(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 692 871**

(21) Número de solicitud: 201890049

(51) Int. CI.:

G06F 17/30 (2006.01)
G06Q 20/36 (2012.01)
G06Q 20/38 (2012.01)

(12) SOLICITUD DE PATENTE A2

(22) Fecha de presentación:

29.03.2016

(30) Prioridad:

28.03.2016 US 16024776 US

(43) Fecha de publicación de la solicitud:

05.12.2018

(71) Solicitantes:

BLACK GOLD COIN, INC. (100.0%)
7495 Azure Drive, Suite 100
89130 Las Vegas US

(72) Inventor/es:

ANDRADE, Marcus

(74) Agente/Representante:

SALVÀ FERRER, Joan

(54) Título: **SISTEMAS Y PROCEDIMIENTOS PARA PROPORCIONAR UNA VERIFICACIÓN DE IDENTIDAD PERSONAL MULTIFACTORIAL BASADA EN UNA CADENA DE BLOQUES**

(57) Resumen:

Se puede proporcionar una verificación de identidad personal multifactorial basada en una cadena de bloques.

Las direcciones de verificación pueden establecerse en una cadena de bloques por: asociación de identificadores con individuos que han verificado previamente identidades personales, asignación de direcciones de verificación en una cadena de bloques a los individuos y registro de los identificadores y datos biométricos asociados con los individuos en las direcciones de verificación correspondientes. La verificación de identidad personal multifactorial en basada en una cadena de bloques utilizando las direcciones de verificación se puede realizar por: recepción de uno o más identificadores en relación con una o más solicitudes para verificar una identidad de uno o más individuos, extracción de los datos biométricos asociados con uno o más individuos a partir de las direcciones de verificación correspondientes y verificación de la identidad de uno o más individuos tras la recepción de datos biométricos y claves privadas coincidentes.

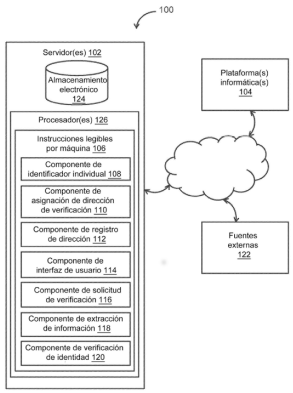

FIG. 1

ES 2 692 871 A2

DESCRIPCION

SISTEMAS Y PROCEDIMIENTOS PARA PROPORCIONAR UNA VERIFICACIÓN DE IDENTIDAD PERSONAL MULTIFACTORIAL BASADA EN UNA CADENA DE BLOQUES

La presente descripción se refiere a sistemas y procedimientos para proporcionar una verificación de identidad personal multifactorial basada en una cadena de bloques.

Un aspecto de la descripción se refiere a un sistema para proporcionar una verificación de identidad personal multifactorial basada en una cadena de bloques. El sistema puede incluir uno o más procesadores de hardware configurados mediante instrucciones legibles por máquina para establecer direcciones de verificación en una cadena de bloques y/o realizar una verificación de identidad personal multifactorial basada en una cadena de bloques utilizando las direcciones de verificación. El establecimiento de direcciones de verificación en la cadena de bloques puede incluir la asociación de identificadores con individuos que han verificado previamente sus identidades personales, un primer identificador está asociado a un primer individuo, el primer individuo tiene una identidad personal previamente verificada; asignación de direcciones de verificación en una cadena de bloques a los individuos, una dirección de verificación dada que incluye una clave pública y una clave privada, una primera dirección de verificación es asignada al primer individuo, la primera dirección de verificación incluye una primera clave pública y una primera clave privada; y registro de los identificadores y los datos biométricos asociados con los individuos en las direcciones de verificación correspondientes, el primer identificador y los primeros datos biométricos asociados con el primer individuo se registran en la primera dirección de verificación. La realización de una verificación de identidad personal multifactorial basada en una cadena de bloques utilizando las direcciones de verificación puede incluir la recepción de uno o más identificadores en relación con una o más solicitudes para verificar una identidad de uno o más individuos, el primer identificador es recibido en relación con una solicitud para verificar una identidad del primer individuo; extracción de los datos biométricos asociados con uno o más individuos a partir de las direcciones correspondientes de verificación, los primeros datos biométricos asociados con el primer individuo se extraen de la primera dirección de verificación; y verificación de la identidad de uno o más individuos tras la recepción de datos biométricos y claves privadas coincidentes, la identidad personal del primer individuo se verifica tras la recepción de (1) datos biométricos que coinciden con los primeros datos biométricos y (2) una clave privada que coincide con la primera clave privada.

Otro aspecto de la descripción se refiere a un procedimiento para establecer direcciones de verificación en una cadena de bloques con el fin de proporcionar una verificación de identidad personal multifactorial basada en una cadena de bloques. El procedimiento puede ser realizado por uno o más procesadores de hardware configurados por instrucciones legibles por máquina. El procedimiento puede incluir la asociación de identificadores con individuos que tienen identidades personales previamente verificadas, un primer identificador está asociado a un primer individuo, el primer individuo tiene una identidad personal previamente verificada; asignación de direcciones de verificación en una cadena de bloques a los individuos, una dirección de verificación dada que incluye una clave pública y una clave privada, una primera dirección de verificación es asignada al primer individuo, la primera dirección de verificación incluye una primera clave pública y una primera clave privada; y registro de los identificadores y los datos biométricos asociados con los individuos en las direcciones correspondientes de verificación, el primer identificador y los primeros datos biométricos asociados con el primer individuo se registran en la primera dirección de verificación. La identidad de uno o más individuos puede ser verificable tras la recepción de los datos biométricos y las claves privadas coincidentes, de modo que la identidad personal del primer individuo sea verificable tras la recepción de (1) datos biométricos que coinciden con los primeros datos biométricos y (2) una clave privada que coincide con la primera clave privada.

Otro aspecto de la descripción se refiere a un procedimiento para realizar una verificación de identidad personal multifactorial basada en una cadena de bloques utilizando direcciones de verificación. El procedimiento puede ser realizado por uno o más procesadores de hardware configurados por instrucciones legibles por máquina. El procedimiento puede incluir la recepción de uno o más identificadores en relación con una o más solicitudes para verificar una identidad de uno o más individuos, un primer identificador es recibido en relación con una solicitud para verificar una identidad de un primer individuo; extracción de datos biométricos asociados con uno o más individuos a partir de direcciones correspondientes de verificación en una cadena de bloques, una dirección de verificación dada que incluye una clave pública y una clave privada, los primeros datos biométricos asociados con el primer individuo se extraen de una primera dirección de verificación asignada al primer individuo, la primera dirección de verificación incluye una primera clave pública y una primera clave privada; y verificación de la identidad de uno o más individuos tras la recepción de los datos biométricos y las claves privadas coincidentes, la identidad personal del primer individuo se verifica tras la recepción de (1) datos biométricos que coinciden con los primeros datos

biométricos y (2) una clave privada que coincide con la primera clave privada.

Estos y otros rasgos y características de la tecnología actual, así como los procedimientos de operación y funciones de los elementos relacionados de la estructura y la combinación de partes y economías de fabricación, resultarán más evidentes al considerar la siguiente descripción y las reivindicaciones adjuntas con referencia a los dibujos anexos, todos los cuales forman parte de la presente memoria descriptiva, en la que los números de referencia idénticos designan partes correspondientes en las diversas figuras. Sin embargo, queda expresamente entendido que los dibujos son solo con fines ilustrativos y descriptivos y no tienen por objeto ser una definición de los límites de la invención. Como se utiliza en la memoria descriptiva y en las reivindicaciones, la forma en singular de "un", "una" y "el", "la" incluyen referentes en plural a menos que el contexto indique claramente lo contrario.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

FIG. 1 ilustra un sistema para proporcionar una verificación de identidad personal multifactorial basada en una cadena de bloques, según una o más implementaciones.

FIG. 2 ilustra un procedimiento para establecer direcciones de verificación en una cadena de bloques con el fin de proporcionar una verificación de identidad personal multifactorial basada en una cadena de bloques, según una o más implementaciones.

FIG. 3 ilustra un procedimiento para realizar una verificación de identidad personal multifactorial basada en una cadena de bloques utilizando direcciones de verificación, según una o más implementaciones.

DESCRIPCIÓN DETALLADA

FIG. 1 ilustra un sistema 100 para proporcionar una verificación de identidad personal multifactorial basada en una cadena de bloques, según una o más implementaciones. En algunas implementaciones, el sistema 100 puede incluir uno o más servidores 102. El(los) servidor(es) 102 puede(n) configurarse para comunicarse con una o más plataformas informáticas 104 según una arquitectura cliente/servidor, una arquitectura unidad a unidad,

y/u otras arquitecturas. Los usuarios pueden acceder al sistema 100 a través de plataforma(s) informática(s) 104.

El(los) servidor(es) 102 puede(n) estar configurados para ejecutar instrucciones legibles por máquina 106. Las instrucciones legibles por máquina 106 pueden incluir uno o más de un componente de identificador individual 108, un componente de asignación de dirección de verificación 110, un componente de registro de dirección 112, un componente de interfaz de usuario 114, un componente de solicitud de verificación 116, un componente de extracción de información 118, un componente de verificación de identidad 120; y/u otros componentes de instrucciones legibles por máquina.

Las instrucciones legibles por máquina 106 pueden ser ejecutables para establecer direcciones de verificación en una cadena de bloques. En términos generales, una cadena de bloques es una base de datos de transacciones compartida por algunos o todos los nodos que participan en el sistema 100. Dicha participación puede basarse en el protocolo Bitcoin, protocolo Ethereum y/u otros protocolos relacionados con monedas digitales y/o cadenas de bloques. Una copia completa de la cadena de bloques contiene todas las transacciones que se han ejecutado alguna vez con una moneda digital asociada. Además de las transacciones, cualquier otra información puede ser contenida por la cadena de bloques, tal como se describe adicionalmente en esta solicitud.

La cadena de bloques se puede basar en varios bloques. Un bloque puede incluir un registro que contiene y confirma una o más transacciones en espera. Periódicamente (por ejemplo, aproximadamente cada minuto), se puede anexar a la cadena de bloques un nuevo bloque que incluye transacciones y/u otra información. En algunas implementaciones, un bloque dado en la cadena de bloques contiene un código de comprobación del bloque anterior. Esto puede tener el efecto de crear una cadena de bloques a partir de un bloque de origen (es decir, el primer bloque en la en la cadena de bloques) hasta un bloque actual. Se puede garantizar que el bloque dado surja cronológicamente después de un bloque anterior debido a que de otro modo no se conocería el código de comprobación del bloque anterior. El bloque dado puede ser poco factible desde el punto de vista computacional para modificarse una vez que se incluye en la cadena de bloques ya que cada bloque posterior también debería regenerarse.

Una dirección de verificación dada puede incluir una ubicación específica en la cadena de bloques en la que se almacena determinada información. En algunas implementaciones, una dirección de verificación individual se puede referir como "*AtenVerify Address*". Las direcciones de verificación se describen con más detalle a continuación en relación con el componente de asignación de dirección de verificación 110.

El componente de identificador individual 108 puede configurarse con identificadores asociados con individuos que tienen identidades personales previamente verificadas. Por ejemplo, un primer identificador puede estar asociado a un primer individuo. El primer individuo puede tener una identidad personal previamente verificada. En términos generales, un identificador puede incluir uno o más de un número, un código alfanumérico, un nombre de usuario y/u otra información que se puede vincular a un individuo. En algunas implementaciones, un identificador individual puede referirse como "*Aten ID*".

Según algunas implementaciones, un individuo que tiene una identidad personal previamente verificada puede haber obtenido la identidad personal previamente verificada a través de una variedad de estrategias. Por ejemplo, en algunas implementaciones, el individuo se puede requerir para que proporcione evidencia de la identidad del individuo. Dicha evidencia puede incluir una o más de una proporción de una copia de una identificación emitida por el gobierno (por ejemplo, pasaporte y/o permiso de conducción), proporción de una copia del correo recibido por el individuo (por ejemplo, una factura de servicios), evidencia proporcionada por un tercero y/u otra evidencia sobre la identidad de un individuo. La evidencia se puede proporcionar a una entidad asociada con el(los) servidor(es) 102.

El componente de asignación de dirección de verificación 110 puede configurarse para asignar direcciones de verificación en una cadena de bloques a los individuos. Una dirección de verificación dada puede incluir una clave pública y una clave privada. A modo de ejemplo, se puede asignar una primera dirección de verificación al primer individuo. La primera dirección de verificación puede incluir una primera clave pública y una primera clave privada.

En términos generales, se puede utilizar un par de claves públicas y privadas para el cifrado y el descifrado según uno o más algoritmos de clave pública. A modo de ejemplo no limitativo, se puede utilizar un par de claves para firmas digitales. Tal par de claves puede

incluir una clave privada para firmar y una clave pública para la verificación. La clave pública puede estar ampliamente distribuida, mientras que la clave privada se mantiene en secreto (por ejemplo, es solo conocida por su propietario). Las claves pueden estar relacionadas matemáticamente, pero el cálculo de la clave privada de la clave pública es inviable.

En algunas implementaciones, el componente de asignación de dirección de verificación 110 puede configurarse de manera que las claves privadas puedan almacenarse dentro de la(s) plataforma(s) informática(s) 104. Por ejemplo, la primera clave privada puede almacenarse dentro de una plataforma informática 104 y/u otras ubicaciones asociadas con el primer individuo. Según alguna implementación, una clave privada puede almacenarse en uno o más de un archivo "verify.dat", una tarjeta SIM y/u otras ubicaciones.

En algunas implementaciones, el componente de asignación de dirección de verificación 110 puede configurarse de manera que se pueden asignar múltiples direcciones de verificación a individuos distintos. Por ejemplo, además de la primera dirección de verificación, se puede asignar una segunda dirección de verificación al primer individuo. Se pueden asignar una o más direcciones de verificación adicionales al primer individuo, según una o más implementaciones.

El componente de registro de dirección 112 puede configurarse para registrar identificadores y datos biométricos asociados con los individuos en las direcciones de verificación correspondientes. Por ejemplo, el primer identificador y los primeros datos biométricos asociados con el primer individuo pueden registrarse en la primera dirección de verificación. La grabación de información en una dirección de verificación dada puede incluir la grabación de un código de comprobación u otra representación encriptada de la información. En algunas implementaciones, se pueden registrar diferentes datos biométricos en múltiples direcciones de verificación asignadas a un solo individuo dado. Por ejemplo, además del primer identificador y los primeros datos biométricos asociados con el primer individuo que se registran en la primera dirección de verificación, el primer identificador y los segundos datos biométricos asociados con el primer individuo pueden registrarse en una segunda dirección de verificación.

En términos generales, los datos biométricos pueden incluir métricas relacionadas con las características humanas. Los identificadores biométricos son características distintivas y

medibles que se pueden utilizar para etiquetar y describir individuos. Los identificadores biométricos incluyen normalmente características fisiológicas, pero también pueden incluir características conductuales y/u otras características. Las características fisiológicas pueden estar relacionadas con la forma del cuerpo de un individuo. Los ejemplos de características fisiológicas utilizadas como datos biométricos pueden incluir una o más huellas dactilares, venas en la palma, reconocimiento facial, ADN, huella palmar, geometría de mano, reconocimiento del iris, retina, olor o aroma, y/u otras características fisiológicas. Las características conductuales pueden estar relacionadas con un patrón de comportamiento de un individuo. Los ejemplos de características conductuales utilizadas como datos biométricos pueden incluir uno o más de la velocidad de tecleo, marcha, voz y/u otras características conductuales.

Los datos biométricos pueden incluir una o más de una imagen u otra representación visual de una característica fisiológica, un registro de una característica conductual, una plantilla de una característica fisiológica y/o característica conductual, y/u otros datos biométricos. Una plantilla puede incluir una síntesis de rasgos relevantes extraídos de la fuente. Una plantilla puede incluir uno o más de un vector que describe rasgos de una característica fisiológica y/o característica conductual, una representación numérica de una característica fisiológica y/o característica conductual, una imagen con propiedades particulares, y/u otra información.

Los datos biométricos pueden recibirse a través de plataformas informáticas 104 asociadas con los individuos. Por ejemplo, los datos biométricos asociados con un primer individuo pueden recibirse a través de una primera plataforma informática 104 asociada con el primer individuo. La primera plataforma informática 104 puede incluir un dispositivo de entrada (no representado) configurado para capturar y/o registrar una característica fisiológica y/o característica conductual del primer individuo. Los ejemplos de dicho dispositivo de entrada pueden incluir uno o más de una cámara y/u otro dispositivo de imagen, un escáner de huellas dactilares, un micrófono, un acelerómetro y/u otros dispositivos de entrada.

El componente de interfaz de usuario 114 puede configurarse para proporcionar una interfaz de presentación a individuos a través de plataformas informáticas 104 asociadas. La interfaz puede incluir una interfaz de usuario gráfica presentada a través de plataformas informáticas 104. Según algunas implementaciones, la interfaz puede configurarse para permitir que un

individuo dado añada o elimine direcciones de verificación asignadas al individuo dado, siempre que al individuo se le asigne al menos una dirección de verificación.

En algunas implementaciones, el componente de interfaz de usuario 114 puede configurarse para acceder y/o gestionar uno o más perfiles de usuario y/o información de usuario asociada a usuarios del sistema 100. Uno o más perfiles de usuario y/o información de usuario pueden incluir información almacenada por el(los) servidor(es) 102, una o más de las plataformas informáticas 104, y/u otras ubicaciones de almacenamiento. Los perfiles de usuario pueden incluir, por ejemplo, información que identifica a los usuarios (por ejemplo, un nombre de usuario o identificador persistente, un número, un identificador y/u otra información de identificación), información de inicio de sesión de seguridad (por ejemplo, un código de inicio de sesión o contraseña), información de cuenta del sistema, información de suscripción, información de cuenta de moneda digital (por ejemplo, relacionada con una moneda mantenida en crédito para un usuario), información de relación (por ejemplo, información relacionada con relaciones entre usuarios en el sistema 100), información de uso del sistema, información demográfica asociada con los usuarios, historial de interacción entre los usuarios del sistema 100, información declarada por los usuarios, información de compra de los usuarios, historial de navegación de los usuarios, una identificación de plataforma informática asociada a un usuario, un número de teléfono asociado con un usuario y/u otra información relacionada con los usuarios.

Las instrucciones legibles por máquina 106 pueden ser ejecutables para realizar una verificación de identidad personal multifactorial basada en una cadena de bloques utilizando las direcciones de verificación.

El componente de solicitud de verificación 116 puede configurarse para recibir uno o más identificadores en relación con una o más solicitudes para verificar una identidad de uno o más individuos. Por ejemplo, el primer identificador puede recibirse en relación con una solicitud para verificar una identidad del primer individuo. Las solicitudes de verificación de identidad pueden proporcionarse en relación con y/o transacciones relacionadas a financieras, intercambios de información; y/u otras interacciones. Las solicitudes pueden ser recibidas de otros individuos y/u otros terceros.

El componente de extracción de información 118 puede configurarse para extraer los datos

biométricos asociados con uno o más individuos de las direcciones de verificación correspondientes. Por ejemplo, los primeros datos biométricos asociados con el primer individuo se pueden extraer de la primera dirección de verificación. La extracción de información (por ejemplo, datos biométricos) a partir de una dirección de verificación puede incluir información de descifrado.

Según algunas implementaciones, el componente de extracción de información 118 puede configurarse de modo que, en respuesta a la recepción de la solicitud para verificar la identidad del primer individuo, se puede proporcionar un aviso al primer individuo para los datos biométricos que coinciden con los primeros datos biométricos y una clave privada que coincide con la primera clave privada. El aviso puede transmitirse a través de una plataforma informática 104 asociada con el primer individuo. El aviso puede transmitirse a través de una interfaz de usuario gráfica y/u otra interfaz de usuario proporcionada por la plataforma informática 104 asociada con el primer individuo. El aviso puede incluir una indicación de que es una o más de las indicaciones visuales, audibles, hápticas y/u otras indicaciones.

En algunas implementaciones, el componente de extracción de información 118 puede configurarse de manera que, en respuesta a la recepción de la solicitud para verificar la identidad del primer individuo, se pueda proporcionar un aviso a una plataforma informática 104 asociada con el primer individuo. El aviso puede provocar que la plataforma informática 104 proporcione automáticamente, al(los) servidor(es) 102, datos biométricos que coinciden con los primeros datos biométricos y/o una clave privada que coincide con la primera clave privada.

El componente de verificación de identidad 120 puede configurarse para verificar la identidad de uno o más individuos tras, o en respuesta a, la recepción de datos biométricos y claves privadas coincidentes. Por ejemplo, la identidad personal del primer individuo puede verificarse tras la recepción de (1) datos biométricos que coinciden con los primeros datos biométricos y (2) una clave privada que coincide con la primera clave privada. La verificación de la identidad personal del primer individuo puede incluir la comparación de la información almacenada con la información recién recibida.

Según algunas implementaciones, el componente de verificación de identidad 120 puede configurarse de manera que la identidad personal del primer individuo pueda verificarse tras

la recepción de (1) datos biométricos que coinciden con los primeros datos biométricos o los segundos datos biométricos y (2) una clave privada que coincide con la primera clave privada. Tales implementaciones pueden proporcionar las denominadas firmas "M de N" para la verificación de identidad en la que se requiere algún subconjunto de un conjunto más grande de información de identificación.

En algunas implementaciones, el componente de verificación de identidad 120 puede configurarse de manera que los datos biométricos que coinciden con los primeros datos biométricos y la clave privada que coincide con la primera clave privada se puedan utilizar para firmar la verificación de la identidad personal del primer individuo.

Una firma criptográfica es un mecanismo matemático que permite que alguien demuestre la propiedad. En el caso de Bitcoin, una billetera de Bitcoin y su(s) clave(s) privada(s) están unidas por alguna magia matemática. Cuando tu software de Bitcoin firma una transacción con la clave privada apropiada, la red por completo puede ver que la firma coincide con los bitcoins que se están gastando. Sin embargo, no hay forma de que el mundo adivine su clave privada para robar los bitcoins ganados con tanto esfuerzo.

En algunas implementaciones, al menos un nodo dedicado realiza la firma de la verificación de la identidad personal del primer individuo. Un nodo dedicado dado puede incluir uno o más de los servidores 102. El nodo dedicado dado puede ser un nodo público o un nodo privado configurado para crear nuevos bloques y/o para firmar la verificación.

En algunas implementaciones, el(los) servidor(es) 102, plataforma(s) informática(s) 104, y/o recursos externos 122 pueden estar conectados operativamente a través de uno o más enlaces de comunicación electrónica. Por ejemplo, tales enlaces de comunicación electrónica pueden establecerse, al menos en parte, a través de una red tal como Internet y/u otras redes. Se apreciará que esto no tiene por objeto ser limitante, y que el alcance de la presente descripción incluye implementaciones en las que el(los) servidor(es) 102, plataforma(s) informática(s) 104 y/o recursos externos (122) pueden estar operativamente conectados a través de algún otro medio de comunicación.

Una plataforma informática 104 dada puede incluir uno o más procesadores configurados

para ejecutar instrucciones legibles por máquina. Las instrucciones legibles por máquina pueden configurarse para permitir que un experto o usuario asociado con la plataforma informática 104 dada interactúe con el sistema 100 y/o recursos externos 122, y/o proporcione otra funcionalidad atribuida en esta solicitud a la(s) plataforma(s) informática(s) 104. Por medio de un ejemplo no limitativo, la plataforma informática 104 dada puede incluir uno o más de un ordenador de sobremesa, un ordenador portátil, un ordenador de mano, una plataforma de computación con tabletas, un NetBook, un teléfono inteligente, una consola de juegos y/u otra plataforma de computación.

Los recursos externos 122 pueden incluir fuentes de información, servidores y/o proveedores de entornos virtuales fuera del sistema 100, entidades externas que participan con el sistema 100 y/u otros recursos. En algunas implementaciones, parte o la totalidad de la funcionalidad atribuida en esta solicitud a recursos externos 100 puede ser proporcionada por recursos incluidos en el sistema 100.

El(los) servidor(es) 102 pueden incluir almacenamiento electrónico 124, uno o más procesadores 126 y/u otros componentes. El(los) servidores 102 puede(n) incluir líneas de comunicación o puertos para permitir el intercambio de información con una red y/u otras plataformas informáticas. La ilustración del(los) servidor(es) 102 en la FIG. 1 no tiene por objeto ser limitante. El(los) servidores 102 puede(n) incluir una pluralidad de componentes de hardware, software y/o firmware que funcionan conjuntamente para proporcionar la funcionalidad atribuida en esta solicitud al(los) servidor(es) 102. Por ejemplo, el(los) servidor(es) 102 puede(n) ser implementado(s) por una nube de plataformas informáticas que funcionan conjuntamente como servidor(es) 102.

El almacenamiento electrónico 124 puede comprender medios de almacenamiento no transitorios que almacenan electrónicamente información. Los medios de almacenamiento electrónico del almacenamiento electrónico 124 pueden incluir uno o ambos de almacenamiento en el sistema que se proporciona de forma integral (es decir, esencialmente no extraíble) con servidor(es) 102 y/o almacenamiento extraíble que se puede conectar de forma extraíble a un servidor(es) 102 a través de, por ejemplo, un puerto (por ejemplo, un puerto USB, un puerto firewire, etc.) o una unidad (por ejemplo, una unidad de disco, etc.). El almacenamiento electrónico 124 puede incluir uno o más medios de almacenamiento ópticamente legibles (por ejemplo, discos ópticos, etc.), medios de almacenamiento legibles

magnéticamente (por ejemplo, cinta magnética, disco duro magnético, unidad de disquete, etc.), medios de almacenamiento basados en carga eléctrica (por ejemplo, EEPROM, RAM, etc.), medios de almacenamiento de estado sólido (por ejemplo, unidad de memoria flash, etc.) y/u otros medios de almacenamiento electrónicamente legibles. El almacenamiento electrónico 124 puede incluir uno o más recursos de almacenamiento virtual (por ejemplo, almacenamiento en la nube, una red privada virtual y/u otros recursos de almacenamiento virtual). El almacenamiento electrónico 124 puede almacenar algoritmos de software, información determinada por el(los) procesador(es) 126, información recibida del servidor(es) 102, información recibida de la plataforma(s) informática(s) 104 y/u otra información que permite que el(los) servidor(es) 102 funcione(n), como se describe en esta solicitud.

El(los) procesador(es) 126 puede(n) configurarse para proporcionar capacidades de procesamiento de información en el(los) servidor(es) 102. Como tal, el(los) procesador(es) 126 puede(n) incluir uno o más de un procesador digital, un procesador analógico, un circuito digital diseñado para procesar información, un circuito analógico diseñado para procesar información, una máquina de estado y/u otros mecanismos para procesar información electrónicamente. Aunque el(los) procesador(es) 126 se muestra(n) en la FIG. 1 como una entidad única, esto es solo para fines ilustrativos. En algunas implementaciones, el(los) procesador(es) 126 puede(n) incluir una pluralidad de unidades de procesamiento. Estas unidades de procesamiento pueden estar físicamente ubicadas dentro del mismo dispositivo, o el(los) procesador(es) 126 puede(n) representar la funcionalidad de procesamiento de una pluralidad de dispositivos que funcionan en coordinación. El(los) procesador(es) 126 puede(n) estar configurado(s) para ejecutar los componentes de instrucciones legibles por máquina 108, 110, 112, 114, 116, 118, 120 y/u otros componentes de instrucciones legibles por máquina. El(los) procesador(es) 126 puede(n) estar configurado(s) para ejecutar los componentes de instrucciones legibles por máquina 108, 110, 112, 114, 116, 118, 120, y/u otros componentes de instrucciones legibles por máquina por software; hardware; firmware; alguna combinación de software, hardware y/o firmware; y/u otros mecanismos para configurar capacidades de procesamiento en un procesador(es) 126. Como se utiliza en esta solicitud, la expresión "componente de instrucciones legibles por máquina" puede referirse a cualquier componente o conjunto de componentes que realizan la funcionalidad atribuida al componente de instrucciones legibles por máquina. Esto puede incluir uno o más procesadores físicos durante la ejecución de instrucciones legibles por procesador, las instrucciones legibles por procesador, conjunto de circuitos, hardware, medios de

almacenamiento o cualquier otro componente.

Debe apreciarse que aunque los componentes de instrucciones legibles por máquina 108, 110, 112, 114, 116, 118 y 120 se ilustran en la FIG. 1 por estar implementadas dentro de una única unidad de procesamiento, en implementaciones en las que el(los) procesador(es) 126 incluye(n) múltiples unidades de procesamiento, uno o más de los componentes de instrucciones legibles por máquina 108, 110, 112, 114, 116, 118, y/o 120 pueden implementarse remotamente desde los otros componentes de instrucciones legibles por máquina. La descripción de la funcionalidad proporcionada por los diferentes componentes de instrucciones legibles por máquina 108, 110, 112, 114, 116, 118 y/o 120 descritos a continuación es para fines ilustrativos, y no tiene por objeto ser limitante, como cualquiera de los componentes de instrucciones legibles por máquina 108, 110, 112, 114, 116, 118 y/o 120 que pueden proporcionar más o menos funcionalidades de las que se describen. Por ejemplo, se pueden eliminar uno o más de los componentes de instrucciones legibles por máquina 108, 110, 112, 114, 116, 118 y/o 120, y una parte o la totalidad de su funcionalidad puede ser proporcionada por otros componentes de instrucciones legibles por máquina 108, 110, 112, 114, 116, 118 y/o 120. Como otro ejemplo, el(los) procesadores 126 puede(n) configurarse para ejecutar uno o más componentes de instrucciones legibles por máquina adicionales que pueden realizar algunas o todas las funcionalidades atribuidas a continuación a uno de los componentes de instrucciones legibles por máquina 108, 110, 112, 114, 116, 118 y/o 120.

FIG. 2 ilustra un procedimiento 200 para establecer direcciones de verificación en una cadena de bloques con el fin de proporcionar una verificación de identidad personal multifactorial basada en una cadena de bloques, según una o más implementaciones. Las operaciones del procedimiento 200 presentado a continuación tienen por objeto ser ilustrativas. En algunas implementaciones, el procedimiento 200 puede realizarse con una o más operaciones adicionales no descritas, y/o sin una o más de las operaciones discutidas. Adicionalmente, el orden en el que se ilustran las operaciones del procedimiento 200 en la FIG. 2 y describen a continuación no tiene por objeto ser limitante.

En algunas implementaciones, una o más operaciones del procedimiento 200 pueden implementarse en uno o más dispositivos de procesamiento (por ejemplo, un procesador digital, un procesador analógico, un circuito digital diseñado para procesar información, un circuito analógico diseñado para procesar información, una máquina de estado y/u otros

mecanismos para procesar información electrónicamente). Uno o más dispositivos de procesamiento pueden incluir uno o más dispositivos que ejecutan algunas o todas las operaciones del procedimiento 200 en respuesta a instrucciones almacenadas electrónicamente en un medio de almacenamiento electrónico. Uno o más dispositivos de procesamiento pueden incluir uno o más dispositivos configurados a través de hardware, firmware y/o software que son diseñados específicamente para la ejecución de una o más de las operaciones del procedimiento 200.

En una operación 202, los identificadores pueden estar asociados con individuos que tienen identidades personales previamente verificadas. Un primer identificador puede estar asociado a un primer individuo. El primer individuo puede tener una identidad personal previamente verificada. La operación 202 puede realizarse por uno o más procesadores de hardware configurados para ejecutar un componente de instrucciones legibles por máquina que es igual o similar al componente de identificador individual 108 (como se describe en relación con la FIG. 1), según una o más implementaciones.

En una operación 204, las direcciones de verificación en una cadena de bloques se pueden asignar a los individuos. Una dirección de verificación dada puede incluir una clave pública y una clave privada. Se puede asignar una primera dirección de verificación al primer individuo. La primera dirección de verificación puede incluir una primera clave pública y una primera clave privada. La operación 204 puede realizarse por uno o más procesadores de hardware configurados para ejecutar un componente de instrucciones legibles por máquina que es igual o similar al componente de asignación de dirección de verificación 110 (como se describe en relación con la FIG. 1), según una o más implementaciones.

En una operación 206, los identificadores y los datos biométricos asociados con los individuos pueden registrarse en las direcciones de verificación correspondientes. El primer identificador y los primeros datos biométricos asociados con el primer individuo pueden registrarse en la primera dirección de verificación. La identidad de uno o más individuos puede ser verificable tras, o en respuesta a, la recepción de datos biométricos y claves privadas coincidentes. La identidad personal del primer individuo puede ser verificable tras, o en respuesta a, la recepción de (1) datos biométricos que coinciden con los primeros datos biométricos y (2) una clave privada que coincide con la primera clave privada. La operación 206 puede realizarse por uno o más procesadores de hardware configurados para ejecutar un componente de instrucciones legibles por máquina que es igual o similar al componente

de registro de dirección 112 (como se describe en relación con la FIG. 1), según una o más implementaciones.

FIG. 3 ilustra un procedimiento 300 para realizar una verificación de identidad personal multifactorial basada en una cadena de bloques utilizando direcciones de verificación, según una o más implementaciones. Las operaciones del procedimiento 300 presentado a continuación tienen por objeto ser ilustrativas. En algunas implementaciones, el procedimiento 300 puede realizarse con una o más operaciones adicionales no descritas, y/o sin una o más de las operaciones discutidas. Adicionalmente, el orden en el que se ilustran las operaciones del procedimiento 300 en la FIG. 3 y describen a continuación no tiene por objeto ser limitante.

En algunas implementaciones, el procedimiento 300 puede implementarse en uno o más dispositivos de procesamiento (por ejemplo, un procesador digital, un procesador analógico, un circuito digital diseñado para procesar información, un circuito analógico diseñado para procesar información, una máquina de estado y/u otros mecanismos para procesar información electrónicamente). Uno o más dispositivos de procesamiento pueden incluir uno o más dispositivos que ejecutan algunas o todas las operaciones del procedimiento 300 en respuesta a instrucciones almacenadas electrónicamente en un medio de almacenamiento electrónico. Uno o más dispositivos de procesamiento pueden incluir uno o más dispositivos configurados a través de hardware, firmware y/o software que son diseñados específicamente para la ejecución de una o más de las operaciones del procedimiento 300.

En una operación 302, se pueden recibir uno o más identificadores en relación con una o más solicitudes para verificar una identidad de uno o más individuos. Se puede recibir un primer identificador en relación con una solicitud para verificar la identidad de un primer individuo. La operación 302 puede realizarse por uno o más procesadores de hardware configurados para ejecutar un componente de instrucciones legibles por máquina que es igual o similar al componente de solicitud de verificación 116 (como se describe en relación con la FIG. 1), según una o más implementaciones.

En una operación 304, los datos biométricos asociados con uno o más individuos pueden extraerse a partir de las direcciones de verificación correspondientes en una cadena de bloques. Una dirección de verificación dada puede incluir una clave pública y una clave

privada. Los primeros datos biométricos asociados con el primer individuo pueden extraerse de una primera dirección de verificación asignada al primer individuo. La primera dirección de verificación puede incluir una primera clave pública y una primera clave privada. La operación 304 puede ser realizada por uno o más procesadores de hardware configurados para ejecutar un componente de instrucciones legibles por máquina que es igual o similar al componente de extracción de información 118 (como se describe en relación con la FIG. 1), según una o más implementaciones.

En una operación 306, la identidad de uno o más individuos puede verificarse tras, o en respuesta a, la recepción de datos biométricos y claves privadas coincidentes. La identidad personal del primer individuo puede verificarse tras, o en respuesta a, la recepción de (1) datos biométricos que coinciden con los primeros datos biométricos y (2) una clave privada que coincide con la primera clave privada. La operación 306 puede realizarse por uno o más procesadores de hardware configurados para ejecutar un componente de instrucciones legibles por máquina que es igual o similar al componente de verificación de identidad 120 (como se describe en relación con la FIG. 1), según una o más implementaciones.

Las implementaciones ejemplares pueden facilitar el almacenamiento de datos personales en una cadena de bloques. Los datos personales pueden almacenarse en la cadena de bloques de forma encriptada. Una persona puede ser identificada a nivel de cadena de bloques con una o más de una clave privada, una huella dactilar, un código de comprobación de huellas dactilares, una retina de un ojo, un código de comprobación de una retina de un ojo y/u otra información única. Los datos almacenados pueden incluir o relacionarse con uno o más de un pasaporte, un documento de identidad, información extraída del pasaporte, un permiso de conducción, información extraída del permiso de conducción, huella dactilar, retina de un ojo y/u otra información. Según algunas implementaciones, si se cambian algunos de los datos, se puede crear un nuevo registro para esa persona en la cadena de bloques. Es decir, todos los cambios son añadidos como nuevos registros. El registro antiguo siempre se almacenará en la cadena de bloques. En términos generales, todos los registros en la cadena de bloques se almacenan para siempre y no se pueden eliminar. Existirá más de una copia de la cadena de bloques para garantizar que los registros no se manipulen.

Las implementaciones ejemplares pueden facilitar el acceso a los datos personales. Pueden existir múltiples niveles de acceso para los datos personales en la cadena de bloques. Los

controles de acceso pueden ser detectados en niveles de pares de claves públicas/privadas. Los ejemplos de niveles de acceso pueden incluir uno o más de súper administrador (acceso completo a la cadena de bloques), autoridades a nivel nacional (acceso completo de solo lectura), autoridades a nivel estatal/local (acceso limitado de solo lectura), policía y otros servicios que incluyen emergencias (acceso a ciertos datos personales por huellas dactilares/retina de un ojo de esa persona solamente), comerciantes participantes (acceso limitado) y/u otros niveles de acceso.

Las implementaciones ejemplares pueden facilitar la comprobación de la verificación. Pueden existir niveles múltiples de cómo es posible comprobar la verificación. Por ejemplo, algunas implementaciones pueden garantizar que una persona tenga un registro en una "empresa", pero no se proporcionan datos personales. Algunas implementaciones pueden garantizar que una persona tenga un registro en la empresa y obtener información personal muy básica, tal como nombre completo, fecha de nacimiento, sexo y/u otra información básica. Algunas implementaciones pueden garantizar que una persona tenga un registro en la empresa y obtener todos los datos personales.

Si bien la presente tecnología ha sido descrita en detalle con el fin de ilustrar en base a lo que actualmente se considera que son las implementaciones más prácticas y preferidas, queda entendido que tal detalle es únicamente para ese fin y que la tecnología no se limita a las implementaciones descritas, sino, al contrario, tienen por objeto cubrir modificaciones y disposiciones equivalentes que están dentro del espíritu y alcance de las reivindicaciones adjuntas. Por ejemplo, queda entendido que la presente tecnología contempla que, en la medida de lo posible, uno o más rasgos de cualquier implementación se pueden combinar con uno o más rasgos de cualquier otra implementación.

REIVINDICACIONES

1. Un sistema para proporcionar una verificación de identidad personal multifactorial basada en una cadena de bloques, el sistema comprende:

uno o más procesadores de hardware configurados por instrucciones legibles por máquina para:

establecer direcciones de verificación en una cadena de bloques por:

asociación de identificadores con individuos que han verificado previamente identidades personales, un primer identificador está asociado a un primer individuo, el primer individuo tiene una identidad personal previamente verificada;

asignación de direcciones de verificación en una cadena de bloques a los individuos, una dirección de verificación dada que incluye una clave pública y una clave privada, una primera dirección de verificación es asignada al primer individuo, la primera dirección de verificación incluye una primera clave pública y una primera clave privada; y

grabación de identificadores y datos biométricos asociados con los individuos en las direcciones de verificación correspondientes, el primer identificador y los primeros datos biométricos asociados con el primer individuo se registran en la primera dirección de verificación; y

realización de la verificación de identidad personal multifactorial basada en cadena de bloques utilizando las direcciones de verificación mediante:

recepción de uno o más identificadores en relación con una o más solicitudes para verificar una identidad de uno o más individuos, el primer identificador es recibido en relación con una solicitud para verificar una identidad del primer individuo; extracción de los datos biométricos asociados con uno o más individuos de las direcciones de verificación correspondientes, los primeros datos biométricos asociados con el primer individuo se extraen de la primera dirección de verificación; y

verificación de la identidad de uno o más individuos tras la recepción de datos biométricos y claves privadas coincidentes, la identidad personal del primer individuo se verifica tras la recepción de (1) datos biométricos que coinciden con los primeros datos biométricos y (2) una clave privada que coincide con la primera clave privada.

2. El sistema de la reivindicación 1, en el que la primera clave privada se almacena dentro de una plataforma informática asociada con el primer individuo.

3. El sistema de la reivindicación 1, en el que se asignan múltiples direcciones de verificación a individuos distintos de manera que, además de la primera dirección de verificación, se asigna una segunda dirección de verificación al primer individuo.

4. El sistema de la reivindicación 1, en el que uno o más procesadores de hardware están configurados además por instrucciones legibles por máquina para proporcionar una interfaz para presentación a individuos a través de plataformas informáticas asociadas, la interfaz está configurada para permitir que un individuo dado añada o elimine direcciones de verificación asignadas al individuo dado siempre que se le asigne al menos una dirección de verificación al individuo dado.

5. El sistema según la reivindicación 1, en el que diferentes datos biométricos se registran en múltiples direcciones de verificación asignadas a un individuo dado de manera que, además del primer identificador y los primeros datos biométricos asociados con el primer individuo se registran en la primera dirección de verificación, el primer identificador y los segundos datos biométricos asociados con el primer individuo se registran en la segunda dirección de verificación.

6. El sistema de la reivindicación 5, en el que la identidad personal del primer individuo se verifica tras la recepción de (1) datos biométricos que coinciden con los primeros datos biométricos o los segundos datos biométricos y (2) una clave privada que coincide con la primera clave privada.

7. El sistema de la reivindicación 1, en el que los datos biométricos incluyen una o más de una imagen, una grabación, o una plantilla.

8. El sistema de la reivindicación 1, en el que los datos biométricos están relacionados con una o más huellas dactilares, venas en la palma, reconocimiento facial, ADN, huella palmar, geometría de mano, reconocimiento del iris, retina, olor o aroma, velocidad de tecleo, marcha, o voz.

9. El sistema de la reivindicación 1, en el que los primeros datos biométricos se reciben a través de una plataforma informática asociada con el primer individuo.

10. El sistema de la reivindicación 1, en el que uno o más procesadores de hardware están configurados adicionalmente mediante instrucciones legibles por máquina que son sensibles a la recepción de la solicitud para verificar la identidad del primer individuo, solicitación al primer individuo de datos biométricos que coinciden con los primeros datos biométricos y una clave privada que coincide con la primera clave privada, el aviso se transmite a través de una plataforma informática asociada con el primer individuo.

11. El sistema de la reivindicación 1, en el que uno o más procesadores de hardware están configurados adicionalmente mediante instrucciones legibles por máquina que son sensibles a la recepción de la solicitud para verificar la identidad del primer individuo, solicitación de una plataforma informática asociada con el primer individuo para que proporcione automáticamente datos biométricos que coinciden con los primeros datos biométricos y una clave privada que coincide con la primera clave privada.

12. El sistema de la reivindicación 1, en el que los datos biométricos que coinciden con los primeros datos biométricos y la clave privada que coincide con la primera clave privada se utilizan para firmar la verificación de la identidad personal del primer individuo.

13. El sistema de la reivindicación 1, en el que al menos un nodo dedicado realiza la firma de la verificación de la identidad personal del primer individuo.

14. Un procedimiento para establecer direcciones de verificación en una cadena de bloques con el fin de proporcionar una verificación de identidad personal multifactorial basada en una cadena de bloques, el procedimiento se realiza por uno o más procesadores de hardware configurados mediante instrucciones legibles por máquina, comprendiendo el procedimiento:

asociación de identificadores con individuos que han verificado previamente identidades personales, un primer identificador está asociado a un primer individuo,

el primer individuo tiene una identidad personal previamente verificada;

asignación de direcciones de verificación en una cadena de bloques a los individuos, una dirección de verificación dada que incluye una clave pública y una clave privada, una primera dirección de verificación es asignada al primer individuo, la primera dirección de verificación incluye una primera clave pública y una primera clave privada; y

registro de identificadores y datos biométricos asociados con los individuos en las direcciones de verificación correspondientes, el primer identificador y los primeros datos biométricos asociados con el primer individuo se registran en la primera dirección de verificación;

en el que la identidad de uno o más individuos es verificable tras la recepción de datos biométricos y claves privadas coincidentes, la identidad personal del primer individuo es verificable tras la recepción de (1) datos biométricos que coinciden con los primeros datos biométricos y (2) una clave privada que coincide con la primera clave privada.

15. El procedimiento de la reivindicación 14, que comprende además la asignación de múltiples direcciones de verificación a individuos distintos de manera que, además de la primera dirección de verificación, se asigna una segunda dirección de verificación al primer individuo.

16. El procedimiento de la reivindicación 14, que comprende además proporcionar una interfaz para presentación a individuos a través de plataformas informáticas asociadas, la interfaz se configura para permitir que un individuo dado añada o elimine direcciones de verificación asignadas al individuo dado, siempre y cuando al menos una dirección de verificación se le asigne al individuo dado.

17. El procedimiento de la reivindicación 14, que comprende además registrar diferentes datos biométricos en múltiples direcciones de verificación asignadas a un individuo dado de manera que, además del primer identificador y los primeros datos biométricos asociados con el primer individuo se registran en la primera dirección de verificación, el primer identificador y los segundos datos biométricos asociados con el primer individuo se registran en la segunda dirección de verificación.

18. Un procedimiento para realizar una verificación de identidad personal multifactorial basada en una cadena de bloques utilizando direcciones de verificación, el procedimiento es realizado por uno o más procesadores de hardware configurados mediante instrucciones legibles por máquina, comprendiendo el procedimiento:

recepción de uno o más identificadores en relación con una o más solicitudes para verificar una identidad de uno o más individuos, un primer identificador se recibe en relación con una solicitud para verificar la identidad de un primer individuo;

extracción de datos biométricos asociados con uno o más individuos de direcciones de verificación correspondientes en una cadena de bloques, una dirección de verificación dada incluye una clave pública y una clave privada, los primeros datos biométricos asociados con el primer individuo se extraen a partir de una primera dirección de verificación asignada al primer individuo, la primera dirección de verificación incluye una primera clave pública y una primera clave privada; y

verificación de la identidad de uno o más individuos tras la recepción de datos biométricos y claves privadas coincidentes, la identidad personal del primer individuo se verifica tras la recepción de (1) datos biométricos que coinciden con los primeros datos biométricos y (2) una clave privada que coincide con la primera clave privada.

19. El procedimiento de la reivindicación 18, que comprende además, sensible a la recepción de la solicitud verificar la identidad del primer individuo:

solicitación al primer individuo de datos biométricos que coinciden con los primeros datos biométricos y una clave privada que coincide con la primera clave privada, el aviso se transmite a través de una plataforma informática asociada con el primer individuo; o

solicitación de una plataforma informática asociada con el primer individuo para proporcionar automáticamente datos biométricos que coincidan con los primeros datos biométricos y una clave privada que coincida con la primera clave privada.

20. El procedimiento de la reivindicación 18, en el que los datos biométricos que coinciden con los primeros datos biométricos y la clave privada que coincide con la primera clave privada se utilizan para firmar la verificación de la identidad personal del primer individuo.

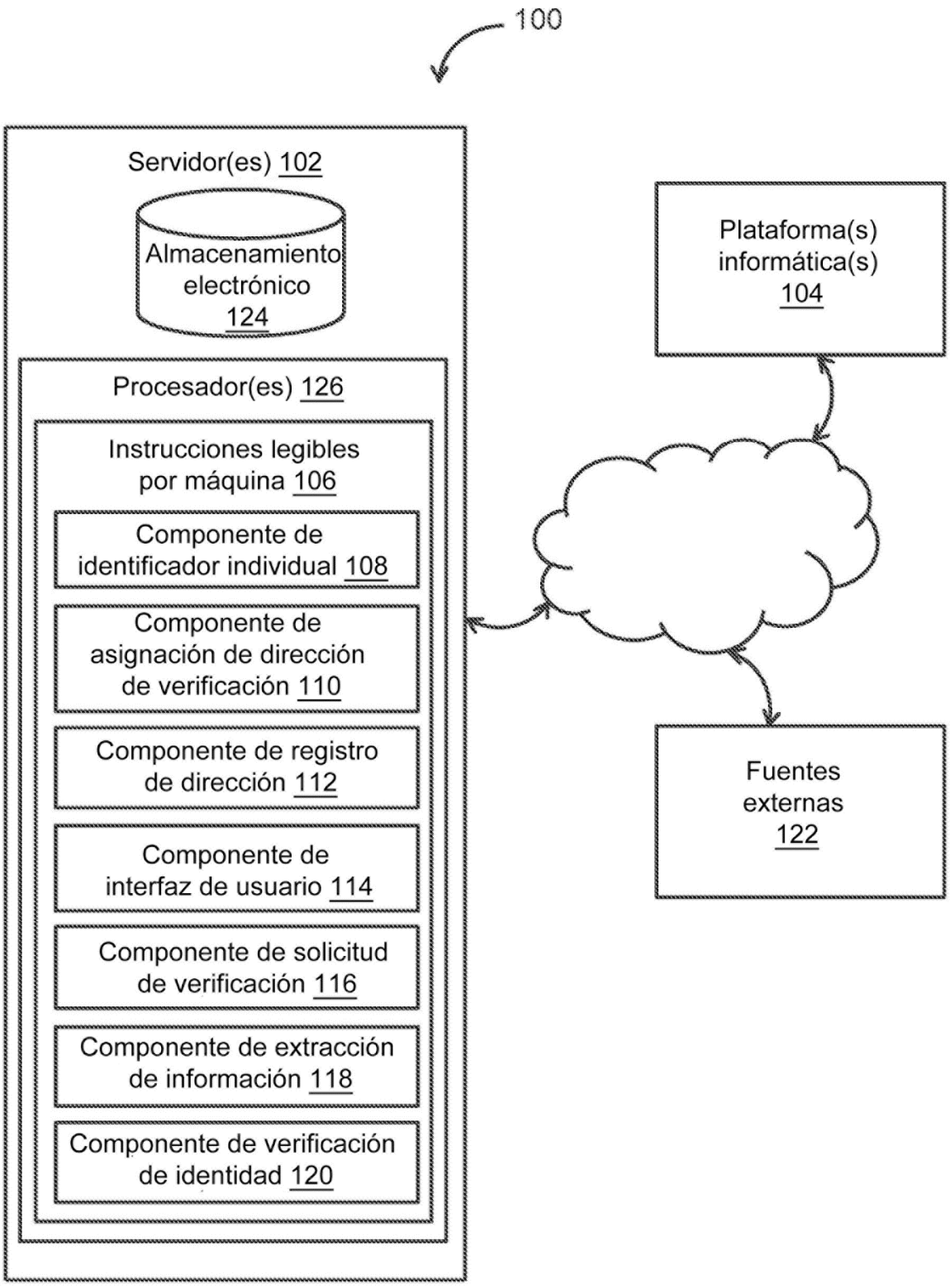
100
Servidor(es) 102
Almacenamiento electrónico 124
Procesador(es) 126
Instrucciones legibles por máquina 106
Componente de identificador individual 108
Componente de asignación de dirección de verificación 110
Componente de registro de dirección 112
Componente de interfaz de usuario 114
Componente de solicitud de verificación 116
Componente de extracción de información 118
Componente de verificación de identidad 120
Plataforma(s) informática(s) 104
Fuentes externas 122

FIG. 1

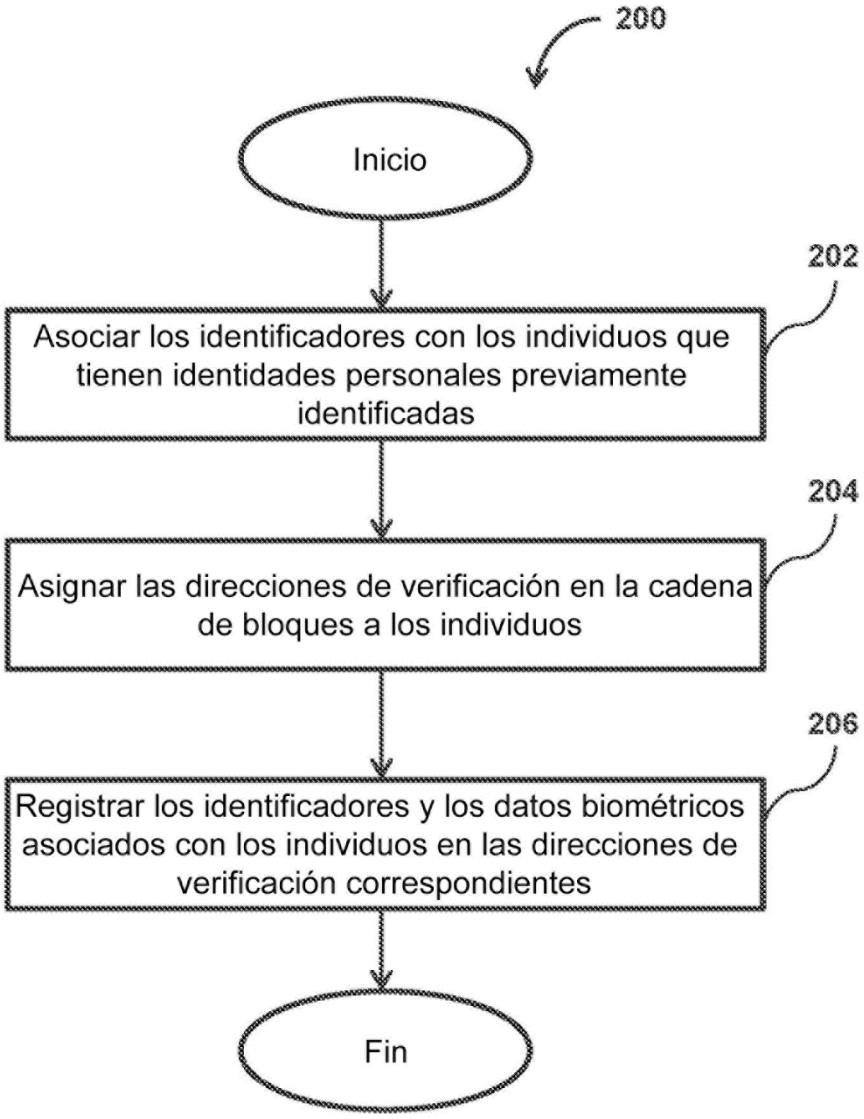
200
Inicio
202
Asociar los identificadores con los individuos que tienen identidades personales previamente identificadas
204
Asignar las direcciones de verificación en la cadena de bloques a los individuos
206
Registrar los identificadores y los datos biométricos asociados con los individuos en las direcciones de verificación correspondientes
Fin

FIG. 2

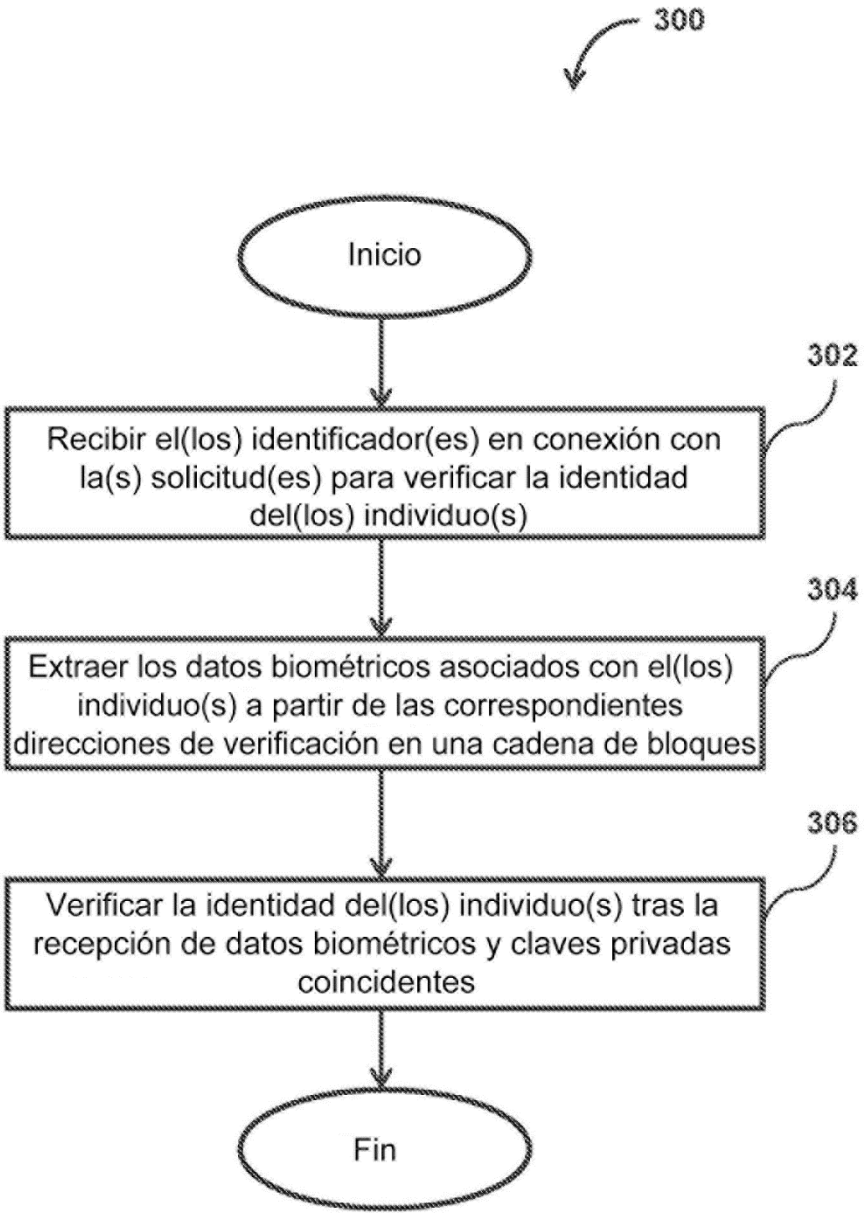
300
Inicio
302
Recibir el(los) identificador(es) en conexión con la(s) solicitud(es) para verificar la identidad del(los) individuo(s)
304
Extraer los datos biométricos asociados con el(los) individuo(s) a partir de las correspondientes direcciones de verificación en una cadena de bloques
306
Verificar la identidad del(los) individuo(s) tras la recepción de datos biométricos y claves privadas coincidentes
Fin

FIG. 3