(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 894 500**

(51) Int. CI.:

H04L 9/32 (2006.01)
H04L 9/06 (2006.01)
G06F 21/41 (2013.01)
H04L 29/06 (2006.01)
G06F 21/62 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **01.02.2017 PCT/US2017/016061**

(87) Fecha y número de publicación internacional: **09.08.2018 WO18143983**

(96) Fecha de presentación y número de la solicitud europea: **01.02.2017 E 17894846 (9)**

(97) Fecha y número de publicación de la concesión europea: **14.07.2021 EP 3577850**

(54) Título: **Verificación de una identidad basada en múltiples fuentes de datos distribuidas utilizando una cadena de bloques para salvaguardar la identidad**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
14.02.2022

(73) Titular/es:

EQUIFAX, INC. (100.0%)
1550 Peachtree Street, N. W.
Atlanta, GA 30309, US

(72) Inventor/es:

KRISHNAMACHARYA, SRI;
LE, QUANG;
TIGRETT, STAN y
AYRES, RUSS

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Verificación de una identidad basada en múltiples fuentes de datos distribuidas utilizando una cadena de bloques para salvaguardar la identidad

Campo técnico

Esta descripción en general se relaciona con la información seguridad y, más particularmente, se relaciona con la verificación de una identidad basada en múltiples fuentes de datos distribuidas utilizando una cadena de bloques para salvaguardar la identidad.

Estado de la técnica

Una entidad (por ejemplo, un individuo o una empresa) puede tener una identidad en línea basada en una variedad de información o características sobre la entidad, los activos asociados con la entidad o los dispositivos asociados con la entidad. La identidad en línea puede ser utilizada por un servicio en línea para distinguir la entidad de otras entidades antes de una transacción, a través del servicio en línea, entre la entidad y el servicio en línea.

Se pueden utilizar diferentes fuentes de identidad o formas de identificación para proporcionar una prueba de una identidad en línea. Por ejemplo, un individuo puede tener varias formas diferentes de identificación, incluida información de identificación personal (por ejemplo, un número de licencia de conducir, un número de seguridad social, etc.) o biométrica (por ejemplo, una huella dactilar). Un servidor que ejecuta un servicio en línea puede solicitar una combinación de fuentes de identificación de un dispositivo informático asociado con una entidad remota para verificar la identidad en línea de la entidad remota antes de que el servidor proporcione a la entidad remota un producto, servicio, o acceso a información sensible. Diferentes servicios en línea pueden solicitar diferentes formas de identificación. Por ejemplo, un servidor que ejecuta un sitio web para un proveedor de préstamos puede solicitar información tal como un número de seguro social, un nombre y un historial crediticio, mientras que un servidor que ejecuta un sitio web para un proveedor de automóviles de alquiler puede solicitar un número de licencia de conducir, un número de tarjeta de crédito y una dirección particular.

Algunas de las fuentes de identificación pueden tener un larga vida. Por ejemplo, un número de seguro social o una dirección postal pueden estar asociados con una persona determinada durante muchos años. Por lo tanto, proporcionar múltiples fuentes de identificación que tengan una larga vida a los servicios en línea puede exponer a una entidad al riesgo de robo de identidad si las comunicaciones electrónicas de estas fuentes de identificación son interceptadas por partes distintas de los servicios en línea. El documento EP 2809042 A1 describe un procedimiento para autenticar a un usuario asociado a un agente/cliente de usuario implementado sobre un protocolo SIP, utilizando tokens OAuth obtenidos a partir de un servicio de tokens de seguridad STS) OAuth en el que se reconoce al usuario. El documento US 2013/0047218 A1 describe un procedimiento y un sistema para aplicar la itinerancia entre redes heterogéneas.

Compendio

La invención es como se especifica en las reivindicaciones. Se divulgan aspectos y ejemplos para verificar una identidad basada en múltiples fuentes de datos distribuidas utilizando una cadena de bloques para salvaguardar la identidad. Por ejemplo, un dispositivo de procesamiento puede recibir una solicitud de un token de una entidad para autenticar una identidad en línea de la entidad en un servicio en línea. El dispositivo de procesamiento puede almacenar la solicitud en una cadena de bloques que representa la identidad en línea de la entidad añadiendo un nuevo bloque a la cadena de bloques. Una cadena de bloques puede ser una base de datos con bloques ordenados que se generan en base a una o más fuentes de identidad que representan información de identificación personal de la entidad. El nuevo bloque que se ha añadido a la cadena de bloques puede incluir datos que indican la solicitud del token. El dispositivo de procesamiento puede generar el token basado en los bloques ordenados de la cadena de bloques. El dispositivo de procesamiento puede transmitir el token a la entidad y, posteriormente, recibir el token del servicio en línea. El dispositivo de procesamiento puede transmitir, basándose en la recepción del token del servicio en línea, una confirmación de la identidad en línea de la entidad al servicio en línea. Opcionalmente, la cadena de bloques es una primera cadena de bloques, y el dispositivo de procesamiento también puede verificar, basándose en el token, una identidad del servicio en línea basada en una segunda cadena de bloques que representa la identidad en línea del servicio en línea, y verificar que la entidad ha solicitado el token para autenticar la identidad en línea de la entidad en el servicio en línea.

Este ejemplo ilustrativo se menciona no para limitar o definir la invención, sino para ayudar a comprenderla. Otros aspectos, ventajas y rasgos característicos de la presente invención resultarán evidentes después de revisar la descripción completa y las figuras, que incluye las siguientes secciones: breve descripción de las figuras, descripción detallada, y reclamaciones.

Breve descripción de los dibujos

Muchos aspectos de la presente descripción pueden comprenderse mejor en referencia a los siguientes diagramas. Los dibujos no están necesariamente a escala, sino que se pone el énfasis en ilustrar claramente determinados rasgos característicos de la descripción.

La FIGURA 1 representa un ejemplo de un entorno informático para verificar una identidad basada en múltiples fuentes de datos distribuidas utilizando una cadena de bloques para salvaguardar la identidad según un aspecto de la presente descripción.

La FIGURA 2 representa un ejemplo de una cadena de bloques que representa una identidad en línea según un aspecto de la presente descripción.

La FIGURA 3 representa un ejemplo de un sistema de servicio de identidad para verificar una identidad basada en múltiples fuentes de datos distribuidas que utilizan una cadena de bloques para salvaguardar la identidad según un aspecto de la presente descripción.

La FIGURA 4 representa otro ejemplo de un sistema de servicio de identidad para verificar una identidad basada en múltiples fuentes de datos distribuidas que utilizan una cadena de bloques para salvaguardar la identidad según un aspecto de la presente descripción.

La FIGURA 5 representa un ejemplo de un flujo de información en un entorno informático para verificar una identidad basada en múltiples fuentes de datos distribuidas utilizando una cadena de bloques para salvaguardar la identidad según un aspecto de la presente descripción.

La FIGURA 6 representa un ejemplo de un diagrama de flujo de un proceso para verificar una identidad basada en múltiples fuentes de datos distribuidas utilizando una cadena de bloques para salvaguardar la identidad según un aspecto de la presente descripción.

La FIGURA 7 representa un ejemplo de un sistema de servicio de identidad para verificar una identidad basada en múltiples fuentes de datos distribuidas utilizando una cadena de bloques para salvaguardar la identidad según un aspecto de la presente descripción.

Descripción detallada

Determinados aspectos de esta descripción se relacionan con la verificación de una identidad basada en múltiples fuentes de datos distribuidas utilizando una cadena de bloques para salvaguardar la identidad. Un sistema de servicio de identidad puede procesar múltiples fuentes de identidad (por ejemplo, documentos emitidos por el gobierno o medidas biométricas) asociadas con una entidad (por ejemplo, un individuo o una empresa) para generar una cadena de bloques que representa una identidad en línea para la entidad. Una cadena de bloques puede ser una base de datos que incluye múltiples bloques de datos que están enlazados en serie, donde cada bloque de datos es resistente al cambio y se añaden nuevos datos a la cadena de bloques añadiendo un nuevo bloque de datos al final de la cadena de bloques. El sistema de servicio de identidad puede generar una cadena de bloques que representa una identidad en línea vinculando bloques de datos codificados formados a partir de fuentes de identidad asociadas con una entidad. El almacenamiento de la identidad en una cadena de bloques puede permitir que el sistema de servicios de identidad genere tokens de un solo uso para autenticar la identidad en línea de una entidad en un servicio en línea. Un token puede incluir una señal, un paquete de información o un segmento de código que representa información que se puede transferir entre dispositivos informáticos. En algunos aspectos, el uso de tokens puede permitir que se verifiquen las identidades de las entidades sin que los servicios en línea accedan a las fuentes de identidad.

En algunos aspectos, las fuentes de identidad pueden incluir uno o más de una variedad de formatos (por ejemplo, datos de texto, datos biométricos y datos de identidad digital) asociados con una entidad que es, por ejemplo, un consumidor. Cada fuente de identidad o formato de fuente de identidad se puede almacenar por separado en una base de datos segura, que está acoplada (o incluida en) de forma comunicativa con el sistema de servicio de identidad. Se puede generar una identidad en línea utilizando datos basados en texto (por ejemplo, un número de seguro social ("SSN"), un nombre, una dirección o un número de licencia de conducir). También se puede generar una identidad en línea utilizando datos biométricos, que pueden basarse en una característica almacenada de la entidad, como un rostro, voz, huella dactilar, iris o ADN. El sistema de servicio de identidad puede almacenar un archivo de imagen real o una plantilla personalizada extraída de una imagen original. También se puede generar una identidad en línea basada en la identidad digital de los dispositivos asociados con la entidad, tal como un identificador de dispositivo móvil (por ejemplo, una dirección MAC), una identificación de dispositivo de Internet de las cosas, un número de teléfono o una ubicación geográfica. El sistema de servicio de identidad puede codificar las fuentes de identidad y enlazar las fuentes de identidad para formar una cadena de bloques que represente la identidad en línea. Puede utilizarse cualquier proceso de codificación adecuado para codificar valores de datos en una cadena de bloques (por ejemplo, los valores de datos pueden ser hash mediante una función hash para ofuscar los datos).

Un sistema de servicio de identidad puede añadir nuevos bloques ordenados a la cadena de bloques en respuesta a la recepción de nuevas fuentes de identidad o transacciones de identidad (por ejemplo, un evento de autenticación en el que el sistema de servicio de identidad recibe una solicitud de autenticación de una identidad en línea). Cada bloque ordenado puede tener una marca de tiempo y puede ser resistente a la modificación. Por lo tanto, la cadena de bloques puede representar un historial de la identidad en línea asociada con la entidad. En una transacción de identidad, se puede generar un valor hash basado en la cadena de bloques. Al añadir un nuevo bloque ordenado a la cadena de bloques se puede modificar el valor hash asociado con la cadena de bloques de modo que el valor hash cambia en respuesta a cada transacción de identidad.

En algunos aspectos, se puede generar un token para verificar la identidad de una entidad paren un servicio en línea (u otra entidad) mientras impide que el servicio en línea acceda a cualquier dato que pueda utilizarse para determinar una fuente de identidad asociado con la entidad. Por ejemplo, un servidor que ejecuta un sitio web para un proveedor de alquiler de automóviles puede solicitar la verificación de que una entidad tiene una licencia de conducir y está

asociada con una tarjeta de crédito antes de completar una transacción de alquiler. El sistema de servicio de identidad puede verificar que la entidad tiene licencia de conducir y que la entidad está asociada a la tarjeta de crédito. El sistema de servicio de identidad puede generar un token que es un paquete de información con un valor hash basado en la cadena de bloques actual y una dirección del servidor. El sistema de servicio de identidad puede transmitir el token a un dispositivo informático asociado con la entidad. El dispositivo informático transmite el token al servidor. El servidor asociado con el sitio web puede transmitir el token o un mensaje que indique la recepción del token por parte del servidor al sistema de servicio de identidad con una solicitud de verificación de la identidad en línea de la entidad.

En este ejemplo, el sistema de servicio de identidad puede transmitir una autenticación de la identidad en línea y un nivel de confianza en la autenticación al servidor en respuesta a la determinación de un valor hash incluido en el token que coincide con el valor hash actual de la cadena de bloques. El sistema de servicio de identidad también puede añadir un nuevo bloque a la cadena de bloques en respuesta a la transmisión de la autenticación, lo que puede alterar el valor hash de la cadena de bloques e impedir que se reutilice el token. En aspectos adicionales o alternativos, se puede generar un token que autoriza a un servicio en línea a tener acceso temporal a una fuente de identidad específica. Por ejemplo, un servidor que ejecuta un sitio web para un programa gubernamental puede solicitar una fuente de identidad específica (por ejemplo, un SSN) y el sistema de servicio de identidad puede recibir una solicitud de la entidad que solicita el acceso temporal al servidor.

Un sistema de servicio de identidad puede dar control de información sensible (por ejemplo, información de identificación personal) a la entidad que está asociada con la información sensible. Por ejemplo, la entidad puede reducir la cantidad de servicios en línea que almacenan, procesan o visualizan las fuentes de identidad (por ejemplo, un SSN, un número de licencia de conducir o un patrón vocal) al transmitir tokens a los servicios en línea para que sirvan como verificación en lugar de una fuente de identidad. En aspectos adicionales o alternativos, el sistema de servicio de identidad puede enlazar múltiples fuentes de identificación para crear identidades universales que capturen fuentes de identidad de diferentes países. Por ejemplo, un ciudadano estadounidense que ha nacido en la India puede tener un certificado de nacimiento indio y un pasaporte estadounidense enlazados. Las fuentes de identidad asociadas con el certificado de nacimiento de la India (por ejemplo, crédito en la India) se pueden enlazar con fuentes de identidad asociadas con el pasaporte estadounidense (por ejemplo, crédito en Estados Unidos) para formar una única identidad en línea.

Los rasgos característicos analizados en la presente memoria no se limitan a cualquier configuración o arquitectura de hardware en particular. Un dispositivo informático puede incluir cualquier disposición adecuada de componentes que proporcionen un resultado condicionado a una o más entradas. Los dispositivos informáticos adecuados incluyen sistemas informáticos multipropósito basados en microprocesadores que acceden al software almacenado que programa o configura el sistema informático desde un aparato informático de propósito general hasta un aparato informático especializado que implementa uno o más aspectos de la presente materia objeto. Se puede utilizar cualquier programación, secuencia de comandos u otro tipo de lenguaje o combinaciones de lenguajes adecuados para implementar las enseñanzas contenidas en la presente memoria en el software que se utilizará en la programación o en la configuración de un dispositivo informático.

En referencia ahora a los dibujos, la FIGURA 1 representa un ejemplo de un entorno 100 informático que puede utilizarse para verificar una identidad basada en múltiples fuentes de datos distribuidas utilizando una cadena de bloques para salvaguardar la identidad. El entorno 100 informático puede ser un entorno informático especializado que puede utilizarse para procesar grandes cantidades de datos utilizando un gran número de ciclos de procesamiento informático. El entorno 100 informático puede incluir dispositivos 102a-c informáticos, un sistema 106 de servicio de identidad y uno o más almacenes de datos conectados a la red ("NAS") 110. El entorno 100 informático también puede incluir una red 104 de datos para acoplar de forma comunicativa los dispositivos 102a-c informáticos con el sistema 106 de servicio de identidad.

El NAS 110 puede incluir dispositivos de memoria para almacenar fuentes 116 de identidad proporcionadas al sistema 106 de servicio de identidad por uno o más componentes del entorno 100 informático. Las fuentes 116 de identidad pueden incluir información de identificación personal sobre una entidad (por ejemplo, un individuo o una empresa). En algunos aspectos, las fuentes 116 de identidad pueden incluir datos de texto (por ejemplo, SSN, un número de teléfono o una dirección), datos biométricos (por ejemplo, una cara o una composición de voz), datos de identidad digital (por ejemplo, una dirección MAC del dispositivo 102a informático asociado con la entidad), o una combinación de los mismos.

El NAS 110 también puede almacenar una cadena de bloques 112 que representa una identidad en línea de una entidad. La cadena de bloques 112 puede incluir bloques 114 que son generados por el sistema 106 de servicio de identidad en base a las fuentes 116 de identidad. En aspectos adicionales o alternativos, los bloques 114 se pueden generar en respuesta a solicitudes recibidas en el sistema 106 de servicio de identidad.

El NAS 110 también puede almacenar una variedad de diferentes tipos de datos organizados en una variedad de formas diferentes y a partir de una variedad de fuentes diferentes. Por ejemplo, el NAS 110 puede incluir almacenamiento distinto del almacenamiento principal ubicado dentro del sistema 106 de servicio de identidad que es directamente accesible por procesadores ubicados en el mismo. El NAS 110 puede incluir almacenamiento secundario,

terciario o auxiliar, como discos duros grandes, servidores, memoria virtual, entre otros tipos. Los dispositivos de almacenamiento pueden incluir dispositivos de almacenamiento portátiles o no portátiles, dispositivos de almacenamiento ópticos y diversos otros medios capaces de almacenar, contener datos. Un medio de almacenamiento legible por máquina o un medio de almacenamiento legible por ordenador puede incluir un medio no transitorio en el que se puedan almacenar datos. Ejemplos de un medio transitorio pueden incluir, por ejemplo, un disco o cinta magnéticos, un medio de almacenamiento óptico tal como un disco compacto o un disco versátil digital, memoria flash o dispositivos de memoria.

El sistema 106 de servicio de identidad puede ser un ordenador especializado u otra máquina que procese los datos recibidos dentro del entorno 100 informático. El sistema 106 de servicio de identidad puede incluir uno o más dispositivos de procesamiento que ejecutan código de programa, que incluye un módulo 108 de identidad y se almacena medio no transitorio legible por ordenador. El sistema 106 de servicio de identidad también puede incluir un puerto 130 de red de comunicaciones para acoplar de forma comunicativa el sistema 106 de servicio de identidad a otros componentes y redes en el entorno 100 informático. En algunos aspectos, el sistema 106 de servicio de identidad puede recibir, a través del puerto 130 de red de comunicaciones, una solicitud para verificar la identidad de una entidad a partir de los dispositivos 102a-c informáticos. El módulo 108 de identidad puede actualizar la cadena de bloques 112 basándose en la solicitud y generar un token que incluya un valor hash basado en la cadena de bloques 112. El módulo 108 de identidad puede transmitir el token al dispositivo 102a-c informático a través del puerto 130 de red de comunicaciones para verificar la identidad de la entidad. En aspectos adicionales o alternativos, el módulo 108 de identidad puede recibir el token a través del puerto 130 de red de comunicaciones, comparar el valor hash con el valor hash actual de la cadena de bloques 112, y proporcionar confirmación de la identidad en respuesta al valor hash que coincide con el valor hash actual. En algunos aspectos, la confirmación puede incluir una indicación de que una identidad en línea asociada con la entidad se almacena en la cadena de bloques 112. En aspectos adicionales o alternativos, la confirmación puede incluir una indicación de que la identidad en línea está asociada con una fuente de identidad específica solicitada por el servicio en línea. En aspectos adicionales o alternativos, la confirmación puede incluir la fuente de identidad específica solicitada por el servicio en línea.

En algunos aspectos, el sistema 106 de servicio de identidad puede recibir una corrección a una o más de las fuentes 116 de identidad. El sistema 106 de servicio de identidad puede actualizar las fuentes 116 de identidad con la corrección y actualizar la cadena de bloques 112 para incluir otro bloque 114 que indica una actualización a una o más de las fuentes 116 de identidad.

El sistema 106 de servicio de identidad puede incluir uno o más de otros sistemas. Por ejemplo, el sistema 106 de servicio de identidad puede incluir un sistema de base de datos para acceder al NAS 110, una malla de comunicaciones o ambos. La malla de comunicaciones puede ser un sistema de servicio de identidad basado en la malla para procesar grandes cantidades de datos.

Los dispositivos 102a-c informáticos pueden asociarse con una entidad o un servicio en línea y pueden comunicarse con el sistema 106 de servicio de identidad. Por ejemplo, el dispositivo 102a informático puede ser un teléfono móvil asociado con una entidad que puede transmitir datos de la fuente de identidad al sistema 106 de servicio de identidad para ser procesados. En aspectos adicionales o alternativos, el dispositivo 102a informático puede transmitir una solicitud al sistema 106 de servicio de identidad para generar una ficha para autenticar la identidad en línea de una entidad asociada con el dispositivo 102a informático. Los dispositivos 102a-c informáticos pueden interactuar con el sistema 106 de servicio de identidad a través de la red 104 de datos. En algunos aspectos, los dispositivos 102a-c informáticos pueden incluir ordenadores en red, sensores, bases de datos u otros dispositivos que pueden transmitir o proporcionar datos al sistema 106 de servicio de identidad. Por ejemplo, los dispositivos 102a-c informáticos pueden incluir dispositivos de red de área local, tales como enrutadores, concentradores, conmutadores u otros dispositivos de redes informáticas.

El entorno 100 informático también puede incluir una o más redes 120 en la nube. Una red 120 en la nube puede incluir un sistema de infraestructura en la nube que proporcione servicios en la nube. En determinados ejemplos, los servicios proporcionados por la red 120 en la nube pueden incluir una gran cantidad de servicios que se ponen a disposición de los usuarios del sistema de infraestructura en la nube bajo demanda. Una red 120 en la nube se muestra en la FIGURA 1 como acoplado de forma comunicativa al puerto 130 de la red de comunicaciones del sistema 106 de servicio de identidad (y, por lo tanto, que tiene el sistema 106 de servicio de identidad como su cliente o usuario), pero la red 120 en la nube puede estar acoplada de forma comunicativa o ser utilizada por cualquier de los dispositivos de la FIGURA 1. Los servicios proporcionados por la red 120 en la nube pueden escalar dinámicamente para satisfacer las necesidades de sus usuarios. La red 120 en la nube puede incluir uno o más ordenadores, servidores o sistemas. En algunos aspectos, uno o más dispositivos de usuario final, tales como uno o más de los dispositivos 102a-c informáticos, pueden acceder al sistema 106 de servicio de identidad, el NAS 110, o alguna combinación de los mismos a través de la red 120 en la nube. Los dispositivos de usuario final pueden transmitir, a través de la red 120 en la nube y al sistema 106 de servicio de identidad, datos asociados con fuentes 116 de identidad adicionales o solicitudes de verificación de una identidad.

Cada comunicación dentro del entorno informático 100 (por ejemplo, entre dispositivos cliente o entre un servidor y un dispositivo) puede producirse a través de una o más redes 104. Las redes 104 pueden incluir uno o más de una

variedad de diferentes tipos de redes, incluida una red inalámbrica, una red cableada o una combinación de red cableada e inalámbrica. Entre los ejemplos de redes adecuadas se incluyen Internet, una red de área personal, una red de área local ("LAN"), una red de área amplia ("WAN"), o una red inalámbrica de área local ("WLAN"). Una red inalámbrica puede incluir una interfaz inalámbrica o una combinación de interfaces inalámbricas. Una red cableada puede incluir una interfaz cableada. Las redes cableadas o inalámbricas se pueden implementar utilizando enrutadores, puntos de acceso, puentes, puertas de enlace, o similares, para conectar dispositivos en la red 104. Las redes 104 pueden incorporarse completamente dentro de (o pueden incluir) una intranet, una extranet o una combinación de las mismas. En un ejemplo, las comunicaciones entre dos o más sistemas o dispositivos se pueden lograr mediante un protocolo de comunicaciones, tal como la capa de conexión segura ("SSL") o la seguridad de la capa de transporte ("TLS"). Además, los datos o detalles transaccionales pueden estar cifrados.

El número de dispositivos representados en la FIGURA 1 se proporcionan con fines ilustrativos. Se pueden utilizar diferentes números de dispositivos. Por ejemplo, aunque cada dispositivo, servidor y sistema de la FIGURA 1 se muestra como un solo dispositivo, en su lugar se pueden utilizar múltiples dispositivos.

La FIGURA 2 representa un ejemplo de una cadena de bloques 212 que representa una identidad en línea. La cadena de bloques 212 incluye un conjunto de bloques ordenados 230 enlazados en serie. Si se proporcionan nuevas fuentes de identidad para una entidad, o se realizan nuevas transacciones de identidad para una entidad, se pueden añadir los nuevos bloques 230 ordenados al final de la cadena de bloques 212. A cada bloque 230 ordenado se le puede asignar una marca de tiempo 232 respectiva. Una marca de tiempo 232 puede indicar cuándo se ha añadido el bloque 230 ordenado a la cadena de bloques 212. Cada bloque 230 ordenado también puede incluir datos 234. En algunos aspectos, los datos 234 pueden indicar que se ha producido una transacción de identidad (por ejemplo, se ha proporcionado una fuente de identidad) o un evento de autenticación (por ejemplo, un servicio en línea ha solicitado la verificación de la identidad en línea). En aspectos adicionales o alternativos, los datos 234 pueden incluir datos basados en (o asociados con) una fuente de identidad para una entidad particular asociada con la cadena de bloques 212. Por ejemplo, los datos 234 pueden ser una versión codificada de un SSN o un enlace codificado a un escaneo de la retina almacenado en la memoria. Los datos 234 también pueden indicar una obligación fiduciaria asumida por el titular de la identidad en línea.

La identidad en línea representada por la cadena de bloques 212 puede estar separada de cualquier documentación que corrobore la existencia o legitimidad de la entidad que está asociada con la identidad en línea. La identidad en línea puede ser preestablecida por el sistema 106 de servicio de identidad representado en la FIGURA 1. El sistema 106 de servicio de identidad puede determinar que la identidad en línea está asociada con la entidad basándose en la recepción de fuentes de identidad desde la entidad. Las fuentes de identidad pueden incluir documentos emitidos por el gobierno tales como, individualmente o combinados, un certificado de nacimiento, una tarjeta SSN, un pasaporte, una licencia de conducir, datos biométricos (por ejemplo, una foto, una huella dactilar, datos de voz, un escaneo del iris, una muestra de ADN) u otros documentos justificativos, tales como un registro de empleo de la empresa o una autenticación por parte de un notario público. Las versiones digitales de estas fuentes de identidad se pueden almacenar y validar como prueba de que la identidad en línea que está asociada con la entidad.

En respuesta a una solicitud de verificación de la identidad en línea que está asociada con una entidad, el sistema 106 de servicio de identidad puede confirmar la identidad en línea de la entidad y proporcionar un nivel de confianza basado en la cantidad y tipo de fuentes de identidad que la entidad ha proporcionado. La confirmación se puede proporcionar sin distribuir la versión digital de las fuentes de identidad o cualquier dato que pueda utilizarse para determinar la identidad de la entidad y las fuentes de identidad. Por ejemplo, la entidad puede solicitar un token para autenticar la identidad en línea de la entidad en un servicio en línea. El sistema de servicio de identidad puede generar el token y proporcionar el token a la entidad. El sistema de servicio de identidad puede proporcionar confirmación al servicio en línea en respuesta a la recepción del token de los servicios en línea. En aspectos adicionales o alternativos, el sistema de servicio de identidad puede proporcionar una versión digital de una o más de las fuentes de identidad para autenticar la identidad en línea de la entidad.

La FIGURA 3 representa un ejemplo de un sistema 310 de servicio de identidad para verificar una identidad basada en múltiples fuentes de datos distribuidas utilizando una cadena de bloques para salvaguardar la identidad. El sistema 310 de servicio de identidad puede incluir fuentes 320 de datos dispares, un procesador de datos 330, una cadena de bloques 340 y una interfaz de programación de aplicaciones ("API") 350. El ejemplo representado en la FIGURA 3 se puede utilizar para implementar el sistema 106 de servicio de identidad representado en la FIGURA 1.

Las fuentes 320 de datos dispares pueden incluir bases de datos privadas para múltiples fuentes de identidad que tienen múltiples formatos tales como datos de texto 322, datos biométricos 324 e identificadores 326 digitales. Las bases de datos privadas se pueden proteger y codificar para impedir el acceso público a la información confidencial. En algunos aspectos, los datos de texto 322 pueden incluir un SSN, un nombre, una dirección o un número de licencia de conducir. Los datos 324 biométricos pueden ser datos que representan uno o más rasgos característicos de un cliente 370 (por ejemplo, un individuo que accede al sistema 310 de servicio de identidad). Ejemplos de estos rasgos característicos incluyen un rostro, voz, huella dactilar, iris y ADN. Los archivos de imagen reales o las plantillas personalizadas se pueden extraer de una imagen original y almacenada. Los identificadores 326 digitales pueden incluir información de identificación sobre dispositivos asociados con el cliente 370 tal como un identificador de

dispositivo móvil (por ejemplo, una dirección MAC), un identificador de dispositivo de Internet de las cosas, un número de teléfono o una ubicación geográfica.

La API 350 puede interactuar con un aplicación 360 de software cliente para permitir la comunicación entre el sistema 310 de servicio de identidad y el cliente 370. La API 350 puede recibir, desde el cliente 370, fuentes de identidad que se van a almacenar en las fuentes 320 de datos dispares. La API 350 también puede recibir solicitudes de transacciones de identidad (por ejemplo, una solicitud para autenticar la identidad en línea del cliente 370 en otra entidad).

El procesador de datos 330 se puede acoplar de forma comunicativa a la API 350 para recibir fuentes de identidad y solicitudes de transacciones de identidad del cliente 370. El procesador de datos 330 también se puede acoplar de forma comunicativa a las fuentes 320 de datos dispares y a la cadena de bloques 340 para ejecutar las instrucciones recibidas del cliente 370. Por ejemplo, el procesador de datos 330 puede actualizar las fuentes de datos distantes 320 basándose en la recepción de fuentes de identidad del cliente 370.

La cadena de bloques 340 se puede almacenar en una base de datos que permite acceder a, y auditar, la cadena de bloques 340 por parte del cliente 370 u otras entidades. El procesador de datos 330 puede generar la cadena de bloques 340 basándose en las fuentes 320 de datos dispares. El procesador de datos 330 puede mantener la cadena de bloques 340 añadiendo bloques a una cadena de bloques 340 en respuesta a transacciones de identidad. Una transacción de identidad puede incluir una solicitud del cliente para actualizar las fuentes 320 de datos dispares, una solicitud del cliente para verificar una identidad en línea del cliente 370, o alguna otra transacción que implique el uso de la identidad del cliente.

El procesador de datos 330 puede generar un token basado en la cadena de bloques 340 y transmitir el token al cliente 370. El token puede incluir un valor hash basado en el tamaño de la cadena de bloques 340 y los datos codificados en la cadena de bloques 340. En algunos aspectos, el tamaño de la cadena de bloques 340 se puede determinar en función del número de bloques ordenados de la cadena de bloques 340 o la cantidad de datos almacenados en la cadena de bloques 340. El valor hash se puede determinar en función del tamaño de la cadena de bloques 340 sin verse afectado por el significado de los datos almacenados en los bloques ordenados.

El procesador de datos 330 puede recibir el token de otra entidad y autenticar la identidad en línea del cliente 370 a la otra entidad en función del valor hash incluido en el token que coincide con el valor hash actual de la cadena de bloques 340. En respuesta a la autenticación de la identidad en línea del cliente 370, el procesador de datos 330 puede añadir un nuevo bloque a la cadena de bloques 340 que puede cambiar el valor hash actual de la cadena de bloques 340.

Aunque el sistema 310 de servicio de identidad de la FIGURA 3 se describe como la generación de un token para autenticar una identidad en línea de una entidad en un servicio en línea, son posibles otras implementaciones. En algunos aspectos, el sistema 310 de servicio de identidad puede utilizar la cadena de bloques 340 para verificar la identidad en línea de una entidad sin utilizar un token. Por ejemplo, el cliente 370 puede ser un servicio en línea y el sistema 310 de servicio de identidad puede recibir una solicitud del cliente 370 para verificar una identidad de la entidad. La solicitud puede incluir una forma de identificación (por ejemplo, datos biométricos) y el sistema 106 de servicio de identidad puede identificar la cadena de bloques 340 como asociada con la entidad, y proporcionar confirmación de la identidad en línea de la entidad al cliente 370.

La FIGURA 4 representa un ejemplo de un sistema 410 de servicio de identidad que está separado de las cadenas de bloques 440 y las fuentes de identidad. El sistema 410 de servicio de identidad representado en la FIGURA 4 se puede utilizar para implementar el sistema 106 de servicio de identidad representado en la FIGURA 1. El sistema 410 de servicio de identidad puede recibir señales de dispositivos informáticos asociados con las entidades 470. Las entidades 470 pueden incluir empresas 472 y particulares 474. En algunos aspectos, las cadenas de bloques 440 se pueden generar y gestionar mediante un sistema separado. Las cadenas de bloques 440 pueden generarse basándose en fuentes de identidad que incluyen datos de texto 422 y datos 424 biométricos, que pueden almacenarse por separado de las cadenas de bloques 440. Los datos 424 biométricos se pueden actualizar al recibir un identificador 426 biométrico y digital de los dispositivos informáticos asociados con las entidades 470.

El sistema 410 de servicio de identidad puede recibir fuentes de identidad de las entidades 470 y asociar una entidad específica de las entidades 470 con una cadena de bloques específica de las cadenas de bloques 440. El sistema de servicio de identidad puede recibir una solicitud de la entidad específica para verificar la identidad en línea de la entidad específica en un servicio en línea y generar un token basado en la cadena de bloques específica. El sistema de servicio de identidad puede transmitir el token a la entidad específica, que puede proporcionar el token al servicio en línea. El sistema de servicio de identidad puede recibir el token del servicio en línea, comparar el token con la cadena de bloques específica y verificar la identidad en línea de la entidad específica.

La FIGURA 5 representa un flujo de información en un entorno informático para verificar una identidad basada en múltiples fuentes de datos distribuidas utilizando una cadena de bloques para salvaguardar la identidad. Un sistema 506 de servicio de identidad (por ejemplo, uno o más de los sistemas 106, 310, 410 de servicio de identidad) puede

mejorar la seguridad de la identidad transmitiendo un token en lugar de fuentes de identidad (por ejemplo, SSN) para verificar la identidad en línea.

En el bloque 520, el sistema 506 de servicio de identidad se comunica con una entidad 570 para autenticar la entidad 570 o determinar de otro modo una identidad en línea de la entidad 570. El sistema 506 de servicio de identidad puede recibir una señal en un módulo 512 de servicio de identidad desde un dispositivo informático (por ejemplo, un teléfono móvil) asociado con la entidad 570 proporcionando prueba de la identidad en línea de la entidad 570 o proporcionando de otro modo datos que se utilizan para autenticar la entidad 570. En algunos aspectos, la prueba puede ser un nombre de usuario y una contraseña. En aspectos adicionales o alternativos, la prueba puede ser una combinación de datos de texto, datos biométricos y datos de identidad digital. Por ejemplo, la señal puede incluir uno o más de un nombre de la entidad 570, un escaneo de la retina de la entidad 570 y una dirección MAC del dispositivo informático. El módulo 512 de servicio de identidad puede determinar que la entidad 570 coincide con una identidad en línea y transmitir una señal de respuesta al dispositivo informático que solicita instrucciones.

En el bloque 530, el sistema 506 de servicio de identidad transmite un token a la entidad 570 en respuesta a una solicitud de la entidad 570 para verificar la identidad en línea de la entidad 570. El sistema 506 de servicio de identidad puede recibir la solicitud en un módulo 514 API de datos de identificador, que puede procesar la solicitud y transmitir una solicitud del token a un módulo 516 de contrato inteligente. El módulo 516 de contrato inteligente puede determinar un valor hash de una cadena de bloques y generar un token que incluye el valor hash. El módulo 516 de contrato inteligente puede transmitir el token al módulo 514 API de datos de identificador, que puede transmitir el token a la entidad 570. En algunos aspectos, la solicitud de la entidad 570 puede indicar restricciones tales como un servicio en línea o un tiempo específicos para proporcionar autenticación de la identidad en línea. El módulo 514 API de datos de identificador puede almacenar las restricciones en el token.

En el bloque 540, el sistema 506 de servicio de identidad transmite datos de la fuente de identidad a la entidad 570 en respuesta a la recepción del token de la entidad 570. El módulo 514 API de datos de identificador puede recibir una señal de la entidad 570 que incluye el token. El módulo 514 API de datos de identificador puede verificar el token para determinar las restricciones impuestas al token (por ejemplo, el uso por parte de un servicio en línea específico o en un momento específico). El módulo 514 API de datos de identificador también puede verificar el token para determinar la cantidad de información que se transmitirá a la entidad 570. En este ejemplo, el token puede incluir una solicitud de datos sin procesar o datos de la fuente de identidad. El módulo 514 API de datos de identificador transmite una señal al módulo 516 de contrato inteligente para determinar si el token es válido (por ejemplo, comparando el valor hash en el token con un valor hash actual en la cadena de bloques). En respuesta a la determinación de que el valor hash en el token es válido, el módulo 516 de contrato inteligente puede añadir un nuevo bloque a la cadena de bloques indicando la transacción de identidad. Añadir el nuevo bloque puede modificar el valor hash de la cadena de bloques. El módulo 516 de contrato inteligente puede transmitir una señal al módulo 514 API de datos de identificador que confirma la identidad en línea de la entidad 570 e incluye datos codificados de una fuente de identidad o una ubicación de los datos de la fuente de identidad solicitados en el token. En algunos aspectos, el módulo 514 API de datos de identificador puede transmitir una señal a un módulo 518 de datos especializado que solicita los datos de la fuente de identidad y recibir los datos sin procesar del módulo 518 de datos especializado. En aspectos adicionales o alternativos, el módulo 514 API de datos de identificador puede determinar datos de la fuente de identidad decodificando los datos codificados utilizando un proceso de decodificación que corresponde al proceso de codificación utilizado para codificar los datos en la cadena de bloques. El módulo 514 API de datos de identificador puede transmitir una señal a la entidad 570 verificando la identidad en línea de la entidad 570 y proporcionando los datos de la fuente de identidad solicitados en el token.

Aunque se describe que el sistema 506 de servicio de identidad como que recibe el token de la entidad 570,

otras implementaciones son posibles. En algunos aspectos, la entidad 570 puede proporcionar el token a un servicio en línea, que podría ser una entidad o un dispositivo solicitante (por ejemplo, un dispositivo de Internet de las cosas). El sistema 506 de servicio de identidad puede recibir el token del servicio en línea y proporcionar confirmación de la identidad en línea al servicio en línea.

La cadena de bloques gestionada por el sistema 506 de servicio de identidad puede representar una única identidad en línea que puede enlazar diferentes identidades nacionales. En algunos aspectos, los países tienen identificadores nacionales asignados a los ciudadanos que pueden ser reconocidos solo en el país porque el país regula la protección de los datos en un área geográfica específica. En aspectos adicionales o alternativos, la identidad en línea es una identidad universal que puede proporcionar la verificación de diversas formas de identidad con una única confirmación.

La FIGURA 6 es un diagrama de flujo de un proceso para verificar una identidad basada en múltiples fuentes de datos distribuidas utilizando una cadena de bloques para salvaguardar la identidad. El proceso puede impedir el robo de identidad al reducir las instancias de fuentes de identidad que se transmiten, almacenan y visualizan.

En el bloque 610, un dispositivo de procesamiento recibe una solicitud de un token de una entidad para autenticar una identidad en línea de la entidad en un servicio en línea. La solicitud puede incluir restricciones que indiquen la cantidad

de información transmitida al servicio en línea. En algunos aspectos, la entidad puede ser un individuo o una empresa que busca participar en una transacción con el servicio en línea.

En el bloque 620, el dispositivo de procesamiento almacena la solicitud en una cadena de bloques que representa la identidad en línea de la entidad. En algunos aspectos, el dispositivo de procesamiento almacena la solicitud añadiendo un nuevo bloque a la cadena de bloques, el nuevo bloque que incluye datos que indican la solicitud del token. La cadena de bloques puede ser una base de datos que incluye uno o más bloques ordenados basados en fuentes de identidad que representan información de identificación personal de la entidad. En algunos aspectos, la cadena de bloques es una base de datos pública y los bloques ordenados incluyen versiones codificadas de fuentes de identidad asociadas con la entidad.

En el bloque 630, el dispositivo de procesamiento genera el token basado en la cadena de bloques. El dispositivo de procesamiento puede determinar un valor hash basado en los datos almacenados en los bloques ordenados o el tamaño de la cadena de bloques. El token puede incluir el valor hash y cualquier restricción recibida como parte de la solicitud del token de la entidad.

En el bloque 640, el dispositivo de procesamiento transmite el token a la entidad. La entidad puede asociarse con un dispositivo informático (por ejemplo, un teléfono móvil) y el dispositivo de procesamiento puede transmitir una señal al dispositivo informático que incluye el token. En algunos aspectos, el dispositivo de procesamiento puede transmitir la señal a través de una red inalámbrica.

En el bloque 650, el dispositivo de procesamiento recibe el token del servicio en línea. En algunos aspectos, el servicio en línea puede incluir un servidor que ha recibido el token de un dispositivo informático asociado con la entidad. El dispositivo de procesamiento puede recibir el token del servidor a través de una red inalámbrica.

En el bloque 660, el dispositivo de procesamiento transmite confirmación de la identidad en línea de la entidad al servicio en línea basándose en la recepción del token del servicio en línea. En algunos aspectos, el dispositivo de procesamiento puede transmitir la confirmación basándose en la determinación de que un valor hash incluido en el token coincide con un valor hash actual de la cadena de bloques. En aspectos adicionales o alternativos, el dispositivo de procesamiento puede añadir un nuevo bloque a la cadena de bloques que indica la transacción de identidad.

En algunos aspectos, el token puede incluir una solicitud de acceso a una o más fuentes de identidad. El dispositivo de procesamiento puede determinar las fuentes de identidad mediante la decodificación de datos en la cadena de bloques o mediante la recepción de las fuentes de identidad a partir de una memoria separada que almacena las fuentes de identidad.

Cualquier sistema informático adecuado o grupo de sistemas informáticos se puede utilizar para gestionar y verificar una identidad basada en datos de múltiples fuentes de identidad que se almacenan en una cadena de bloques como se describe en la presente memoria. Por ejemplo, la FIGURA 7 es un diagrama de bloques que representa un sistema 700 de servicio de identidad, que puede ser un ejemplo de uno o más de los sistemas 106, 310, 410 y 506 de servicios de identidad representados en las FIGURA 1 y 3-5. El sistema 700 de servicio de identidad puede incluir diversos dispositivos para comunicarse con otros dispositivos en el entorno 100 informático, como se describe con respecto a la FIGURA 1. El sistema 700 de servicio de identidad puede incluir diversos dispositivos para realizar uno o más de las etapas descritas anteriormente con respecto a la FIGURA 5.

El sistema 700 de servicio de identidad puede incluir un procesador 702 que está acoplado de forma comunicativa a una memoria 704. El procesador 702 ejecuta el código de programa ejecutable por ordenador en la memoria 704, accede a la información almacenada en la memoria 704, o ambos. El código de programa puede incluir instrucciones ejecutables por máquina que pueden representar un procedimiento, una función, un subprograma, un programa, una rutina, una subrutina, un módulo, un paquete de software, una clase o cualquier combinación de instrucciones, estructuras de datos o declaraciones de programa. Un segmento de código puede estar acoplado a otro segmento de código o un circuito de hardware pasando o recibiendo información, datos, argumentos, parámetros o contenido de memoria. La información, argumentos, parámetros, datos, etc. pueden pasarse, reenviarse o transmitirse a través de cualquier medio adecuado, incluido el intercambio de memoria, el intercambio de mensajes, el paso de tokens, la transmisión de red, entre otros.

Los ejemplos de un procesador 702 incluyen un microprocesador, un circuito integrado de aplicación específica, una matriz de puertas programables por campo o cualquier otro dispositivo de procesamiento adecuado. El procesador 702 puede incluir un número cualquiera de dispositivos de procesamiento, incluido uno. El procesador 702 puede incluir o comunicarse con una memoria 704. La memoria 704 almacena código de programa que, cuando es ejecutado por el procesador 702, hace que el procesador realice las operaciones descritas en esta descripción.

La memoria 704 puede incluir cualquier medio no transitorio legible por ordenador adecuado. El medio legible por ordenador puede incluir cualquier dispositivo de almacenamiento electrónico, óptico, magnético o de otro tipo capaz de proporcionar un código de programa legible por ordenador u otro código de programa a un procesador. Ejemplos no limitantes de un medio legible por ordenador incluyen un disco magnético, memoria chip, almacenamiento óptico,

memoria flash, memoria de clase de almacenamiento, un CD-ROM, DVD, ROM, RAM, un ASIC, cinta magnética u otro almacenamiento magnético, o cualquier otro medio desde el cual un procesador de ordenador puede leer y ejecutar código de programa. El código del programa puede incluir código de programa específico de procesador generado por un compilador o un intérprete a partir de código escrito en cualquier lenguaje de programación de ordenadores adecuado. Ejemplos de lenguaje de programación adecuado incluyen C, C++, C#, Visual Basic, Java,Python, Perl, JavaScript, ActionScript, etc.

El sistema 700 de servicio de identidad también puede incluir varios dispositivos externos o internos, tales como dispositivos de entrada o salida. Por ejemplo, el sistema 700 de servicio de identidad se muestra con una interfaz de entrada/salida 708 que puede recibir datos de entrada desde dispositivos de entrada y proporcionar datos de salida a dispositivos de salida. También se puede incluir un bus 706 en el sistema 700 de servicio de identidad. El bus 706 puede acoplar de forma comunicativa uno o más componentes del sistema 700 de servicio de identidad.

El sistema 700 de servicio de identidad puede ejecutar código de programa que incluye el módulo 108 de identidad. El código de programa para el módulo 108 de identidad puede residir en cualquier medio legible por ordenador adecuado y puede ejecutarse en cualquier dispositivo de procesamiento adecuado. Por ejemplo, como se representa en la FIGURA 7, el código de programa para el módulo 108 de identidad puede residir en la memoria 704 en el sistema 700 de servicio de identidad. La ejecución del módulo 108 de identidad puede configurar el procesador 702 para realizar las operaciones que se describen en la presente memoria.

En algunos aspectos, el sistema 700 de servicio de identidad puede incluir uno o más dispositivos de salida. Un ejemplo de un dispositivo de salida es el dispositivo 710 de interfaz de red representado en la FIGURA 6. Un dispositivo 710 de interfaz de red puede incluir cualquier dispositivo o grupo de dispositivos adecuados para establecer una conexión de datos cableada o inalámbrica a una o más redes 104 de datos. Los ejemplos no limitantes del dispositivo 710 de interfaz de red incluyen un adaptador de red Ethernet, un módem, etc. En algunos aspectos, el dispositivo 710 de interfaz de red puede incluir uno o más puertos de red de comunicaciones, tales como el puerto 130 de red de comunicaciones representado en la FIGURA 1.

Otro ejemplo de un dispositivo de salida es el dispositivo 712 de presentación representado en la FIGURA 7. Un dispositivo 712 de presentación puede incluir cualquier dispositivo o grupo de dispositivos adecuados para proporcionar una salida visual, auditiva u otra salida sensorial adecuada. Los ejemplos no limitantes del dispositivo 712 de presentación incluyen una pantalla táctil, un monitor, un altavoz, un dispositivo informático móvil separado, etc.

Consideraciones generales

En la presente memoria se exponen numerosos detalles específicos. para proporcionar una comprensión exhaustiva de la materia objeto reivindicada. Sin embargo, los expertos en la técnica entenderán que la materia objeto reivindicada puede llevarse a la práctica sin estos detalles específicos. En otros casos, los procedimientos, aparatos o sistemas que alguien medianamente experto en la técnica conocería no se han descrito en detalle para no oscurecer la materia objeto reivindicada.

A menos que se indique específicamente lo contrario, a lo largo de esta memoria descriptiva, términos como "procesamiento", "computación", "cálculo", "determinación" e "identificación" o similares se refieren a acciones o procesos de un dispositivo informático, tales como uno o más ordenadores o un dispositivo o dispositivos informáticos electrónicos similares, que manipulan o transforman datos representados como cantidades físicas electrónicas o magnéticas dentro de memorias, registros u otros dispositivos de almacenamiento de información dispositivos de transmisión o dispositivos de visualización de la plataforma informática.

El sistema o sistemas analizados en la presente memoria no se limitan a ninguna arquitectura o configuración de hardware en particular. Un dispositivo informático puede incluir cualquier disposición adecuada de componentes que proporcione un resultado condicionado a una o más entradas. Los dispositivos informáticos adecuados incluyen sistemas informáticos multipropósito basados en microprocesadores que acceden a software almacenado que programa o configura el sistema informático desde un aparato informático de propósito general hasta un aparato informático especializado que implementa uno o más aspectos de la presente materia objeto. Cualquier programación adecuada, secuencias de comandos u otro tipo de lenguaje o combinaciones de lenguajes se pueden utilizar para implementar las enseñanzas contenidas en la presente memoria en el software que se utilizará en la programación o en la configuración de un dispositivo informático.

Los aspectos de los procedimientos descritos en la presente memoria pueden realizarse en el funcionamiento de dichos dispositivos informáticos. El orden de los bloques presentados en los ejemplos anteriores se puede variar, por ejemplo, los bloques se pueden reordenar, combinar o dividir en subbloques. Determinados bloques o procesos se pueden realizar en paralelo.

El uso de "adaptado a" o "configurado para" en la presente memoria se entiende como un lenguaje abierto e inclusivo que no excluye los dispositivos adaptados o configurados para ejecutar tareas o etapas adicionales. Además, el uso de "basado en" está destinado a abierto e inclusivo, en el sentido de que un proceso, etapa, cálculo u otra acción

"basada en" una o más de las condiciones o valores mencionadas puede, en la práctica, estar basada en condiciones o valores adicionales más allá de los mencionados. Los encabezados, las listas y la numeración que se incluyen en la presente memoria son solo para facilitar la explicación y no pretenden ser limitantes.

Si bien la presente materia objeto se ha descrito en detalle con respecto a aspectos específicos de la misma, se apreciará que los expertos en la técnica, tras lograr una comprensión de los párrafos anteriores pueden producir fácilmente alteraciones, variaciones y equivalentes de dichos aspectos. Cualquier aspecto o ejemplo puede combinarse con otros aspectos o ejemplos. En consecuencia, debe entenderse que la presente descripción se ha presentado con fines de ejemplo más que de limitación, y no excluye la inclusión de dicha modificaciones, variaciones o incorporaciones a la presente materia objeto como sería fácilmente evidente para una persona con experiencia ordinaria en la técnica.

REIVINDICACIONES

1. Un sistema (106, 310, 410, 506, 700) que comprende:

un dispositivo (330, 702) de procesamiento;
un puerto (130, 710) de red de comunicaciones configurado para ser controlado mediante el dispositivo de procesamiento; y
un dispositivo de memoria en el que se almacenan instrucciones que son ejecutables por el dispositivo de procesamiento para:

recibir (610), a través del puerto de red de comunicaciones, una solicitud de un token de una entidad (470, 570) para autenticar una identidad en línea de la entidad en un servicio en línea;
almacenar (620) la solicitud en una cadena de bloques (112, 212, 340, 440) que representa la identidad en línea de la entidad añadiendo un nuevo bloque (114, 230) a la cadena de bloques, la cadena de bloques que es una base de datos que incluye uno o más bloques ordenados basados en una o más fuentes (116, 320) de identidad que representan información de identificación personal de la entidad, el nuevo bloque que incluye datos que indican la solicitud del token;
generar (630) el token basado en el uno o más bloques ordenados de la cadena de bloques;
transmitir (640), a través del puerto de red de comunicaciones, el token a la entidad;
recibir (650), a través del puerto de red de comunicaciones, el token del servicio en línea; y
transmitir (660), a través del puerto de red de comunicaciones y en base a la recepción del token del servicio en línea, una confirmación de la identidad en línea de la entidad en el servicio en línea
en el que: las instrucciones ejecutables por el dispositivo de procesamiento para generar el token son también ejecutables por el dispositivo de procesamiento para:

determinar un primer valor hash para la cadena de bloques basada en el uno o más bloques ordenados de la cadena de bloques; y generar el token basado en el primer valor hash de modo que el token esté asociado con la cadena de bloques,
en el que las instrucciones ejecutables por el dispositivo de procesamiento para transmitir la confirmación de la identidad en línea de la entidad son ejecutables por el dispositivo de procesamiento para:
determinar un valor hash actual para la cadena de bloques basada en el uno o más bloques ordenados de la cadena de bloques en respuesta a la recepción del token;
transmitir, a través del puerto de red de comunicaciones, la confirmación de la identidad en línea de la entidad mientras impide que la identidad en línea acceda a la una o más fuentes de identidad en respuesta a la determinación de que el primer valor hash coincida con el valor hash actual; y
almacenar un evento de autenticación como otro bloque nuevo en la cadena de bloques de modo que se modifique el valor hash actual de la cadena de bloques.

2. El sistema (106, 310, 410, 506, 700) de la reivindicación 1, en el que la cadena de bloques (112, 212, 340, 440) es una primera cadena de bloques, y en el que las instrucciones que son ejecutables por el dispositivo de procesamiento para transmitir (660) la confirmación de la identidad en línea de la entidad (470, 570) al servicio en línea son ejecutables además por el dispositivo (330, 702) de procesamiento para:

verificar, basándose en el token, una identidad del servicio en línea basada en una segunda cadena de bloques que representa la identidad en línea del servicio en línea; y
verificar que la entidad ha solicitado el token para autenticar la identidad en línea de la entidad en el servicio en línea.

3. El sistema (106, 310, 410, 506, 700) de la reivindicación 1, en el que el uno o más bloques (114, 230) ordenados incluyen datos codificados de la una o más fuentes (116, 320) de identidad, y en el que las instrucciones que son ejecutables por el dispositivo de procesamiento para transmitir la confirmación de la identidad en línea de la entidad (470, 570) en el servicio en línea son además ejecutables por el dispositivo (330, 702) de procesamiento para:

descodificar, basándose en el token, la una o más fuentes de identidad a partir de los datos codificados en la cadena de bloques; y
transmitir, a través del puerto (130, 710) de la red de comunicaciones, la una o más fuentes de identidad al servicio en línea para procesar la una o más fuentes de identidad.

4. El sistema (106, 310, 410, 506, 700) de la reivindicación 1, en el que las instrucciones son ejecutables además por el dispositivo (330, 702) de procesamiento para:

recibir, a través del puerto (130, 710) de la red de comunicaciones, la una o más fuentes (116, 320) de identidad de la entidad (470, 570);
almacenar la una o más fuentes de identidad en una base de datos privada; y

generar la cadena de bloques (112, 212, 340, 440) que representa la identidad en línea asociada con la entidad mediante la generación de un bloque (114, 230) ordenado basado en cada fuente de identidad de la una o más fuentes de identidad.

5. El sistema (106, 310, 410, 506, 700) de la reivindicación 4, en el que las instrucciones que son ejecutables por el dispositivo (330, 702) de procesamiento para transmitir (660) la confirmación de la identidad en línea de la entidad (470, 570) al servicio en línea son además ejecutables por el dispositivo de procesamiento para:

determinar, basándose en el token, una fuente de identidad (116, 320) de la una o más fuentes de identidad de la base de datos privada; y transmitir, a través del puerto (130, 710) de la red de comunicaciones, la fuente de identidad al servicio en línea para procesar la fuente de identidad.

6. El sistema (106, 310, 410, 506, 700) de la reivindicación 1, en el que las instrucciones son ejecutables además por el dispositivo (330, 702) de procesamiento para:

recibir, a través del puerto (130, 710) de la red de comunicaciones, una corrección de la una o más fuentes (116, 320) de identidad de la entidad (470, 570); y
almacenar la corrección en otro bloque nuevo (114, 230) de la cadena de bloques (112, 212, 340, 440) de modo que se modifica un valor hash basado en la cadena de bloques.

7. Un procedimiento que comprende:

recibir (610), mediante un dispositivo (330, 702) de procesamiento, una solicitud de un token de una entidad (470, 570) para autenticar una identidad en línea de la entidad en un servicio en línea;
almacenar (620), mediante el dispositivo de procesamiento, la solicitud en una cadena de bloques (112, 212, 340, 440) que representa la identidad en línea de la entidad añadiendo un nuevo bloque (114, 230) a la cadena de bloques, la cadena de bloques que es una base de datos que incluye uno o más bloques ordenados basados en una o más fuentes (116, 320) de identidad que representan información de identificación personal de la entidad, el nuevo bloque que incluye datos que indican la solicitud del token;
generar (630), mediante el dispositivo de procesamiento, el token basado en el uno o más bloques ordenados de la cadena de bloques;
transmitir (640), mediante el dispositivo de procesamiento, el token a la entidad;
recibir (650), mediante el dispositivo de procesamiento, el token del servicio en línea; y
transmitir (660), mediante el dispositivo de procesamiento, una confirmación de la identidad en línea de la entidad al servicio en línea en base a la recepción del token del servicio en línea en el que: generar el token además comprende:

determinar, mediante el dispositivo de procesamiento, un primer valor hash para la cadena de bloques basándose en el uno o más bloques ordenados de la cadena de bloques; y
generar, mediante el dispositivo de procesamiento, el token basado en el primer valor hash de modo que el token está asociado con la cadena de bloques,
en el que transmitir la confirmación de la identidad en línea de la entidad además comprende:

determinar, mediante el dispositivo de procesamiento, un valor hash actual para la cadena de bloques basándose en el uno o más bloques ordenados de la cadena de bloques en respuesta a la recepción del token;
transmitir, mediante el dispositivo de procesamiento, la confirmación de la identidad en línea de la entidad mientras impide que la identidad en línea acceda a la una o más fuentes de identidad en respuesta a la determinación de que el primer valor hash coincida con el valor hash actual; y
almacenar, mediante el dispositivo de procesamiento, un evento de autenticación como otro bloque nuevo en la cadena de bloques de modo que se modifica el valor hash actual de la cadena de bloques.

8. El procedimiento de la reivindicación 7, en el que la cadena de bloques (112, 212, 340, 440) es una primera cadena de bloques, y en el que transmitir (660) la confirmación de la identidad en línea de la entidad (470, 570) al servicio en línea además comprende:

verificar, basándose en el token mediante el dispositivo (330, 702) de procesamiento, una identidad del servicio en línea basada en una segunda cadena de bloques que representa la identidad en línea del servicio en línea; y
verificar, mediante el dispositivo de procesamiento, que la entidad ha solicitado el token para autenticar la identidad en línea de la entidad en el servicio en línea.

9. El procedimiento de la reivindicación 7, en el que el uno o más bloques (114, 230) ordenados incluyen datos codificados basados en la una o más fuentes (116, 320) de identidad, y en el que transmitir (660) la confirmación de la identidad en línea de la entidad (470, 570) al servicio en línea además comprende:

descodificar, mediante el dispositivo (330, 702) de procesamiento, basándose en el token, una fuente de identidad a partir de los datos codificados en la cadena de bloques (112, 212, 340, 440); y
transmitir, mediante el dispositivo de procesamiento, la fuente de identidad al servicio en línea para el procesamiento de la fuente de identidad.

10. El procedimiento de la reivindicación 7, que comprende además:

recibir, mediante el dispositivo (330, 702) de procesamiento, la una o más fuentes (116, 320) de identidad de la entidad (470, 570);
almacenar, mediante el dispositivo de procesamiento, la una o más fuentes de identidad en una base de datos privada; y generar, mediante el dispositivo de procesamiento, la cadena de bloques (112, 212, 340, 440) que representa la identidad en línea asociada con la entidad generando un bloque (114, 230) ordenado basado en cada fuente de identidad de la una o más fuentes de identidad.

11. El procedimiento de la reivindicación 10, que además comprende:

determinar, mediante el dispositivo (330, 702) de procesamiento, y basándose en el token, una fuente de identidad de la una o más fuentes (116, 320) de identidad de la base de datos privada; y
transmitir, mediante el dispositivo de procesamiento, la fuente de identidad al servicio en línea para procesar la fuente de identidad.

12. El procedimiento de la reivindicación 7, que comprende además:

recibir, mediante el dispositivo (330, 702) de procesamiento, una corrección de la una o más fuentes (116, 320) de identidad desde la entidad (470, 570); y
almacenar, mediante el dispositivo de procesamiento, la corrección en otro bloque nuevo (114, 230) de la cadena de bloques (112, 212, 340, 440) de modo que se modifique un valor hash basado en la cadena de bloques.

13. Un medio no transitorio legible por ordenador en el que se almacenan instrucciones ejecutables por un dispositivo (330, 702) de procesamiento para hacer que el dispositivo de procesamiento ponga en práctica el procedimiento de cualquiera de las reivindicaciones 7-12.

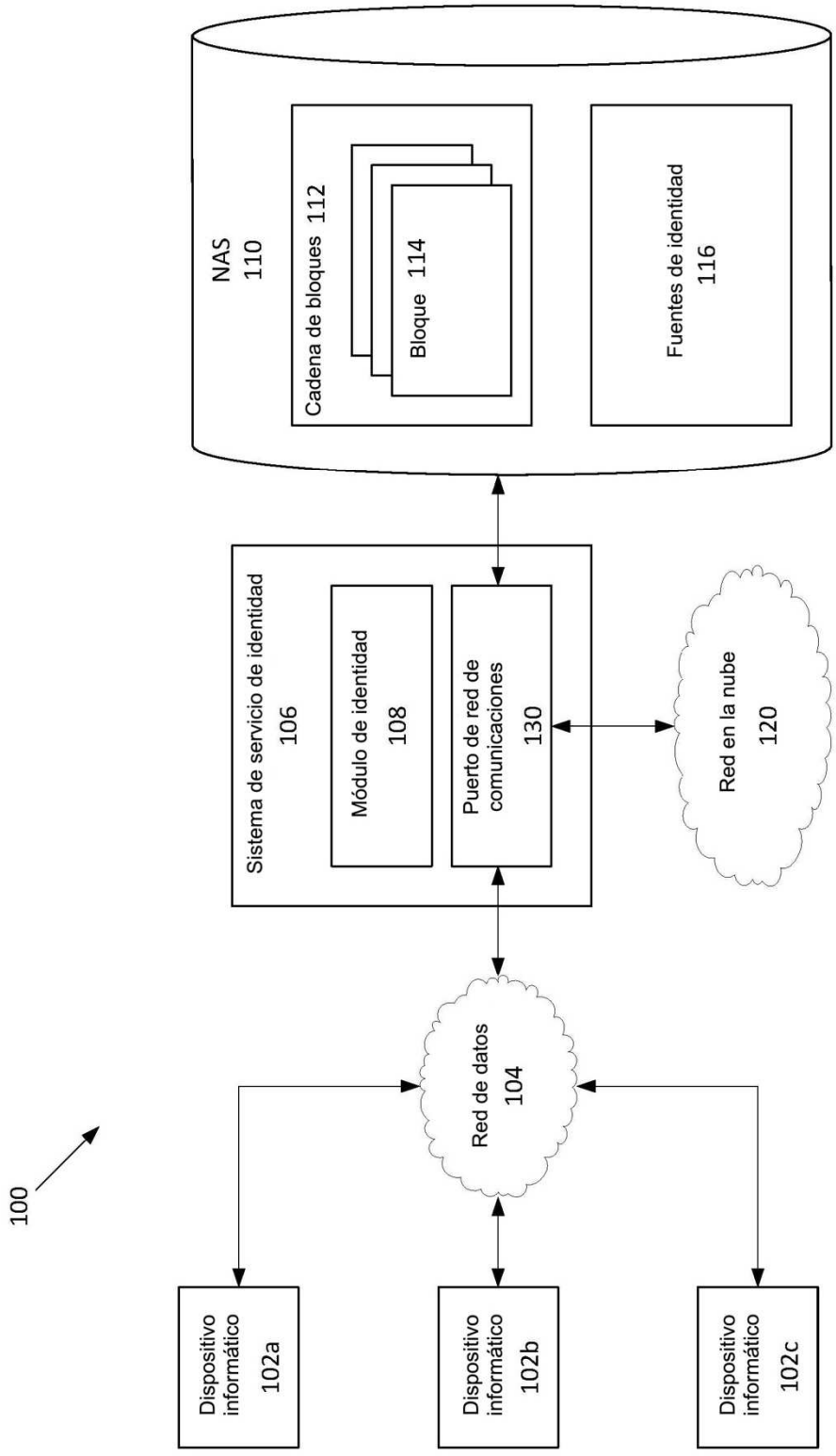
100
NAS
110
Cadena de bloques 112
Bloque 114
Fuentes de identidad
116
Sistema de servicio de identidad
106
Módulo de identidad
108
Puerto de red de comunicaciones
130
Red en la nube
120
Red de datos
104
Dispositivo informático
102a
Dispositivo informático
102b
Dispositivo informático
102c

FIG. 1

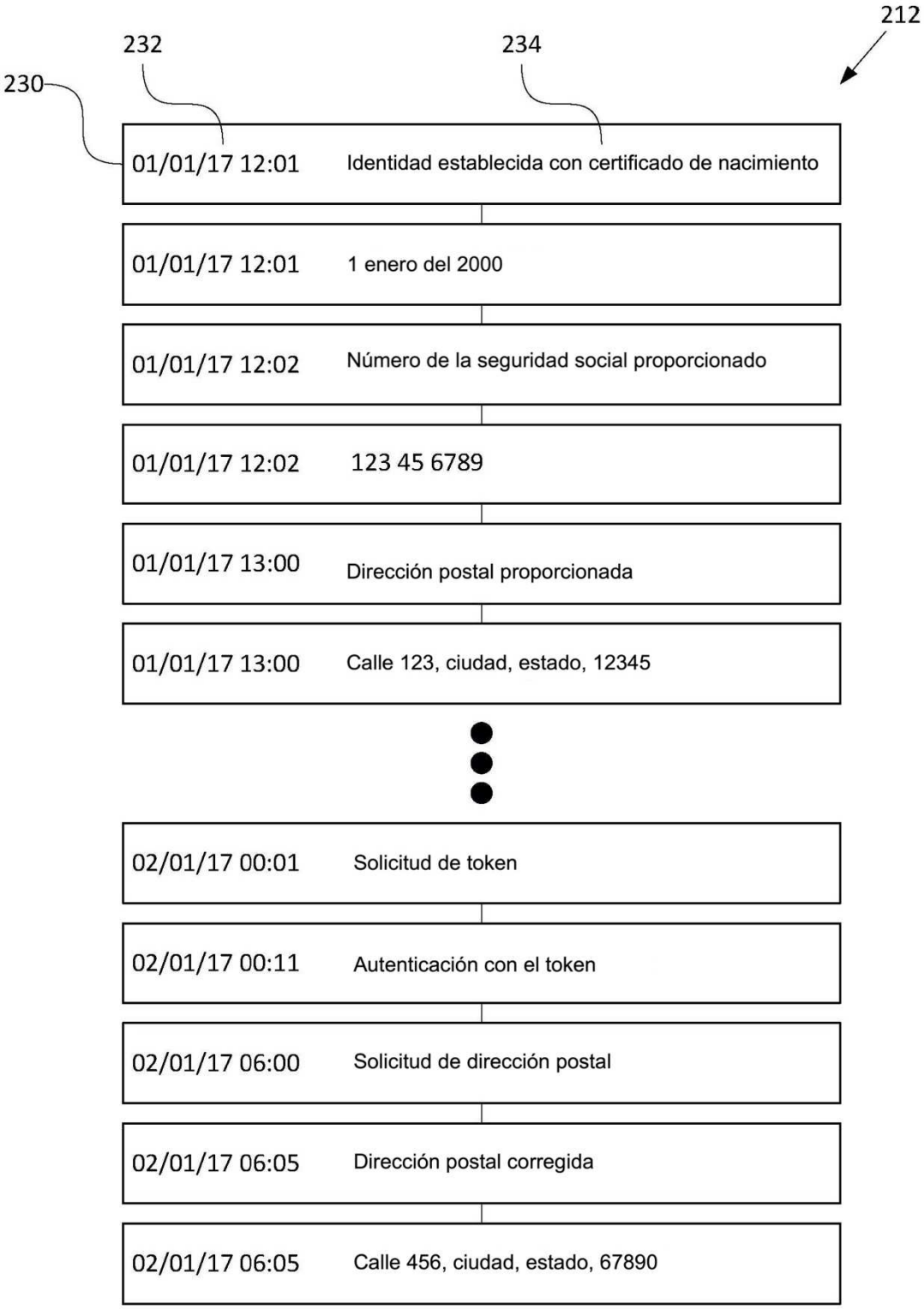
212
232
234
230
01/01/17 12:01
Identidad establecida con certificado de nacimiento
01/01/17 12:01
1 enero del 2000
01/01/17 12:02
Número de la seguridad social proporcionado
01/01/17 12:02
123 45 6789
01/01/17 13:00
Dirección postal proporcionada
01/01/17 13:00
Calle 123, ciudad, estado, 12345
02/01/17 00:01
Solicitud de token
02/01/17 00:11
Autenticación con el token
02/01/17 06:00
Solicitud de dirección postal
02/01/17 06:05
Dirección postal corregida
02/01/17 06:05
Calle 456, ciudad, estado, 67890

FIG. 2

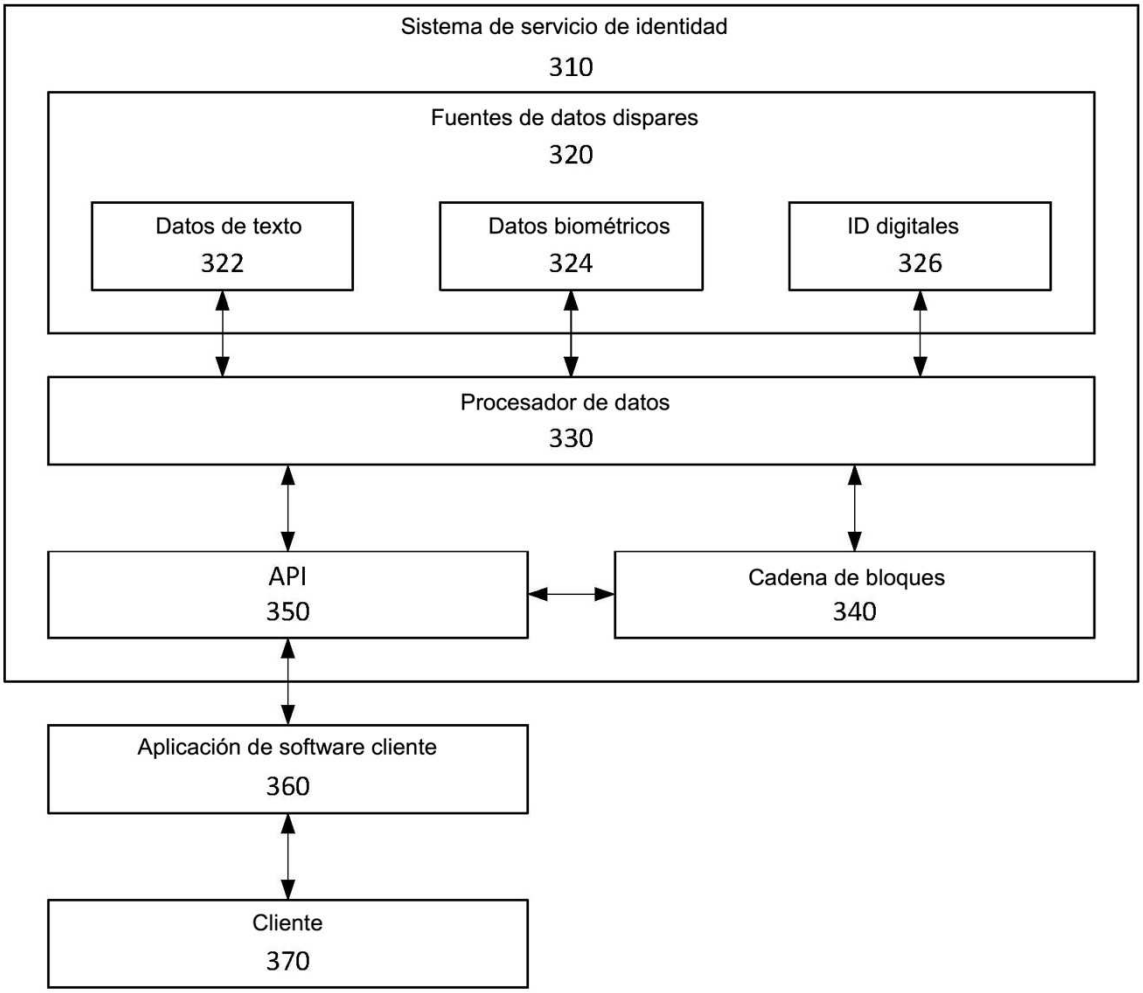
Sistema de servicio de identidad
310
Fuentes de datos dispares
320
Datos de texto
322
Datos biométricos
324
ID digitales
326
Procesador de datos
330
API
350
Cadena de bloques
340
Aplicación de software cliente
360
Cliente
370

FIG. 3

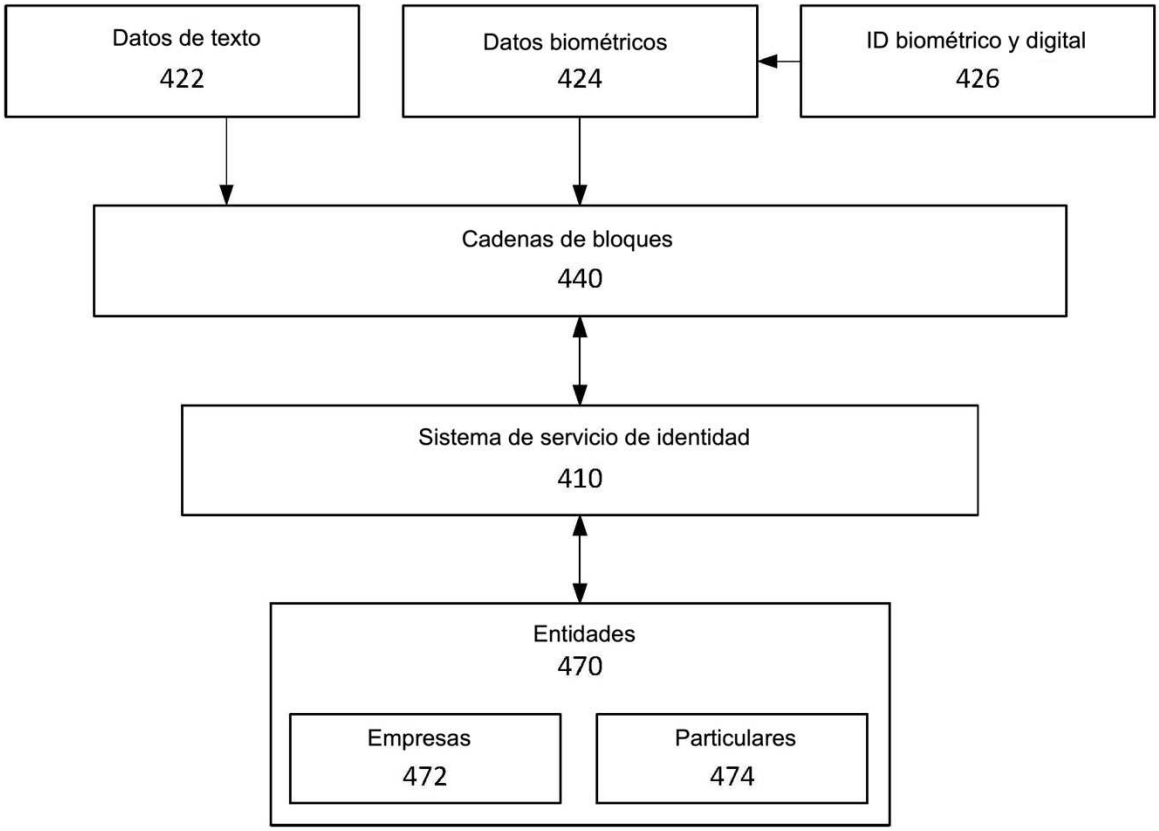
Datos de texto
422
Datos biométricos
424
ID biométrico y digital
426
Cadenas de bloques
440
Sistema de servicio de identidad
410
Entidades
470
Empresas
472
Particulares
474

FIG. 4

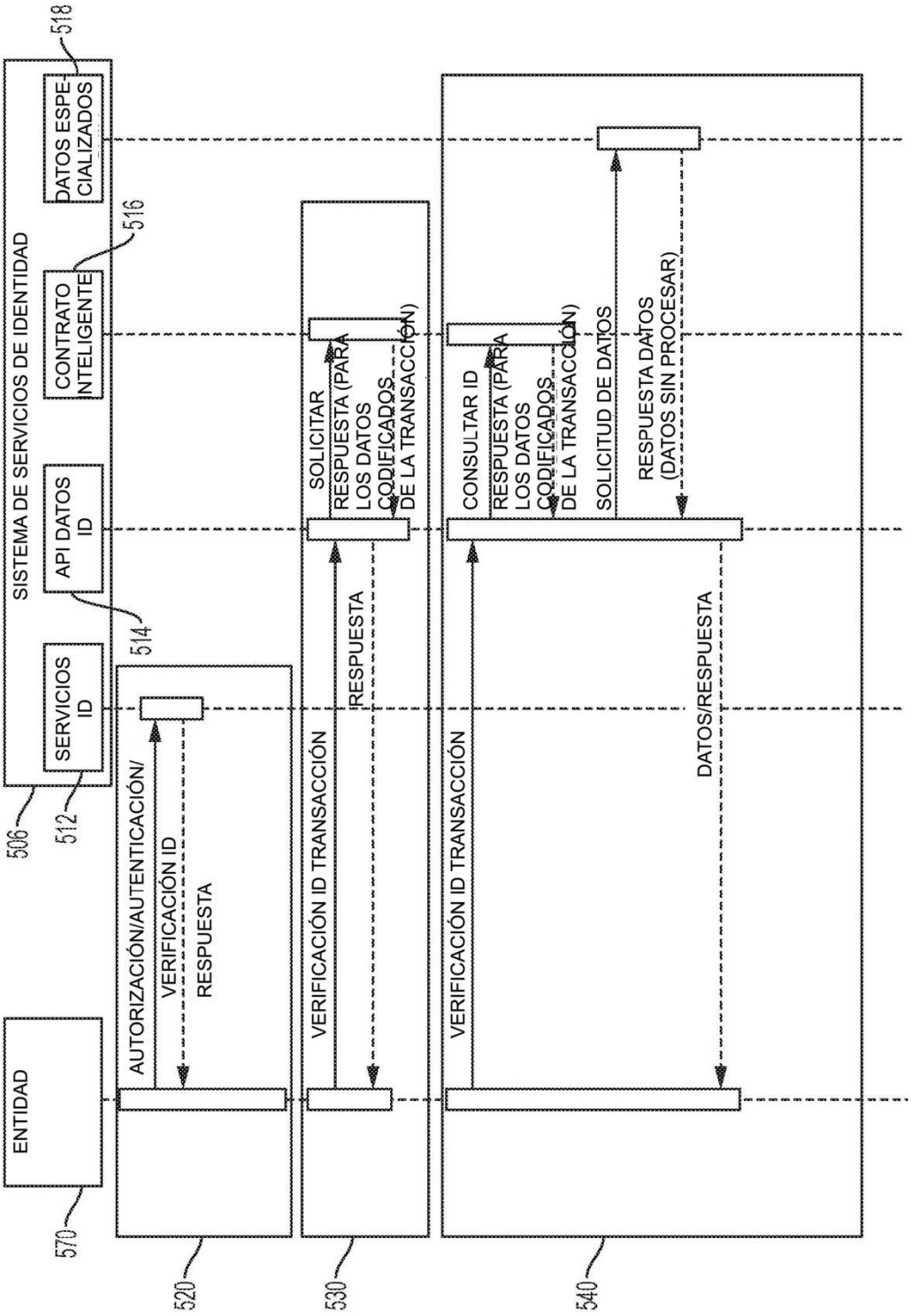
SISTEMA DE SERVICIOS DE IDENTIDAD
SERVICIOS ID
API DATOS ID
CONTRATO INTELIGENTE
DATOS ESPECIALIZADOS
ENTIDAD
AUTORIZACIÓN/AUTENTICACIÓN/
VERIFICACIÓN ID
RESPUESTA
VERIFICACIÓN ID TRANSACCIÓN
SOLICITAR
RESPUESTA (PARA LOS DATOS CODIFICADOS DE LA TRANSACCIÓN)
RESPUESTA
VERIFICACIÓN ID TRANSACCIÓN
CONSULTAR ID
RESPUESTA (PARA LOS DATOS CODIFICADOS DE LA TRANSACCIÓN)
SOLICITUD DE DATOS
RESPUESTA DATOS (DATOS SIN PROCESAR)
DATOS/RESPUESTA
506
512
514
516
518
520
530
540
570

FIG. 5

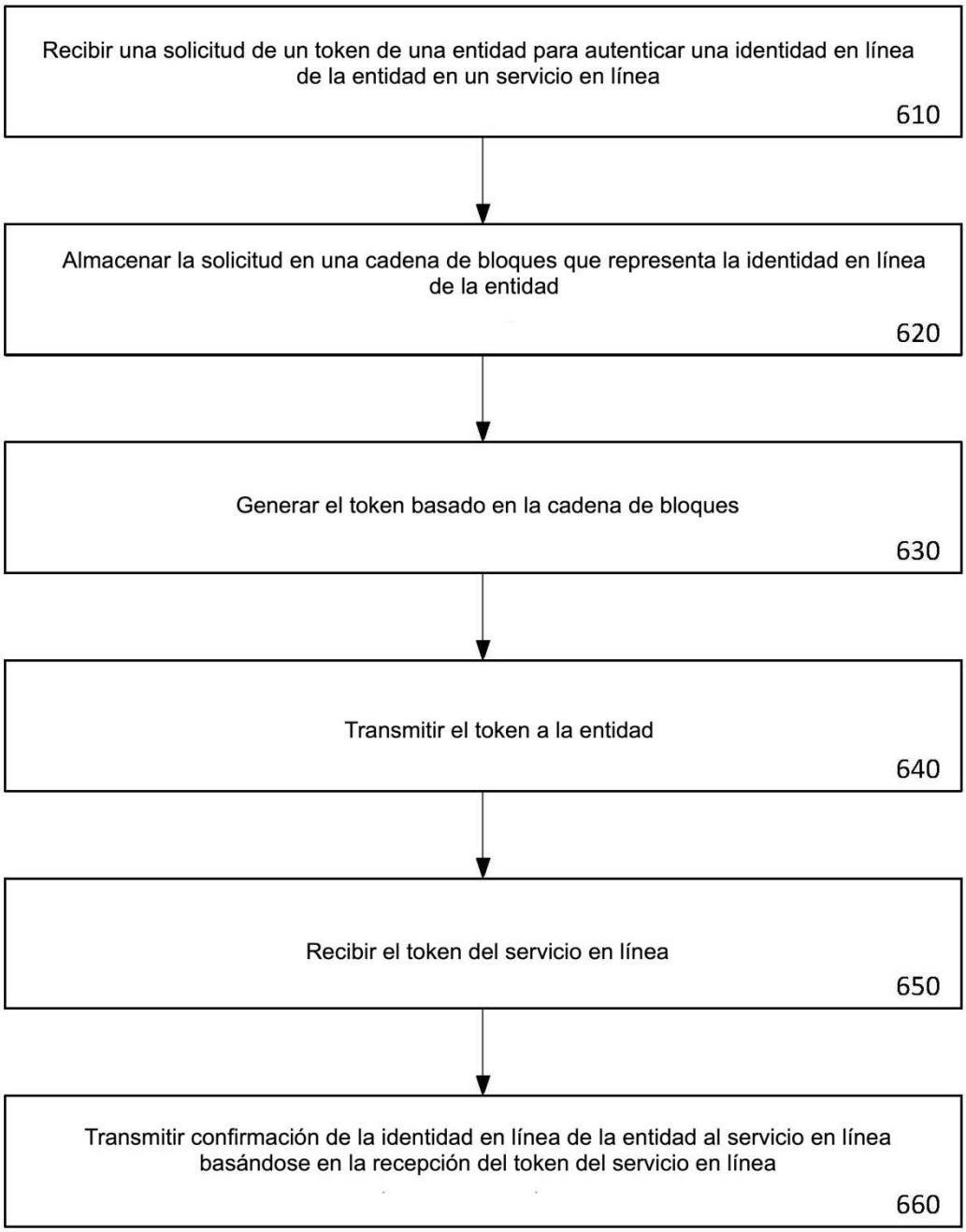
Recibir una solicitud de un token de una entidad para autenticar una identidad en línea de la entidad en un servicio en línea
610
Almacenar la solicitud en una cadena de bloques que representa la identidad en línea de la entidad
620
Generar el token basado en la cadena de bloques
630
Transmitir el token a la entidad
640
Recibir el token del servicio en línea
650
Transmitir confirmación de la identidad en línea de la entidad al servicio en línea basándose en la recepción del token del servicio en línea
660

FIG. 6

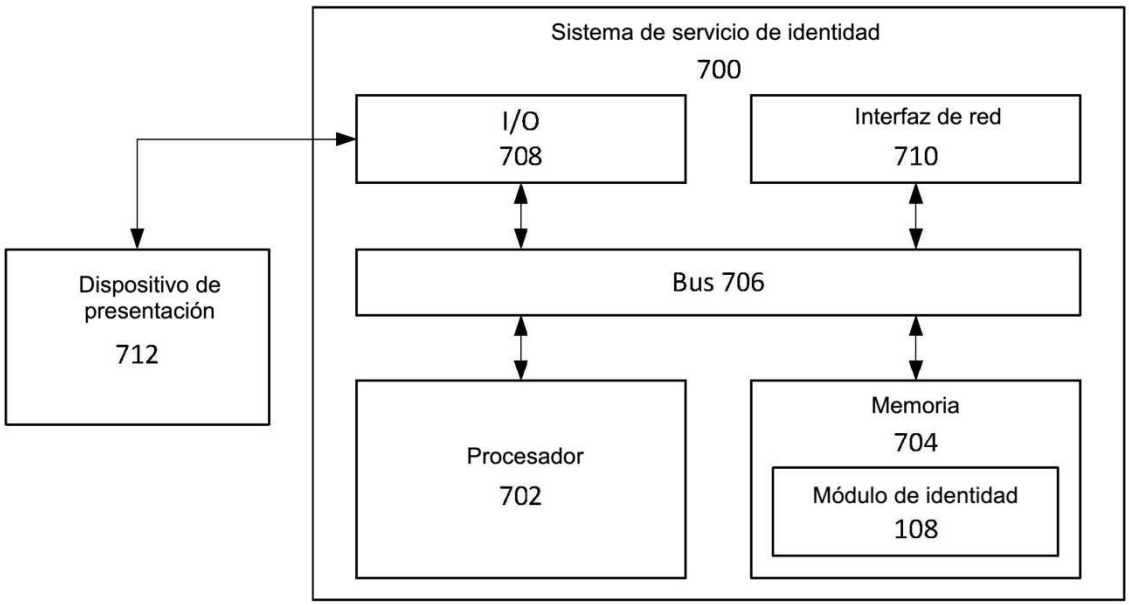
Sistema de servicio de identidad
700
I/O
708
Interfaz de red
710
Dispositivo de presentación
712
Bus 706
Procesador
702
Memoria
704
Módulo de identidad
108

FIG. 7