves se generan a partir de una semilla conocida por el usuario, y se almacenan, generalmente, en los dispositivos personales de los usuarios. Es más, el usuario es el responsable único de sus claves y debe encargarse de mantenerlas a buen recaudo incluso aunque no disponga de conocimientos técnicos. Si un usuario pierde el acceso a su semilla o a sus claves pierde de manera irreversible el control sobre su identidad. En caso de que esa identidad tuviese asociados fondos de algún tipo (criptomonedas u otro tipo de activos criptográficos) o derechos de acceso a algún servicio, el usuario no podrá volver a movilizar esos fondos o acceder a los servicios.

Actualmente todos los modelos de recuperación de claves blockchain de un usuario requieren delegar la recuperación a un tercero de confianza, o confiar en un modelo de identidad digital soberana sobre una plataforma de cadena de bloques basada en Contratos Inteligentes específica:

- Los modelos de identidad digital soberana basados en tecnología de cadena de bloques permiten a un usuario delegar el proceso de recuperación (gestionado a través de un contrato inteligente), a custodios de confianza. De manera que una modificación de las claves del usuario exija ser aceptado por un número mínimo de custodios de confianza.
- Otra posible alternativa de recuperación consistiría en delegar el almacenamiento de la semilla de las claves a terceros de confianza, como una plataforma online, una gran compañía, o a un grupo de custodios a los que se distribuye una parte de la semilla a cada uno.

No obstante, la gestión de las claves de identidad en las plataformas de cadena de bloques actuales es muy ineficiente. Las claves se generan a partir de una semilla aleatoria (secuencia alfanumérica aleatoria), y los usuarios deben generarla, gestionarla y almacenarla ellos mismos. Para hacer esto pueden utilizar una *wallet* software (i.e. billeteras que se instalan a través de un software en dispositivos de computación) que almacena y gestiona el par de claves, o utilizar hardware especializado que debe introducirse en un dispositivo cada vez que se quiera firmar una transacción.

Las wallets software generan y almacenan las claves directamente en el dispositivo en el que se encuentra instalado el software. Esto favorece a la experiencia de usuario, ya que, al almacenar las claves en el dispositivo, cada vez que se dispara una transacción en la red de cadena de bloques se puede firmar de manera directa desde el dispositivo. Esta solución

plantea problemas de seguridad: el hecho de almacenar las claves directamente sobre un dispositivo conectado a Internet lo hace vulnerable a ciberataques, un hacker que obtuviese el control del dispositivo podría obtener fácilmente acceso a las claves y tomar el control de la identidad en la red.

Por otro lado, las wallets hardware consisten en dispositivos hardware de propósito específico (con un aspecto similar al de una memoria flash USB) que almacena las claves de los usuarios. La seguridad de estos dispositivos es mayor que la de las wallet software debido a que se encuentran cifradas en un dispositivo offline, el inconveniente de este tipo de soluciones es la experiencia de usuario. Cada vez que se quiera hacer una transacción con la identidad a través de un dispositivo, debe conectarse la wallet hardware, descifrar las claves y firmar la transacción en la wallet para enviar las transacciones firmadas al dispositivo y lanzarlas en la red.

Este tipo de soluciones de gestión de claves en redes de cadena de bloques plantean un problema todavía no resuelto en el ecosistema, si el usuario pierde el control de sus claves (ya sea porque pierde su wallet hardware, o el dispositivo en el que tiene instalada la wallet software y almacenadas las claves) perderá completamente el control sobre su identidad, con todo lo que ello conlleva. Los principales problemas de los mecanismos de recuperación de claves que existen ahora mismo son los siguientes:

- Para evitar la pérdida de sus claves, un usuario puede optar por almacenar la secuencia alfanumérica de generación de sus claves (la semilla) en un dispositivo offline seguro (ya sea guardándola en un fichero de texto plano almacenado en un disco duro offline, o escribiéndola directamente en un trozo de papel), o seguir un planteamiento similar guardando directamente su clave pública y clave privada para poder regenerarlas en caso de pérdida. Esto supone una gran incomodidad, y no es un método fiable, ya que pueden cometerse errores en la transcripción de las claves, o el almacenamiento offline puede perderse, perdiéndose una vez más de manera irreversible la identidad.
- Los modelos de identidad digital soberana basados en tecnología de cadena de bloques introducen algunos mecanismos de recuperación de claves, pero estos procedimientos deben realizarse *onchain* (es decir, todas las acciones para la recuperación de las identidades deben realizarse sobre la plataforma de cadena de bloques a través del disparo de transacciones sobre la red y el uso de Contratos Inteligentes, sin que su identidad real entre en juego), y requieren que los custodios

de la identidad dispongan de una serie de claves válidas (con el riesgo de pérdida de claves que estos usuarios también tienen) de forma que, si más de un número mínimo de custodios perdiesen sus identidades, las claves serían irrecuperables.

- El problema de la delegación de claves a terceros es el exceso de confianza que hay que depositar sobre ellos. Delegar la semilla o la clave privada de un usuario implica que se puede suplantar su identidad de manera directa. Esto además atenta contra el paradigma de descentralización de la tecnología blockchain. Las redes de cadena de bloques se pensaron como una infraestructura descentralizada con confianza distribuida en la que se eliminan los intermediarios y terceros de confianza. La delegación de claves a una entidad de confianza supondría romper con el paradigma introducido por la tecnología.

Adicionalmente, no existe una forma sencilla de hacer una correspondencia entre la identidad digital única del usuario y su identidad física sin el uso de terceros de confianza o aplicaciones adicionales.

Exposición de la invención

La presente invención proporciona de acuerdo a un primer aspecto, un método para recuperación de claves criptográficas de una red de cadena de bloques (o *blockchain* tal como se conoce en inglés), en donde un dispositivo de computación de un usuario, por ejemplo un teléfono móvil o una tableta, entre otros, o un elemento asociado al dispositivo de computación, tiene almacenadas un par de claves criptográficas asimétricas representativas de la identidad de dicho usuario en al menos la citada red de cadena de bloques, incluyendo dicho par de claves una clave pública y una clave privada. Asimismo, un gestor de identidades, operativamente conectado a la red de cadena de bloques mantiene un registro del usuario en un directorio distribuido de identidades. El citado registro incluye información de la clave pública del usuario y de un contrato inteligente del usuario en la red de cadena de bloques.

Particularmente, el método comprende eliminar, por el gestor de identidades, del citado registro, la información de la clave pública del usuario y revocar al usuario como propietario del contrato inteligente al recibir una solicitud del usuario debido a la perdida o robo de su clave privada; generar, por el dispositivo de computación o en el elemento asociado al dispositivo de computación, un nuevo par de claves criptográficas asimétricas representativas de la identidad del usuario en la red de cadena de bloques, en donde dicho

nuevo par de claves comprende una nueva clave pública y una nueva clave privada; almacenar el nuevo par de claves generadas en el dispositivo de computación o en el elemento asociado al dispositivo de computación; identificar y autentificar al usuario, por el gestor de identidades, mediante un mecanismo de autentificación proporcionado por una entidad garante de la identidad; y una vez que el usuario ha sido autentificado correctamente, recibir, por el gestor de identidades, del dispositivo de computación, la nueva clave pública del usuario, y actualizar el registro del usuario en el directorio distribuido de identidades con la nueva clave pública recibida y actualizar a la nueva clave pública la propiedad del contrato inteligente.

En un ejemplo de realización, el elemento asociado al dispositivo de computación es una tarjeta SIM, siendo la entidad garante de la identidad del usuario el operador de telecomunicaciones emisor de la tarjeta SIM. Alternativamente, el elemento asociado al dispositivo de computación puede ser un documento de identificación electrónico del usuario, por ejemplo, el DNI. En este último caso, la entidad garante de la identidad del usuario sería el Estado emisor del DNI.

Particularmente, el citado registro se realiza mediante una secuencia de identificación que incluye: un identificador del usuario, un identificador del contrato inteligente de la cadena de bloques y la clave pública. En casos en los que la clave pública del usuario no coincida con la dirección del identificador del usuario en la red de cadena de bloques, la citada secuencia de identificación podría también incluir la citada dirección.

En un ejemplo de realización, el mecanismo de autentificación comprende el envío de un código de un solo uso mediante un mensaje de texto al dispositivo de computación. El mecanismo de autentificación puede comprender la utilización de un servicio web que autentifica al usuario mediante la introducción de su número de teléfono en dicho servicio web y posterior confirmación de la identidad del usuario con el dispositivo de computación.

En otro ejemplo de realización, el mecanismo de autentificación comprende la utilización de un sistema de autenticación biométrica del usuario.

En un ejemplo de realización, la generación del nuevo par de claves criptográficas está condicionada a una aceptación y validación de las mismas por una tercera parte. La generación del nuevo par de claves criptográficas la puede realizar un mecanismo criptográfico, en donde el usuario, el operador de la red de cadena de bloques y,

opcionalmente, la tercera parte, comparten parte de una semilla para generar el nuevo par de claves criptográficas.

La presente invención proporciona de acuerdo a un segundo aspecto un sistema para recuperación de claves criptográficas de una red de cadena de bloques. Los elementos/módulos/unidades/dispositivos que forman parte del sistema del segundo aspecto están adaptados y configurados para implementar/ejecutar el método del primer aspecto de la invención.

Por tanto, la presente invención utiliza la infraestructura de una red de cadena de bloques, un dispositivo de computación de un usuario, una forma de identificación electrónica única (como una SIM o un DNI electrónico), y un sistema de autenticación de usuarios para realizar la correspondencia entre identidad física (utilizando la identificación electrónica) e identidad digital (identidad en redes de cadena de bloques), y realizar la gestión y recuperación segura de las claves del usuario.

La invención permite realizar la regeneración y recuperación de las claves de un usuario sin delegar el control o almacenamiento de las claves criptográficas a ninguna tercera parte. Hasta el momento no se ha implementado ningún mecanismo técnico que permita la recuperación de la identidad de un usuario en sistemas basados en tecnología de cadena de bloques ante la pérdida de la semilla de generación de las claves y las propias claves.

Además, la invención aporta un mecanismo de asignación y correspondencia de la identidad digital de un usuario con su identidad física a través de un elemento físico (por ejemplo, la tarjeta SIM de un dispositivo) permitiendo salvar la barrera entre el mundo físico y el digital que supone una fricción importante en el desarrollo de muchas propuestas de soluciones basadas en cadena de bloques.

Finalmente, la invención proporciona un modelo de recuperación de claves extensible a múltiples plataformas de cadena de bloques y contextos diferentes, al contrario que todas las propuestas de recuperación basados en identidad digital soberana basadas en cadena de bloques actuales, que están muy ligadas a las plataformas sobre las que se implementan.

Breve descripción de los dibujos

Las anteriores y otras características y ventajas se comprenderán más plenamente a partir de la siguiente descripción detallada de unos ejemplos de realización, meramente ilustrativa y no limitativa, con referencia a los dibujos que la acompañan, en los que:

La Fig. 1 ilustra esquemáticamente la arquitectura del sistema propuesto, según un ejemplo de realización.

La Fig. 2 ilustra esquemáticamente la arquitectura del sistema con dos redes de cadena de bloques independientes, según un ejemplo de realización.

La Fig. 3 es un diagrama que muestra la creación de una nueva identidad, según un ejemplo de realización.

La Fig. 4 es un diagrama que ilustra el proceso de revocación y recuperación de claves, según un ejemplo de realización.

Descripción detallada de la invención y de unos ejemplos de realización

La presente invención plantea un híbrido entre los modelos de recuperación de claves utilizados por los modelos de identidad digital soberana a través de un contrato inteligente, y los modelos de delegación de claves a terceros, sin que exista la necesidad de delegar la semilla o la clave privada en ningún momento. La invención es compatible con cualquier red de cadena de bloques que permita la ejecución de contratos inteligentes.

La Fig. 1 muestra un ejemplo de realización de la arquitectura del sistema propuesto. El sistema incluye o utiliza:

- Par de claves criptográficas: Representan las claves para el control de la identidad de un usuario 1 en las diferentes plataformas blockchain en las que participa. Para su generación se utiliza como semilla, material criptográfico almacenado en una tarjeta SIM 101 de un dispositivo de computación 100 (por ejemplo un teléfono móvil inteligente, entre otros) de un usuario 1. Las claves podrán generarse y almacenarse directamente en la tarjeta SIM 101 (sin que la abandonen en ningún momento como si de un hardware wallet se tratase), o el usuario puede generar sus propias claves personales y almacenarlas directamente en el dispositivo de computación 100. La implementación de la presente invención será igual independientemente del origen y la forma de almacenamiento de las claves por parte del usuario 1. La principal

diferencia entre que las claves del usuario 1 se almacenen y generen en la SIM 101 o en el dispositivo de computación 100 es su nivel de seguridad, el almacenamiento de claves en la SIM 101 equivaldrá al nivel de seguridad de una hardware wallet, mientras que, si el usuario 1 genera y almacena sus claves directamente en su dispositivo de computación 100, obtendrá un nivel de seguridad de las claves equivalente al de una software wallet.

- Plataforma blockchain de identidades 120: Es la red de cadena de bloques principal de gestión de identidades de las operadoras, es decir, la infraestructura de cadena de bloques por defecto del sistema. En esta red se gestiona el directorio de identidades del usuario 1 en las diferentes redes de cadena de bloques donde hacen uso de su identidad. Esta red 120 sirve para integrar todas las identidades de cadena de bloques del usuario 1, no obstante, esta invención puede implementarse directamente sobre redes de cadenas de bloques independientes sin necesidad de esta red principal 120 (la única diferencia será que en vez de existir un registro de identidades 123 único en la red de cadena de bloques principal 120, deberá existir un registro de identidades 133, 143 en cada red de cadena de bloques independiente 130, 140. Ver Figura 2).

- Gestor de identidades 110: Sistema encargado de la gestión de las identidades. Solo el proveedor de la infraestructura de identidad (la operadora), a través de unas claves válidas de gestores de identidad pueden hacer uso de él. El gestor de identidad 100 particularmente está formado por dos módulos:
    - Una API 113 única que escucha eventos en la red 105 (como el registro de una nueva SIM en la infraestructura, o su revocación), dispara el proceso de autenticación e identificación del usuario 1, y sirve de pasarela para las operadoras (entidades de confianza) entre la infraestructura de red 105, el mundo físico y las diferentes redes de cadena de bloques 120, 130, 140.
    - Un contrato inteligente gestor de identidad 122, 132, 142 en cada una de las redes de cadena de bloques 120, 130, 140 a las que se conecta el sistema que sirve de *gateway* (o puerto de enlace) de operadoras o entidades de confianza (su identidad única en la red) para realizar actualizaciones sobre el contrato de directorio de identidad (en la plataforma de cadena de bloques

principal 120), y para devolver el control de su contrato proxy 121, 131, 141 al usuario 1 que haya regenerado sus claves.

- Contrato Proxy 121, 131, 141: contrato inteligente sobre las diferentes infraestructuras redes de cadena de bloques 120, 130, 140 que representan la identidad del usuario 1 en cada una de las redes. La lógica de los contratos inteligentes permite limitar el disparo de funciones para que solo sea posible a través de transacciones firmadas por parte de una identidad específica, como el propietario del contrato. Esto se determina en la implementación del contrato definiendo la dirección del usuario 1 (es decir, la clave pública) para la cual se permite que transacciones firmadas con su clave privada puedan ejecutar la función. Los propietarios de este contrato proxy 121, 131, 141 son el usuario 1, a través de su par de claves de control, y el gestor de identidad 110. Este contrato tiene dos funcionalidades principales:
    - Delegar la firma de todas las transacciones del usuario 1 (las transacciones enviadas al contrato firmadas utilizando las claves de control del usuario 1). Esto permite que todas las acciones realizadas sobre la red de cadena de bloques 120, 130, 140 ya no pertenezcan directamente al par de claves del usuario 1, si no a este contrato inteligente. Esta función del contrato solo puede ser disparado a través de una transacción firmada utilizando las claves activas para el usuario 1 dueño del contrato proxy 121, 131, 141.
    - Funcionalidad de actualización de propietario del contrato. Solo puede ser disparada por el gestor de identidades 110 (a través de una transacción firmada por el contrato de gestor de identidades 110 que solo puede ser llamado utilizando las claves criptográficas de las operadoras, o entidad distribuida de confianza). Esta función actualiza a un nuevo par de claves el control del contrato proxy 121, 131, 141 modificando el propietario del contrato proxy 121, 131, 141.

- Registro de identidades 123, 133, 143: Sirve como directorio distribuido de identidades. Registra, particularmente, todas las identidades del sistema a través de la siguiente tupla: *(ID_único (e.j. MSISDN, ID electrónico), Proxy Contract Blockchain A, Address A, Public Key A [, Proxy Contract Blockchain B, Address B, Public Key B,…, Proxy Contract Blockchain N, Address N, Public Key N]).* Este registro (que a

su vez es un contrato inteligente 123, 133, 143 sobre las redes 120, 130, 140) solo puede ser manipulado por el gestor de identidades 110 (la operadora, o entidad de confianza, responsable del usuario 1), y las únicas funcionalidades disponibles son la creación, modificación y revocación de identidades de usuarios. En un ejemplo de realización, este registro reside solamente en la red de cadena de bloques principal 120 y registra información de todas las redes de bloques para la identidad del usuario 1. Alternativamente, si se opta por un patrón de diseño del sistema de redes de cadena de bloques independientes 130, 140 (Fig. 2), existe un registro de identidades 133, 143 independiente en cada red, y la tupla para cada usuario 1 solo registraría información sobre esa red, siendo la tupla resultante en este caso la siguiente: *(ID_único (e.j. MSISDN, ID electrónico), Proxy Contract Blockchain, Address, Public Key).*

- Sistema de autenticación de usuarios de la operadora, o en general, de la entidad garante de identidad (no ilustrado en las figuras): Se utiliza como sistema de autenticación segura *offchain* (externo e independiente de las redes de cadena de bloques) de los operadores, y sirve como mecanismo de correspondencia entre la identidad física y digital. Forma parte de la API 113 (módulo offchain) del gestor de identidades 110. Cada operador, a través de la API 113 del gestor de identidades 110, puede elegir el sistema de autenticación que quiere utilizar para identificar a sus usuarios. La API 113 lanzaría una petición al sistema de autenticación correspondiente que contestaría al gestor de identidades 110 con el resultado de la autenticación del usuario 1. Entre los procesos de autenticación que se pueden utilizar por la presente invención se encuentran el envío de un código de un solo uso mediante un mensaje de texto (tal como un SMS) al dispositivo de computación 100 verificado del usuario 1, el uso de soluciones de autenticación de las operadoras como *Mobile Connect* (https://mobileconnect.io), o incluso el uso de sistemas de autenticación biométrica.

En relación ahora a la Fig. 3, en la misma se muestra un ejemplo de realización de la creación de una nueva identidad. En el momento en el que el usuario 1 recibe su nueva SIM 101, se generará un nuevo par de claves criptográficas asimétricas a partir de material criptográfico de la SIM 101. Las claves pueden generarse y almacenarse directamente en la tarjeta SIM 101 (a modo de hardware wallet) sin que el usuario 1 deba realizar ninguna acción, o este puede decidir generar su propio par de claves con un algoritmo a su elección.

Cuando una SIM 101 es entregada y activada en la red 105, esta informa al gestor de identidades 110. El gestor de identidades 110 a través del mecanismo de autenticación pertinente, lanza un proceso de identificación del usuario 1 al número de teléfono para el que ha sido registrada la tarjeta SIM 101. Si el usuario 1 se autentica satisfactoriamente, el dispositivo de computación 100 del usuario 1 transmitirá de manera segura su nueva clave pública al gestor de identidades 110, y este procederá al despliegue del contrato proxy 121, del usuario 1 haciéndole propietario de él a través de su clave pública, y a la actualización de la tupla del usuario 1 en el registro de identidades 123. A partir de este momento el contrato proxy 121 representa la identidad soberana del usuario 1 en el sistema. Si el usuario 1 estuviera utilizando su identidad en más de una plataforma blockchain (y no solo en la plataforma blockchain principal de identidades 120), entonces se desplegará un nuevo contrato proxy 133, 143 para el usuario 1 en cada red de cadena de bloques 130, 140 en la que esté participando el usuario 1, actualizando el registro de identidades 133, 143 correspondientemente.

La Fig. 4 muestra el proceso de revocación y recuperación de claves según un ejemplo de realización. Si el usuario 1 perdiese el control de sus claves (extraviase el dispositivo de computación 100 que almacena sus claves, le robasen la SIM 101, o perdiese el control sobre su clave privada, etc.) el proceso de recuperación de la identidad particularmente sería el siguiente. En primer lugar, el usuario 1 comunica la pérdida de las claves, y el operador responsable del usuario 1 informa a la red 105 de la eliminación de la correspondencia entre tarjeta SIM 101, clave pública y número de teléfono del usuario 1 (ya sea por pérdida de claves, de SIM 101, o ambas, entre otras). Cuando la red 105 detecta un evento de eliminación de SIM 101 informa al gestor de identidades 110, que se encarga, para el usuario 1 responsable del evento, de eliminar (revocar) al usuario 1 como propietario de todos los contratos proxy 121, 131, 141 de las redes de cadena de bloques 120, 130, 140 pertinentes, y de eliminar la clave pública en el directorio de identidades 123, 133, 143. Seguidamente, se provee al usuario 1 con una nueva tarjeta SIM 101, y a partir del material criptográfico de esta se generan un nuevo par de claves pública/privada para cada una de las redes de cadena de bloques 120, 130, 140, tal y como ocurría con la creación de un nuevo usuario 1. La activación de la nueva SIM 101 dispara un nuevo evento en la red 105 que informa al gestor de identidades 110 encargado de lanzar el proceso de autenticación. De igual manera a como ocurría con la creación de una nueva identidad, el gestor de identidades 110 identifica al usuario 1, y el dispositivo de computación 100 transmite de manera segura su clave pública recién generada en el momento de recepción de la SIM

101. Si la autenticación es correcta, es decir el usuario ha sido autenticado correctamente (por ejemplo a través de un mecanismo de usuario/contraseña en la que el usuario 1 dice quién es, es decir se identifica mediante el usuario y lo demuestra autentificándose con la contraseña), el operador en cuestión a través del gestor de identidades 110 actualiza el directorio de identidades 121, 131, 141 con la nueva clave pública para el usuario 1, y actualiza a las nuevas claves la propiedad del contrato proxy 121, 131, 141. De esta forma el usuario 1 habría recuperado completamente el control de su identidad con sus nuevas claves.

Es importante tener en cuenta que la clave pública del usuario 1 se genera en la tarjeta SIM 101 de su dispositivo de computación 100 (salvo que este decida generar sus propias claves), y la entidad garante de la identidad del usuario 1 en ningún momento tiene acceso a la clave privada del usuario 1, solo se comporta como sistema de gestión y autenticación de usuarios, y la única pieza de la identidad del usuario 1 que conoce es la clave pública. Al realizarse una autenticación satisfactoria, un *applet* en la tarjeta SIM 101 se encarga de la extracción y transmisión segura de la clave pública al gestor de identidades 110 para que no pueda fugarse información sobre el par de claves al dispositivo 100 (la clave puede estar almacenada en la SIM 101 o directamente en el dispositivo 100 en función de la gestión de claves elegida por el usuario 1). Consecuentemente, a pesar de ser la operadora un tercero de confianza en el proceso de recuperación de las claves, en ningún momento es capaz de tomar el control del contrato proxy 121, 131, 141, y por tanto de la identidad del usuario 1.

Indicar que la presente invención no se limita a su implementación por parte de operadoras como proveedores del sistema de gestión de identidad y como garantes confiables de identidad, sino que en ambos roles otras entidades de confianza pueden jugar ese rol.

En ese sentido, en otros ejemplos de realización, la invención podría basarse en cualquier entidad confiable garante de identidad que se apoyase sobre un sistema seguro de identificación de usuarios. Así, podría utilizarse un documento de identificación electrónico, por ejemplo el DNI electrónico, como identificación única y sistema de autenticación del usuario 1 (siendo en este caso el Estado la entidad garante de identidad), de manera que, si el usuario 1 pierde sus claves, podría autenticarse a través de su DNIe.

De igual forma, el sistema de gestión de la identidad de la presente invención podría estar gestionado por parte de cualquier otra organización confiable. Ante la pérdida de sus claves, si la autenticación del usuario 1 fuera satisfactoria, se enviaría de manera segura su nueva

clave pública al gestor de identidades 110, que sería el encargado de comunicarse con la infraestructura correspondiente para devolverle el control de su identidad al usuario 1.

Como funcionalidad adicional, la presente invención permite el uso de un servicio web de autentificación de usuarios mediante utilización de su número de teléfono en el servicio web, por ejemplo *Mobile Connect,* como sistema de autenticación física para la identidad digital soberana (a la hora de permitir acceso a las claves, otorgar permisos de acceso a los datos, o validación de acciones varias sobre la identidad digital soberana).

Adicionalmente o alternativamente, en otros ejemplos de realización, se pueden utilizar mecanismos más complejos para la recuperación de las claves, de manera que no solo puedan hacerlo el usuario 1 y la operadora (con la generación de una nueva SIM 101 y la devolución del control del contrato proxy 121, 131, 141 al usuario 1), sino que el usuario 1 pueda asignar una serie de custodios que deberán también aceptar y validar la recuperación y generación de nuevas claves de identidad para un usuario 1 (utilizando el sistema de autenticación de sus operadoras pertinentes, permitiendo así distribuir aún más la confianza y el proceso de recuperación de las claves). Es decir, la generación del nuevo par de claves criptográficas puede estar condicionada a una aceptación y validación de las mismas por una tercera parte. Por ejemplo, en una empresa podría ser necesario que dos o más representantes de la empresa validen la generación de nuevas claves.

Asimismo, se puede utilizar un sistema de generación de claves donde ya no es el usuario 1 a través de la SIM 101 quien genera las claves para la identidad, sino un mecanismo criptográfico por el que el usuario 1, la operadora, y si fuera necesario los custodios, comparten parte de la semilla para poder regenerar las claves del usuario 1.

La invención propuesta puede implementarse en hardware, software, firmware o cualquier combinación de los mismos. Si se implementa en software, las funciones pueden almacenarse en o codificarse como una o más instrucciones o código en un medio legible por ordenador.

El alcance de la presente invención está definido en las reivindicaciones adjuntas.

REIVINDICACIONES

1. Método para recuperación de claves criptográficas de una red de cadena de bloques, en donde un dispositivo de computación (100) de un usuario (1) o un elemento (101) asociado al dispositivo de computación (100) tiene almacenadas un par de claves criptográficas asimétricas representativas de la identidad de dicho usuario (1) en al menos una red de cadena de bloques (120, 130, 140), incluyendo dicho par de claves una clave pública y una clave privada, y en donde un gestor de identidades (110), operativamente conectado a la red de cadena de bloques (120, 130, 140), que es al menos una, mantiene un registro del usuario (1) en un directorio distribuido de identidades (123, 133, 143), en donde dicho registro incluye información de la clave pública del usuario (1) y de al menos un contrato inteligente (121,131, 141) del usuario (1) en la red de cadena de bloques (120, 130, 140), el método comprende:

- eliminar, por el gestor de identidades (110), de dicho registro, la información de la clave pública del usuario (1) y revocar al usuario (1) como propietario del contrato inteligente (121,131, 141) al recibir una solicitud del usuario (1) debido a la pérdida o robo de la clave privada de su identidad;

- generar, por el dispositivo de computación del usuario (100) o por el elemento asociado al dispositivo de computación (101), un nuevo par de claves criptográficas asimétricas representativas de la identidad del usuario (1) en la red de cadena de bloques (120, 130, 140), en donde dicho nuevo par de claves comprende una nueva clave pública y una nueva clave privada;

- almacenar dicho nuevo par de claves generadas en el dispositivo de computación (100) del usuario (1) o en dicho elemento (101) asociado al dispositivo de computación (100);

- identificar y autentificar al usuario (1), por el gestor de identidades (110), mediante un mecanismo de autentificación proporcionado por una entidad garante de la identidad; y

- una vez que el usuario (1) ha sido autentificado correctamente, recibir, por el gestor de identidades (110), del dispositivo de computación (100), la nueva clave pública del usuario (1), y actualizar el registro del usuario (1) en el directorio distribuido de identidades (123, 133, 143) con la nueva clave pública recibida y actualizar a la nueva clave pública la propiedad del contrato inteligente (121,131, 141).

2. Método según la reivindicación 1, en donde el elemento (101) comprende una tarjeta SIM, y en donde dicha entidad garante de la identidad del usuario (1) es el operador de telecomunicaciones emisor de dicha tarjeta SIM.

3. Método según las reivindicaciones anteriores, en donde el registro en el directorio distribuido de identidades se realiza mediante una secuencia de identificación que incluye: un identificador del usuario (1), un identificador del contrato inteligente de la cadena de bloques y la clave pública.

4. Método según las reivindicaciones anteriores, en donde dicho mecanismo de autentificación comprende el envío de un código de un solo uso mediante un mensaje de texto al dispositivo de computación (100).

5. Método según las reivindicaciones 1 a 3, en donde dicho mecanismo de autentificación comprende la utilización de un servicio web que autentifica al usuario (1) mediante la introducción de su número de teléfono en dicho servicio web y posterior confirmación de la identidad del usuario (1) con el dispositivo de computación (100).

6. Método según las reivindicaciones 1 a 3, en donde dicho mecanismo de autentificación comprende la utilización de un sistema de autenticación biométrica del usuario (1).

7. Método según la reivindicación 1, en donde el elemento (101) comprende un documento de identificación electrónico del usuario (1).

8. Método según la reivindicación 1, en donde la generación del nuevo par de claves criptográficas está condicionada a una aceptación y validación de las mismas por una tercera parte.

9. Método según la reivindicación 1 u 8, en donde la generación del nuevo par de claves criptográficas la realiza un mecanismo criptográfico, en donde el usuario (1), el operador de la red de cadena de bloques (120, 130, 140) y, opcionalmente, dicha tercera parte, comparten parte de una semilla para generar el nuevo par de claves criptográficas.

10. Sistema para recuperación de claves criptográficas de una red de cadena de bloques, comprende:

- al menos una red de cadena de bloques (120, 130, 140);
- un dispositivo de computación (100) de un usuario (1) y/o un elemento (101) asociado al dispositivo de computación (100), configurado para almacenar un par de claves

criptográficas asimétricas representativas de la identidad de dicho usuario (1) en dicha red de cadena de bloques (120, 130, 140), que es al menos una, incluyendo dicho par de claves una clave pública y una clave privada;

- un gestor de identidades (110), operativamente conectado a la red de cadena de bloques (120, 130, 140), y configurado para mantener un registro del usuario (1) en un directorio distribuido de identidades (123, 133, 143), en donde dicho registro incluye información de la clave pública del usuario (1) y de al menos un contrato inteligente (121,131, 141) del usuario (1) en la red de cadena de bloques (120, 130, 140); y

- una entidad garante de la identidad de dicho usuario (1);

en donde el gestor de identidades (110) está configurado además para:

- eliminar, de dicho registro, la información de la clave pública del usuario (1) y revocar al usuario (1) como propietario del contrato inteligente al recibir una solicitud del usuario (1) debido a la pérdida o robo de la clave privada, en donde el dispositivo de computación (100) de un usuario (1) y/o el elemento (101) asociado al dispositivo de computación (100) está configurado para generar un nuevo par de claves criptográficas asimétricas representativas de la identidad del usuario (1) en la red de cadena de bloques (120, 130, 140), dicho nuevo par de claves comprendiendo una nueva clave pública y una nueva clave privada, y en donde el dispositivo de computación (100) o dicho elemento (101) asociado al dispositivo de computación (100) está configurado para almacenar dicho nuevo par de claves generadas;

- identificar y autentificar al usuario (1) mediante un mecanismo de autentificación proporcionado por una entidad garante de la identidad; y

- una vez que el usuario (1) ha sido autentificado correctamente, recibir, del dispositivo de computación (100), la nueva clave pública del usuario (1), y actualizar el registro del usuario (1) en el directorio distribuido de identidades (123, 133, 143) con la nueva clave pública recibida y actualizar a la nueva clave pública la propiedad del contrato inteligente (121,131, 141).

11. Sistema según la reivindicación 10, en donde el elemento (101) comprende una tarjeta SIM, y en donde dicha entidad garante de la identidad del usuario (1) es el operador de telecomunicaciones emisor de dicha tarjeta SIM.

12. Sistema según la reivindicación 10, en donde el elemento (101) comprende un documento de identificación electrónico del usuario (1).

13. Sistema según la reivindicación 10, en donde el gestor de identidades (110) está configurado para realizar dicho registro mediante una secuencia de identificación que incluye: un identificador del usuario (1), un identificador del contrato inteligente de la cadena de bloques y la clave pública.

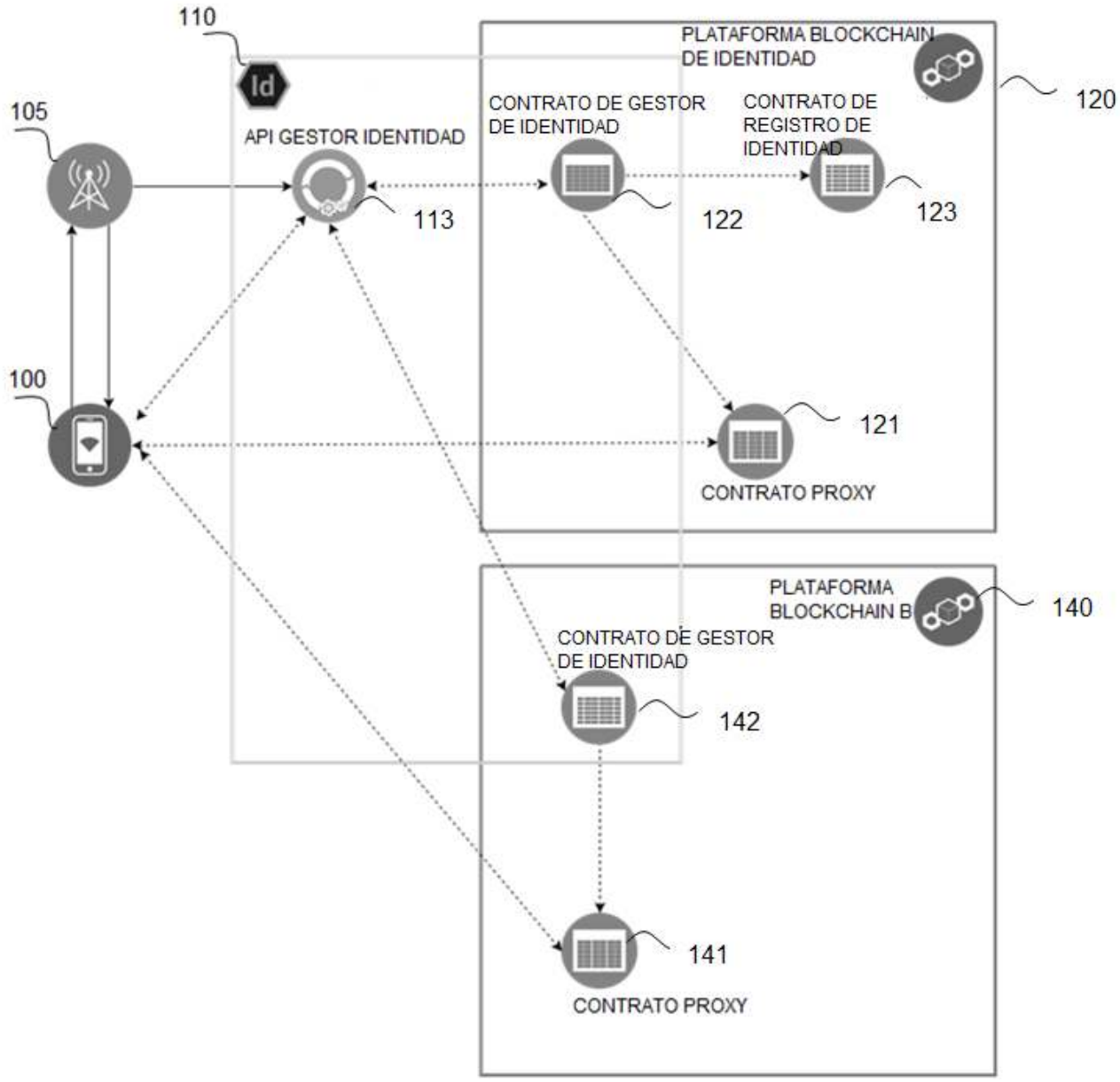
110
Id
API GESTOR IDENTIDAD
105
100
113
PLATAFORMA BLOCKCHAIN
DE IDENTIDAD
120
CONTRATO DE GESTOR
DE IDENTIDAD
CONTRATO DE
REGISTRO DE
IDENTIDAD
122
123
121
CONTRATO PROXY
PLATAFORMA
BLOCKCHAIN B
140
CONTRATO DE GESTOR
DE IDENTIDAD
142
141
CONTRATO PROXY

Fig. 1

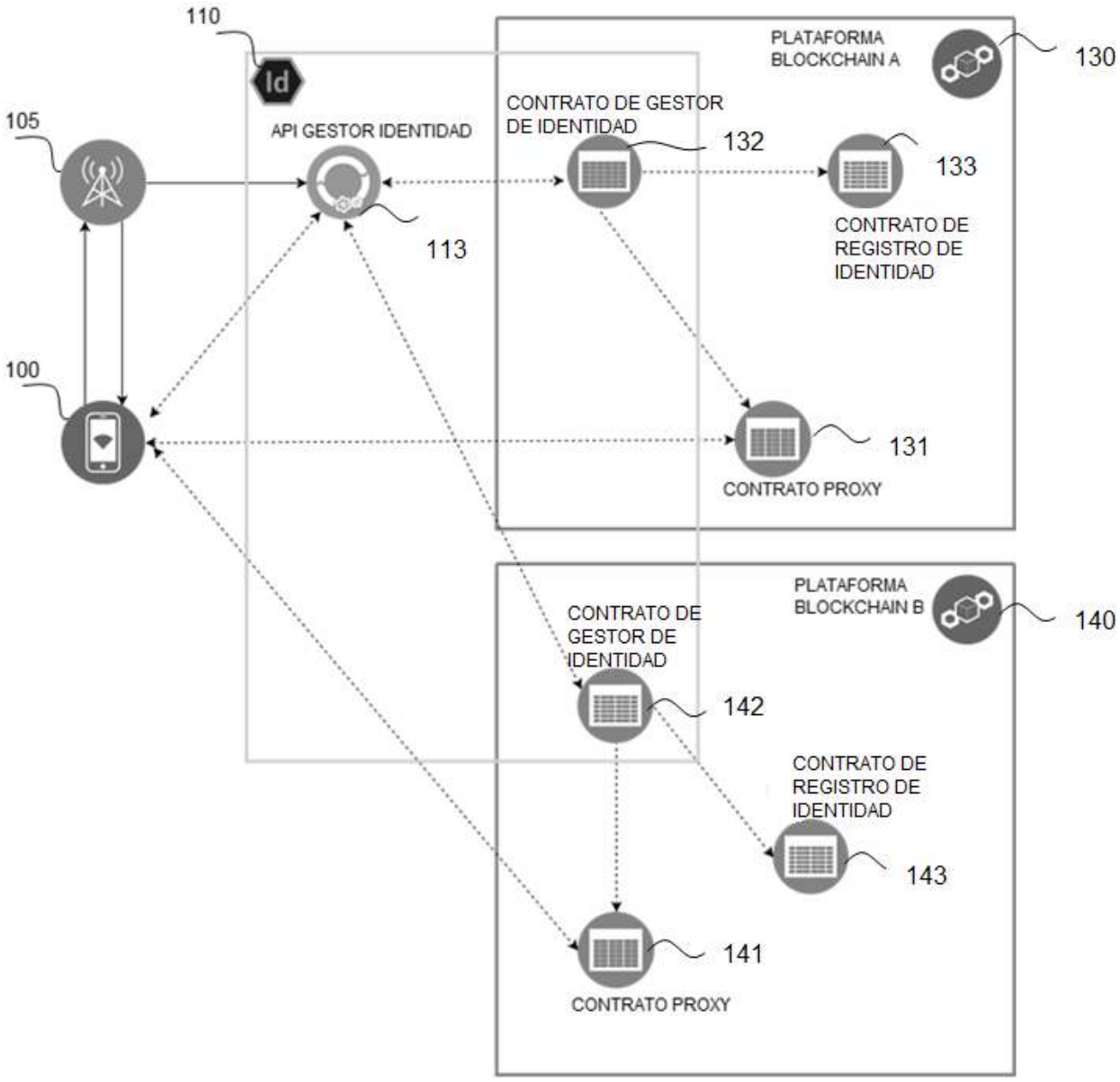
110
Id
API GESTOR IDENTIDAD
113
105
100
PLATAFORMA BLOCKCHAIN A
130
CONTRATO DE GESTOR DE IDENTIDAD
132
133
CONTRATO DE REGISTRO DE IDENTIDAD
131
CONTRATO PROXY
PLATAFORMA BLOCKCHAIN B
140
CONTRATO DE GESTOR DE IDENTIDAD
142
CONTRATO DE REGISTRO DE IDENTIDAD
143
141
CONTRATO PROXY

Fig. 2

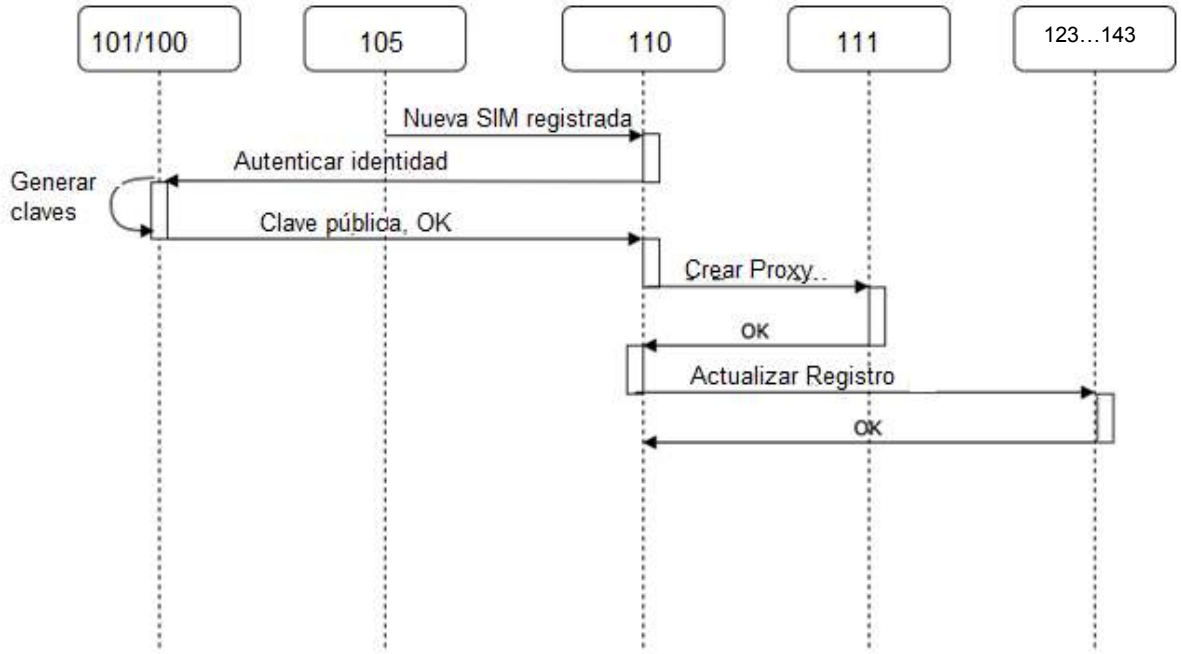
101/100
105
110
111
123…143
Nueva SIM registrada
Autenticar identidad
Generar claves
Clave pública, OK
Crear Proxy..
OK
Actualizar Registro
OK

Fig. 3

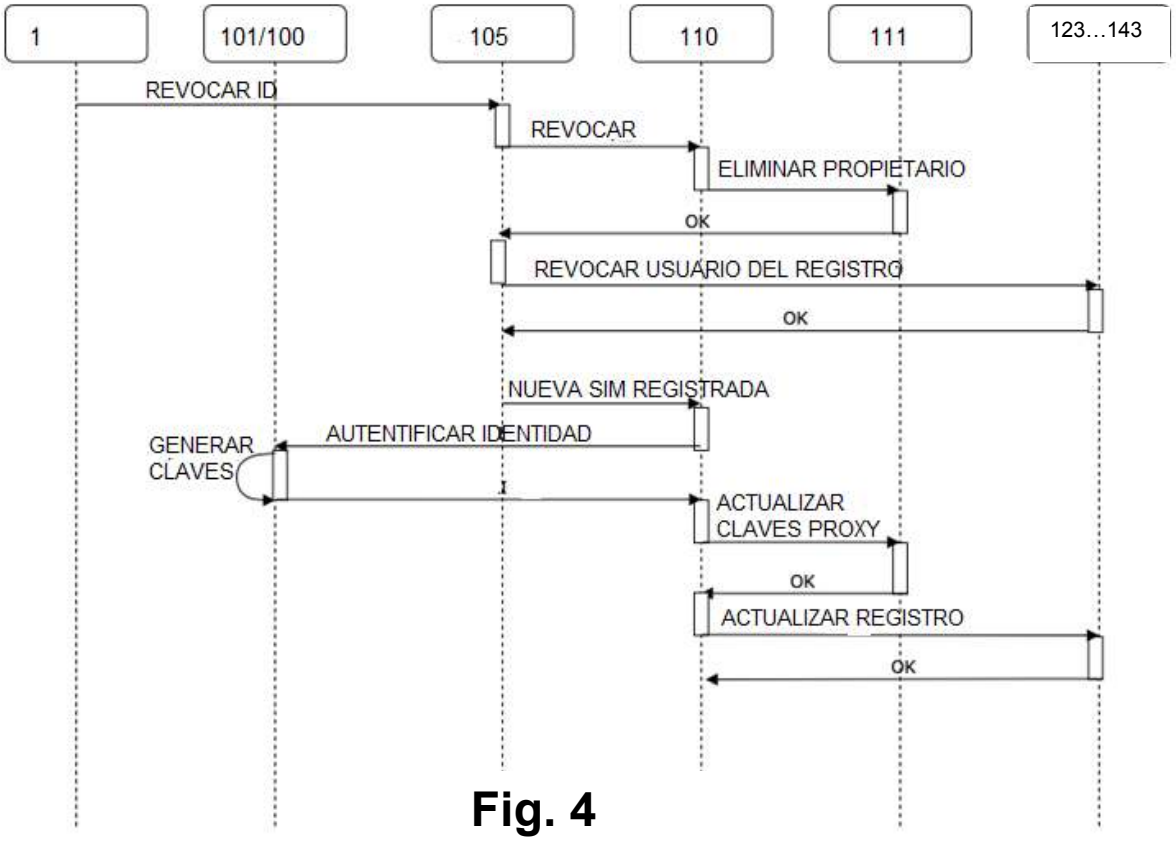
1
101/100
105
110
111
123…143
REVOCAR ID
REVOCAR
ELIMINAR PROPIETARIO
OK
REVOCAR USUARIO DEL REGISTRO
OK
NUEVA SIM REGISTRADA
AUTENTIFICAR IDENTIDAD
GENERAR CLAVES
ACTUALIZAR CLAVES PROXY
OK
ACTUALIZAR REGISTRO
OK

Fig. 4

OFICINA ESPAÑOLA
DE PATENTES Y MARCAS

ESPAÑA

(21) N.º solicitud: 201930030

(22) Fecha de presentación de la solicitud: 18.01.2019

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TECNICA

(51) **Int. Cl. :** ***H04L9/32*** (2006.01)
G06F16/00 (2019.01)

DOCUMENTOS RELEVANTES

Categoría	(56) Documentos citados	Reivindicaciones afectadas
A	CN 107609876 A (BEIJING YUNZHI TECH CO LTD) 19/01/2018, Todo el documento.	1-13
A	CN 108282339 A (HEFEI INST PHYSICAL SCI CAS) 13/07/2018, Todo el documento.	1-13
A	CN 109150547 A (YAO QIAN) 04/01/2019, Todo el documento.	1-13
A	US 2018262493 A1 (ANDRADE MARCUS) 13/09/2018, Todo el documento.	1-13
A	WO 2018089098 A1 (AWARE INC) 17/05/2018, Todo el documento;	1-13
A	CN 108270780 A (NO 30 INSTITUTE OF CHINA ELECTRONIC TECH GROUP CORPORATION) 10/07/2018, Todo el documento.	1-13
A	WO 2018144150 A1 (NORTHERN TRUST CORP) 09/08/2018, Todo el documento.	1-13
A	WO 2018229608 A1 (NCHAIN HOLDINGS LTD) 20/12/2018, Todo el documento.	1-13
A	WO 2018157788 A1 (TENCENT TECH SHENZHEN CO LTD) 07/09/2018, Todo el documento.	1-13

Categoría de los documentos citados
X: de particular relevancia
Y: de particular relevancia combinado con otro/s de la misma categoría
A: refleja el estado de la técnica
O: referido a divulgación no escrita
P: publicado entre la fecha de prioridad y la de presentación de la solicitud
E: documento anterior, pero publicado después de la fecha de presentación de la solicitud

El presente informe ha sido realizado

☒ para todas las reivindicaciones ☐ para las reivindicaciones nº:

Fecha de realización del informe	Examinador	Página
03.09.2019	M. Muñoz Sanchez	1/2

Documentación mínima buscada (sistema de clasificación seguido de los símbolos de clasificación)

H04L, G06F

Bases de datos electrónicas consultadas durante la búsqueda (nombre de la base de datos y, si es posible, términos de búsqueda utilizados)

INVENES, EPODOC, WPI