

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

CAMPO DE LA DIVULGACIÓN

Esta divulgación se refiere a sistemas y métodos para proporcionar una verificación de identidad personal multifactorial basada en una cadena de bloques (*block chain*).

SÍNTESIS

Un aspecto de la divulgación 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* (soporte físico) configurados mediante instrucciones legibles por una máquina para establecer direcciones de verificación en una cadena de bloques y/o llevar a cabo la verificación de identidad personal multifactorial basada en una cadena de bloques utilizando las direcciones de verificación. El establecimiento de las direcciones de verificación en la cadena de bloques puede incluir la asociación de identificadores con individuos habiendo verificado previamente las identidades personales, asociándose un primer identificador con un primer individuo, donde el primer individuo tiene una identidad personal previamente verificada; la asignación de direcciones de verificación en una cadena de bloques a los individuos, donde una dirección de verificación determinada incluye una clave pública y una clave privada, asignándose una primera dirección de verificación al primer individuo, donde la primera dirección de verificación incluye una primera clave pública y una primera clave privada; y el registro de identificadores y

de datos biométricos asociados con los individuos en direcciones de verificación correspondientes, donde el primer identificador y los primeros datos biométricos asociados con el primer individuo se registran en la primera dirección de verificación. La realización de la verificación de la identidad personal multifactorial basada en una cadena de bloques mediante el uso de direcciones de verificación puede incluir la recepción de uno o varios identificadores en relación con una o varias peticiones de verificación de una identidad de uno o varios individuos, recibándose el primer identificador en relación con una petición de verificación de una identidad del primer individuo; extracción de los datos biométricos asociados con uno o varios individuos de las direcciones de verificación correspondientes, donde 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 varios individuos tras recibir datos biométricos y claves privadas coincidentes, verificándose la identidad personal del primer individuo 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 divulgación se refiere a un método para establecer direcciones de verificación en una cadena de bloques a fin de proporcionar una verificación de identidad personal multifactorial basada en una cadena de bloques. El método puede llevarse a cabo mediante uno o varios procesadores de *hardware* configurados mediante instrucciones legibles por una máquina. El método puede incluir la asociación de identificadores con individuos quienes ya han verificado previamente sus identidades personales, asociándose un primer identificador con un primer individuo, donde el primer individuo ya ha verificado con anterioridad su identidad personal; asignación de direcciones de verificación en una cadena de bloques a los individuos, donde una dirección de verificación determinada incluye una clave pública y una clave privada, asignándose una primera dirección de verificación al

primer individuo, donde la primera dirección de verificación incluye una primera clave pública y una primera clave privada; y el registro de identificadores y datos biométricos asociados con los individuos en direcciones de verificación correspondientes, registrándose el primer identificador y los primeros datos biométricos asociados con el primer individuo en la primera dirección de verificación.

Se puede verificar la identidad de uno o varios individuos tras recibir datos biométricos y claves privadas coincidentes, de tal modo que se puede verificar la identidad personal del primer individuo tras recibir (1) datos biométricos coincidentes con los primeros datos biométricos y (2) una clave privada que coincide con la primera clave privada.

Aún otro aspecto de la divulgación se refiere a un método para realizar una verificación de identidad personal multifactorial basada en una cadena de bloques utilizando direcciones de verificaciones. El método puede llevarse a cabo mediante uno o varios procesadores de *hardware* configurados mediante instrucciones legibles por una máquina. El método puede incluir la recepción de uno o varios identificadores en relación con una o varias peticiones de verificación de una identidad de uno o varios individuos, donde se recibe un primer identificador en relación con una petición de verificación de una identidad de un primer individuo; la extracción de datos biométricos asociados con uno o varios individuos de direcciones de verificación correspondientes en una cadena de bloques, donde una dirección de verificación determinada incluye una clave pública y una clave privada, donde los primeros datos biométricos asociados con el primer individuo se extraen de una primera dirección de verificación asignada al primer individuo, donde la primera dirección de verificación incluye una primera clave pública y una primera clave privada; y la verificación de la identidad de uno o varios individuos tras recibir datos biométricos y claves privadas coincidentes, donde la identidad personal del primer individuo se verifica tras la recepción de (1) los datos biométricos que coinciden con los primeros datos biométricos y (2) una

clave privada que coincide con la primera clave privada.

Estas y otras características, y las características de la presente tecnología, así como también los métodos de operación y las funciones de los elementos estructurales relacionados y la combinación de las partes y economías de fabricación, serán más evidentes al tener en cuenta la siguiente descripción y las reivindicaciones adjuntas con referencia a los dibujos acompañantes, todo en conjunto forma parte de la presente memoria descriptiva, donde los números de referencia similares designan partes correspondientes en las diversas figuras. Sin embargo, se entiende claramente que los dibujos son ilustrativos y descriptivos solamente y no tienen la intención de definir los límites de la invención. En el contexto de la memoria descriptiva y de las reivindicaciones, las formas en singular “un”, “una”, “el” y “la” incluyen los referentes en plural a menos que el contexto indique claramente lo contrario.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La FIG. 1 ilustra un sistema para proporcionar la verificación de identidad personal multifactorial basada en una cadena de bloques, de acuerdo con una o varias implementaciones.

La FIG. 2 ilustra un método para establecer direcciones de verificación en una cadena de bloques a fin de proporcionar la verificación de identidad personal multifactorial basada en una cadena de bloques, de acuerdo con una o varias implementaciones.

La FIG. 3 ilustra un método para realizar una verificación de identidad personal multifactorial basada en una cadena de bloques utilizando direcciones de verificación, de acuerdo con una o varias implementaciones.

DESCRIPCIÓN DETALLADA

La FIG. 1 ilustra un sistema 100 para proporcionar una verificación de identidad personal multifactorial basada en una cadena de bloques, de acuerdo con una o varias implementaciones. En algunas implementaciones, el sistema 100 puede incluir uno o varios servidores 102. El(los) servidor(es) 102 puede(n) estar configurado(s) para comunicarse con una o varias plataformas informáticas 104 de acuerdo con una arquitectura cliente/servidor, una arquitectura entre pares (“peer-to-peer”) y/u otras arquitecturas. Los usuarios pueden acceder al sistema 100 por medio de plataforma(s) informática(s) 104.

El(los) servidor(es) 102 puede(n) estar configurado(s) para ejecutar instrucciones legibles por una máquina 106. Las instrucciones legibles por una máquina 106 pueden incluir uno o varios de lo que sigue: un componente identificador de individuos 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 petición de verificación 116, un componente de extracción de información 118, un componente de verificación de identidad 120, y/u otros componentes de las instrucciones legibles por una máquina.

Las instrucciones legibles por una 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 estar basada en el protocolo de Bitcoin, en el protocolo de Ethereum, y/o en otros protocolos relacionados con monedas digitales y/o cadenas de bloques. Una copia completa de la cadena de bloques contiene toda transacción alguna vez realizada en una moneda digital asociada. Además de las transacciones, la cadena de bloques puede contener otra información, tal como se describe más adelante.

La cadena de bloques puede basarse en diversos bloques. Un bloque puede incluir un registro que contiene y confirma una o varias

transacciones en espera. Regularmente, (por ejemplo, aproximadamente cada un minuto), puede añadirse a la cadena de bloques un bloque nuevo que incluye transacciones y/u otra información. En algunas implementaciones, un bloque determinado en la cadena de bloques contiene un hash [función criptográfica] del bloque previo. Esto puede tener el efecto de crear una cadena de bloques a partir de un bloque génesis (es decir, el primer bloque en la cadena de bloques) a un bloque actual. Se puede garantizar que el bloque determinado venga cronológicamente después de un bloque previo debido a que el hash del bloque previo no sería conocido de otro modo. La modificación del bloque determinado puede ser poco práctica desde el punto de vista informático una vez que es incluido en la cadena de bloques ya que también tendría que regenerarse cada uno de bloques que le siguen.

Una dirección de verificación determinada puede incluir una ubicación específica en la cadena de bloques donde se almacena cierta información. En algunas implementaciones, se puede hacer referencia a una dirección de verificación individual como una "Dirección AtenVerify". Más adelante se describen en forma más detallada las direcciones de verificación en relación con el componente de asignación de direcciones de verificación 110.

El componente identificador de individuos 108 puede estar configurado para asociar identificadores con individuos que tienen identidades personales verificadas previamente. Por ejemplo, un primer identificador puede estar asociado con un primer individuo. El primer individuo puede tener una identidad personal previamente verificada. En términos generales, un identificador puede incluir uno o varios de lo siguiente: un número, un código alfanumérico, un nombre de usuario y/u otra información que puede estar vinculada con un individuo. En algunas implementaciones, un identificador de individuo puede ser denominado "Aten ID."

De acuerdo con algunas implementaciones, un individuo que tiene

una identidad personal previamente verificada pudo haber obtenido la identidad personal previamente verificada a través de diversos métodos. Por ejemplo, en algunas implementaciones, se le puede solicitar al individuo que proporcione evidencia de la identidad del individuo. Tal evidencia puede incluir una o varias de las siguientes posibilidades: proporcionar una copia de una identificación emitida por el gobierno (por ejemplo, pasaporte y/o la licencia de conducir), proporcionar una copia del correo electrónico recibido por el individuo (por ejemplo, una factura de un servicio público), evidencia proporcionada por un tercero, y/u otra evidencia sobre la identidad del individuo. La evidencia puede ser proporcionada a una entidad asociada con el(los) servidor(es) 102.

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

En general, puede utilizarse un par de claves pública y privada para el encriptado y desencriptado de acuerdo con uno o varios algoritmos de claves públicas. A modo de ejemplo no excluyente, se puede utilizar un par de claves para las firmas digitales. Un par de claves de ese tipo puede incluir una clave privada y una clave pública para verificación. La clave pública puede ser distribuida ampliamente, mientras que la clave privada se mantiene en secreto (por ejemplo, es conocida solamente por su propietario). Las claves pueden estar relacionadas matemáticamente, aunque el cálculo de la clave privada a partir de la clave pública es imposible.

En algunas implementaciones, el componente de asignación de direcciones de verificación 110 puede estar configurado de tal modo que se puedan almacenar las claves privadas dentro de plataforma(s)

informática(s) 104. Por ejemplo, la primera clave privada puede estar almacenada dentro de una plataforma informática 104 y/u otras ubicaciones asociadas con el primer individuo. De acuerdo con alguna implementación, se puede almacenar una clave privada en uno o más de: un archivo "verify.dat", una tarjeta SIM [módulo de identificación de suscripción, por sus siglas en inglés] y/o en otras ubicaciones.

En algunas implementaciones, el componente de asignación de direcciones de verificación 110 puede estar configurado de tal modo que puedan asignarse múltiples direcciones de verificación a diferentes individuos. Por ejemplo, además de la primera dirección de verificación, puede asignarse una segunda dirección de verificación al primer individuo. Puede asignarse una o varias direcciones de verificación adicionales al primer individuo, de acuerdo con una o varias implementaciones.

El componente de registro de direcciones 112 puede estar configurado para registrar identificadores y datos biométricos asociados con los individuos en direcciones de verificación correspondientes. Por ejemplo, el primer identificador y los primeros datos biométricos asociados con el primer individuo pueden estar registrados en la primera dirección de verificación. El registro de la información en una dirección de verificación determinada puede incluir el registro de un hash o de otra representación encriptada de la información. En algunas implementaciones, pueden registrarse diferentes datos biométricos en múltiples direcciones de verificación asignadas a un solo individuo determinado. Por ejemplo, además del primer identificador y de los primeros datos biométricos asociados con el primer individuo que se están registrando en la primera dirección de verificación, pueden registrarse el primer identificador y los segundos datos biométricos asociados con el primer individuo en una segunda dirección de verificación.

En general, los datos biométricos pueden incluir medidas

relacionadas con características humanas. Los identificadores biométricos son características medibles, distintivas, que se pueden utilizar para etiquetar y describir individuos. En general, los identificadores biométricos incluyen características fisiológicas, aunque también pueden incluir características conductuales y/u otras características. Las características fisiológicas pueden estar relacionadas con la figura del cuerpo de un individuo. Los ejemplos de características fisiológicas utilizadas como datos biométricos pueden incluir uno o varios de: huella digital, venas de la palma, reconocimiento facial, ADN, huella palmar, geometría de la mano, reconocimiento del iris, la 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: digitación, andares, voz, y/u otras características conductuales.

Los datos biométricos pueden incluir uno o varios de los siguientes: una imagen u otra representación visual de una característica fisiológica, un registro de una característica conductual, un patrón de una característica fisiológica y/o de una característica conductual, y/u otros datos biométricos. Un patrón puede incluir una síntesis de características relevantes extraídas de la fuente. Un patrón puede incluir uno o varios de los siguientes: un vector que describe características de un rasgo distintivo 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 otro tipo de información.

Los datos biométricos pueden ser recibidos por medio de plataformas informáticas 104 asociadas con los individuos. Por ejemplo, los datos biométricos asociados con un primer individuo pueden ser recibidos 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 ilustrado) configurado para capturar y/o registrar una característica fisiológica y/o característica conductual del primer individuo. Los ejemplos de un dispositivo de entrada de ese tipo pueden incluir uno o varios de los siguientes: una cámara y/u otro dispositivo de toma de imágenes, un escáner de huellas digitales, un micrófono, un acelerómetro, y/u otros dispositivos de entrada.

El componente de interfaz de usuario 114 puede estar configurado para proporcionar una interfaz para la presentación a individuos por medio de plataformas informáticas asociadas 104. La interfaz puede incluir una interfaz de usuario gráfica presentada por medio de plataformas informáticas individuales 104. De acuerdo con algunas implementaciones, la interfaz puede estar configurada para permitirle a un individuo determinado agregar o eliminar direcciones de verificación asignadas al individuo determinado siempre y cuando se asigne al menos una dirección de verificación al individuo determinado.

En algunas implementaciones, el componente de interfaz de usuario 114 puede estar configurado para acceder y/o gestionar uno o varios perfiles de los usuarios y/o información del usuario asociada con usuarios del sistema 100. Uno o varios perfiles de los usuarios y/o información del usuario pueden incluir información almacenada por el servidor(es) 102, una o varias plataforma(s) informática(s) 104, y/u otras ubicaciones de almacenamiento. Los perfiles de los usuarios pueden incluir, por ejemplo, información identificatoria de los usuarios (por ejemplo, un nombre de usuario o apodo, un número, un identificador, y/u otra información identificatoria), información de seguridad para el acceso (por ejemplo, un código de acceso o contraseña), información de la cuenta del sistema, información sobre la suscripción, información sobre la cuenta de moneda digital (por ejemplo, relacionada con la moneda mantenida en crédito para un usuario), información sobre relaciones (por ejemplo, información relacionada con relaciones entre usuarios en el sistema 100), información sobre el uso del sistema, información

demográfica asociada con los usuarios, historial de interacciones entre los usuarios en el sistema 100, información declarada por los usuarios, información sobre compras de los usuarios, historial de navegación de los usuarios, una identificación de la plataforma informática asociada con un usuario, un número telefónico asociado con un usuario, y/u otra información relacionada con los usuarios.

Las instrucciones legibles por una 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 petición de verificación 116 puede estar configurado para recibir uno o varios identificadores en relación con una o varias peticiones para verificar una identidad de uno o varios individuos. Por ejemplo, se puede recibir el primer identificador en relación con una petición para verificar una identidad del primer individuo. Pueden proporcionarse peticiones de verificación de identidad en relación con y/o relacionadas con transacciones financieras, intercambios de información, y/u otras interacciones. Pueden recibirse peticiones de otros individuos y/o de otros terceros.

El componente de extracción de información 118 puede estar configurado para extraer los datos biométricos asociados con uno o varios individuos de las direcciones de verificación correspondientes. Por ejemplo, los primeros datos biométricos asociados con el primer individuo pueden ser extraídos de la primera dirección de verificación. La extracción de información (por ejemplo, datos biométricos) de una dirección de verificación puede incluir información de descifrado.

De acuerdo con algunas implementaciones, el componente de extracción de información 118 puede estar configurado de tal modo que, como respuesta a la recepción de la petición de verificación de la identidad del primer individuo, se pueda proporcionar un “*prompt*” (símbolo del sistema) al primer individuo para solicitar datos biométricos

que coincidan con los primeros datos biométricos y una clave privada que coincida con la primera clave privada. El prompt puede ser transmitido por medio de una plataforma informática 104 asociada con el primer individuo. El prompt puede ser transmitido por medio de una interfaz de usuario gráfica y/u otra interfaz de usuario proporcionada por la plataforma informática 104 asociada con el primer individuo. El prompt puede incluir una indicación que sea una o varias indicaciones visuales, audibles, táctiles y/u otro tipo de indicaciones.

En algunas implementaciones, el componente de extracción de información 118 puede estar configurado de tal modo que, como respuesta a la recepción de la petición de verificación de la identidad del primer individuo, pueda proporcionarse un prompt a una plataforma informática 104 asociada con el primer individuo. El prompt puede hacer que la plataforma informática 104 proporcione automáticamente, al (a los) servidor(es) 102, datos biométricos que coincidan con los primeros datos biométricos y/o una clave privada que coincida con la primera clave privada.

El componente de verificación de identidad 120 puede estar configurado para verificar la identidad de uno o varios individuos al recibir, o como respuesta a la recepción de, datos biométricos y claves privadas coincidentes. Por ejemplo, se puede verificar la identidad personal del primer individuo al recibir (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 información recibida recientemente.

De acuerdo con algunas implementaciones, el componente de verificación de identidad 120 puede estar configurado de tal modo que se pueda verificar la identidad personal del primer individuo al recibir (1) datos biométricos que coinciden con los primeros datos biométricos o con los segundos datos biométricos y (2) una clave privada que coincide con

la primera clave privada. Las implementaciones de ese tipo pueden proporcionar las llamadas firmas "M-de-N" para la verificación de identidad donde se requiere cierto subconjunto de un conjunto más grande de información identificatoria.

En algunas implementaciones, el componente de verificación de identidad 120 puede estar configurado de tal modo que puedan utilizarse los datos biométricos que coinciden con los primeros datos biométricos y la clave privada que coincide con la primera clave privada para firmar la verificación de la identidad personal del primer individuo.

Una firma criptográfica es un mecanismo matemático que le permite a alguien probar su derecho de propiedad. En el caso de Bitcoin, una billetera Bitcoin y su(s) clave(s) privada(s) están vinculadas por cierta magia matemática. Cuando su *software* Bitcoin firma una transacción con la clave privada apropiada, toda la red puede ver que la firma coincide con las bitcoins que se están gastando. Sin embargo, el mundo jamás podrá adivinar su clave privada para robar sus bitcoins ganados con el sudor de la frente.

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

En algunas implementaciones, el(los) servidor(es) 102, las plataforma(s) informática(s) 104, y/o los recursos externos 122 pueden estar vinculados operativamente por medio de uno o varios enlaces de comunicación electrónica. Por ejemplo, pueden establecerse enlaces de comunicación electrónica de ese tipo, al menos parcialmente, por medio de una red tal como la Internet y/u otras redes. Se apreciará que esto no pretende ser una limitación, y que el alcance de la presente descripción incluye implementaciones en las cuales el(los) servidor(es) 102, la(s) plataforma(s) informática(s) 104, y/o los recursos

externos 122 pueden estar vinculados operativamente por medio de algún otro medio de comunicación.

Una plataforma informática determinada 104 puede incluir uno o varios procesadores configurados para ejecutar instrucciones legibles por una máquina. Las instrucciones legibles por una máquina pueden estar configuradas para permitir a un experto o usuario asociado con la plataforma informática determinada 104 comunicarse mediante interfaz con el sistema 100 y/o con los recursos externos 122, y/o proporcionar otra funcionalidad atribuida en la presente a la(s) plataforma(s) informática(s) 104. A modo de ejemplo no limitante, la plataforma informática determinada 104 puede incluir uno o varios de: una computadora de escritorio, una computadora portátil, una plataforma informática para tableta, una mini computadora portátil (NetBook), un teléfono inteligente, una consola de juegos, y/u otras plataformas informáticas.

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, algunas o todas las funciones atribuidas en la presente invención a los recursos externos 100 pueden ser proporcionadas por recursos incluidos en el sistema 100.

El(los) servidor(es) 102 puede(n) incluir almacenamiento electrónico 124, uno o varios procesadores 126, y/u otros componentes. El(los) servidor(es) 102 pueden incluir líneas de comunicación, o puertos para dar lugar al intercambio de información con una red y/u otras plataformas informáticas. La ilustración del(de los) servidor(es) 102 en la FIG. 1 no pretende ser limitativa. El(los) servidor(es) 102 puede(n) incluir una pluralidad de componentes de *hardware*, *software*, y/o *firmware* (microprogramación) que operan en forma conjunta para proporcionar la funcionalidad atribuida en la presente invención al(a los) servidor(es) 102. Por ejemplo, el(los) servidor(es) 102 puede(n) ser implementados por una

nube de plataformas informáticas que operan en forma conjunta como servidor(es) 102.

El almacenamiento electrónico 124 puede comprender un medio de almacenamiento no transitorio que almacena electrónicamente información. El medio de almacenamiento electrónico 124 puede incluir uno o ambos de los siguientes: almacenamiento del sistema que es proporcionado de manera integral (es decir, sustancialmente no removible) con el(los) servidor(es) 102 y/o almacenamiento removible que se puede conectar de manera removible al(a los) servidor(es) 102 por medio de, por ejemplo, un puerto (por ejemplo, un puerto USB, un puerto Firewire, etc.) o un lector (por ejemplo, un disco, etc.). El almacenamiento electrónico 124 puede incluir uno o varios medios de almacenamiento legibles ópticamente (por ejemplo, discos ópticos, etc.), medios de almacenamiento legibles magnéticamente (por ejemplo, cinta magnética, disco duro magnético, disquetera, etc.), medios de almacenamiento basados en carga eléctrica (por ejemplo, EEPROM, RAM, etc.), medios de almacenamiento en estado sólido (por ejemplo, USB, etc.), y/u otros medios de almacenamiento legibles electrónicamente. El almacenamiento electrónico 124 puede incluir uno o varios 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(de los) servidor(es) 102, información recibida de plataforma(s) informática(s) 104, y/u otra información que permita al(a los) servidor(es) 102 funcionar según lo descrito en la presente invención.

El(los) procesador(es) 126 pueden estar configurados para proporcionar capacidades de procesamiento de información en el(los) servidor(es) 102. Como tal(es), el(los) procesador(es) 126 puede(n) incluir uno o varios procesadores digitales, procesadores análogos, circuitos digitales diseñados para procesar información, circuitos análogos para

procesar información, máquina de estado y/u otros mecanismos para el procesamiento electrónico de la información. Si bien el(los) procesador(es) 126 se muestra(n) en la FIG. 1 como una entidad única, esto tiene propósitos ilustrativos solamente. En algunas implementaciones, el(los) procesador(es) 126 puede(n) incluir una pluralidad de unidades de procesamiento. Estas unidades de procesamiento pueden estar ubicadas físicamente dentro del mismo dispositivo, o el(los) procesador(es) 126 puede(n) representar una funcionalidad de procesamiento de una pluralidad de dispositivos que operan en coordinación. El(los) procesador(es) 126 puede(n) estar configurado(s) para ejecutar componentes de las instrucciones legibles por una máquina 108, 110, 112, 114, 116, 118, 120, y/u otros componentes de las instrucciones legibles por una máquina. El(los) procesador(es) 126 puede(n) estar configurado(s) para ejecutar componentes de las instrucciones legibles por una máquina 108, 110, 112, 114, 116, 118, 120, y/u otros componentes de las instrucciones legibles por una máquina mediante *software*; *hardware*; *firmware*; alguna combinación de *software*, *hardware*, y/o *firmware*; y/u otros mecanismos para configurar capacidades de procesamiento en el(los) procesador(es) 126. En el presente contexto, el término "componente de las instrucciones legibles por una máquina" puede hacer referencia a cualquier componente o conjunto de componentes que realizan la funcionalidad atribuida al componente de las instrucciones legibles por una máquina. Esto puede incluir uno o varios procesadores físicos durante la ejecución de instrucciones legibles por un procesador, las instrucciones legibles por un procesador, circuitos, *hardware*, medio de almacenamiento o cualquier otro componente.

Debe apreciarse que si bien los componentes de las instrucciones legibles por una máquina 108, 110, 112, 114, 116, 118, y 120 son ilustrados en la FIG. 1 como estando implementados dentro de una única unidad de procesamiento, en implementaciones en las cuales el(los)

procesador(es) 126 incluye múltiples unidades de procesamiento, uno o varios componentes de las instrucciones legibles por una máquina 108, 110, 112, 114, 116, 118, y/o 120 pueden ser implementados en forma remota de los otros componentes de las instrucciones legibles por una máquina. La descripción de la funcionalidad proporcionada por los diferentes componentes de las instrucciones legibles por una máquina 108, 110, 112, 114, 116, 118, y/o 120 descritos más adelante tiene fines ilustrativos, y no pretende ser una limitación, ya que cualquier componente de las instrucciones legibles por una máquina 108, 110, 112, 114, 116, 118, y/o 120 puede proporcionar más o menos funcionalidad que la descrita. Por ejemplo, puede eliminarse uno o varios componentes de las instrucciones legibles por una máquina 108, 110, 112, 114, 116, 118, y/o 120, y algo o la totalidad de su funcionalidad puede ser proporcionada por otros componentes de las instrucciones legibles por una máquina 108, 110, 112, 114, 116, 118, y/o 120. Como otro ejemplo, el(los) procesador(es) 126 puede(n) estar configurado(s) para ejecutar uno o varios componentes de las instrucciones legibles por una máquina adicionales que pueden llevar a cabo de manera parcial o total la funcionalidad atribuida más adelante a uno de los componentes de las instrucciones legibles por una máquina 108, 110, 112, 114, 116, 118, y/o 120.

La FIG. 2 ilustra un método 200 para establecer direcciones de verificación en una cadena de bloques a fin de proporcionar una verificación de la identidad personal multifactorial basada en la cadena de bloques, de acuerdo con una o varias implementaciones. Las operaciones del método 200 presentadas más adelante tienen el propósito de ser ilustrativas. En algunas implementaciones, el método 200 puede llevarse a cabo con una o varias operaciones adicionales no descritas, y/o sin uno o varias de las operaciones descritas. Adicionalmente, el orden en que se ilustran las operaciones del método 200 en la FIG. 2 y se describen más adelante no tiene el propósito de ser limitante.

En algunas implementaciones, puede implementarse una o varias operaciones del método 200 en uno o varios dispositivos de procesamiento (por ejemplo, un procesador digital, un procesador análogo, un circuito digital diseñado para procesar información, un circuito análogo diseñado para procesar información, una máquina de estado, y/u otros mecanismos para procesar información electrónicamente). Uno o varios dispositivos de procesamiento pueden incluir uno o varios dispositivos que ejecutan algunas o todas las operaciones del método 200 como respuesta a instrucciones almacenadas electrónicamente en un medio de almacenamiento electrónico. Uno o varios dispositivos de procesamiento pueden incluir uno o varios dispositivos configurados a través de *hardware*, *firmware*, y/o *software* para ser diseñados específicamente para la ejecución de una o varias operaciones del método 200.

En una operación 202, los identificadores pueden estar asociados con individuos que tengan identidades personales previamente verificadas. Un primer identificador puede estar asociado con un primer individuo. El primer individuo puede tener una identidad personal previamente verificada. La operación 202 puede ser realizada por uno o varios procesadores de *hardware* configurados para ejecutar un componente de las instrucciones legibles por una máquina que es el mismo que el componente identificador de individuos 18 o similar (según lo descrito en relación con la FIG. 1), de acuerdo con una o varias implementaciones.

En una operación 204, pueden asignarse direcciones de verificación en una cadena de bloques a los individuos. Una dirección de verificación determinada puede incluir una clave pública y una clave privada. Puede asignarse una primera dirección de verificación al primer individuo. La primera dirección de verificación puede incluir una primera clave pública y una primera clave privada. Puede llevarse a cabo la operación 204 por medio de uno o varios procesadores de *hardware*

configurados para ejecutar un componente de instrucciones legibles por una máquina que es igual o similar al componente de asignación de direcciones de verificación 110 (según lo descrito en relación con la FIG. 1), de acuerdo con una o varias implementaciones.

En una operación 206, pueden registrarse identificadores y datos biométricos asociados con los individuos en direcciones de verificación correspondientes. Pueden registrarse el primer identificador y los primeros datos biométricos asociados con el primer individuo en la primera dirección de verificación. La identidad de uno o varios individuos puede ser verificable al recibir, o como respuesta a la recepción de, datos biométricos y claves privadas coincidentes. Se puede verificar la identidad personal del primer individuo al recibir, o como respuesta a la recepción de, (1) datos biométricos coincidentes con los primeros datos biométricos y (2) una clave privada que coincide con la primera clave privada. La operación 206 puede ser llevada a cabo por uno o más procesadores de *hardware* configurados para ejecutar un componente de las instrucciones legibles por una máquina que es el mismo o similar al componente de registro de direcciones 112 (según lo descrito en relación con la FIG. 1), de acuerdo con una o varias implementaciones.

La FIG. 3 ilustra un método 300 para llevar a cabo una verificación de identidad personal multifactorial basada en la cadena de bloques utilizando direcciones de verificación, de acuerdo con una o varias implementaciones. Las operaciones del método 300 presentadas más adelante tienen el propósito de ser ilustrativas. En algunas implementaciones, se puede llevar a cabo el método 300 con una o varias operaciones adicionales no descritas, y/o sin una o varias de las operaciones descritas. Adicionalmente, el orden en el cual se ilustran y describen más adelante las operaciones del método 300 en la FIG. 3 no tiene el propósito de ser limitativo.

En algunas implementaciones, el método 300 puede ser implementado en uno o varios dispositivos de procesamiento (por

ejemplo, un procesador digital, un procesador análogo, un circuito digital diseñado para procesar información, un circuito análogo diseñado para procesar información, una máquina de estado, y/u otros mecanismos para el procesamiento electrónico de la información). Uno o varios dispositivos de procesamiento pueden incluir uno o varios dispositivos que ejecutan algunas o todas las operaciones del método 300 como respuesta a las instrucciones almacenadas electrónicamente en un medio de almacenamiento electrónico. Uno o varios dispositivos de procesamiento pueden incluir uno o varios dispositivos configurados a través de *hardware*, *firmware*, y/o *software* para estar específicamente diseñados para la ejecución de una o varias operaciones del método 300.

En una operación 302, puede recibirse uno o varios identificadores en relación con una o varias peticiones de verificación de una identidad de uno o varios individuos. Puede recibirse un primer identificador en relación con una petición de verificación de una identidad de un primer individuo. La operación 302 puede ser realizada por uno o varios procesadores de *hardware* configurados para ejecutar un componente de instrucciones legibles por una máquina que es el mismo o similar al componente de petición de verificación 116 (según lo descrito en relación con la FIG. 1), de acuerdo con una o varias implementaciones.

En una operación 304, pueden extraerse los datos biométricos asociados con uno o varios individuos de direcciones de verificación correspondientes en una cadena de bloques. Una dirección de verificación determinada puede incluir una clave pública y una clave privada. Pueden extraerse los primeros datos biométricos asociados con el primer individuo 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 varios procesadores de *hardware* configurados para ejecutar un componente de instrucciones legibles por

una máquina que es igual o similar al componente de extracción de información 118 (según lo descrito en relación con la FIG. 1), de acuerdo con una o varias implementaciones.

En una operación 306, puede verificarse la identidad de uno o varios individuos tras la recepción, o como respuesta a la recepción, de datos biométricos y claves privadas coincidentes. Se puede verificar la identidad personal del primer individuo tras la recepción, o como 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 ser realizada por uno o varios procesadores de *hardware* configurados para ejecutar un componente de instrucciones legibles por una máquina que es el mismo que el componente de verificación de identidad 120 o similar al dicho componente (según lo descrito en relación con la FIG. 1), de acuerdo con una o varias implementaciones.

Ejemplos de implementaciones pueden facilitar el almacenamiento de datos personales en la cadena de bloques. Pueden almacenarse los datos personales en la cadena de bloques en forma encriptada. Una persona puede ser identificada en el nivel de la cadena de bloques con uno o varios de los siguientes: una clave privada, una huella digital, un hash huella digital, una retina ocular, un hash de la retina ocular, y/u otra información única. Los datos almacenados pueden incluir, o se refieren a, uno o varios de los siguientes: un pasaporte, una cédula de identidad, información extraída del pasaporte, un carnet de conducir, información extraída del carnet de conducir, huella digital, retina ocular, y/u otra información. De acuerdo con algunas implementaciones, si se modifica algún dato, se puede crear un nuevo registro para esa persona en la cadena de bloques. Es decir, todos los cambios son agregados como nuevos registros. El registro anterior quedará siempre almacenado en la cadena de bloques. En general, todos los registros en la cadena de bloques son almacenados para siempre y no pueden ser eliminados.

Habr   m  s de una copia de la cadena de bloques para garantizar que los registros no sean manipulados.

Los ejemplos de las implementaciones pueden facilitar el acceso a los datos personales. Puede haber m  ltiples niveles de acceso para los datos personales en la cadena de bloques. Pueden generarse controles de acceso en niveles de pares de claves p  blicas/privadas. Los ejemplos de niveles de acceso pueden incluir uno o varios niveles entre los siguientes: Super Admin (total acceso a la cadena de bloques), Nivel de autoridades de pa  s (total acceso de solo lectura), Nivel autoridades estatales/locales (acceso limitado de solo lectura), Polic  a y otros servicios incluido Emergencia (acceso a ciertos datos personales por huella digital/retina ocular de esa persona solamente, Comerciantes Participantes (acceso limitado) y/u otros niveles de acceso.

Ejemplos de implementaciones pueden facilitar el control de la verificaci  n. Puede haber m  ltiples niveles para el modo en que es posible realizar el control de la verificaci  n. Por ejemplo, algunas implementaciones pueden garantizar que una persona tenga un registro en "Compa   a" pero no se proporciona informaci  n personal alguna. Algunas implementaciones pueden garantizar que una persona tenga un registro en Compa   a y obtener informaci  n muy b  sica tal como Nombre Completo, Fecha de Nacimiento, Sexo, y/u otra informaci  n b  sica. Algunas implementaciones pueden garantizar que una persona tenga un registro en Compa   a y obtener todos los datos personales.

Si bien la presente tecnolog  a ha sido descrita en forma detallada con fines ilustrativos sobre la base de lo que se considera en la actualidad que son las implementaciones m  s pr  cticas y preferidas, debe entenderse que un detalle de ese tipo tiene ese   nico prop  sito y que la tecnolog  a no se encuentra limitada a las implementaciones descritas, sino que, por el contrario, tiene el prop  sito de cubrir las modificaciones y disposiciones equivalentes que se encuentran dentro del esp  ritu y

alcance de las reivindicaciones adjuntas. Por ejemplo, debe entenderse que la presente tecnología contempla que, en la medida de lo posible, puede combinarse una o varias características de cualquier implementación con una o varias características de cualquier otra implementación.

REIVINDICACIONES

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

uno o varios procesadores de *hardware* configurados mediante instrucciones legibles por una máquina para:

establecer direcciones de verificación en una cadena de bloques mediante:

asociación de identificadores con individuos que tienen identidades personales previamente verificadas, estando asociado un primer identificador con un primer individuo, teniendo el primer individuo una identidad personal previamente verificada;

asignación de direcciones de verificación en una cadena de bloques a los individuos, donde una dirección de verificación determinada incluye una clave pública y una clave privada, asignándose una primera dirección de verificación al primer individuo, donde 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 direcciones de verificación correspondientes, donde 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 una cadena de bloques utilizando las direcciones de verificación mediante:

recepción de uno o varios identificadores en relación con una o varias peticiones de verificación de una identidad de uno o varios individuos, donde se recibe el primer identificador en relación con una petición de verificación de una identidad del

primer individuo;

extracción de los datos biométricos asociados con uno o varios individuos de las direcciones de verificación correspondientes, donde 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 varios individuos tras recibir datos biométricos y claves privadas coincidentes, donde 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 acuerdo con la reivindicación 1, donde la primera clave privada es almacenada dentro de una plataforma informática asociada con el primer individuo.

3. El sistema de acuerdo con la reivindicación 1, donde se asignan múltiples direcciones de verificación a individuos separados de tal modo que, además de la primera dirección de verificación, se asigna una segunda dirección de verificación al primer individuo.

4. El sistema de acuerdo con la reivindicación 1, donde uno o varios procesadores de *hardware* están adicionalmente configurados mediante instrucciones legibles por una máquina para proporcionar una interfaz para la presentación a individuos por medio de plataformas informáticas asociadas, configurándose la interfaz para permitir que un individuo determinado añada o elimine direcciones de verificación asignadas al individuo determinado siempre y cuando se asigne al menos una dirección de verificación al individuo determinado.

5. El sistema de acuerdo con la reivindicación 1, donde se registran diferentes datos biométricos en múltiples direcciones de verificación asignadas a un individuo determinado de tal modo que, además del registro en la primera dirección de verificación del primer identificador y de los primeros datos biométricos asociados con el primer individuo, se registra en la segunda dirección de verificación el primer identificador y los segundos datos biométricos asociados con el primer individuo.

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

7. El sistema de acuerdo con la reivindicación 1, donde los datos biométricos incluyen uno o varios de los siguientes: una imagen, un registro o un patrón.

8. El sistema de acuerdo con la reivindicación 1, donde los datos biométricos se relacionan con uno o varios de los siguientes: una huella digital, venas palmares, reconocimiento facial, ADN, huella palmar, geometría de la mano, reconocimiento del iris, retina, olor o aroma, digitación, andares o la voz.

9. El sistema de acuerdo con la reivindicación 1, donde se reciben los primeros datos biométricos por medio de una plataforma informática asociada con el primer individuo.

10. El sistema de acuerdo con la reivindicación 1, donde uno o varios procesadores de *hardware* están adicionalmente configurados mediante instrucciones legibles por una máquina para recibir, responder a

la recepción de, la petición de verificación de la identidad del primer individuo, solicitar al primer individuo datos biométricos coincidentes con los primeros datos biométricos y una clave privada que coincida con la primera clave privada, siendo transmitido el prompt por medio de una plataforma informática asociada con el primer individuo.

11. El sistema de acuerdo con la reivindicación 1, donde uno o varios procesadores de *hardware* están adicionalmente configurados mediante instrucciones legibles por una máquina para recibir, responder a la recepción de, la petición de verificación de la identidad del primer individuo, solicitar a una plataforma informática asociada con el primer individuo que proporcione automáticamente datos biométricos coincidentes con los primeros datos biométricos y una clave privada coincidente con la primera clave privada.

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

13. El sistema de acuerdo con la reivindicación 1, donde al menos un nodo dedicado realiza la firma de la verificación de la identidad personal del primer individuo.

14. Un método para establecer direcciones de verificación en una cadena de bloques a fin de proporcionar la verificación de la identidad personal multifactorial basada en una cadena de bloques, llevándose a cabo el método mediante uno o varios procesadores de *hardware* configurados mediante instrucciones legibles por una máquina, comprendiendo el método:

asociación de identificadores con individuos que tienen

identidades personales previamente verificadas, estando asociado un primer identificador con un primer individuo, teniendo el primer individuo una identidad personal previamente verificada;

asignación de direcciones de verificación en una cadena de bloques a los individuos, donde una dirección de verificación determinada incluye una clave pública y una clave privada, asignándose una primera dirección de verificación al primer individuo, donde 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 direcciones de verificación correspondientes, donde el primer identificador y los primeros datos biométricos asociados con el primer individuo se registran en la primera dirección de verificación;

donde se puede verificar la identidad de uno o varios individuos tras recibir datos biométricos y claves privadas coincidentes, pudiéndose verificar la identidad personal del primer individuo tras la recepción de (1) datos biométricos coincidentes con los primeros datos biométricos y (2) una clave privada coincidente con la primera clave privada.

15. El método de acuerdo con la reivindicación 14, el cual comprende además la asignación de múltiples direcciones de verificación para separar individuos de tal modo que, además de la primera dirección de verificación, se asigna una segunda dirección de verificación al primer individuo.

16. El método de acuerdo con la reivindicación 14, el cual comprende además la provisión de una interfaz para la presentación a individuos por medio de plataformas informáticas asociadas, configurándose la interfaz para permitir que un individuo determinado

añada o elimine direcciones de verificación asignadas al individuo determinado siempre y cuando se asigne al menos una dirección de verificación al individuo determinado.

17. El método de acuerdo con la reivindicación 14, el cual comprende además el registro de diferentes datos biométricos en múltiples direcciones de verificación asignadas a un individuo determinado de tal modo que, además del registro en la primera dirección de verificación del primer identificador y de los primeros datos biométricos asociados con el primer individuo, se registran en la segunda dirección de verificación el primer identificador y los segundos datos biométricos asociados con el primer individuo.

18. Un método para llevar a cabo la verificación de la identidad personal multifactorial basada en una cadena de bloques utilizando direcciones de verificación, llevándose a cabo el método por uno o varios procesadores de *hardware* configurados mediante instrucciones legibles por una máquina, comprendiendo el método:

la recepción de uno o varios identificadores en relación con una o varias peticiones de verificación de una identidad de uno o varios individuos, donde se recibe un primer identificador en relación con una petición de verificación de una identidad de un primer individuo;

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

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

19. El método de acuerdo con la reivindicación 18, el cual comprende además, como respuesta a la recepción de la petición de verificación de la identidad del primer individuo:

la solicitud al primer individuo de datos biométricos coincidentes con los primeros datos biométricos y de una clave privada coincidente con la primera clave privada, transmitiéndose el prompt por medio de una plataforma informática asociada con el primer individuo; o

la solicitud a una plataforma informática asociada con el primer individuo de que proporcione automáticamente datos biométricos coincidentes con los primeros datos biométricos y una clave privada coincidente con la primera clave privada.

20. El método de acuerdo con la reivindicación 18, en el cual los datos biométricos coincidentes con los primeros datos biométricos y la clave privada coincidente con la primera clave privada se utilizan para firmar la verificación de la identidad personal del primer individuo.

RESUMEN

Puede proporcionarse la verificación de la identidad personal multifactorial basada en una cadena de bloques. Pueden establecerse direcciones de verificación en una cadena de bloques mediante: la asociación de identificadores con individuos que tienen identidades personales previamente verificadas, la asignación de direcciones de verificación en una cadena de bloques a los individuos, y el registro de identificadores y datos biométricos asociados con los individuos en direcciones de verificación correspondientes. Puede realizarse una verificación de identidad personal multifactorial basada en una cadena de bloques utilizando las direcciones de verificación mediante: la recepción de uno o varios identificadores en relación con una o varias peticiones de verificación de una identidad de uno o varios individuos, la extracción de los datos biométricos asociados con uno o varios individuos de las direcciones de verificación correspondientes, y la verificación de la identidad de uno o varios individuos tras recibir datos biométricos y claves privadas coincidentes.